

Review

A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication

Lilia Tightiz  and Hyosik Yang 

Department of Computer Engineering, Sejong University, 209, Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea; liliatightiz@sju.ac.kr

* Correspondence: hsyang@sejong.edu; Tel.: +82-02-3408-3840

Received: 25 March 2020; Accepted: 27 May 2020; Published: 1 June 2020



Abstract: Since the smart grid deals with a large mass of data and critical missions, it requires ubiquitous, reliable, and real-time communication. The Internet of Things (IoT) technology, which has the potential of connecting all objects over the globe through the Internet, excels in providing robust information transmission infrastructure in the smart grid. There are a multitude of possible protocols, standards, and configurations for communication in the smart grid. A commonly applied communication standard IEC 61850 recommends the use of Manufacturing Message Specification (MMS) protocol for communication in Local Area Network (LAN) and eXtensible Messaging and Presence Protocol (XMPP) in Wide Area Network (WAN). However, a plethora of research on this topic compares the behavior of other IoT protocols and standard recommendations in the smart grid. On the other hand, the sky-rocketing penetration of Renewable Energy Sources (RES), especially in the form of micro grid, transformed the central control structure of the smart grid into a distributed style called Multi-Agent Systems (MAS). This new approach defined new communication requirements and more particular IoT protocol characteristic requirements. However, a limited number of the existing studies have considered IoT protocol characteristic requirements of the smart grid and its new control structures. In this paper, we initially investigate the communication requirements of the smart grid and introduce all IoT protocols and their specifications. We analyze IoT protocol characteristics and performances in the smart grid through literature review based on the smart grid communication requirements. In this approach, we highlight weak points of these practices making them fail to acquire the holistic guidelines in utilizing proper IoT protocol that can meet the smart grid environment interaction requirements. Using the existing facilities, the public Internet, we follow the arrangement of cost-effective high penetration communication requirements for new structures of the smart grid, i.e., the MAS and multi-micro grid. In this case, we consider IoT protocol Quality of Services (QoS) requirements, especially in the case of security and reliability, to satisfy stakeholders, namely utilities and prosumers. Addressing effective elements in applying IoT in the smart grid's future trends is another contribution to this paper.

Keywords: smart grid; IoT; constraint devices; quality of services; IEC 61850; multi-agent systems

1. Introduction

During the recent era, many new concepts such as RES, the smart grid, Energy Storage Systems (ESS), Electric Vehicles (EV), and the electricity market have been exposed to power electric networks [1]. The necessity of monitoring and controlling power networks revolutionized the one-directional power grid to a bidirectional grid for both power and information flow called the smart grid [2–4]. Growing electricity consumption and fossil-fuel burning drive ever-increasing global warming and environmental pollution, introducing RES as an emission-free and endless supply [5]. Since ESS can compensate for the absence in the duration of nature-based resources, it is applied in the power

system to overcome the intermittent nature of RES [6]. The other outcome of RES is prosumer, which means a power grid customer in the smart grid can not only be a consumer but also be a producer by selling their electricity production surplus to the grid. This outcome requires the electricity market to offer electricity prices to stockholders [7]. A robust communication infrastructure requires the coordination and integration of heterogeneous smart grid elements [8,9]. The endeavor to find a common language in this complex environment could publish a plethora of standards and protocols. In 1964, the formation of Technical Committee 57 Working group in IEC was the first attempt to define a standard for telecommunication in the power system [10,11]. Commonly used protocols, i.e., the Profibus, Modbus, Distributed Network Protocol 3 (DNP3), and IEC 60870, are serial communication and Substation Automation Systems (SAS) that suffer from low response time for real-time communications [12,13]. Additionally, being a vendor-oriented solution and not a comprehensive roadmap is another problem that causes legacy protocols not to be interoperable with other systems [13,14]. Although legacy protocols were embedded inside the Transmission Control Protocol (TCP)/IP, during following years, the IEC 61850 standard was developed in 2003 based on the Utility Communications Architecture 2.0 (UCA2.0) to overcome weak points of the legacy protocols. The second edition of the standard was published in 2007 since communication between substation to substation, and substation to control center were neglected in the previous edition. This edition extended its scope to all power automation, including the micro grid, EVs, and distribution automation, and was not limited to substation automation as in the first edition. Hence, IEC 61850 not only overcame the limitations of its predecessor, but also reflected fast development in technology, especially the communication aspect, split data definition aspect, and the methods of exchanging data to cope with the diversity of communication solutions required by the new targeted domains, while keeping the same data model [12]. IEC 61850 protocol uses client–server communication based on the IEC 61850-8-1 that is mapped on MMS, which is applicable in LAN [15]. Since RES has slowly become dedicated elements of the power grid, IEC 61850-7-420 and IEC 61850-90-7, which specify information models for Distributed Energy Resources (DER), have been published as new parts of the standard [16,17]. Moreover, the sizeable number of sensors and actuators are applied to the power grid in the form of Intelligent Electronic Devices (IED), such as switchgears, reclosers, breakers, Phasor Measurement Units (PMU), and smart meters.

IoT is a technology, which aids the smart grid to collect, monitor, and analyze power grid status and performance, as well as issue control signals [18–20]. In 2018, IEC 61850-8-2, a new mapping of information based on XMPP was published to support the integration of the smart grid and IoT, which requires communication in WAN [21]. However, smart grid communication requires different characteristics, including latency, jittery, bandwidth, and security, based on applications. A large number of other protocols have been nominated for communication in the smart grid over a public network in the literature. The most prominent ones are Common Object Request Broker Architecture (CORBA), Open Platform Communications United Architecture (OPC UA), Data Distribution Services (DDS), Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Advanced Message Queuing Protocol (AMQP), and Zero Message Queue (ZeroMQ), all of which can be investigated based on their features in the smart grid and their pros and cons to facilitate the smart grid application communication requirements.

1.1. Related Works

Applying IoT assists the integration of the smart grid elements into the conventional power system, which become popular research areas in the smart grid. The latest related surveys, which have been published in the last five years, are summarized in Table 1. After investigation of communication protocols characteristics and the smart grid application communication requirements, Al-Ali et al. [22] planned an IoT structure for the smart grid by devoting an IP address to each of the interactive smart grid elements using the 6LowPAN protocol. Despite Kaur et al. [23] considering power grid monitoring, smart metering, and the smart home as the main applications of IoT in the smart

grid, another attempt [24] recognized the smart home as the principal application of IoT in the smart grid. The authors implemented the smart grid services, such as the dynamic price, Energy Management System (EMS), and home automation, by applying the IoT protocol, including XMPP and Representational State Transfer ful (RESTful) HTTP. They also presented a brief comparison among IoT protocols, such as XMPP, RESTful HTTP, MQTT, and CoAP. Dalipi et al. [25], and Sakhini et al. [26] concentrated on the security and privacy issues related to IoT applications in the smart grid. The authors in [25] classified the issues to three scopes, including information and communication, customers, and grid, while researchers in [26] provided a comprehensive statistical reference of IoT security issues literature. Additionally, Refs. [27–29] presented IoT architecture, including application, network, aggregation, and sensing layers. These surveys provided new achievements, including conducting EMS, monitoring of power system transmission, smart metering, and asset management as the smart grid applications, which can be aided by IoT. Ref. [30] thoroughly clarified the adherence of the smart grid implementation, suggesting the conversion of proprietary connection to IP allocation to be for all elements of the power grid. In [31], the author visualizes a comprehensive smart grid that IoT enabled. The grid contained an emphasis on security as this was the main challenge of IoT, including a focus on energy acquisition, data fusion, congestion, and other issues related to this trend. Bedi et al. [32] highlighted the role of IoT in making power system intelligence and investigated the economic and social impact of this intelligence. This paper also mentioned some challenges in applying IoT in the smart grid, including the standards for the heterogeneous environment of the smart grid, energy acquisition solutions for the huge number of IoT sensors, dependency reduction of central computation requirements by applying fog computing in gateways, and security issues.

Research in the area of IoT should deal with two approaches, including internal and external requirements. Despite the external one embracing sensors and actuators, internal requirements involve different layers of communication platform, including physical, network transmission, and application layers [33]. IoT message protocol addresses the main objective of IoT, ensuring a resilient interaction among all elements of the system. As seen in Table 1, papers rarely utilize the point of view of the IoT protocol's performance on IoT applications. Furthermore, authors in [27] discussed the introduction of IoT protocols, and Refs. [24,34] provided a short brief comparison of IoT protocols characteristics. In this paper, we explore the research on accomplished IoT protocols performance in the smart grid and consider the implementation of IEC 61850 as the main standard for the interoperability provision, i.e., the target of the smart grid.

1.2. Contribution

To address the above-mentioned objectives, the main contributions of this paper are summarized as follows:

- Determination of the smart grid communication specification requirements;
- Study the smart grid protocols and standards;
- Performance evaluation of IoT protocols in the smart grid environments through literature review;
- Investigation of attaining roadmap for application of IoT protocols according to future trends in the smart grid control structures.

The remainder of this paper is organized as follows. Section 2 describes the smart grid application communication requirements. Section 3 lists the smart grid communication standards and protocols and their revision requirements to facilitate IoT deployment, and Section 4 summarizes the introduction and the performance evaluation of IoT protocols through the investigation of relevant literature. Later on, Section 5 discloses the roadmap for IoT protocols application in the smart grid and future trends. After opening a new horizon for our paper research area in Section 6, Section 7 presents the most relevant conclusions of our work.

2. Smart Grid Application Communication Requirements in the IoT Environment

2.1. Smart Grid Structure

The necessity of providing stable, safe, reliable, and cost-effective services revolutionized the conventional power grid to the smart grid, introducing the next generation of power grid that follows the bidirectional flow of current and the information structure [36–38]. High penetration of RES has intensified smart grid development due to the reduction of dependency on finite fossil-fuel resources and their nature-based characteristics [39,40]. The Supervisory Control and Data Acquisition (SCADA) system holds the responsibility of monitoring and controlling the power system before the advent of the smart grid. This system monitors the electricity network, detects faults based on the acquisition of data from on-site sensors, and controls the network by Power Line Carrier (PLC) as an interface. The main disadvantage of this system is the lack of real-time characteristics [41]. The appearance of the smart grid, which includes a large amount of actors and applications, has made it a challenge for the power grid to recognize equilibrium among application, communication, and interoperability. Overcoming this challenge is necessary to achieve advantages of the intelligent grid, which Figure 1 visualizes.

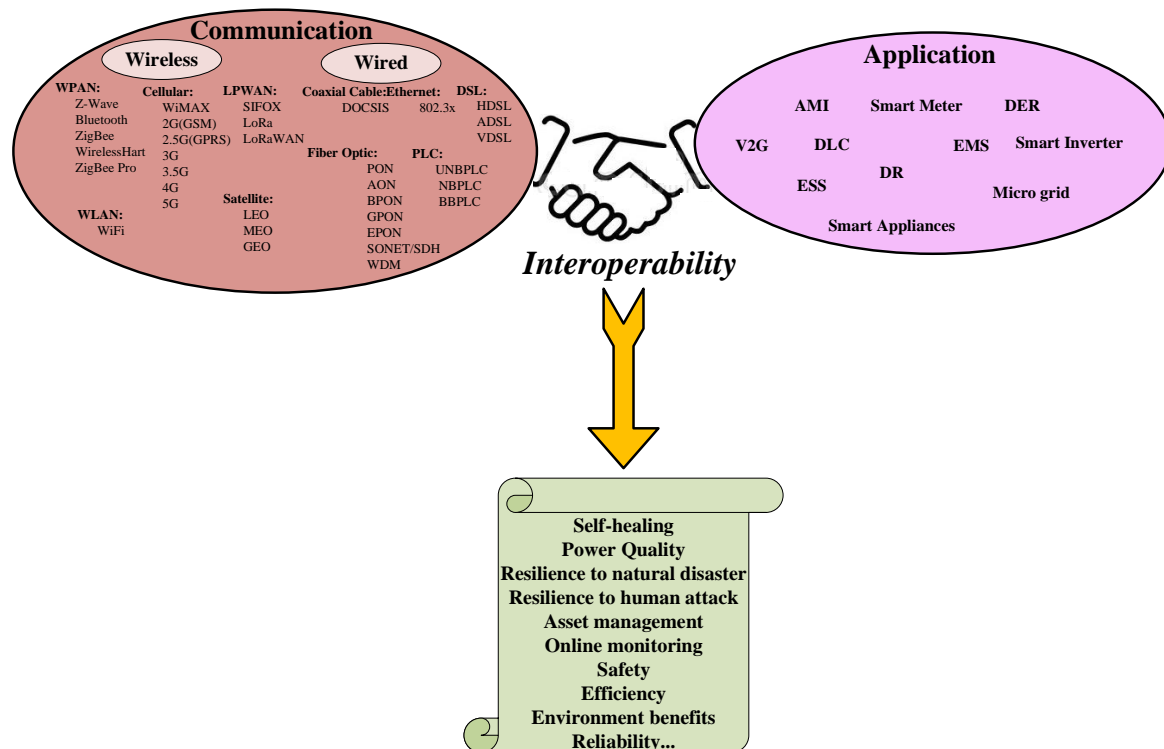


Figure 1. Achievement of the smart grid advantages by equilibrium among applications, communication, and interoperability.

As mentioned before, the main objective of the smart grid is to interact with the whole elements of the power grid. To integrate this tension into practice, different applications have been introduced. Among them, the utilization of RES as clean resources of energy is most prominent. The prosumer concept emerged from RES with aid from ESS, causing electricity consumers to act as producers and take part in the energy market to trade with their surplus energy. Technologies, such as smart meters, home appliances, and Advanced Metering Interface (AMI), profoundly interact with their consumers and the supervision of the power system. This phenomenon provides energy efficiency, load profile detection, price signals issuing to customers, fraud detection, power outage management, reliability, and power quality monitoring through facilitating Demand Response (DR) [42–44]. DR is

an application that controls the amount of energy consumption during the peak demand period determined by the dynamical contribution of consumers. DR is implemented by offering incentive regulations or time-dependent programs. While some techniques, such as Direct Load Control (DLC) operators, directly control demand of consumers in incentive ways, others allow consumers to decide to cooperate with the utility in peak shaving based on dynamic prices and schedules, such as time of use, critical peak pricing, and real-time pricing [45,46]. Peak shaving and Ancillary Services (AS), such as frequency control are the primary outcomes of the smart grid through DR [47,48]. EV is another element capable of acting as a prosumer through technologies such as ESS and Vehicle-to-Grid (V2G). Micro grid, a combination of the loads, RES, and ESS, is another opportunity rocketing penetration of the smart grid and RES that accommodates an independent grid, especially in remote places. Another application is EMS, which balances generation and consumption levels. This application is in the micro grid and supervisory level of the power system, i.e., Distribution System Operator (DSO) and Transmission System Operator (TSO). Additionally, the Home Energy Management System (HEMS), Building Energy Management Systems (BEMS), Community Energy Management Systems (CEMS) for urban areas and remote places, and even Data center Energy Management System (DEMS) [49] can include EMS. The power grid takes the countless advantages of the smart grid, the prominent ones of which are self-healing, reliability, and security. Through online monitoring of the system and fully automated control center, the smart grid turns into a self-healing grid. This characteristic, combined with the micro grid and prediction tools in the operator level of the system provides, a secure system against any cyber-attack [50].

Communication is the backbone in the creation of all the applications and technologies mentioned above in the smart grid. Based on application characteristics, the smart grid applies different communication technologies to be discussed in depth in the next section. Interoperability allows communication and technologies to assist the smart grid in making the power system intelligence. Since the smart grid is a collection of different and heterogeneous actors and applications, interaction in this environment requires interoperability. Several protocols and standards practice this enhancement, and the investigation of their performance in the smart grid is the main objective of this paper.

IoT is a recent technology that utilizes technologies and applications, such as Frequency Identification (RFID) tags, Geographical Position System (GPS), smart meters, laser scanners, smartphones, and more. IoT is known to be an infrastructure of interoperability and connection, which accomplishes the smart grid's responsibility of providing the bidirectional flow of electricity and information in the power network. Therefore, it can be applied to three domains: monitoring, gathering the information, and controlling of smart grid components [51]. It is necessary to determine the smart grid's domains to recognize accurate required standards and protocols. The National Institute of Standards and Technology (NIST) released the smart grid conceptual model as shown in Figure 2, based on seven territories, including Customer, Service Provider, Transmission, Distribution, Bulk Generation Market, and Operation [52,53]. Other relevant standard organizations confirmed this as well. This figure also expresses the protocols and standards, which will be discussed in depth later in Section 3.

2.2. Smart Grid Communication Requirements

The success of real-time interaction among power system elements as the leading smart grid mission depends on the implementation of a secure, robust, reliable, scalable, integrated, interoperable, and ubiquitous communication systems [54]. Figure 3 shows the communication network in the smart grid that is classified into three domains, including Home Area Network (HAN), Field Area Network (FAN), and WAN [55]. HAN embraces the customer side, including home appliances, DER, and EV, and requires applications such as Home Energy Management System (HEMS), V2G, and smart inverters.

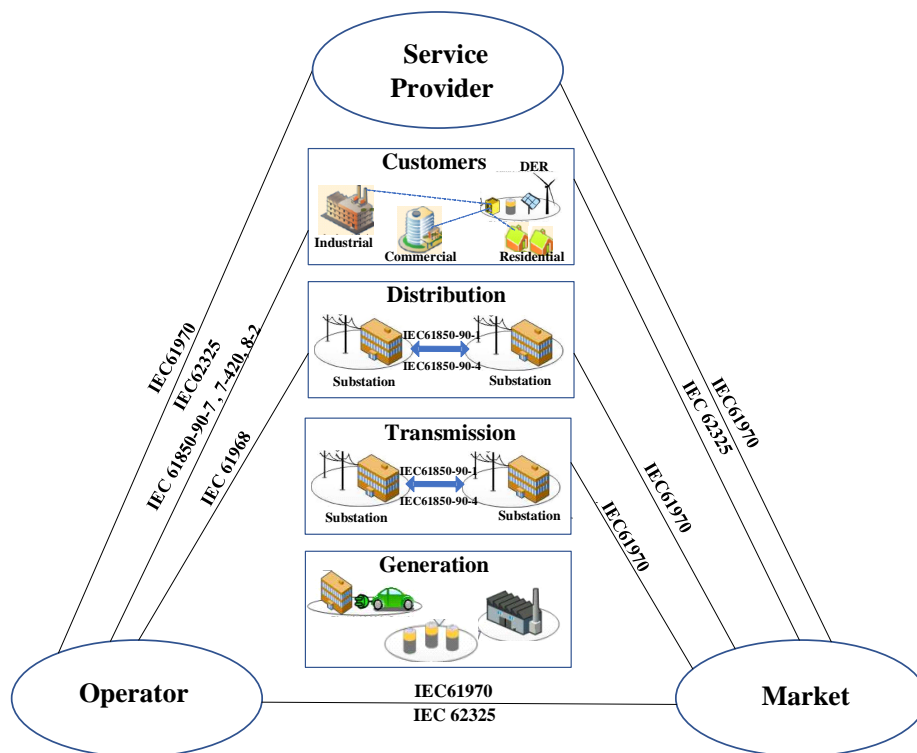


Figure 2. The smart grid conceptual model and its relevant standards.

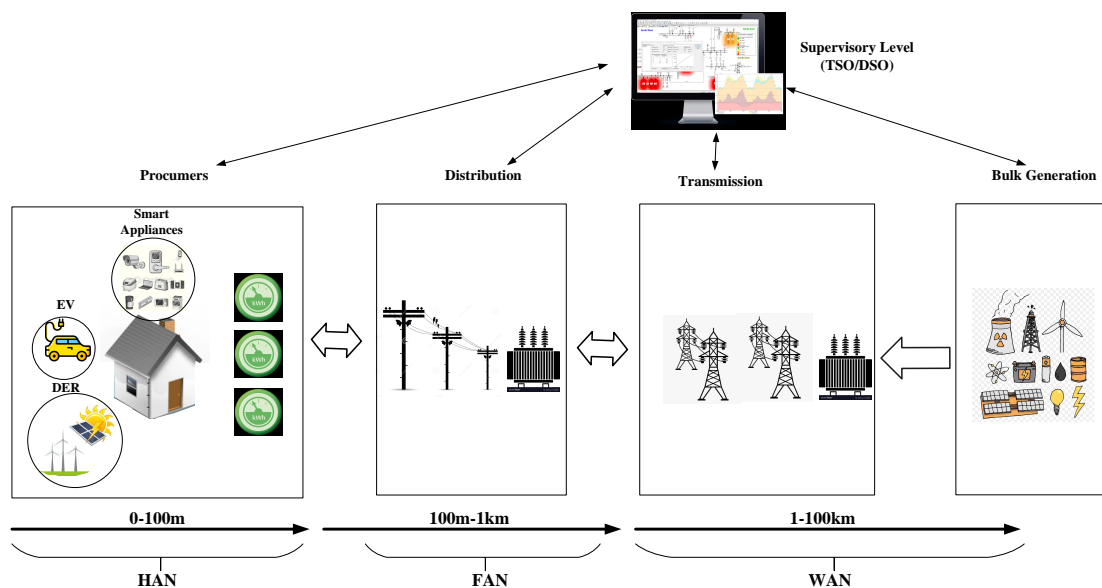


Figure 3. Communication level in the smart grid.

FAN is a domain that arranges the interconnection of the customer side and the electricity grid. At this level of communication, concentrators collect data from customer meters and DER for the supervisory level. Power system operators apply this information to offer services in WAN, such as DR, Distribution Management System (DMS), and Wide-Area Situational Awareness (WASA). Additionally, AMI can be in all three domains based on utility policies. Since it gathers information from metering in the consumption side to the supervisory side, we consider AMI to be part of the FAN domain. Since the main objective of this paper is to explore appropriate middleware for the smart grid application, the previous information is necessary to recognize the communication requirements of

each domain. Table 2 shows preferred communication technologies, applications, and requirements of those applications, such as bandwidth and latency [22,56].

Table 2. Bandwidth and latency in the smart grid.

Communication Level	Communication Technologies		Application	Bandwidth	Latency
	Wired	Wireless			
HAN	Coaxial Cable, Ethernet, PLC	Bluetooth, ZigBee, Z-wave	HEMS	9.6–56 kbps	200 ms–2 sec
			EV Charging	9.6–56 kbps	2 sec–5 min
			V2G	9.6–56 kbps	2 sec–5 min
FAN	Coaxial Cable, Ethernet, DSL, Fiber optic, PLC	ZigBee Pro, WiFi, Cellular, Low Power WAN (LPWAN), Satellite	AMI	node: 10–100 kbps backhaul: 500 kbps	2–15 sec
			DER and ESS	9.6–56 kbps	20 ms–15 sec
			DR	14–100 kbps	500 ms– several minutes
WAN	Coaxial Cable, DSL, Fiber optic	Cellular, LPWAN, Satellite	DMS	9.6–100 kbps	100 ms–2 sec
			SAS	9.6–56 kbps	15–20 ms
			WASA	600–1500 kbps	15–200 ms
			Outage management	56 kbps	2000 ms

3. Smart Grid Communication Protocols and Standards

The main characteristics of the communication system in the smart grid are safety, reliability, and security in data exchanging, allowing the introduction of several standards. Table 3 summarizes the essential standards out of the substantial amount of IEC standards and several IEEE standards that support the smart grid [57].

The background of the IEC 61850 standard series includes spreading the usage of IED in the power system, which requires real-time communication to accommodate controlling, monitoring, metering, and protection in the substation. Components of SAS contribute to the monitoring, controlling, and configuration of the substation in three levels: process level, bay level, and station level. Sensors and actuators are located on the process bus at the bay level and send information, such as current and voltage measurements to the IED. The IED accomplish controlling, monitoring, and protection by processing information received from the process level. The station level is the location of power network supervision, including databases, operators, and interfaces for remote control and communication [58,59]. This standard defines three types of messages to interact with these communication levels. MMS is used for non-critical information with low or medium priority and in the format of request–response. On the other hand, critical-information with high priority such as trip signals utilize Generic Object Oriented Substation Event (GOOSE) service and measurement units with high priority utilize Sampled Value (SV) service. Although the GOOSE and the SV both have a multicast format, each of these messages has a time limitation and is mapped according to the communication stack proposed in part 8–1 of standard, which uses the Open System Interconnection (OSI) model and Ethernet as a physical layer in the LAN environment. The recent edition of standard has been considered a fast innovation of technology and split the data model part and communication model to deal with that. This standard also extended the information model to support DER in part 7–420, 90–7 and provided communication stack for interconnection in WAN based on the application of XMPP to map information in part 8–2. Such developments make this standard appropriate for utilization in the smart grid communication environment. However, other literature and laboratory experiences suggests other IoT protocols rather than XMPP, since their performance was better in the provision of QoS, implementation infrastructure requirements, and future development specifications.

In the supervisory outlook of the smart grid, another standard, called IEC 61970, represents an information model named Common Information Model (CIM) that embraces power system elements to facilitate the access of information requirements from this horizon application, such as EMS and DMS.

Another relevant smart grid communication standard is IEC 61400-25-2. This standard presents a uniform platform of information exchange and a data model of all participants in the wind power station and serves a communication stack for mapping this information. This standard deploys

common data classes of IEC 61850, and the recent version has extended its data object to cooperate with the smart grid.

In the IEEE domain, 1547 is a series of standards that determine operation, control, monitoring, and integration of the micro grid for utility network AS provision. The main drawback of this standard is the unclear detail of establishing communication in the micro grid through the supervisory level of power system such as TSO/DSO [60].

Table 3. Main communication standards for the smart grid.

Standard	Subject
IEC 61850	Communication networks and systems for power utility automation
IEC 61970	Energy management system application program interface including the common information model
IEC 61968	System interfaces for distribution management
IEC 61400-25	Communications for monitoring and control of wind power plants
IEC 62325	Framework for energy market communication
IEC 62351	Standard for the data transfer security
IEC 62056	Data exchange for meter reading, tariff and load control
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61131	Programmable controllers
IEC 61334	Distribution automation using distribution line carrier systems
ISO/IEC 14543	Home Electronic System (HES) architecture
IEC 61499	Distributed control and automation
IEEE 1547	IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces

4. Classification of IoT Protocols Based on Smart Grid Application

4.1. IoT Protocols Architecture and Specification

The main challenge of smart grid implementation is the communication of heterogeneous distributed elements. Middleware works as an interface of services and software applications in communication architecture to facilitate this interaction by hiding the complexity of the operating system for application software developers. Many estimate that middleware expedites the integration of heterogeneous entities, information gathering, security in data exchange, and situation assessment in the smart grid [61]. The description and characteristic of more popularly deployed IoT protocols in the smart grid that maps onto IEC 61850 or CIM are as follows.

4.1.1. AMQP

AMQP is an open standard publish–subscribe protocol architecture introduced in 2003 and standardized later by the Organization for the Advancement of Structured Information Standards (OASIS) in 2011. Displayed in Figure 4, Exchange, Queue, and Binding are the three elements that establish the transfer of messages in this protocol. Exchange, which is the broker of this protocol, sends messages to a queue based on their priorities. Binding defines priority with different methods, including direct, topic, and fanout. Transport Layer Security (TLS) offers the security of transmission in this protocol. AMQP is not a lightweight protocol and, in the case of memory, bandwidth, and power, it cannot support standalone sensors [62].

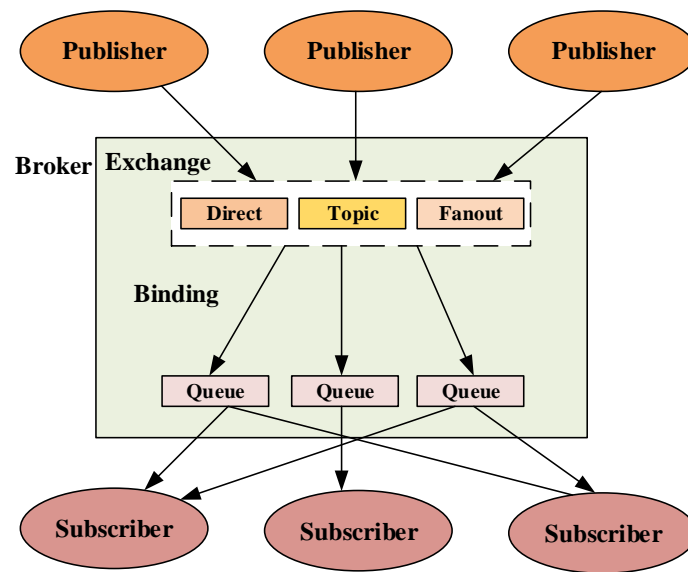


Figure 4. AMQP architecture.

4.1.2. CORBA

CORBA is a middleware defined by the Object Management Group (OMG) to facilitate the dedicated language and the platform-free interconnection of distributed objects. Objects in this protocol can be clients or servers communicating through Object Request Broker (ORB). According to Figure 5, ORB, which is the core of the CORBA model, has several interfaces defined in the Interface Definition Language (IDL) or located in the interface repository service. While the client sends a request by Dynamic Invocation Interface (DII), IDL stubs, or ORB interfaces, the server receives requests through Dynamic Skeleton Interface (DSI) and IDL Skeleton. An object adapter, another interface between the ORB and server, is responsible for mapping object references in ORB to the corresponding object in the server.

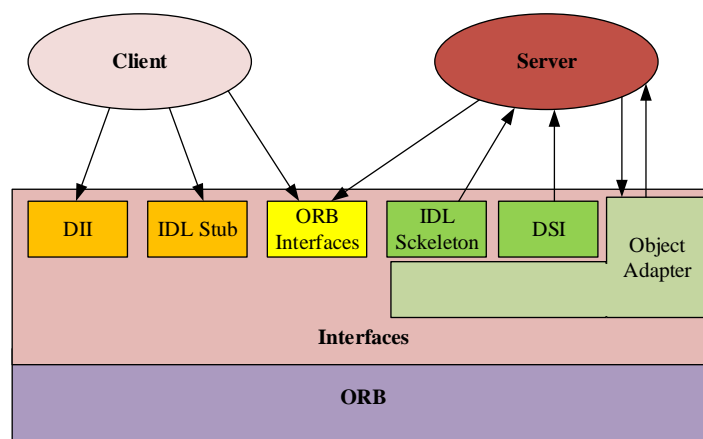


Figure 5. CORBA architecture.

4.1.3. CoAP

CoAP is the Internet protocol standardized by the Internet Engineering Task Force (IETF) Constrained Resource Environments (CoRE) working group that uses the request–response model

and follows REST over the User Datagram Protocol (UDP) to minimize bandwidth and overhead in comparison with TCP. Due to the unreliability of UDP, CoAP represents reliability by issuing a confirmation message continuously until the approving message receives from the other communication participant. This protocol employs Datagram Transport Layer Security (DTLS) as a solution to provide secure transmission. However, DTLS makes CoAP lose multicast specification, which is the prominent specification, in comparison with other IoT protocols [62].

4.1.4. DDS

DDS is an open standard middleware designed by OMG that provides real-time communication through the publish–subscribe message pattern. DDS derives a benefit of no longer needing participants to know each other from applying discovery methods, including the Data Centric Publisher Subscriber (DCPS) discovery method or Real-Time Publisher Subscriber (RTPS). Therefore, DDS is a brokerless information exchange protocol without the risk of bottleneck failure. According to the concept of DCPS revealed in Figure 6, there is a domain space in which all applications can interact through that, and all communication entities are placed in the domain. Domain participants are including Data Reader, Data Writer, Publisher, and Subscriber. Participants have access to data based on domain topic and type.

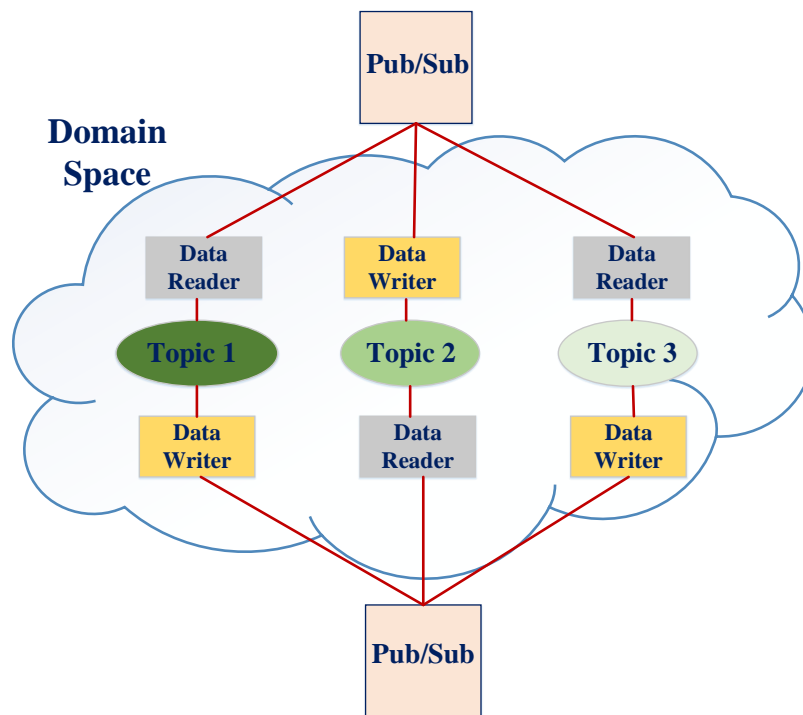


Figure 6. DDS domain space.

4.1.5. MQTT

This protocol is a publish–subscribe protocol architecture, which was originated in 1999 by IBM and was standardized by OASIS in 2013. It is an open standard protocol that can work over TCP/IP and involves three main actors: the publisher, subscriber, and broker. Publishers and subscribers exchange messages based on the topic through brokers, who cross-check their authorities to provide reliable communication by TLS. There are three levels of QoS. Level zero is the lowest level of QoS and the fastest since confirmation messages are not issued. While level one at least once assures the message is delivered, level two ensures delivery of messages and controls duplication. MQTT is a lightweight protocol that does not require high bandwidth; hence, it is suitable for distributed sensors. However, there are some issues in applying MQTT in constraint devices. Long string topic names make

MQTT improper in the Low Rate WPAN application. Since this protocol works over TCP, another drawback appears as it must keep the connection alive for the broker to notify subscribers about any changes in the topic, having the effect of a slower transmission cycle, adding a drawback to the list. There is a sensor network version of MQTT called MQTT-SN, which overcomes the aforementioned drawbacks by employing UDP and using a two-byte alias and sleeping subscribers [62].

4.1.6. OPC UA

OPC is a result of the automation industry's cooperation in providing a device's information for application without access to the device model and performance based on the Microsoft component object model in 1994. The purpose of OPC is to maintain interoperability with other operational systems by a unified architecture called OPC UA. This protocol was standardized by IEC 62541 with a client–server architecture. As shown in Figure 7, OPC UA has two backbones in its architecture, i.e., the transport model and the data model. While servers communicate with clients by two different kinds of transportation, including binary called UA native, or Simple Object Access Protocol (SOAP)/HTTP which calls the UV web services over TCP/IP, the data model determines guidelines for servers on how to depict objects, including variables and methods, through an address space to clients. The base service layer provides services in exchange for information. This protocol information model, including Data Access (DA), Alarms and Conditions (AC), Historical data Access (HA), and Programs (PRG), can be adopted with information models of other organizations, such as the IEC and the International Society of Automation (ISA), or with the information models of vendors [63–65].

OPC UA security architecture prepares authentication, authorization, confidentiality, integrity, auditability, availability, transport, communication, and application layers. While TLS ensures encryption for HTTP protocol in the transport layer, the communication layer provides confidential messages and integrity. The application layer contains the authentication and authorization of the user in the session. OPC UA also supports the publish–subscribe model to apply less session transaction by using UDP packets. This architecture is more unified than others, so it can be applied for all types of IoT applications as it embraces required features of applications developed in the field of IoT.

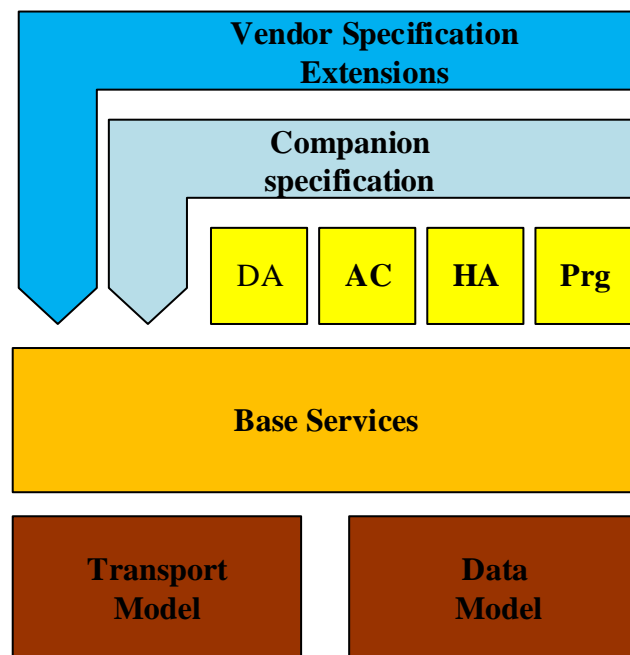


Figure 7. OPC UA architecture.

4.1.7. XMPP

XMPP is one of the open standard IoT protocols and supports an asynchronous and synchronous publish–subscribe model, enabling message exchange with the eXtensible Markup Language (XML) format. It is standardized by IETF RFC 6120, RFC 6121, and RFC 7622. XMPP is a communication protocol that has the highest advantages in scalability, so a variety of unpredictable communication environments contain it. It sends and receives messages using the XML format and uses a unique address for each node called Jabber IDentifiers (JID) to make a connection. The message in XMPP consists of a stream and a stanza, and XML streaming transfers an XML stanza as data. There are three types of stanza, i.e., iq, message, and presence stanza. The iq stanza determines how information is requested and answered. The exchange of messages among participants utilizes the message stanza, and the presence stanza identifies the status of each node. XMPP is a recommended IoT protocol for smart grid applications. However, due to the XML parsing of stanzas, its complexity makes it unable to meet time-critical application, which is XMPP's major drawback.

4.1.8. ZeroMQ

ZeroMQ is an asynchronous middleware that works in a distributed environment over TCP, multicast, in-process, inter-process, and WebSocket. This middleware supports publish–subscribe, request–response, client–server, and push–pull model. ZeroMQ is preferable to other broker-based IoT regarding the release from a single point of failure a drawback because it also provides a queue for messages with a zero broker structure. ZeroMQ is a smart choice in high throughput and time critic applications.

Table 4 represents a comparison of IoT protocols according to supporting QoS, data security, transport layer, message prioritization, architecture, complexity, extensibility, dominant application domain in the smart grid, and main advantages and disadvantages [66,67].

4.2. IoT Protocol Application in Smart Grid

As aforementioned, IEC 61850 is a commonly used communication standard in the smart grid environment. The introduction of IEC 61850-7-420 for DER, IEC 61850-7-410 for hydropower, and IEC 61850-8-2 for communication in WAN along with the application of XMPP instead of MMS protocol for the smart grid's new integrated entities' requirements matured the IEC 61850 standard. There has been a plethora of research on this topic, providing the performance of other IoT protocols in the smart grid environment in comparison with standard recommendations. The papers displayed in Table 5 applied IoT protocols for mapping IEC 61850 in the smart grid environment and evaluated their methods through different metrics and analyzer tools. Each paper applied various IoT protocols to map IEC 61850 or CIM data model on the smart grid. In this table, we classified papers based on the utilized protocol, benchmark protocol, the analyzer and tools they utilized to evaluate their method, and the IEC 61850 or CIIM model implemented on the smart grid application.

Macarulla et al. [68] designed HAN communicating with the supervisory level of the grid to communicate smart meter information. Through the Internet (ADSL for home application and university campus), the authors mapped their interaction structure based on the CIM information model and evaluated their method by the latency and operational costs. Ref. [69] is one of the first attempts to map IEC 61850 on IoT protocol, CORBA, for SAS. However, security issues and satisfactory performance only in low-speed networks are weak points that make CORBA the unsuitable choice for time-critical and sensitive applications. Shin et al. [70] compared the mapping of CoAP on IEC 61850 with that of MQTT and Simple Object Access Protocol (SOAP). They revealed that the CoAP data size is less than the two other protocols despite transmitting the same information. Then, it is concluded that CoAP is a more useful protocol for the smart grid as device capability can be limited and showed that it provides more efficient network traffic and low latency when it is utilized in IEC 61850 as a communication protocol.

Table 4. Comparison of IoT protocols characteristics.

IoT Protocol	QoS	Data Security	Transport Layer	Message Prioritization	Message Pattern	Complexity	Extensibility	Dominant Application in the Smart Grid	Main Advantages	Main Disadvantages
AMQP	✓	TLS SSL	TCP	✓	Req-Res Pub-Sub	Low	✓	Smart meter, AMI	Offer wide message features	Not suitable for resource constrained applications
CoAP	✓	DTLS	UDP	✓	Req-Res Pub-Sub	Low	✓	Smart Home	Suitable for resource constrained application	Limited QoS
CORBA	✓	SSL	UDP	✗	Req-Res Push-Pull	Medium	✗	SAS	Support wide variety of languages	Suitable for slow network (Ethernet)
DDS	✓	SSL DTLS	TCP UDP	✓	Pub-Sub	High	✓	EMS	Extensive QoS	Suitable for large scale system
DPWS	✓	TLS SSL	TCP UDP	✓	Pub-Sub	Medium	✓	Electricity Market	Suitable for resource constrained application	Some security issues in services
MQTT	✓	TLS SSL	TCP	✗	Pub-Sub	Low	✓	Smart Home, Smart meter	Easy implementation	Limited scalability because of broker
OPC UA	✗	SSL	TCP	✗	Req-Res Pub-Sub Push-Pull	High	✓	SAS	Suitable for resource constrained applications	Firewall configuration requirements
XMPP	✗	TLS	TCP	✗	Req-Res Pub-Sub Push-Pull	High	✓	the smart grid application	Recommended by IEC 61850	Not suitable on constrained devices since XML parsing
ZeroMQ	✓	TLS	TCP	✗	Req-Res Pub-Sub Push-Pull	Medium	✓	HEMS	Brokerless	Less QoS compare with DDS

Table 5. Comparison of IoT protocols in the smart grid environment through literature.

Authors	Year	Protocols	Utilization Horizon	Benchmark Protocol	Evaluation Methods	
					Analyzer Tools	Metrics
Sanz et al. [69]	2001	CORBA	SAS	-	-	-
Pedersen et al. [71]	2010	HTTP-REST	MicroCHP, EV	-	-	-
Lenhoff et al. [72]	2010	OPC UA	-	-	-	-
Schmutzler et al. [58]	2011	DPWS	EV	-	-	Latency, Scalability
Sucic et al. [73]	2012	DPWS	VPP	-	-	-
Calvo et al. [74]	2012	DDS+CORBA	-	-	-	Jitter, Latency
Bi et al. [75]	2013	DDS	-	-	-	Reliability(Received/Sent)
Sucic et al. [76]	2013	OPC UA	VPP	-	-	-
Tarek et al. [77]	2016	DDS	Micro grid	-	Matlab	Latency, Throughput
Macarulla et al. [68]	2016	AMQP	HAN	-	-	Latency, Processing time
Ferreira et al. [78]	2017	DDS	Protection, Automation, and Control	-	Testbed on Local Network and Virtual Machine	Latency, Jitter
Shin et al. [70]	2017	CoAP	SAS	MQTT, SOAP	OPNET Modeler 17.1	Packet/Second, Data size, Traffic, Delay
Iglesias et al. [79]	2017	CoAP	-	-	-	-
Hastings et al. [80]	2017	MQTT	Storage Heater	-	-	-
Tarek et al. [81]	2017	DDS	EMS of micro grid	-	MATLAB	Latency
Esfahani et al. [82]	2018	DDS	Micro grid market	-	Ethernet (LAN), Virtual Private Network (VPN)	Energy mismatching in market
Iglesias et al. [83]	2018	CoAP	Smart elevator	HTTP-REST, WS-SOAP	Wireshark	Latency, Data Size, Overhead
Hussain et al. [84]	2018	XMPP	DSTATCOM	-	-	-
Aftab et al. [85]	2018	XMPP	EV	-	-	-
Kim et al. [86]	2019	OPC UA	Micro grid on IEEE 9 bus	-	UACIT OPC UA Compliance Test Tool	-

Iglesias et al. after analyzing mapping IEC 61850 on CoAP in [79], compared CoAP performance in the smart elevator as an experimental setup with HTTP-REST and SOAP Web-services in case of latency, data size, and latency in [83]. Bi et al. [75] proposed a data model mapping IEC 61850 on DDS and tested their model in a LAN environment. They evaluated their model's reliability by calculating the ratio of sent samples to the samples received, but there is no practical comparison between their method and other IoT protocols. Tarek et al. [81] investigated the requirements of real-time communication for EMS in the micro grid and implemented the system with DDS as middleware while exchanging data over the Ethernet network. This paper follows objectives such as peak shaving and bills cost reduction for customers in the micro grid. Esfahani et al. [82] implemented the micro grid market based on the game theory algorithm and mapped IEC 61850 on DDS to meet the communication requirements of the real-time market. Hastings et al. [80] introduced MQTT as a suitable IoT protocol for DER interactions in the smart grid environment and proposed a platform for the heating system contribution in DR based on applying MQTT as the transmission protocol. The authors provided setup and considered the evaluation of latency for their future work. Susic et al. [73] integrated DER and ESS to the Virtual Power Plant (VPP) by deploying OPC UA according to the IEC 61850 protocol. According to the IEC 61850 and CIM information model, Kim et al. [86] proved the efficiency of OPC UA for communication between the micro grid and supervisory levels, such as DMS or EMS. Hussain et al. [84] provided reactive power management in the micro grid by modeling a Distribution Static Compensator (DSTATCOM) based on IEC 61850 information model and secure communication through web protocol XMPP by applying Simple Authentication and Security Layer (SASL) and TLS. The authors presented the distributed resources and loads by IEC 61850 information model, which were supervised by the Distributed Network Operator (DNO), VPP, or smart market operators. However, the authors did not provide the evaluation method and protocol benchmark. Aftab et al. [85] planned EMS in the micro grid with the presence of EV based on the IEC 61850 information model. The controller of each the micro grid entity was considered as XMPP client communicating through WAN with the XMPP server who is the micro grid control center. However, this paper provided a framework and there are no experimental results.

There is limited literature on applying ZeroMQ in the smart grid application. Peterson et al. [87] focused on throughput, message type and pattern, latency, package loss, and memory usage of server and client and provided one of the comprehensive IoT protocol performance comparisons in the smart grid. This paper noticed that interchangeable serialization profoundly affects available bandwidth and throughput pronouncing it as one of the crucial characteristics of middleware highly affects available bandwidth and throughput. The authors identified that, while memory usage of CORBA is negligible, OPC UA and XMPP have the highest range of that among other middleware. Additionally, experimental results of this paper show ZeroMQ and YAMI4 are the most robust middleware for the smart grid application.

The investigation of related studies shows that there is a limited effort in comparing IoT protocols represented on the smart grid, and, specifically, the mapping of the IEC 61850 protocol. It is noted that most of the studies limited their attempts to simulation, and rarely applied real experimental platforms in comparison to IoT protocol performance in the smart grid. Although there are some testbed experiences, they are limited to dedicated network infrastructure and mostly in LAN environments, while the smart grid network is characterized by a more congested network.

5. IoT Protocols Application Roadmap and Future Trends for Smart Grid

To provide a roadmap for IoT protocol application in the smart grid, we need to recognize the framework and infrastructure development of the power grid. The smart grid, which is the integration of communication and power system, was invented to provide real-time services to be like an altered and modernized power grid structure. Meanwhile, the introduction of new technologies, the smart grid mission, and infrastructure have been affected by their relevant application. The RES trend, which is a novel solution to tackle fossil-fuel shortage and gas emission issues, has explicitly risen specifically

in the form of a micro grid. The smart grid objectives, which are mainly equivalent between generation and consumption, monitoring power system stability and faults, handling the electricity market, and issuing prices, should coordinate with RES characteristics. The main issues related to employing RES are their intermittence and weather dependent characteristics, which brings new monitoring and communication requirements to the smart grid.

The hierarchical level control in the power system cannot accomplish the smart grid objectives mentioned above. The control algorithm and monitoring enhancement appeared in the MAS concept. Distributed autonomous territories interaction, which is the main characteristic of MAS, sufficiently fits the smart grid requirements. According to the main feature of MAS, which is an interconnection of autonomous entities, there are several benefits in turning the smart grid control model and architecture to MAS, including fewer data communication traffic and infrastructure based on local decision-making algorithms, reliability, extendibility, and extensibility in joining or rejecting requests of other entities [88]. The multi-micro grid is the other structure in that the smart grid relies on to achieve RES penetration growth, active demand side management, and responsive loads scenario [89,90].

MAS and multi-micro grid architecture of the smart grid increase the independence of each element to participate in AS provision of the power grid such as frequency and voltage regulation, blackout restoration, and so on. VPP, the electricity market, and aggregator are concepts that put this interaction into practice. In this state-of-the-art environment, provision of robust communication infrastructure must offer minimum latency, maximum bandwidth, privacy, security, and scalability. Cloud computing and fog computing are solutions to these requirements. Cloud computing is sharing computer system resources, such as data storage and computing resources on-demand over the Internet. This phenomenon shares resources to minimize investment and operational costs. Fog computing is another concept in a shared analytical services scheme working in the network edge. This characteristic facilitates data processing by reducing the distance that data are required to travel in the network. Communication requirements of the smart grid's enhanced architectures, i.e., MAS and multi-micro grid highlighted cloud computing and fog computing applications in the smart grid. Fog computing is located near the devices producing data such as sensors as opposed to cloud computing, which is far away from the data resources, and processes data in a shared centralized server. Due to the scalable characteristic of cloud computing, it can assist the supervisory level of the system, namely TSO/DSO dealing with massive data computation, whereas, applying fog computing near to the agents leads to an increase in the speed of processing data and improve privacy [91,92]. There is a lack of IoT protocol and integrated standard applied to the system, associating fog and cloud computing.

Security concerns in the smart grid have three aspects: grid, information and communication, and consumers. Since an increase in end-user contributions in the AS schedule of the power system leads to more vulnerability in the security aspects, consumer privacy concerns are one of the important issues in IoT application. The primary mission of smart grid is to control and monitoring the power system along with consumers and the mission can be accomplished by the DR, the AMI, the concept of prosumers, and the micro grid which implements the smart grid. The control can be threatened by hackers trying to get access to the enormous consumers data, such as household appliances, load profiles, and even integrated personal information, and abuse it. Furthermore, the market sector and utilities can receive this information which is an intrusion to consumers privacy. Therefore, the applied IoT protocol in this distributed, heterogeneous environment should meet data integrity, authentication, privacy, data confidentiality, standard, bandwidth, and latency communication requirements as well as treating privacy concerns by implementing some security policies[25,93]. Figure 8 demonstrates the practical elements of IoT application in the smart grid future trends.

The Foundation for Intelligent Physical Agents society (FIPA) has provided a standard model for communication in MAS. There are several platforms for the implementation of MAS, namely JADE, Zeus, Madkit, and JACK. Generally, message content includes two parts syntax and semantic. While syntax is the grammar of a message, semantic refers to the meaning of the applied vocabulary. FIPA-Semantic Language (FIPA-SL), Knowledge Interchange Format, Resource Definition Framework,

and Constraint Choice Language are four different languages introduced by FIPA for interoperability in the case of syntax and semantic. However, IEC 61850 and CIM define syntax and semantic of communication in the smart grid environment. In the interoperability point of view, we need to apply IoT protocols to satisfy the message content of those standards based on XML [94].

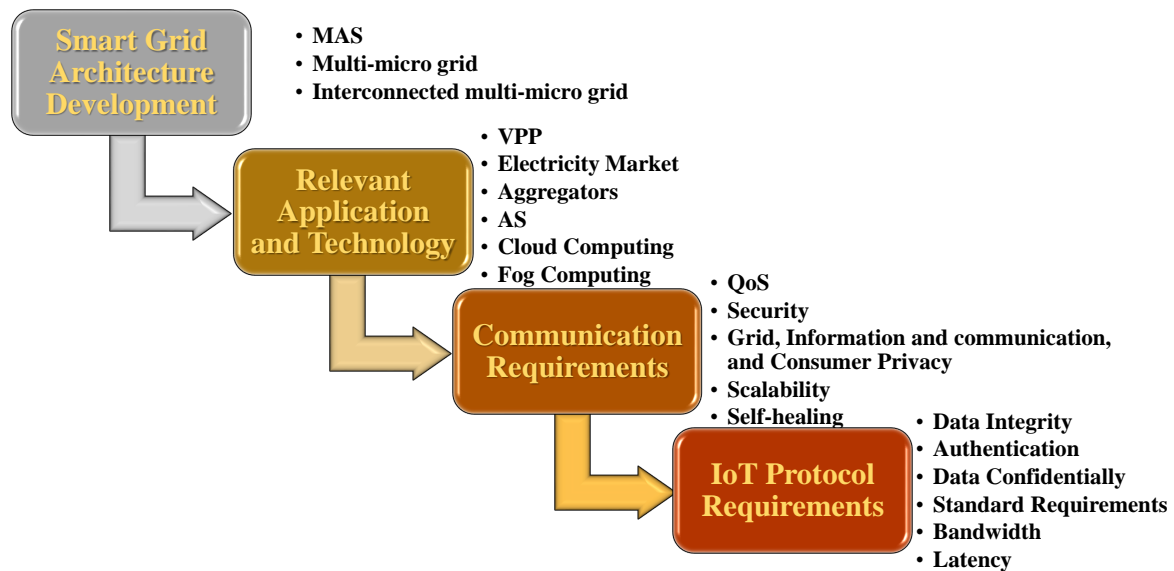


Figure 8. Effective elements in application of IoT in the smart grid future trends.

The smart grid communication architecture, which is shown in Figure 3, has three levels, i.e., HAN, FAN, and WAN that map to those standards and the MAS architecture in Figure 9. This figure delineates the MAS architecture of the smart grid. It also provides a guideline to find a proper IoT protocol for communication at each level of this structure. The communication structure inside each agent is on top of LAN and in accordance with MMS protocol based on IEC 61850. In this architecture, a multi-micro grid, entities can communicate with the supervisory level, such as DSO/TSO, through aggregators. Aggregators are placed in the middle of this architecture to facilitate interaction and cooperation and ensures data management, bundling, matching, and transaction among the micro grid, electricity market, and DSO/TSO. Since we consider economical constraints to provide communication structure, it is recommended to avoid dedicated ones and using existing infrastructure, which is the Internet. Communication exchanged aggregator and micro grid agent happens over the FAN, and IoT protocols recommendations, according to the previous section's investigation for this level are MQTT, CoAP, and XMPP. AMQP and ZeroMQ are suitable protocols applied for communication between the aggregator and the supervisory level. DDS is a robust and mature protocol that can be used in WAN. This protocol takes advantage of free infrastructure by using the Internet. It supports a wide variety of QoS, such as security and reliability, which are essential characteristics that we need for communication through the Internet.

6. Future Work

By applying MAS and multi-micro grid in the smart grid, the number of active nodes in the power system participating in AS increases. This intention results in high penetration of sensors, actuators, and computational units under the concept of IoT. Fog computing and cloud computing are tools for facilitating this scenario. Since there is no dedicated standard to apply them in the smart grid environment, realizing the communication structure, standards, and protocols of this phenomenon encourages future investigation in this area. End-users increase contribution in power grid AS and utilizes the Internet as an infrastructure of communication to release dedicated ones, which are vulnerable. In this case of privacy, this benefit defines a new horizon in data integrity,

authentication, privacy, data confidentiality, standard, bandwidth, and latency requirements of IoT protocol in the smart grid studies.

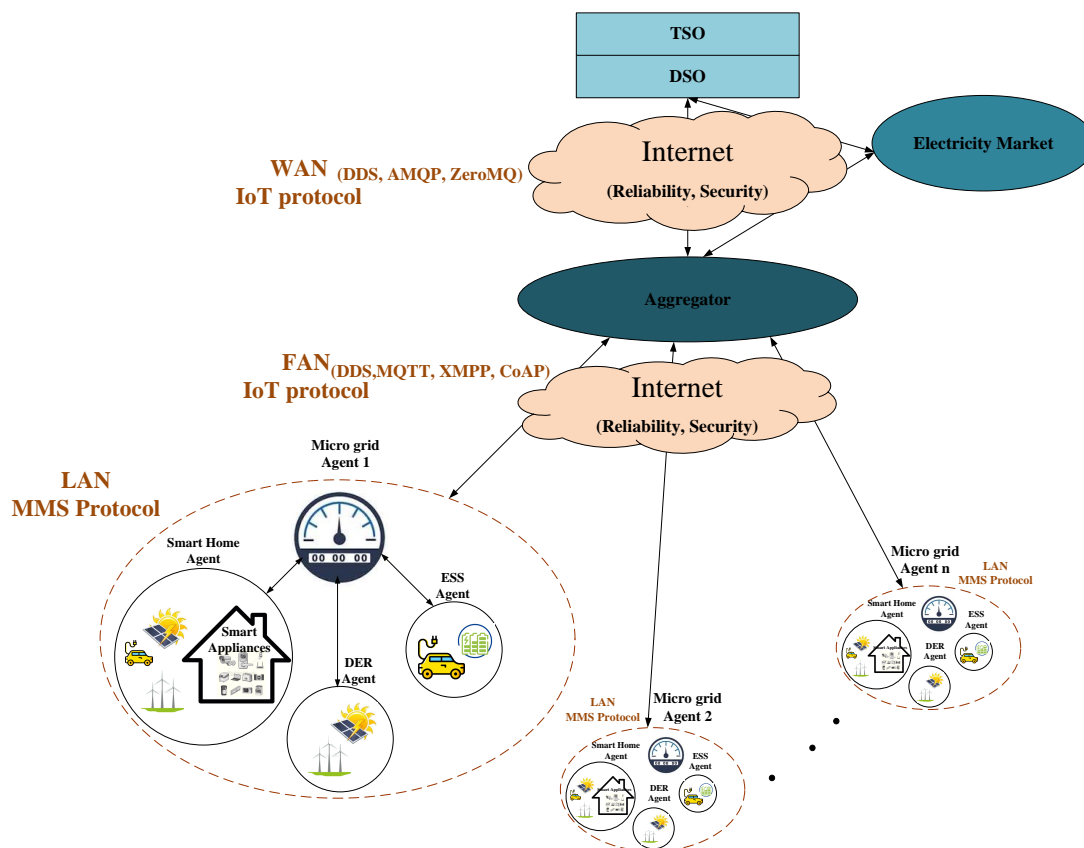


Figure 9. The smart grid MAS architecture based on IEC 61850 and IoT protocol.

7. Conclusions

Deployment of IoT technology in the heterogeneous environment of the smart grid facilitates real-time controlling and monitoring of the power system. Meanwhile, IoT protocol has the effective role in this real-time interaction. Since IEC 61850 and IEC 61970 are widely used communication standards in the smart grid, IoT protocols should meet their constraints. In this paper, we provided an overview of existing works that mapped IEC 61850 onto different IoT protocols and compared their experience results. This investigation revealed there is a limited effort in comparing the performance of IoT protocols in the near to real smart grid communication testbed, which is characterized by a more congested network. We also considered useful elements in the smart grid future trends for the application of IoT. Among all the smart grid development, we focused on altering the smart grid central structure to the MAS and multi-micro grid as the prominent ones since they facilitate the integration of RES and microgrid to the main grid as active elements provide AS. VPP, the electricity market, and aggregators are applications that assist this approach. Interaction in new structures of the smart grid requires minimum latency, maximum bandwidth, privacy, security, and scalability, which can be provided by applying cloud computing and fog computing. We also highlighted a cost-effective communication structure proposal within the FAN and WAN by deploying the public Internet to avoid dedicated communication infrastructure. To fulfill this scheme, we introduced DDS and ZeroMQ as proper protocols since they offer robust security and reliability characteristics.

Author Contributions: Conceptualization, L.T.; Data curation, L.T. and H.Y.; Writing—original draft preparation, L.T.; Writing—review and editing, L.T., H.Y.; Visualization, L.T. and H.Y.; Supervision, H.Y.; Project administration, H.Y.; Funding acquisition, H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019M3F2A1073179) and by Korea Electric Power Corporation (Grant number: R17XA05-66).

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

Abbreviations

The following abbreviations are used in this manuscript:

AC	Alarms and Conditions
AMI	Advanced Metering Interface
AMQP	Advanced Message Queue Telemetry Transport
AS	Ancillary Services
BEMS	Building Energy Management System
CEMS	Community Energy Management System
CIM	Common Information Model
CoAP	Constraint Application Protocols
CORBA	Common Object Request Broker Architecture
CoRE	Constrained Resource Environments
DA	Data Access
DCPS	Data Centric Publisher Subscriber
DDS	Data Distribution Services
DEMS	Data center Energy Management System
DER	Distributed Energy Resources
DII	Dynamic Invocation Interface
DLC	Direct Load Control
DMS	Distribution Management System
DNO	Distribution Network Operator
DNP3	Distributed Network Protocol 3
DR	Demand Response
DSI	Dynamic Skeleton Interface
DSO	Distribution System Operator
DSTATCOM	Distribution Static Compensator
DTLS	Datagram Transport Layer Security
EMS	Energy Management System
ESS	Energy Storage System
EV	Electric Vehicles
FIPA	Foundation for Intelligent Physical Agents Society
FIPA-SL	FIPA-Semantic Language
GOOSE	Generic Object Oriented Substation Event
GPS	Geographical Position System
FAN	Field Area Network
HA	Historical data Access
HAN	Home Area Network
HEMS	Home Energy Management System
HES	Home Electronic System
IDL	Interface Definition Language
IED	Intelligent Electronic Devices
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISA	International Society of Automation
JID	Jabber Identification
LAN	Local Area Network
LPWAN	Low Power WAN
MAS	Multi-Agent System
MMQT	Message Queue Telemetry Transport
MMS	Manufacturing Message Specification
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group
OPC UA	Open Platform Communications Unified Architecture
ORB	Object Request Broker

OSI	Open System Interaction
PLC	Power Line Carrier
PMU	Phasor Measurements Units
PRG	Program
QoS	Quality of Service
RES	Renewable Energy Sources
REST	REpresentational State Transfer
RFID	Radio Frequency Identification
RTPS	Real-Time Publisher Subscriber
SAS	Substation Automation Systems
SASL	Simple Authentication and Security Layer
SCADA	Supervisory Control and Data Acquisition
SOAP	Simple Object Access Protocol
SV	Sampled Value
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
UCA2.0	Utility Communication Architecture 2.0
UDP	User Datagram Protocol
VPP	Virtual Power Plant
V2G	Vehicle-to-Grid
WAN	Wide Area Network
WASA	Wide-Area Situational Awareness
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
ZeroMQ	Zero Message Queue

References

1. Bagdadee, A.H.; Zhang, L. Smart Grid: A Brief Assessment of the Smart Grid Technologies for Modern Power System. *J. Eng. Technol.* **2019**, *8*, 122–142.
2. Heirman, D. What makes Smart Grid-Smart—In addition, who is in the “game”? *IEEE Electromagn. Compat. Mag.* **2012**, *1*, 95–99.
3. Sakthivel, P.; Ganeshkumaran, S. Design of automatic power consumption control system using smart grid—A review. In *World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*; IEEE: Los Alamitos, CA, USA, 2016; pp. 1–4.
4. Dai, J.; Dong, M.; Ye, R.; Ma, A.; Yang, W. A review on electric vehicles and renewable energy synergies in smart grid. In *Proceedings of the China International Conference on Electricity Distribution (CICED)*, Xi’an, China, 10–13 August 2016; pp. 1–4.
5. Qazi, A.; Hussain, F.; Rahim, N.A.; Hardaker, G.; Alghazzawi, D.; Shaban, K.; Haruna, K. Towards Sustainable Energy: A Systematic Review of Renewable Energy Sources, Technologies, and Public Opinions. *IEEE Access* **2019**, *7*, 63837–63851. [[CrossRef](#)]
6. Almehezia, A.A.; Al-Masri, H.M.K.; Ehsani, M. Integration of Renewable Energy Sources by Load Shifting and Utilizing Value Storage. *IEEE Trans. Smart Grid* **2019**, *10*, 4974–4984. [[CrossRef](#)]
7. 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](#)]
8. Rehmani, M.H.; Reisslein, M.; Rachedi, A.; Erol-Kantarci, M.; Radenkovic, M. Integrating Renewable Energy Resources Into the Smart Grid: Recent Developments in Information and Communication Technologies. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2814–2825. [[CrossRef](#)]
9. Ghorbanian, M.; Dolatabadi, S.H.; Masjedi, M.; Siano, P. Communication in Smart Grids: A Comprehensive Review on the Existing and Future Communication and Information Infrastructures. *IEEE Syst. J.* **2019**, *13*, 4001–4014. [[CrossRef](#)]
10. Zhang, Y.; Zhang, Y.; Mu, X.L.; Lei, X.H.; Li, F.; Zhou, J.; Xu, L.; Gao, Y.X.; Liu, X.Z. Development of IEC 61850 and Its Application. In *Proceedings of the International Conference on Computer, Network Security and Communication Engineering (CNSCE)*, Bangkok, Thailand, 26–27 March 2017.
11. Englert, H.; Dawidczak, H. IEC 61850 substation to control center communication—Status and practical experiences from projects. In *Proceedings of the 2009 IEEE Bucharest PowerTech*, Bucharest, Romania, 28 June–2 July 2009; pp. 1–6.

12. Horalek, J.; Matyska, J.; Sobeslav, V. Communication protocols in substation automation and IEC 61850 based proposal. In Proceedings of the IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 19–21 November 2013; pp. 321–326.
13. Gupta, S. Communication in substation automation systems. *Int. J. Res. Adv. Eng. Technol.* **2016**, *2*, 54–58.
14. Ozansoy, C.; Zayegh, A.; Kalam, A. Communications for substation automation and integration. In Proceedings of the Australasian Universities Power Engineering Conference, Melborn, Australia, 29 September–2 October 2002.
15. *Communication Networks and Systems for Power Utility Automation—Part 8-1: Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, 2nd ed.; document IEC 61850-8-1; IEC: Geneva, Switzerland, 2011.
16. *Communication Networks and Systems for Power Utility Automation—Part 7-420: Basic Communication Structure—Distributed Energy Resources Logical Nodes*, 1st ed.; document IEC 61850-7-420; IEC: Geneva, Switzerland, 2009.
17. *Communication Networks and Systems for Power Utility Automation—Part 90-7: Object Models for Power Converters in Distributed Energy Resources (DER) Systems*, 1st ed.; document IEC 61850-90-7; IEC: Geneva, Switzerland, 2013.
18. Zaballos, A.; Vallejo, A.; Selga, J.M. Heterogeneous communication architecture for the smart grid. *IEEE Netw.* **2011**, *25*, 30–37. [[CrossRef](#)]
19. Eriksson, M.; Armendariz, M.; Vasilenko, O.O.; Saleem, A.; Nordström, L. Multiagent-Based Distribution Automation Solution for Self-Healing Grids. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2620–2628. [[CrossRef](#)]
20. Saleem, Y.; Crespi, N.; Rehmani, M.H.; Copeland, R. Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions. *IEEE Access* **2019**, *7*, 62962–63003. [[CrossRef](#)]
21. *Communication Networks and Systems for Power Utility Automation—Part 8-2: Specific Communication Service Mapping (SCSM)—Mapping to Extensible Messaging Presence Protocol (XMPP)*, 1st ed.; document IEC 61850-8-2; IEC: Geneva, Switzerland, 2018.
22. Al-Ali, A. Role of internet of things in the smart grid technology. *J. Comput. Commun.* **2015**, *3*, 229. [[CrossRef](#)]
23. Kaur, M.; Kalra, S. A review on IOT based smart grid. *Int. J. Energy Inf. Commun.* **2016**, *7*, 11–22. [[CrossRef](#)]
24. Viswanath, S.K.; Yuen, C.; Tushar, W.; Li, W.; Wen, C.; Hu, K.; Chen, C.; Liu, X. System design of the internet of things for residential smart grid. *IEEE Wirel. Commun.* **2016**, *23*, 90–98. [[CrossRef](#)]
25. Dalipi, F.; Yayilgan, S.Y. Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. In Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 63–68.
26. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet Things* **2019**, *16*, 100111. [[CrossRef](#)]
27. Bikmetov, R.; Raja, M.Y.A.; Sane, T.U. Infrastructure and applications of Internet of Things in smart grids: A survey. In Proceedings of the North American Power Symposium, Morgantown, WV USA, 17–19 September 2017; pp. 1–6.
28. Jiang, A.; Yuan, H.; Li, D.; Tian, J. Key technologies of ubiquitous power Internet of Things-aided smart grid. *J. Renew. Sustain. Energy* **2019**, *11*, 062702. [[CrossRef](#)]
29. Ghasempour, A. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Invention* **2019**, *4*, 22. [[CrossRef](#)]
30. Collier, S.E. The Emerging Enernet: Convergence of the Smart Grid with the Internet of Things. *IEEE Ind. Appl. Mag.* **2017**, *23*, 12–16. [[CrossRef](#)]
31. Reka, S.S.; Dragicevic, T. Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid. *Renew. Sustain. Energy Rev.* **2018**, *91*, 90–108. [[CrossRef](#)]
32. Bedi, G.; Venayagamoorthy, G.K.; Singh, R.; Brooks, R.R.; Wang, K. Review of Internet of Things (IoT) in Electric Power and Energy Systems. *IEEE Internet Things J.* **2018**, *5*, 847–870. [[CrossRef](#)]
33. Bahashwan, A.A.O.; Manickam, S. A Brief Review of Messaging Protocol Standards for Internet of Things (IoT). *J. Cyber Secur. Mobil.* **2019**, *8*, 1–14. [[CrossRef](#)]
34. Pradeep, K.K.; Vigna, K.R.; Padmanathan, K.; Jia, Y.Y.; Jagadeesh, P.; Arul, R. Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. *Sustain. Cities Soc.* **2020**, *53*, 101957.

35. Pramudhita, A.N.; Asmara, R.A.; Siradjuddin, I.; Rohadi, E. Internet of Things Integration in Smart Grid. In Proceedings of the International Conference on Applied Science and Technology (iCAST), North Sulawesi, Indonesia, 26–27 October 2018; pp. 718–722.
36. Amin, S.M.; Giacomoni, A.M. Smart grid, safe grid. *IEEE Power Energy Mag.* **2011**, *10*, 33–40. [[CrossRef](#)]
37. Annaswamy, A. *IEEE Vision for Smart Grid Control: 2030 and Beyond Roadmap*; IEEE: Los Alamitos, CA, USA, 2013; pp. 1–12.
38. Li, J.; Li, T.; Han, L. Research on the Evaluation Model of a Smart Grid Development Level Based on Differentiation of Development Demand. *Sustainability* **2018**, *10*, 4047. [[CrossRef](#)]
39. Ellabban, O.; Abu-Rub, H.; Blaabjerg, F. Renewable energy resources: Current status, future prospects and their enabling technology. *Renew. Sustain. Energy Rev.* **2014**, *39*, 748–764. [[CrossRef](#)]
40. Dileep, G. A survey on smart grid technologies and applications. *Renew. Energy* **2020**, *146*, 2589–2625. [[CrossRef](#)]
41. Tariq, F.; Dooley, L.S. Smart Grid communication and networking technologies: recent developments and future challenges. In *Smart Grids*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 199–213.
42. Barai, G.R.; Krishnan, S.; Venkatesh, B. Smart metering and functionalities of smart meters in smart grid—A review. In Proceedings of the 2015 IEEE Electrical Power and Energy Conference (EPEC), London, ON, Canada, 26–28 October 2015; pp. 138–145.
43. Wang, Y.; Chen, Q.; Hong, T.; Kang, C. Review of smart meter data analytics: Applications, methodologies, and challenges. *IEEE Trans. Smart Grid* **2018**, *10*, 3125–3148. [[CrossRef](#)]
44. Al-Turjman, F.; Abujubbeh, M. IoT-enabled smart grid via SM: An overview. *Future Gener. Comput. Syst.* **2019**, *96*, 579–590. [[CrossRef](#)]
45. Uddin, M.; Romlie, M.F.; Abdullah, M.F.; Halim, S.A.; Kwang, T.C. A review on peak load shaving strategies. *Renew. Sustain. Energy Rev.* **2018**, *82*, 3323–3332. [[CrossRef](#)]
46. 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](#)]
47. Zhang, X.; Pei, W.; Deng, W.; Du, Y.; Qi, Z.; Dong, Z. Emerging smart grid technology for mitigating global warming. *Int. J. Energy Res.* **2015**, *39*, 1742–1756. [[CrossRef](#)]
48. Shobole, A.; Wadi, M.; Tür, M.R.; Baysal, M. Real time active power control in smart grid. In Proceedings of the 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), San Diego, CA, USA, 5–8 November 2017; pp. 585–590.
49. Nozaki, Y.; Tominaga, T.; Iwasaki, N.; Takeuchi, A. A technical approach to achieve smart grid advantages using energy management systems. In Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 9–11 November 2011; pp. 1–5.
50. Rahman, M.G.; Chowdhury, M.F.B.R.; Al Mamun, M.A.; Hasan, M.R.; Mahfuz, S. Summary of smart grid: Benefits and issues. *Int. J. Sci. Eng. Res.* **2013**, *4*, 1–5.
51. Shu-wen, W. Research on the key technologies of IOT applied on smart grid. In Proceedings of the International Conference on Electronics, Communications and Control (ICECC), Ningbo, China, 9–11 September 2011; pp. 2809–2812.
52. Hossain, E.; Han, Z.; Poor, H.V. *Smart grid communications and networking*; Cambridge University Press: Cambridge, UK, 2012.
53. Tightiz, L.; Yang, H. Survey of IEC61850 M2M Interface based on IoT Protocols in Smart Grid Environment. In Proceedings of the Korea Institute Of Communication Sciences (KICS) Winter Conference, YongPyung Resort, South Korea, 23–25 February 2019; Volume 1; pp. 382–385.
54. Daoud, M.; Fernando, X. On the communication requirements for the smart grid. *Energy Power Eng.* **2011**, *3*, 53. [[CrossRef](#)]
55. Al-Dulaimi, A.; Wang, X.; I, C., Provisioning Unlicensed LAA Interface for Smart Grid Applications. In *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*; IEEE: Los Alamitos, CA, USA, 2018; pp. 603–624.
56. 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](#)]
57. Naumann, A.; Bielchev, I.; Voropai, N.; Styczynski, Z. Smart grid automation using IEC 61850 and CIM standards. *Control. Eng. Pract.* **2014**, *25*, 102–111. [[CrossRef](#)]

58. Schmutzler, J.; Gröning, S.; Wietfeld, C. Management of distributed energy resources in IEC 61850 using web services on devices. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 315–320.
59. *Communication Networks and Systems for Power Utility Automation—Part 1: Introduction and Overview (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, 2nd ed.; document IEC 61850-1; IEC: Geneva, Switzerland, 2013.
60. Tightiz, L.; Yang, H.; Piran, M.J. A Survey on Enhanced Smart Micro-Grid Management System with Modern Wireless Technology Contribution. *Energies* **2020**, *13*, 2258. [[CrossRef](#)]
61. Rodríguez-Molina, J.; Kammen, D.M. Middleware Architectures for the Smart Grid: A Survey on the State-of-the-Art. Taxonomy and Main Open Issues. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2992–3033. [[CrossRef](#)]
62. Pathaka, A.D.; Tembhurne, J.V. Internet of Things: A Survey on IoT Protocols. In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018; pp. 26–27.
63. Graube, M.; Hensel, S.; Iatrou, C.; Urbas, L. Information models in OPC UA and their advantages and disadvantages. In Proceedings of 3rd 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 9–10 May 2017; pp. 1–8.
64. González, I.; Calderón, A.J.; Figueiredo, J.; Sousa, J. A Literature Survey on Open Platform Communications (OPC) Applied to Advanced Industrial Environments. *Electronics* **2019**, *8*, 510. [[CrossRef](#)]
65. Burger, A.; Koziolk, H.; Rückert, J.; Platenius-Mohr, M.; Stomberg, G. Bottleneck identification and performance modeling of OPC UA communication models. In Proceedings of the 2019 ACM/SPEC International Conference on Performance Engineering, Barcelona, Spain, 27–29 November 2019; pp. 231–242.
66. Lee, R. *Big Data, Cloud Computing, and Data Science Engineering*; Springer: Berlin/Heidelberg, Germany, 2019; Volume 844.
67. Fagbemi, D.D.; Wheeler, D.M.; Wheeler, J. *The IoT Architect's Guide to Attainable Security and Privacy*; CRC Press: Boca Raton, FL, USA, 2019.
68. Macarulla, M.; Albano, M.; Ferreira, L.L.; Teixeira, C. Lessons learned in building a middleware for smart grids. *J. Green Eng.* **2016**, *6*, 1–26. [[CrossRef](#)]
69. Sanz, R.; Clavijo, J.A.; Segarra, M.; de Antonio, A.; Alonso, M. CORBA-based substation automation systems. In Proceedings of the 2001 IEEE International Conference on Control Applications (CCA'01) (Cat. No. 01CH37204), Mexico City, Mexico, 5–7 September 2001; pp. 773–777.
70. Shin, I.J.; Song, B.K.; Eom, D.S. International Electrotechnical Committee (IEC) 61850 mapping with constrained application protocol (CoAP) in smart grids based European telecommunications standard institute Machine-to-Machine (M2M) environment. *Energies* **2017**, *10*, 393. [[CrossRef](#)]
71. Pedersen, A.B.; Hauksson, E.B.; Andersen, P.B.; Poulsen, B.; Træholt, C.; Gantenbein, D. Facilitating a generic communication interface to distributed energy resources: Mapping IEC 61850 to RESTful services. In Proceedings of the First, IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 61–66.
72. Lehnhoff, S.; Mahnke, W.; Rohjans, S.; Uslar, M. IEC 61850 based OPC UA communication-The future of smart grid automation. In Proceedings of the 17th Power Systems Computation Conference (PSCC'11), Stockholm, Sweden, 22–26 August 2011.
73. Sucic, S.; Bony, B.; Guise, L. Standards-compliant event-driven SOA for semantic-enabled smart grid automation: Evaluating IEC 61850 and DPWS integration. In Proceedings of the 2012 IEEE International Conference on Industrial Technology, Athens, Greece, 19–21 March 2012; pp. 403–408.
74. Calvo, I.; De Albéniz, O.G.; Noguero, A.; Pérez, F. Towards a modular and scalable design for the communications of electrical protection relays. In Proceedings of the 35th Annual Conference of IEEE Industrial Electronics, Porto, Portugal, 3–5 November 2009; pp. 2511–2516.
75. Bi, Y.; Jiang, L.; Wang, X.J.; Cui, L.Z. Mapping of IEC 61850 to Data Distribute Service for digital substation communication. In Proceedings of the IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013; pp. 1–5.
76. Sučić, S.; Rohjans, S.; Mahnke, W. Semantic smart grid services: Enabling a standards-compliant Internet of energy platform with IEC 61850 and OPC UA. In Proceedings of the Eurocon 2013, Zagreb, Croatia, 1–4 July 2013; pp. 1375–1382.
77. Youssef, T.A.; Elsayed, A.T.; Mohammed, O.A. Data distribution service-based interoperability framework for smart grid testbed infrastructure. *Energies* **2016**, *9*, 150. [[CrossRef](#)]

78. Ferreira, R.D.F.; de Oliveira, R.S. Cloud IEC 61850 A Case Study of a Software Defined Protection, Automation Control System. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy, 4–7 September 2018; Volume 1, pp. 75–82.
79. Iglesias-Urkiá, M.; Urbietá, A.; Parra, J.; Casado-Mansilla, D. IEC 61850 meets CoAP: towards the integration of smart grids and IoT standards. In Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 22–25 October 2017; pp. 1–9.
80. Hastings, J.C.; Laverty, D.M. Modernizing wide-area grid communications for distributed energy resource applications using MQTT publish–subscribe protocol. In Proceedings of the IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; pp. 1–5.
81. Youssef, T.A.; El Hariri, M.; Elsayed, A.T.; Mohammed, O.A. A DDS-based energy management framework for small microgrid operation and control. *IEEE Trans. Ind. Inform.* **2017**, *14*, 958–968. [[CrossRef](#)]
82. Esfahani, M.M.; Hariri, A.; Mohammed, O.A. Game-theory-based Real-Time Inter-Microgrid Market Design Using Hierarchical Optimization Algorithm. In Proceedings of the IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, USA, 5–10 August 2018; pp. 1–5.
83. Iglesias-Urkiá, M.; Casado-Mansilla, D.; Mayer, S.; Urbietá, A. Validation of a CoAP to IEC 61850 Mapping and Benchmarking vs HTTP-REST and WS-SOAP. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Torino, Italy, 4–7 September 2018; Volume 1, pp. 1015–1022.
84. Hussain, S.S.; Aftab, M.A.; Ali, I. IEC 61850 modeling of DSTATCOM and XMPP communication for reactive power management in microgrids. *IEEE Syst. J.* **2018**, *12*, 3215–3225. [[CrossRef](#)]
85. 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](#)]
86. Kim, J.S.; Thus, S.M.; Kim, J.T.; Cho, J.W.; Park, H.J.; Jufri, F.H.; Jung, J. Microgrids platform: A design and implementation of common platform for seamless microgrids operation. *Electr. Power Syst. Res.* **2019**, *167*, 21–38. [[CrossRef](#)]
87. Petersen, B.; Bindner, H.; Poulsen, B.; You, S. Smart grid communication middleware comparison. In Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2017), Portugal, Porto, 22–24 April 2017; pp. 219–226.
88. Choi, J.S. A Hierarchical Distributed Energy Management Agent Framework for Smart Homes, Grids, and Cities. *IEEE Commun. Mag.* **2019**, *57*, 113–119. [[CrossRef](#)]
89. Hatziargyriou, N., Operation of Multi-Microgrids. In *Microgrids: Architectures and Control*; Wiley: Hoboken, NJ, USA, 2014; pp. 165–205.
90. Zou, H.; Mao, S.; Wang, Y.; Zhang, F.; Chen, X.; Cheng, L. A survey of energy management in interconnected multi-microgrids. *IEEE Access* **2019**, *7*, 72158–72169. [[CrossRef](#)]
91. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J.P.C. Fog Computing for Smart Grid Systems in the 5G Environment: Challenges and Solutions. *IEEE Wirel. Commun.* **2019**, *26*, 47–53. [[CrossRef](#)]
92. Hussain, M.; Beg, M. Fog Computing for Internet of Things (IoT)-Aided Smart Grid Architectures. *Big Data Cogn. Comput.* **2019**, *3*, 8. [[CrossRef](#)]
93. Herold, R.; Hertzog, C. *Data Privacy for the Smart Grid*; CRC Press: Boca Raton, FL, USA, 2015.
94. Hasanuzzaman Shawon, M.; Muyeen, S.M.; Ghosh, A.; Islam, S.M.; Baptista, M.S. Multi-Agent Systems in ICT Enabled Smart Grid: A Status Update on Technology Framework and Applications. *IEEE Access* **2019**, *7*, 97959–97973. [[CrossRef](#)]

