

This is a self-archived – parallel-published version of an original article. This version may differ from the original in pagination and typographic details. When using please cite the original.

AUTHOR	Imed Saad Ben Dhaou, Aron Kondoro, Syed Rameez Ullah Kakakhel, Tomi Westerlund, Hannu Tenhunen
TITLE	Internet of Things Technologies for Smart Grid
YEAR	2020
DOI	10.4018/978-1-7998-1974-5.ch010
VERSION	Publisher's PDF
CITATION	Ben Dhaou, Imed Saad, et al. "Internet of Things Technologies for Smart Grid." Tools and Technologies for the Development of Cyber-Physical Systems, edited by Sergey Balandin and Ekaterina Balandina, IGI Global, 2020, pp. 256-284. https://doi.org/10.4018/978-1-7998-1974-5.ch010

Chapter 10

Internet of Things Technologies for Smart Grid

Imed Saad Ben Dhaou

Qassim University, Saudi Arabia & The University of Monastir, Tunisia

Aron Kondoro

University of Dar es Salaam, Tanzania

Syed Rameez Ullah Kakakhel

 <https://orcid.org/0000-0001-5901-2477>

University of Turku, Finland

Tomi Westerlund

 <https://orcid.org/0000-0002-1793-2694>

University of Turku, Finland

Hannu Tenhunen

Royal Institute of Technology, Sweden

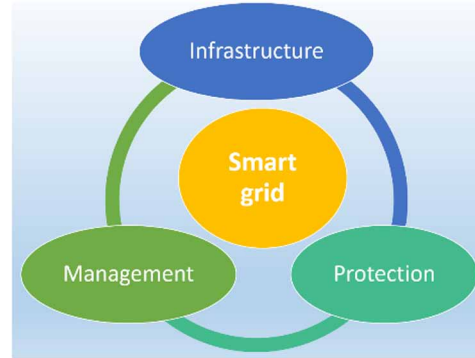
ABSTRACT

Smart grid is a new revolution in the energy sector in which the aging utility grid will be replaced with a grid that supports two-way communication between customers and the utility company. There are two popular smart-grid reference architectures. NIST (National Institute for Standards and Technology) has drafted a reference architecture in which seven domains and actors have been identified. The second reference architecture is elaborated by ETSI (European Telecommunications Standards Institute), which is an extension of the NIST model where a new domain named distributed energy resources has been added. This chapter aims at identifying the use of IoT and IoT-enabled technologies in the design of a secure smart grid using the ETSI reference model. Based on the discussion and analysis in the chapter, the authors offer two collaborative and development frameworks. One framework draws parallels' between IoT and smart grids and the second one between smart grids and edge computing. These frameworks can be used to broaden collaboration between the stakeholders and identify research gaps.

DOI: 10.4018/978-1-7998-1974-5.ch010

Figure 1. Smart grid ingredients proposed

Source: Fang, Misra, Xue, & Yang, 2012



INTRODUCTION

Smart grid is a new paradigm that aims at making the legacy utility grid, efficient, green, reliable and secure. The term was coined in 2007 by the US congress in a bid to modernize the US power grid system (Energy Independence and Security Act of 2007, 2007). As stated in the 2007 Act on energy Independence and Security, a smart grid should have the following ten features: (1) Wide-scale deployment of ICT (Information and communication technologies) to shape-up performance, reliability, and trustworthiness of the utility grid, (2) dynamic optimization of grid operations and resources, (3) integration of effective renewable energy resources, (4) endorsement of advanced demand response scheme, (5) amalgamation of smart technologies for controlling and monitoring the grid operations, (6) consolidation of intelligent appliances, (7) integration of cutting-edge electricity storage and peak-abatement technologies, (8) purveying consumers with timeous information and control options, (9) development of standards for communication and interoperability of appliances and equipment, and (10) battling barriers and obstacles that prevent the adoption of smart grid technologies, practices, and services.

The legacy grid has been built using outdated technologies which cannot address existing shortcomings. Further, the current grid suffers from the interoperability issues among systems and devices which makes the need for a better and efficient grid a hard mission. For instance, the report published by NIST has identified more than 70 gaps in the current grid standards that need to be addressed (National Institute of Standards and Technology, 2014). During recent years, discernible efforts have been put forward to establish a smart grid with the characteristics stated heretofore. A good survey that summarizes the research effort on the permissive technologies for the smart grid until the year 2011 is reported in (Fang, Misra, Xue, & Yang, 2012). The authors reviewed advances in the following three axes: infrastructure, management, and protection. Finally, the researchers digested the omnifarious projects, legislations, programs, standards and trials worldwide in the area of smart grid. Figure 1 elaborates the three essential ingredients in a smart grid.

Communication is a key enabling technology for the smart grid infrastructure. It is believed that the smart grid will integrate multifarious communication technologies like cellular communication, fiber-optic, short-range communication, wireless mesh networks, power-line communication, and satellite communication. The assorted deployment of communication technologies in the smart grid is attributed to factors like the application requirements, the geographic locations, environments, legislations, cost,

and so forth. In (Gungor, et al., A Survey on Smart Grid Potential Applications and Communication Requirements, 2013), the authors summarized the communication requirements for fourteen smart grid applications. They further road mapped future smart grid services and applications.

The intensive deployment of communication technologies in the smart grid has precipitated the need for cyber security. The cyber security solution aims to preserve consumer privacy, protect the data against eavesdropping and prevent embedded systems, used along the smart grid, from running malicious software (Yan Y., Qian, Sharif, & Tipper, 2012).

BACKGROUND

Legacy power grid architecture has been designed to cope with the maximum power demands. It is a centralized architecture in which the power is generated in one place, transported over long distances and then distributed to customers. The traditional power grid is a vertical business, highly deregulated, and monopolized. The snowballing operation costs associated with other epidemic factors such as carbon dioxide emission, increasing demands on electricity, have pushed the power industry and the associated stakeholders to upgrade the power grid to address the challenges, meet the market expansion, and create new business models.

Smart-grid concept evolved from the modernization effort of the legacy grid. Its focal features are the two-way communication between the end-user (customer) and the utility company, bidirectional power flow, and the heavy deployment of ICT to improve grid reliability and efficiency. Smart-grid is viewed as system of systems in which real-time communication is indispensable in achieving distributed intelligence, outage detection, demand-side management, Distributed Generation (DG), remote control, tele-protection, Advanced Metering Infrastructure (AMI), distributed automation, Home Energy Management System (HEMS), Distributed Storage (DS), etc., (Sendin, Sanchez-Fornie, Berganza, Simon, & Urrutia, 2016).

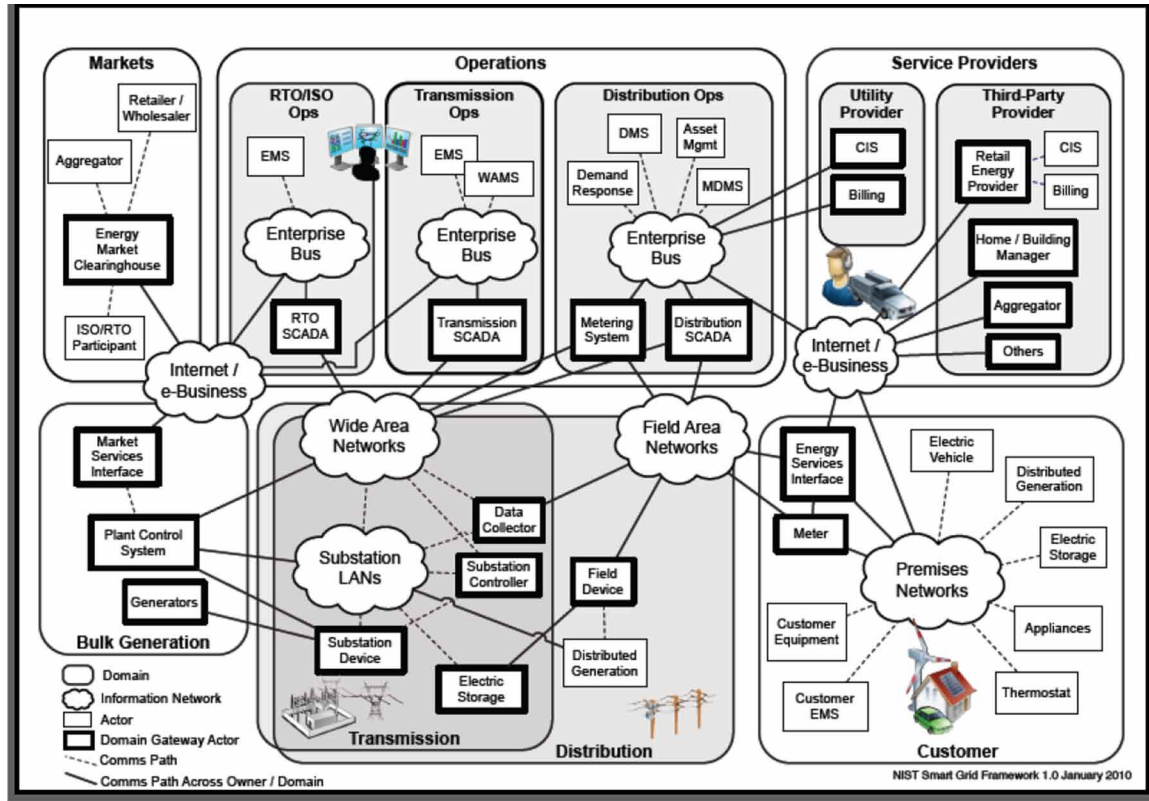
In 2010, NIST released the first smart grid roadmap for interoperability. The ultimate aim is to devise a framework to solve and guide the interoperability smart Grid devices and systems used in the smart grid. The reference model conceived by NIST identified seven major domains that constitute the smart grid. Those domains are as follows: customer, markets, service providers, operations, bulk generation, transmission, and distribution. Each domain has key features such as inter and intra-domain communication requirements, services, and actors. Figure 2 depicted the NIST conceptual reference model.

In an effort to remedy the interoperability concerns, NIST through a specialized group has proposed a stack of eight layers. The arrangement of the stack from the bottom up is as follows: basic connectivity, network interoperability, syntactic interoperability, semantics, business context, business procedures, business objectives, and policies (economic/ regulatory).

The classification of the communication platform deployed in the smart grid is essential to identify the competing solutions. The authors of (Farhangi, 2010) (Yu, et al., 2011) (Yan Y., Qian, Sharif, & Tipper, 2013) (Khan, Rehmani, & Reisslein, 2016) (Erol-Kantarci & Mouftah, 2015) classified the smart grid communication technologies based on the coverage area. This type of classification allows the projection of the existing communication standards to serve the needed communication requirements in the smart grid. Indeed, the distance between the interconnected devices, the QoS requirements, latency, power consumption, operating environments, and other factors guide the suitable communication architecture.

Figure 2. NIST smart grid reference model

Source: National Institute of Standards and Technology, 2014



For instance, home appliances are placed close to each other, which makes the local area network as the preferred communication architecture.

In (Farhangi, 2010), the author described the nascent standards for wide area, local area and home area networks.

Table 1 summarizes the preferred network type for various standards. For HAN, the author claimed that ZigBee as a potential winner as a standard for home energy system, an emerging standard, named oneM2M, is purging its way (Elmangoush, Steinke, Al-Hezmi, & Magedanz, 2014). The third column in Table 1 summarizes the application and preferred communication protocol for oneM2M.

The generic communication architecture presented in (Yan Y., Qian, Sharif, & Tipper, 2013) is inspired from (Yu, et al., 2011). The architecture engenders home area networks (HANs), business area network (BANs), neighborhood area networks (NANs), and wide area networks (WAN). The survey paper written by (Erol-Kantarci & Mouftah, 2015) added field area networks (FAN) and argued that the topology of FAN is similar to NAN.

The works by (Gungor, Sahin, Kocak, & Ergut, Smart grid technologies: communication technologies and standards, 2011) and (Fang, Misra, Xue, & Yang, 2012) categorized the grid communication platform based on the communication medium. This type of classification permits to further select the communication architecture based on the QoS requirements, cost and the environments. For instance,

Table 1. Preferred communication for HAN, NAN and WAN

Standard	Network Type	Preferred communication	Application
IEC 61850	WAN	fiber optic WiMax	Substation automation
ANSI C12.22	LAN	IEEE 802.11 PLC	Smart meter
oneM2M	HAN	BLE, RFID/NFC, WiFi	Home automation

wireless communication in local area network is preferred over wired LAN in case the application needs flexible connectivity, shorter installation time, high mobility (Wickelgren, 1996).

In (Gungor, Sahin, Kocak, & Ergut, Smart grid technologies: communication technologies and standards, 2011), the authors compared and contrasted six available communication technologies: GSM, GPRS, 3G, WiMAX, PLC and Zigbee. They also described four communication requirements security, system reliability, robustness and availability, scalability, and QoS.

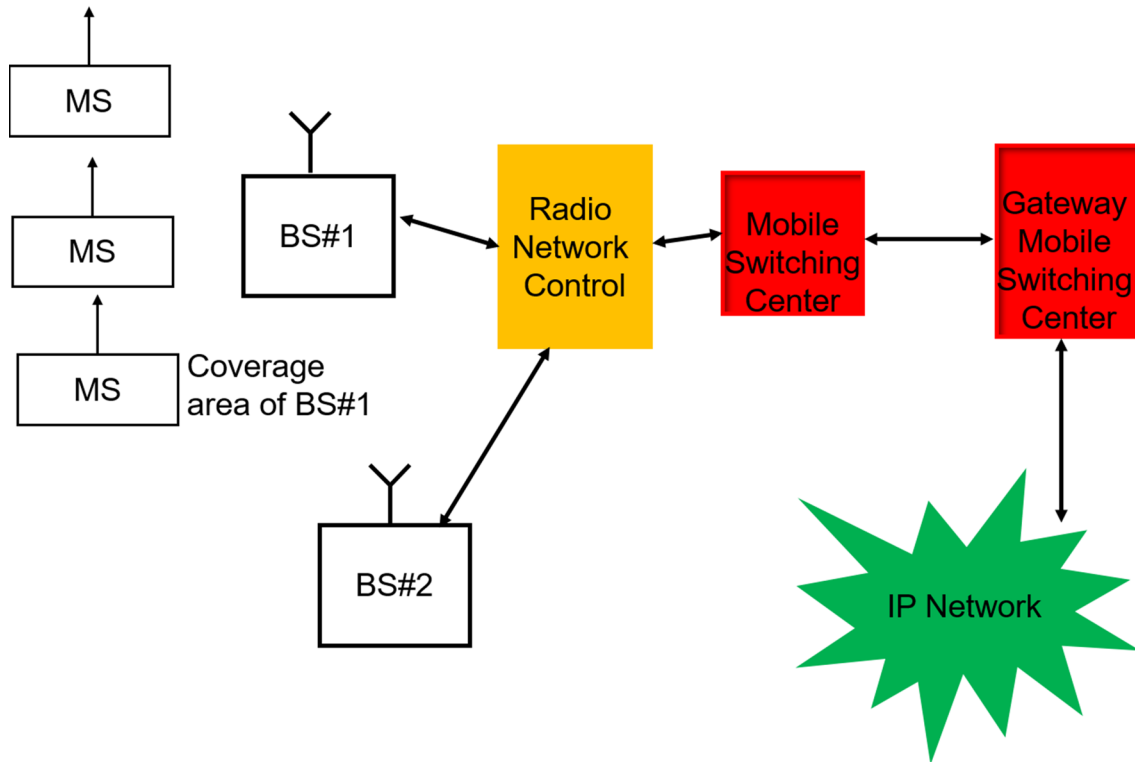
(Fang, Misra, Xue, & Yang, 2012) surveyed the interoperability between the various communication technologies to meet end-to-end requirements and described open research problems.

(Nafi, Ahmed, Gregory, & Datta, 2016) also categorized the smart grid communication architecture based on the standard model of a smart grid as identified in the IEEE 2030 standard (IEEE Std 2030-2011, 2011). This resulted in a three layers' communication network architecture. The core network which covers the generation and transmission domains, wide area network which covers the distribution network, and the private network which involves the customer domain.

(Ma, Chen, Huang, & Meng, 2013) described categories of communication technologies depending on the task they perform in the overall process of delivering power from the supply to demand side. In this way, an electric grid can be viewed as consisting of two systems, transmission and distribution. The authors discussed recent communication technologies such as wide area frequency monitoring networks and cognitive radio based regional area networks in the transmission domain, and 802.15 based smart utility networks, TV white space and Hybrid (WiMAX/Wireless Mesh Networks) in the distribution domain.

While many surveys have categorized the smart grid communication infrastructure and technologies in terms of various smart grid application requirements and supported features (Anzar, Nadeem, & Sohail, 2015) (Kabalci, 2016) (Khan & Khan, 2013), other studies have taken a different perspective. (Ancillotti, Bruno, & Conti, 2013) have taken a data centric approach. The authors have categorized the smart grid communication technologies according to their abilities to facilitate the collection, transmission and storage of critical data for smart grid applications. They described the communication sub-system of a smart grid being made up of mainly two parts. The first part is the communication infrastructure responsible for providing the pathway through which different components can connect. The second part is the middleware platform which sits on top of the communication network, abstracting away the underlying details, and providing a user friendly API for distributed smart grid applications (Ben Dhaou, et al., 2017).

Figure 3. Architecture of a cellular wireless Internet network



Internet of Things Technologies

Traditionally, the Internet was accessed using a fixed computer or laptop. Advances in wireless communications and silicon technologies have enabled access to the internet anywhere anytime. Nowadays, the Internet is accessible using smart-phone, WIFI or other long-range wireless communication technologies (3G, LTE, 4G, etc.). Wireless Internet access using cellular technologies is ensured by the following entities: A base-station (BS) that connects the mobile devices (MS) to cellular network for message or voice exchange, a radio network controller (RNC) is the block that is responsible for spectrum control, a mobile switching center that links the MS to the public switched network, and a gateway mobile switching center (GMSC) that interfaces the cellular network with the Internet. Figure 3 illustrates a generic architecture for wireless internet access using a cellular technology.

Advances in sensing technologies coupled with the miniaturization of the silicon devices (nanometer technologies) have enabled the development of the wireless sensor network. Wireless Sensor Network (WSN) is composed from a number of spatially distributed and communicating sensors. WSN are used to collect data from various domains such as biological system, environment, electrical appliances, machine, and city infrastructure. WSN has enabled the development of a plethora of smart and ubiquitous applications. Broadly speaking, the WSN can be used for tracking or monitoring. Table 2 cites a few applications of WSN.

Table 2. Applications of WSN

Application Name	Area	Category
ECO-driving	Vehicle engine	Monitoring
Healthcare	Human body	Monitoring
ECO-routing	Vehicle	Tracking
Surveillance	Military	Monitoring
Anti-traffic noise	Environment	Monitoring
Industrial automation	Factory	Monitoring
Traffic management system	City	Tracking
Energy saving	Building	Monitoring
Precision agriculture	Agriculture	Monitoring
Oil drilling	Underground	Monitoring
Animal tracking	Agriculture	Tracking
Corrosion monitoring	Underwater	Monitoring
Smart post	Mail system	tracking
Logistic	Production chain	tracking
Smart grid	Energy	Monitoring

Cyber-physical system, CPS, is a three-layer architecture devised to use modern ICT tools for cyber control of physical components. Figure 4. depicts the architecture for a CPS system (Lin, et al., 2017). The lower level of the architecture is the physical sensors that measure physical parameters. The measurements are then forwarded to the communication layer which is responsible for connecting the sensors to the ICT equipment for control, coordination, monitoring and managements. The application layer uses the communication layer for receiving or transmitting messages. Cyber-physical system has been used in a variety of applications such as e-health, transportation, smart-grid, building, defense, etc.

Internet of Things (IoT) is an emerging computing and communication paradigm. Though, there is not yet a globally recognized definition of the IoT, most work refer to the IoT as the interconnection of object, things and humans using Internet technology (Lin, et al., 2017). Similar to the CPS, IoT is a multilayer architecture that interconnects heterogeneous networks; hence, it is often regarded as a network of networks. Figure 5 illustrates the architecture of a service oriented IoT.

CPS and IoT have some similarities and differences. As summarized in (Lin, et al., 2017), IoT interconnects CPS systems horizontally.

IoT Architecture/Layers

There are multiple IoT architecture models available, from conceptual to technology levels. Figure 6 presents a technological and collaborative IoT architecture divided into complementary successive layers. This model is based on information flow where devices (sensors and actuators) make up the lowest layer. For the purposes of this model, a sensor is nothing more than a data generation point. This sensor can thus be a micro-device or a large water flow monitoring system. The data generated by these devices is carried via the network where it lands on edge gateways. Edge gateways are utilized to filter, normalize

Figure 4. CPS Architecture

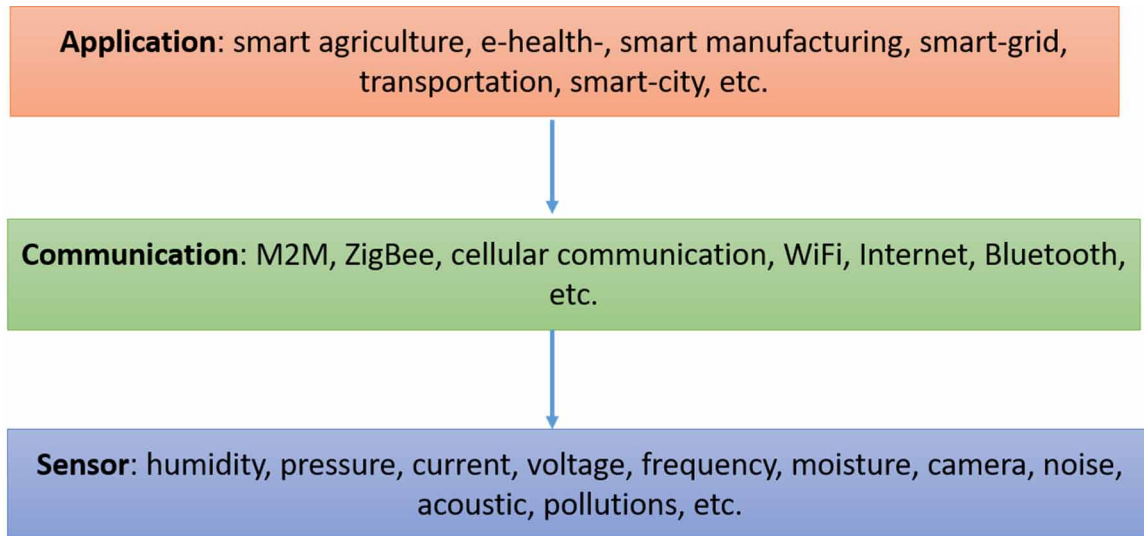


Figure 5. IoT architecture (service and application view)

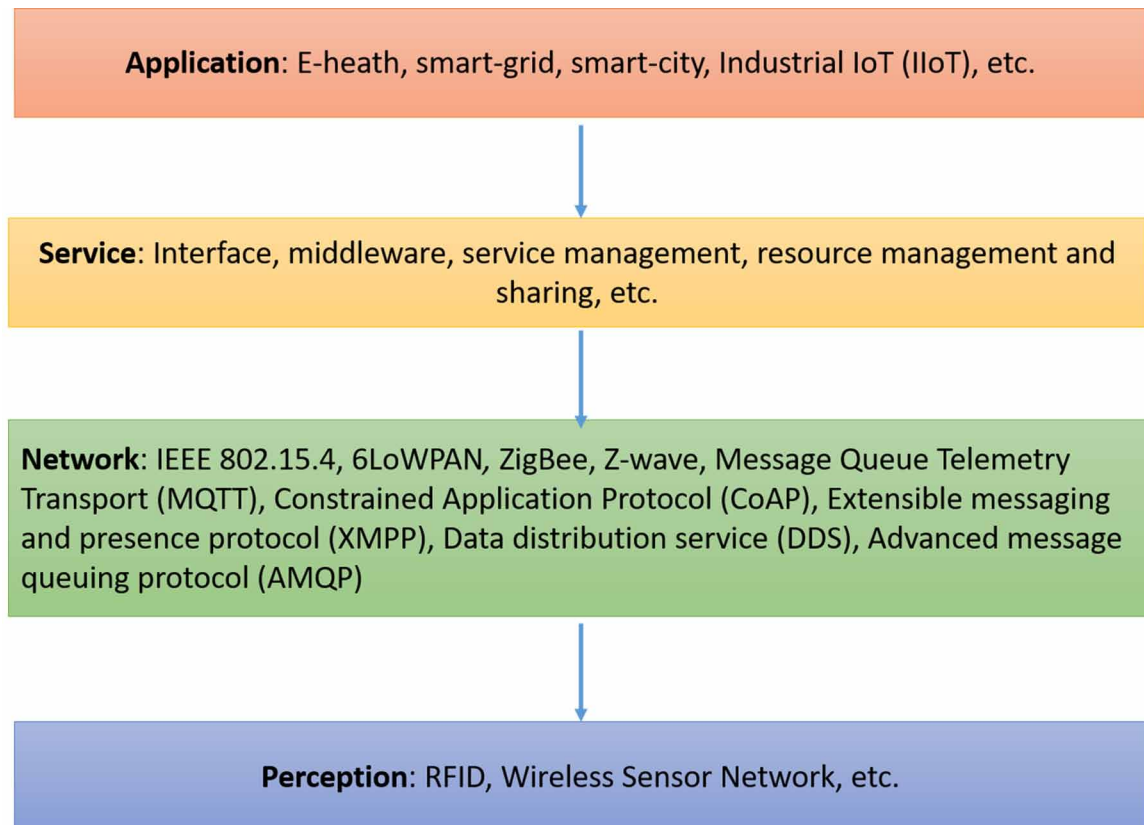
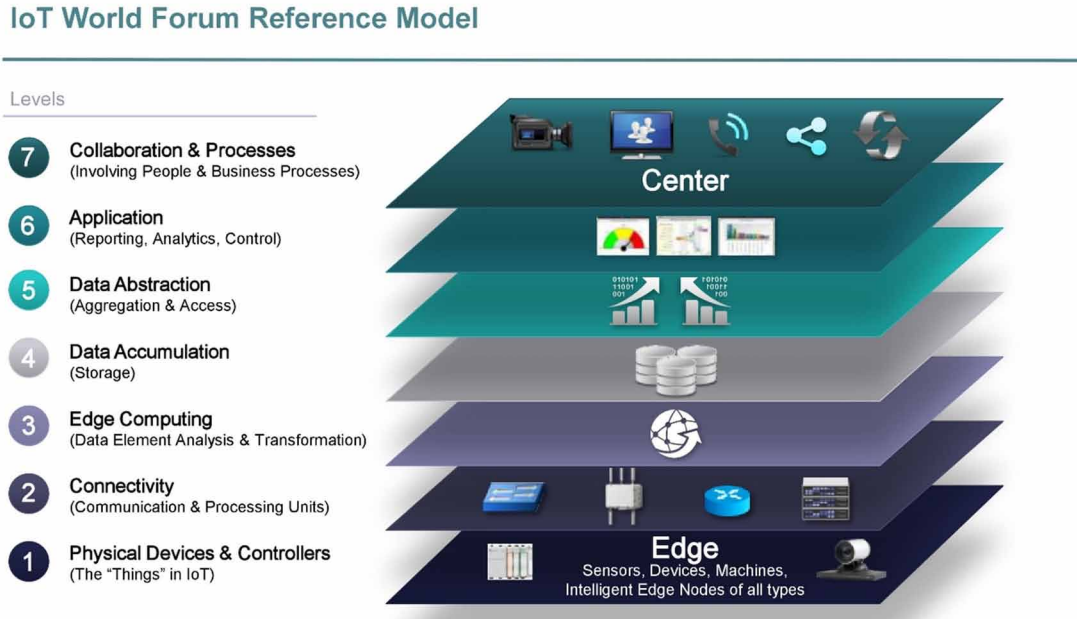


Figure 6. IoT World Forum Architecture Reference Model (device and connectivity view)



and process the data before being sent out. This processed data is then stored in a commonly accessed database, one that is available to all stakeholders. There the data is utilized by applications to offer services such as demand-response, customer notifications, automatic device control etc. The processed data in databases, combined with the decisions then enables the human decision-making process. The human decision making is complemented via visualizations based on historic or real time data, system constraints and regulatory frameworks. Combined, IoT is about taking small pieces of sensor information on a large scale and converting them into actionable information and visualizations for human decision makers. We will have a deeper look at each layer.

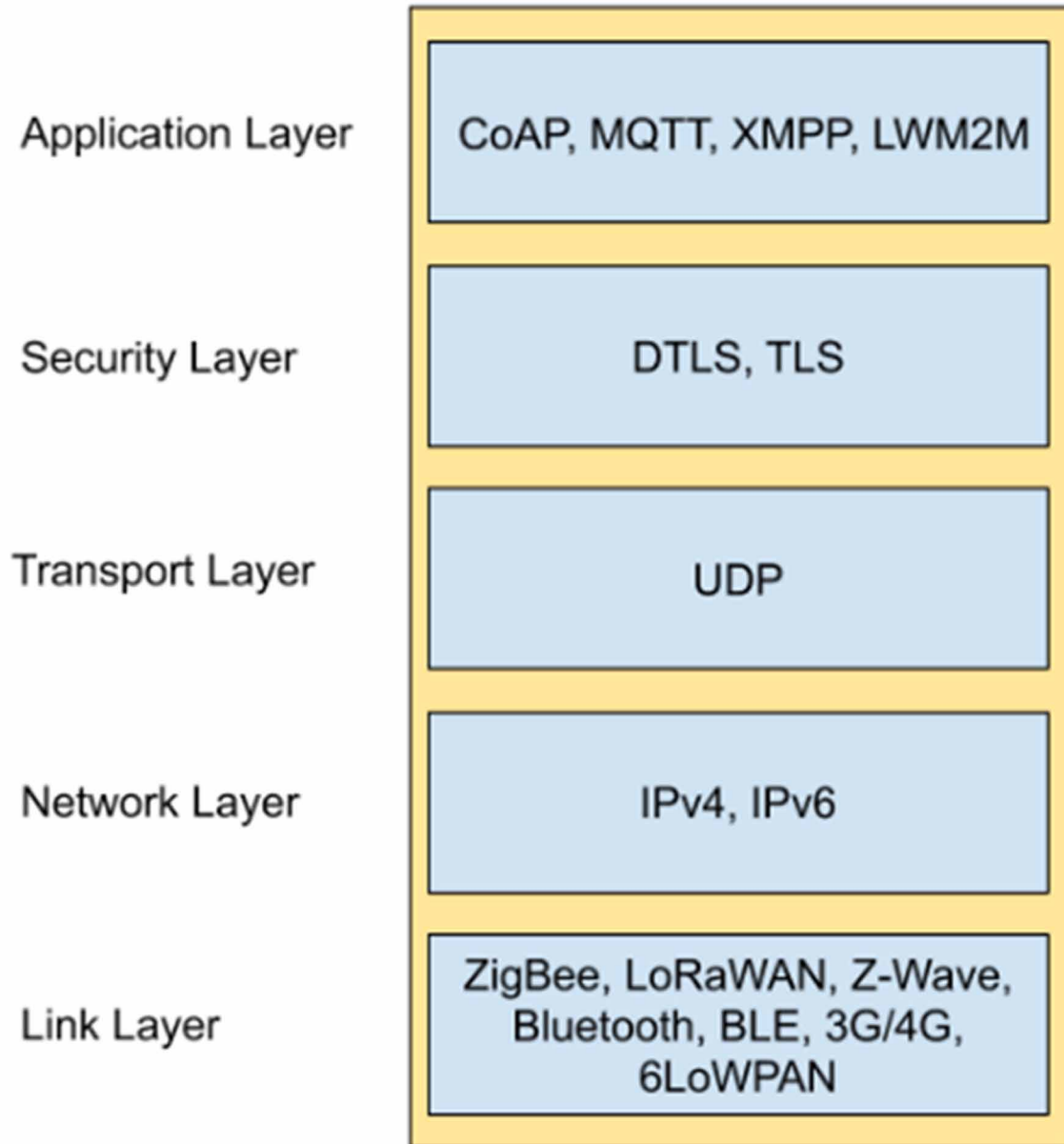
Physical Devices

This is the lowest layer of the IoT model that corresponds to the sensor/perception layer in CPS. Physical devices and controllers constitute everything on the sensor layer in CPS, plus controller entities. In a smart grid environment this would correspond to smart homes and factory nodes, all types of voltage monitoring sensors, home appliances etc.

Connectivity

The connectivity layer includes both network connectivity and enabling sensors and devices to talk to each other and the internet. The set of IoT protocols is large but we will discuss here a subset of them that are most relevant to smart grids. Figure 7 shows the IoT communication stack.

Figure 7. IoT communication stack



The link level protocols can be divided into three major categories: Long-Range Protocols: LoRA, NBIoT; medium range: Wi-Fi, 4G/LTE, 5G; and short Range: Bluetooth, ZigBee. Table 3 summarizes commonly known IoT wireless communication protocol.

The Application Layer Protocols are also of several types as follows:

Table 3. IoT communication protocol

IoT Protocol	SG Domain	SG Application
ZigBee	HAN	Smart home automation, Power consumption monitoring, automatic meter reading
Bluetooth	HAN	Smart home automation
Bluetooth Low Energy	HAN	Smart device/appliances automation
LoRaWAN	WAN	Power transmission monitoring, power equipment management
6LoWPAN	HAN	Advanced Metering Infrastructure, Smart home automation
Z-Wave	HAN	Smart home automation

HTTP

HTTP is the dominant web protocols, forming the backbone of world wide web. HTTP and HTTPS offer a design pattern called REST (Representational State Transfer). REST APIs (application Programming Interface) built on top of HTTP offer simple web connectivity to devices. Whether it is device to cloud, device to database or relaying messages back to a node from the cloud. The most significant benefit of HTTP is enabling web-integration thus enhancing communication and interoperability. HTTP however is insecure and thus HTTPS is recommended. HTTP supports multiple types of payload, from text files to compressed data, audio and video. Thus, it can be easily integrated into any internet connected system.

CoAP

Although diverse, the problem with HTTP is that it is resource intensive. It was not designed for IoT in mind. However, there was a need felt for a protocol that offers web-integration, can be easily translated to and from HTTP and lighter. CoAP is exactly that protocol. It follows similar syntax to HTTP, same identification mechanisms and addressing schemes but is lighter. CoAP is also designed to support one-to-many communication (unlike HTTP).


CoAP Security

The CoAP protocol uses the Datagram Transport Layer Security (DTLS) protocol as its security extension. It provides the following security services: confidentiality, integrity, authentication, non-repudiation, and protection against packet replay attacks. It is the modification of the Transport Layer Protocol (TLS) with additional features that enable it to work with the UDP protocol.

There are four defined security modes that can be used by CoAP (+DTLS):

- **NoSec:** With this mode CoAP messages are exchanged without any security
- **PreSharedKey:** In this mode, CoAP messages are protected using symmetric key encryption. Communicating devices possess shared symmetric keys that they use to encrypt messages. These symmetric keys need to be pre-configured before communication is initiated. It is a mode that is suitable for low end devices, and in small scale deployments.

Figure 8. MQTT username/password fields within CONNECT packet

MQTT-Packet:	
CONNECT	
	
contains:	Example
clientId	"client-1"
cleanSession	true
username (optional)	"hans"
password (optional)	"letmein"
lastWillTopic (optional)	"/hans/will"
lastWillQos (optional)	2
lastWillMessage (optional)	"unexpected exit"
lastWillRetain (optional)	false
keepAlive	60

- **RawPublicKey:** In this mode, messages are protected using asymmetric key encryption. Communicating devices use pre-configured asymmetric key pair to encrypt and authenticate the messages. This mode is used for devices with more processing power but without a supporting public key infrastructure. It is defined as a mandatory mode to implement CoAP.
- **Certificate-Based:** This mode is similar to the RawPublicKey mode but with a supporting public key infrastructure. The infrastructure supports issuing, management, and validation of certificates. Each device possesses an asymmetric key pair with an X.509 certificate signed by a valid certificate authority (CA). When communicating, a device can use the key pair to secure the session, and authenticate the identity of the other party using a valid certification chain.

MQTT

MQTT was designed by IBM to be a very lightweight messaging protocol. It is a light, payload agnostic and network agnostic communication protocol. Theoretically it can even be used over SMS (short messaging service). MQTT offers higher reliability and quality of service over unreliable connections.

MQTT Security

The MQTT protocol aims to be simple and lightweight. As a result, it only offers minimal security mechanisms by default. Additional security protection can be provided by standard security protocols in different layers of the communication stack. MQTT provides authentication capabilities using client

identities, and username/password credentials. A client can optionally send a username and password when it connects to a broker. As Figure 8 shows, there are optional username/password fields in the MQTT CONNECT packet.

The username field is an UTF-8 encoded string while the password field is binary with a maximum of 64k bytes. When the broker receives the username/password combination, it authenticates the client and allows authorized communication to proceed. However, the username/password credentials are exchanged in plain text by default. Extra protection is needed to secure the transmission of these credentials. It can be provided in the network or transport layers.

In the network layer, standard solutions such as VPN can be used to secure the MQTT communication. This solution provides a secure tunnel through which communication can pass. It is used in situations where there are central gateways between the communicating parties.

In the transport layer, TLS/SSL is used to provide confidentiality through encryption. In addition, certificates can be used to provide authentication. In the application layer, MQTT provides client identities, and username/passwords credentials to implement authentication service. Custom encryption of payloads can also be provided by the specific application to implement further security

XMPP

XMPP started as chat/instant messaging protocol. It offers one-to-one and one-to-many communication. XMPP mandates the use of encryption (TLS/SASL) for security. For use-cases where security and node/user authentication are important XMPP is a good choice. For humans it might be a real-time communication protocol but for embedded systems it is slow.

Gateways for Interoperability

Since not all communication protocols might be supported by all the devices, gateways play an important role here. They offer internet access to the extreme low power nodes and interoperability between devices that target a different protocol.

Edge Computing

Edge computing is about bringing the computation from cloud towards the consumer edge. The consumer, in the context of smart grids, can be either home or industrial locations. Edge computing offers a distributed architecture enabling redundancy, masking cloud outages and lower response times in terms of latency. In our context, edge computing can be considered as a resource for integrating Smart Meters and distributed energy resources (DERs) into the IoT based smart grid.

Data Accumulation and Data Aggregation

IoT, in itself, does not care about what type of data is collected and why. Data collection is always context and application dependent. However, IoT architectures and solutions do offer the mechanisms to collect, store and analyze data. In the context of smart grids, data is the underlying decision metric for not only for reporting and billing but for demand predictions, load management and customer communications.

Application

Application layer in IoT deals with the tools that are enabled/envisioned based on the data aggregation from the lower layer. As stated in the previous section, these applications can be; reporting, billing, predicting load/stress and then devising algorithms for mitigating/managing the load.

Collaboration and Processes

The final layer in IoT involves people and regulatory/management processes. The end goal is to enable the business decision makers have a better insight into their operations. Enabling cross-domain and cross-industry and government collaboration. In the later section we will have an overview of how different IoT technologies can help achieve the same goals for smart grids.

IoT SECURITY

To provide the necessary security features, security mechanisms can be applied at different levels across the IoT communication stack. There exist several security extensions that have been developed for communication protocols operating at each of these levels. Each of these extensions have their own advantages and disadvantages.

The 802.15.4 standard which operates at the link layer provides eight different levels of security depending on the application needs (Alharby, Weddell, Reeve, & Harris, 2018). These levels protect each frame and provide confidentiality, authenticity, integrity, and replay detection features. Each level can provide the following security services: encryption only (AES-CTR), authentication and integrity only (AES-CBC-MAC), or all three combined (AES-CCM).

In the network layer, general-purpose security solutions such as IKEv2/IPSec (IETF) are used to provide data authentication, integrity and integrity features. They can provide host-to-host or network-to-network security by establishing secure channels through which communication can pass. The security mechanisms are transparent to all IoT applications protocols operating at the higher levels. This offers simplicity by trading off flexibility.

In the transport layers, TLS/SSL and DTLS are used to provide security services for IoT-based applications. TLS/SSL which relies on the TCP protocol is used to ensure the authenticity between communicating parties by using asymmetric encryption schemes. Certificates are used as the form of identity and a public key infrastructure is needed to support its operation. DTLS (IETF) is the modified form of TLS which operates on top of the UDP protocol. As a result, it is more lightweight and is the preferred option for many security deployments for IoT-based applications.

APPLICATION OF INTERNET OF THINGS IN SMART GRID

One of the promising approaches in the implementation of the ICT systems for powering micro-grids and smart grid has been the use of IoT technologies. These technologies have already revolutionized many other domains where they have been applied. They have allowed microprocessors and communication modules to be embedded in everyday devices, turning them into smarter devices.

In the power sector, the integration of IoT technologies has offered similar opportunities and advantages. By embedding IoT components in nodes making up the power system, the whole process of power generation, transmission, distribution, consumption, and management can be made more efficient and intelligent. These intelligent nodes can perform better by making autonomous decisions and adapting their behaviors based on the context. In addition, they can also communicate with each other and coordinate their activities in order to achieve system wide goals more efficiently.

Multi-Agent Systems

Multi-agent system, MAS, is a new promising technology for control and monitoring of the smart grid enabled by the IoT. MAS is evolved from the distributed computing environment in which agent-oriented programming has been established (Wooldridge, 2009). The development of MAS has been promoted by the Internet technologies. An agent can be a piece of software or hardware that can collaborate to solve an optimization problem with global constraints subject to some objective function. MAS has shown great potential in WSN environment.

Three classes of agents have been established in (Dagdeviren, Korkmaz, Tekbacak, & Erciyes, 2011). Specifically, in WSN agents can be mobile software or mobile hardware or a sensor node. In the smart grid domain, MAS has been used in various levels including protection, control, FLISR (fault identification, isolation, and restoration), and substation automation (Shawon, Muyeen, Ghosh, Islam, & Baptista, 2019). The MAS is a cornerstone technology for the decentralized operation of the smart grid. Multi-level MAS based architecture has been elaborated in substation automation (Wu, Feng, Tang, & Fitch, 2005), demand-side management (Rwegasira, et al., 2019). The lower level is often regarded as the hardware agent which is responsible for actuation, measurement, and control of hardware unit (charge controller, relay, etc.)

Figure 9 pictures physical agents that have been designed to control the operation of a DC microgrid using load-shedding techniques (Rwegasira, et al., 2019). The agents have been modeled using REPAST. The battery agent is responsible for control and monitoring the storage elements. The solar energy agent takes care of simulating the solar radiation. Finally, the load agent monitors and controls the operation of DC loads. Practical realization of the dc-microgrid necessities the incorporation of the communication protocols. A survey work of the MAS platform and the associated ICT infrastructure has been conducted in (Shawon, Muyeen, Ghosh, Islam, & Baptista, 2019). Table 4 summarizes sample work on MAS application and its associated IoT communication protocol.

Previous research has shown that the application of IoT for smart micro-grids can offer unique advantages compared to other existing ICT infrastructure. (Yu, et al., 2011) showed that IoT can help a smart-grid become more context-aware, interactive, autonomous and self-healing. It helps to achieve these goals by facilitating the collection, filtering, analysis and processing of a large amounts of contextual data. Table 5 shows the comparison between IoT based and traditional smart-grid ICT networks.

(Jabłońska, 2014) also describes the role IoT can play in powering and supporting the deployment of smart-grids and micro-grids. As cloud technologies continue to replace humans in performing data analysis, IoT through sensor technologies, can enable objects to collect contextual information and interact with their environment. The author sees these wireless sensor networks as a major part of IoT that enable wide scale collection and communication of sensor data necessary for autonomy and adaptability.

Figure 9. MAS based DSM proposed

Source: Rwegasira, et al., 2019

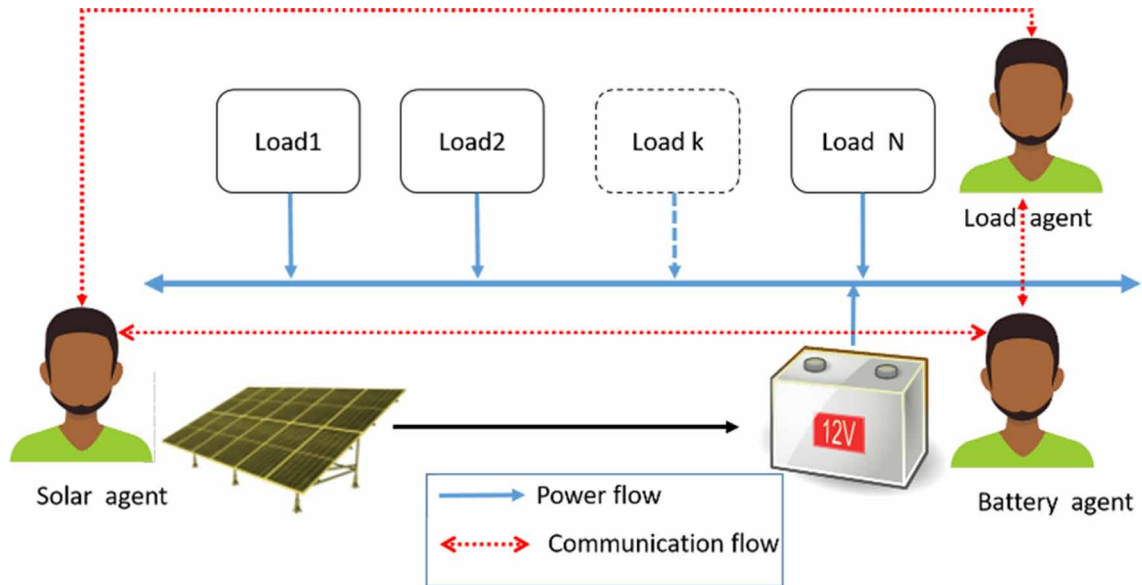


Table 4. MAS application and the associated IoT communication protocol

MAS Application	Smart-Grid Domain	IoT Communication Protocol	References
FLISR and substation automation	Distribution	TCP/IP, IEC 61850	(Ben Meskina, Daggaz, Khalgui, & Li, 2017) (Sekhavatmanesh & Cherkaoui, 2019) (Zhabelova & Vyatkin, 2012)
Energy trading and energy management	Customer	Zigbee, WiFi	(Kahrobaee, Rajabzadeh, Soh, & Asgarpour, 2013) (Rasheed, Javaid, Hussain, Akbar, & Khan, 2017)
Microgrid control	Distribution	WiFi, Zigbee, IEC 61860	(Liang, et al., 2012) (Cintuglu & Mohammed, Multiagent-based decentralized operation of microgrids considering data interoperability, 2015) (Cintuglu, Youssef, & Mohammed, Development and Application of a Real-Time Testbed for Multiagent System Interoperability: A Case Study on Hierarchical Microgrid Control, 2018)

As IoT devices also continue to become smaller, more powerful, and consuming less power, the number and variety of functions that can be implemented in power systems can only increase. The technology has already been transforming the power grid in China turning it into a smarter system ((Liu, Li, Chen, Zhen, & Zeng, 2011). In another example, the integration of an IoT platform in a DC-based grid allowed the creation of a power system that is flexible and adaptable. This resulted in a system that is

Table 5. Comparison between IoT-based and traditional smart grid information and communication networks

	IoT Platform	Present Electric Power Communication Network Platform
Environment perception	Use sensors, RFID to collect data of all processes of electricity	Manual inspection not suited for operations in complex terrain environments
Self-healing	Network nodes have self-recovery ability. Can find, detect, remove hidden faults	Only realizes single dimension, low-level tunnel self-healing and self-recovery.
Interaction	Supports large scale both side data stream supply, both side information interaction for grid and the users	Not realized. Interaction between users and service is simple and one way.
Different character	Supports the backbone network of grid, distribution network. 3G network can also be integrated together	Can integrate many kinds of networks, however, is strictly isolated from the Internet
Security	Can realize real time monitoring, and prevent natural disaster and breakage from external factors	Has information in isolated islands, lack of information sharing, low and inefficient in processing disaster

easily upgradeable and where innovative applications can be implemented easily (Di Zenobio, Steenhaut, Thielemans, & Celidonio, 2017).

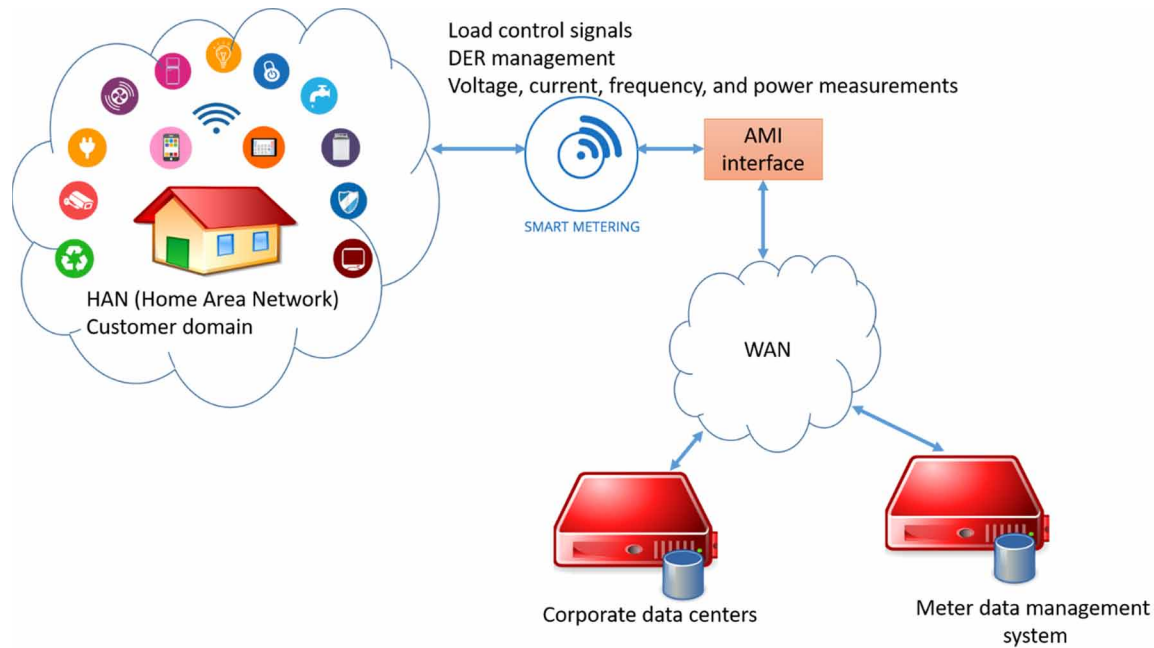
The traditional electric power system is generally divided into three main sections depending on the main function that is performed: transmission, distribution and customer (Kundur, Balu, & Lauby, 1994). In all these parts, IoT technologies have already been implemented with positive results.

In the transmission domain, IoT has been used to improve the reliability and stability of transmission lines. (Chen, Sun, Zhu, Zhen, & Chen, 2012) proposed an IoT based architecture for smart-grids (SG-IoT) that allows for the sensing and monitoring of different adverse conditions that can occur in power transmission lines. These conditions include the leaning of transmission towers, the temperature of the conducting wires, wind conditions that can disrupt power lines, and weather conditions such as temperature, humidity and rainfall that can all affect the normal operation of transmission lines. This capability was achieved by deploying small wireless sensors throughout transmission lines and towers. The data collected then passed through other two layers; network and perception, where it was exchanged and analyzed to produce useful information for decision making. A similar use case is also described by (Ou, Zhen, Li, Zhang, & Zeng, 2012). The authors describe a similar IoT based system for monitoring power transmission lines. The system consists of sensors, a communication network, and data aggregation technologies. By fusing all these technologies together, it was possible to monitor and control the transmission system in real time. There is an opportunity for these technologies to also be applied in other parts or aspects of the smart grid.

Likewise, in the customer domain, IoT has also been applied in different use cases. To seamlessly integrate nodes in homes and buildings into the power system, (Spanò, Di Pascoli, & Iannaccone, 2015) elaborated an approach that utilizes an IoT platform that allows home devices to be embedded with computational and communication abilities. The architecture of the system which consists of sensor and actuator networks, an IoT server, and user interfaces for visualization and control, provides a mechanism for data collection, processing, and monitoring by leveraging existing devices in homes. This use of existing devices minimized the complexity of the deployment and helped with user acceptance.

All these examples highlight the potential of IoT as a driving technology behind an ICT system that can power a smart grid.

Figure 10. AMI architecture



ADVANCED METERING INFRASTRUCTURE

Smart meter is the corner stone technologies for building advanced meter services that allows the customer and utility companies through the two-way communication to optimize the operation of the grid. Demand-side management along with the dynamic pricing are two significant applications of the smart-meter. Smart meter is an embedded system installed on the consumer premises to record various electric parameters that can be used for billing, price adjustment, situation awareness, etc.

Advanced metering infrastructure is composed of smart meters, communication network, data-management software. In the NIST reference model, energy service interface (ESI) communicates with associated domains (service providers, distribution, markets, operations, transmission) through the AMI. Figure 10: AMI architecture shows a basic architecture of an AMI.

The application of IoT in the context of AMI has been studied in several published reports. The work of (Wan, Zhang, & Wang, Demonstrability of Narrowband Internet of Things technology in advanced metering infrastructure, 2019) summarized the communication protocols used in the smart-grid. For the AMI, the authors considered the following communication protocols: cellular networks, WiMAX, PLC, wireless mesh technology, ZigBee, and digital subscriber lines. ZigBee is the winning technology in HAN. In addition to those reviewed communication standards, the author of (our work) considered Lora technology. The potential of NB-IoT in AMI has been investigated in (Wan, Zhang, & Wang, Demonstrability of Narrowband Internet of Things technology in advanced metering infrastructure, 2019). NB-IoT has a good indoor and outdoor coverage, cost efficient, and suitable for battery operated devices.

Distribution management system, DMS, monitors and controls the distribution system. It is an actor in the operations domain. Traditionally, the load at the consumer side are not managed by the DMS. To make advanced DMS services such as demand-response program and DER, (Li, et al., 2010) proposed a

middleware centric architecture for the integration of the of AMI and Distribution Management Systems. The architecture uses IoT connectivity.

SOLUTIONS AND RECOMMENDATIONS

Interoperability and Applications

In this section we will discuss how IoT can enable interoperability into the smart grid and which IoT solutions are directly applicable to the needs of smart grids. For a broader look at the technical and data interoperability between IoT models and Smart Grid, we will utilize the SGAM model (Figure 11). The SGAM is a three-dimensional smart grid model that incorporates smart grid domains, zones and interoperability. The ground grid layer encompasses the complete electrical grid from generation to customer premises. The hierarchical division into zones is based on functional separation and user philosophies. Processes include the physical equipment and energy transformation, energy management systems and microgrid management are in the operational zone all the way up to the market zone which encompasses energy trading and retail markets. The third dimension in this model is vertical interoperability, which is divided into five layers. The lower layer deals with the grid components, communication/connectivity, information, grid functionality and the business processes and policies are at the top that are enabled by the communication and information exchange from below. The SGAM offers a complete outlook at all the physical, functional, informational and associative components of a smart grid in a single framework.

Based on our previous discussion on smart grids and IoT reference models, we can draw a complementary framework between the two paradigms. Figure 12 represents the model that merges these two paradigms together.

Expanding on Figure 12, here we will list a subset of IoT technologies that will be beneficial to smart grids.

- **Component Layer**

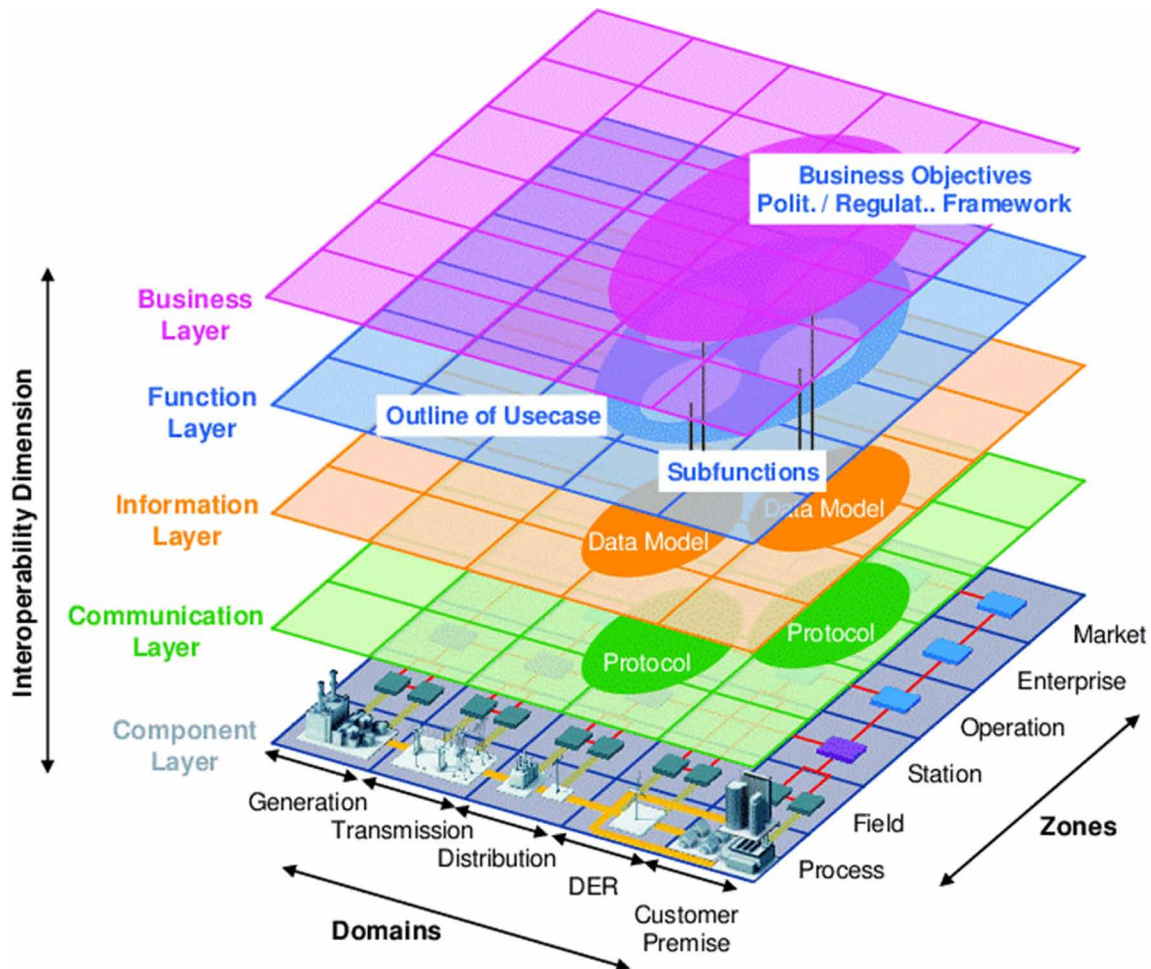
The economies of scale of IoT has made it very economical to produce sensors. The proliferation of mobile devices and supply chain has further reduced the cost of electronic devices. This allows customers to acquire smarter devices and companies to blanket their premises with sensors. This sensor and smart device data are what the smart grid systems and policy makers will utilize for any type of decision making.

- **Communication Layer**

IoT long range protocols like LoRA and NBIoT not only reduce the cost of telemetry but increase the range of communication to kilometers, instead of meters. This is a big advantage for distributed smart grids in remote areas where telecommunications networks might not be available. Light protocols like MQTT and COAP further enhance interoperability with web applications and enterprise systems.

- **Information Layer**

Figure 11. The smart grid architecture model (SGAM)



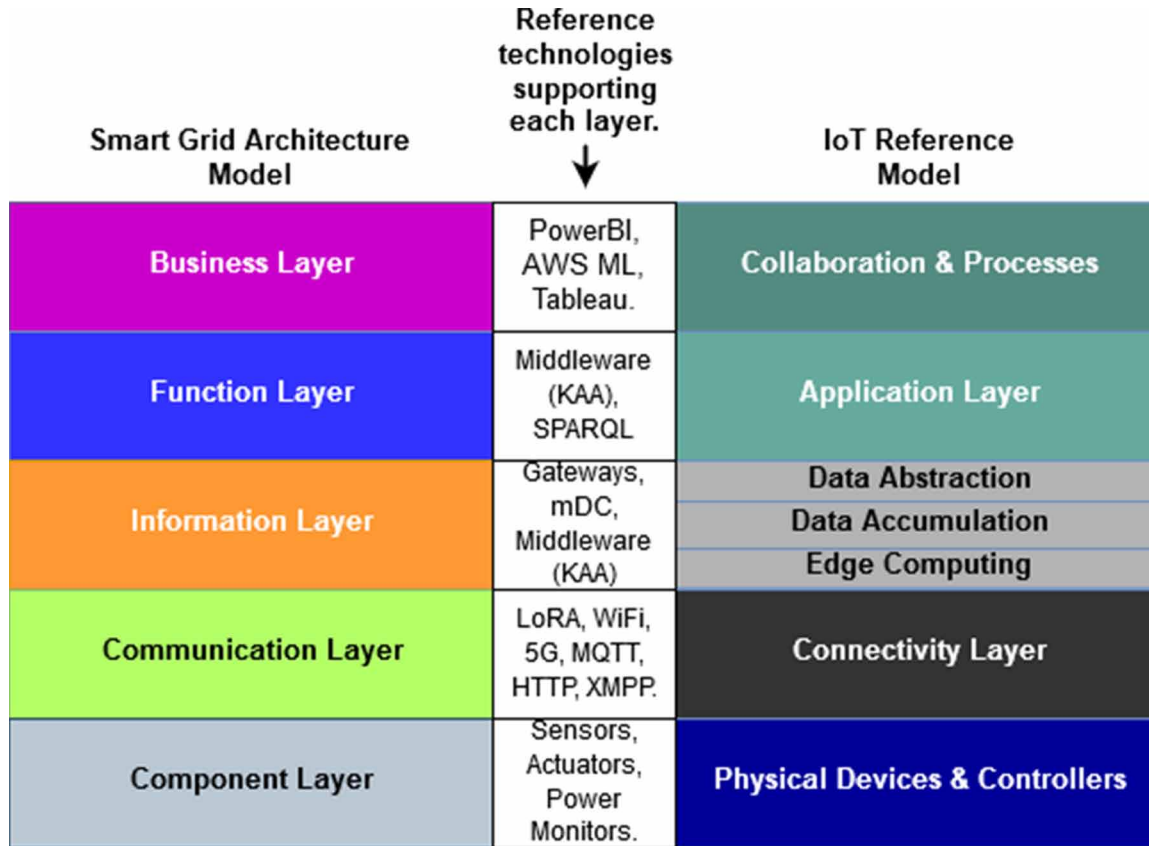
Large scale monitoring will raise the cost of computation and IT infrastructure. however, IoT supported edge computing initiatives can improve privacy (Chen, Lu, & Xiong, n.d.), reduce bandwidth costs (Aazam & Huh, 2016) and improve QoS.

- Function Layer

Middleware like KAA ("Smart Energy, Smart Lighting Solutions with the Kaa IoT Platform," n.d.) allow storage and analysis of sensor data. This enables utilities to monitor assets, perform fault detection, QoS analysis and generate health reports of the grid. Languages like OWL (web ontology language) can annotate and contextualize data by adding semantic information. SPARQL offers contextual information search over semantic links between data. Combined with ML this could enable new applications, services, predictive maintenance and load management that haven not been envisioned yet.

Figure 12. IoT technologies that can support smart grids

Smart Grid Coordination Group. Smart Grid Reference Architecture; Technical Report; CEN-CENELEC-ETSI: Brussels, Belgium, 2012. Link: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf



- Business Layer

The collection of data eventually is to provide smother operations and services. Tableau (“Business Intelligence and Analytics Software,” n.d.) is a leading data visualization platform that enables analytics, data governance and collaboration in one suite. This enables board members to assess the grid and improve data collection efficiency. Governments can have better insights into energy requirements and customers will have a deeper look at their usage behaviors. Amazon AWS ML (“Machine Learning on AWS,” n.d.) enables companies to use machine learning models in the cloud on their sensor data. Utilizing these services, the utility companies do not need to setup their own compute infrastructure and applications to smarten their grid/service offerings.

Edge/Fog Computing and Smart Grids

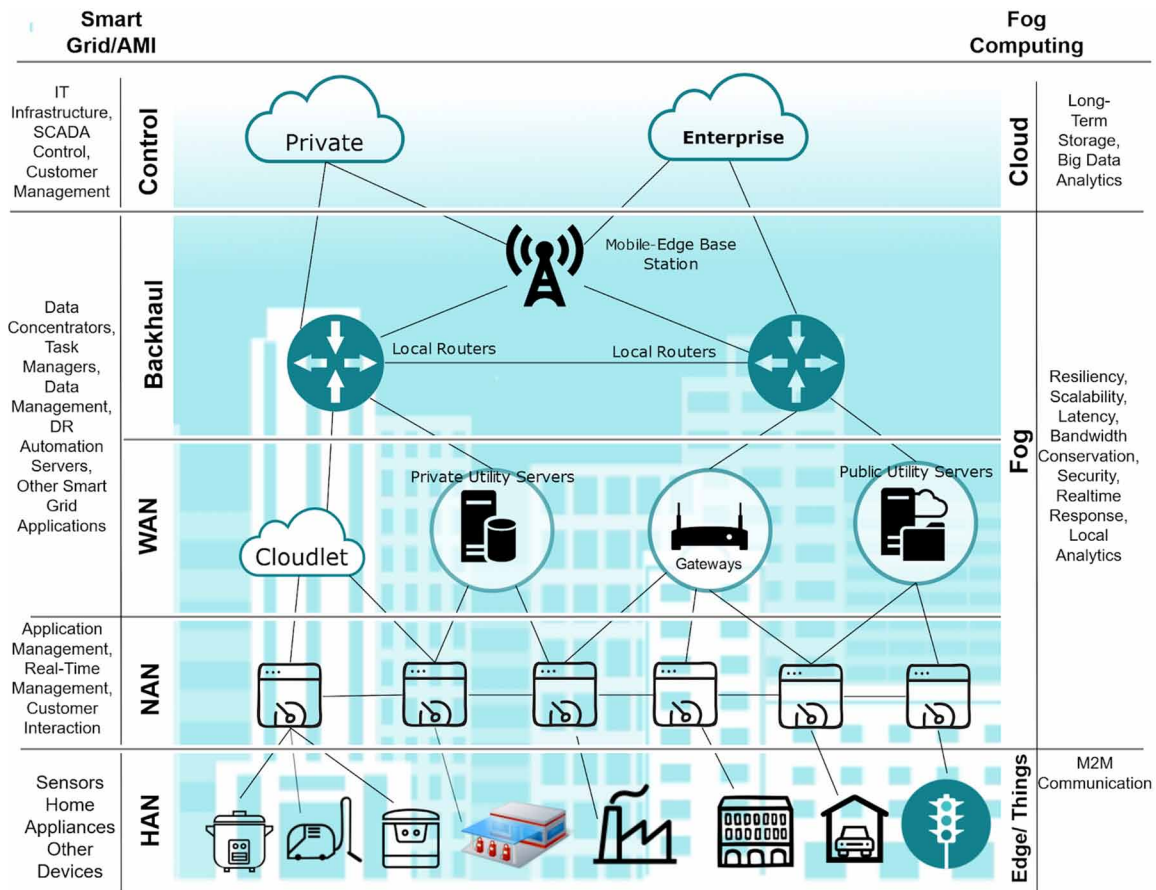
Edge computing is targeted towards using the computational elements available in the network path, from the end user devices, all the way to the cloud. The OpenFog consortium provides a definition of fog computing as “a horizontal, system-level architecture that distributes computing, storage, control

and networking functions closer to the users along a cloud-to-thing continuum.” (OpenFog Consortium Architecture Working Group, 2017) Fog and Edge Computing offer a solution to towards low-latency applications for a myriad of use-cases, such as, augmented and virtual reality, smart cities and infrastructure, smart healthcare and vehicular networks (Mouradian, et al., 2018). Fog/edge computing can be adapted to various paradigms because of its inherent features. It is distributed; not only fog nodes reside along the network path towards the cloud but also east-west in a peer-to-peer fashion. Proximity; Fog/Edge nodes are physically closer to the end-user whether it is a smartphone user or a smart home or a smart city control system. To support proximity and hierarchy, it must be heterogeneous in terms of computational resources. When you have many compute nodes, distributed along the network and geographical pathways, you need autonomy in operations.

Utilizing such a diverse, distributed, hierarchical and autonomic architecture would offer many benefits to Smart Grids such as:

- **Decentralization:** In the context of Fog Computing, there are no central servers. This decentralization is unlike Cloud Computing, where a large pool of resources is concentrated within a data-center. This shift in the decentralization of computing resources aligns with the shift in distributed smart-grids. Instead of one or more large-scale energy producers, there are many, and the consumers themselves can now be producers. Similarly, in Fog Computing, the consumer’s routers can be computing devices as well. The decentralized nature of fog computing nodes is a perfect fit for the decentralized smart grid. Fog computing nodes can be spread around to offer on-demand computation to the distributed smart grid applications. We see the advanced smart meter as a point for bridging the gap between the grid and fog.
- **Scalability:** Increases in smart home deployments, on-premises renewable energy solutions, a vehicle to grid-enabled cars would create scalability challenges for SG/AMI applications. Fog computing has a north-south (things to the cloud), east-west (peer-to-peer) architecture that can help mitigate those challenges. The north-south/east-west architecture means that applications and services can either move to another node in the vicinity or move upwards in the fog towards the cloud. This allows the fog itself and the applications and services to scale all-along the deployed environment. And the most significant benefit is in terms of scalability.
- **Resiliency:** Scalability and decentralization result in the resiliency of deployments. An outage at a datacenter can take out all the applications and services running there; this is not the case with fog computing. In fact, small fog nodes can offer cached services to local users whenever there is a cloud outage. A similar example would be a distributed set of storage batteries offering energy to critical local services in case of a grid outage or balancing the voltage frequency.
- **Mobility:** Decentralization allows services to exist anywhere between the end-node/things, all the way on the network path towards the cloud. Fog computing architecture allows services to be mobile. Vehicle-based fog computing is an active research area. This is in-line with vehicle-2-grid (V2G) technologies (Kester, Noel, Rubens, & Sovacool, 2018). One element of V2G technologies is the communication with the grid provider or the automation services that act as middlemen between the consumer and the grid. Cars are already being bundled with V2G capability. Adding a fog node to the car would enhance its communication, security and identity verification in a highly dynamic environment.

Figure 13. IoT assisted edge-cloud computing for smart grids



Integrating edge/fog computing into the smart grid will lift the communication infrastructure demands from the smart grid community. Furthermore, it will support the grid on each level.

Privacy, Authentication and Confidentiality

The integration of IoT within the smart grid has exposed the system to new security challenges that could impact further developments and expansions (Bekara, 2014) (Mendel, 2017). These challenges can be categorized into three main groups depending on which aspect of security they impact: privacy, confidentiality, integrity, and authentication.

Privacy-based challenges involve mechanisms that can deduce the personal behavioral patterns of users from the collection of residential and device power usage data. Smart meters and appliances generate a large amount of real time data that can be used for this purpose. The fine-grained information can be used to determine personal activities of people within a resident – wake up times, sleeping times, whether they are inside or away from the house, etc., (Mármol, Sorge, Ugus, & Pérez, 2012). To preserve the privacy this information various approaches involving anonymity, encryption, and access control have been adopted (Elmaghraby & Losavio, 2014) (He, Kumar, & Lee, 2015). (Christian, Günther, Armin, &

Dominik, 2013) propose a framework for generating privacy-related requirements for smart grid applications. It is shown that the best results can be obtained by combining and integrating privacy-enhancing approaches. Future research should focus on figuring how to do so without increasing the complexity.

Confidentiality-based challenges arise from the fact that IoT devices embedded within smart grids often communicate via publicly available networks. When data is exchanged in the clear within this environment, unauthorized third parties can access this data. If this information is sensitive in nature e.g. real time power consumption, its disclosure can lead to adverse consequences (Anzalchi & Sarwat, 2015). To tackle these issues many solutions have been proposed and adopted from existing ICT systems (Busom, Petrlc, Seb , Sorge, & Valls, 2016) (Liu, Cheng, Gu, Jiang, & Li, 2016). These approaches typically include the use of various forms of lightweight encryption schemes such elliptic curve and homomorphic cryptography (Mahmood, et al., 2018). These approaches are preferred since they are not resource intensive. However, the efficient management of encryption/decryption keys for these schemes remains as an open research problem.

Integrity-based challenges allow attackers to intercept and modify data exchanged between nodes within the smart grid. An example of this can occur in demand response applications where an attacker can lower dynamic prices during peak hours by modifying the content of the data packets. This can lead to the opposite goal of increased consumption resulting in an overloaded power system. Other attacks involve the injection of false data within legitimate sensor and control messages (Giraldo, Cardenas, & Quijano, 2017). A lot of research is now focused on techniques to distinguish between legitimate and illegitimate data. Machine learning and other artificial technology techniques show a lot of promise in solving these problems (Ozay, Esnaola, Yarman Vural, Kulkarni, & Poor, 2016) (Esmalifalak, Liu, Nguyen, Zheng, & Han, 2017).

Challenges involving authentication result from the ability of one smart node impersonating another by spoofing its identity. For example, a smart meter being maliciously modified to spoof another in order to shift its consumption costs (Punmiya & Choe, 2019). There is need for implementing strong authentication schemes to prevent these problems. However, existing schemes tend to increase latency of communication and involve complex key management procedures. Thus, research is focused on designing mechanisms that are simple and lightweight. For example, (Sule, Katti, & Kavasseri, 2012) have proposed a mechanism that provides strong mutual authentication between smart meters in a smart grid. The mechanism relies on use of a simple MAC instead of the typical HMAC which is more resource intensive. Similar approaches should be considered to ensure efficiency in complex smart grid systems of the future.

CONCLUSION

The utility grid is experiencing a drastic transformation towards adopting two-way communications. Smart-grid is the new generation of the utility grid that is driven by arduous factors such as the need to reduce carbon dioxide, increase the grid efficiency, decrease the cost of operation and maintenance, etc. Information and communication technology, ICT, is the disruptive technology for the realization of the smart-grid functions. The miniaturization of electronic devices coupled with the progress in sensing technology, IoT has emerged as a technological innovation that has been coined to interconnect objects, machines, humans, and systems together using the Internet technology. This chapter has described the application of IoT technologies at the five domains of the smart grid: operations, customer, generation,

distribution, and transmission. IoT has enabled new forms of services and architectures such as advanced smart metering infrastructure, distributed intelligence, demand-response program, volt/var optimization, home energy management system, and substation automations. Those functions and services are enabled by key technologies such as multi-agent systems, fog/ cloud computing, middleware, and communication technologies. Notwithstanding, IoT has enabled the realization of the smart-grid, privacy and security remain one big challenge.

REFERENCES

- Alharby, S., Weddell, A., Reeve, J., & Harris, N. (2018). The Cost of Link Layer Security in IoT Embedded Devices. *IFAC-PapersOnLine*, 51(6), 72–77. doi:10.1016/j.ifacol.2018.07.132
- Ancillotti, E., Bruno, R., & Conti, M. (2013). The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*, 36(17-18), 1665–1697. doi:10.1016/j.comcom.2013.09.004
- Anzalchi, A., & Sarwat, A. (2015). *A survey on security assessment of metering infrastructure in Smart Grid systems*. IEEE. doi:10.1109/SECON.2015.7132989
- Anzar, M., Nadeem, J., & Sohail, R. (2015). A review of wireless communications for smart grid. *Renewable & Sustainable Energy Reviews*, 41, 248–260. doi:10.1016/j.rser.2014.08.036
- Bekara, C. (2014). *Security Issues and Challenges for the IoT-based Smart Grid*. IEEE. doi:10.1016/j.procs.2014.07.064
- Ben Dhaou, I., Kondoro, A., Kelati, A., Rwegasira, D. S., Naiman, S., Mvungi, N. H., & Tenhunen, H. (2017, July). Communication and Security Technologies for Smart Grid. *International Journal of Embedded and Real-Time Communication Systems*, 8(2), 40–65. doi:10.4018/IJERTCS.2017070103
- Ben Meskina, S., Doggaz, N., Khalgui, M., & Li, Z. (2017). Multiagent Framework for Smart Grids Recovery. *IEEE Transactions on Systems, Man, and Cybernetics. Systems*, 47(7), 1284–1300. doi:10.1109/TSMC.2016.2573824
- Busom, N., Petrlc, R., Seb , F., Sorge, C., & Valls, M. (2016). Efficient smart metering based on homomorphic encryption. *Computer Communications*, 82, 95–101. doi:10.1016/j.comcom.2015.08.016
- Cintuglu, M. H., & Mohammed, O. A. (2015). Multiagent-based decentralized operation of microgrids considering data interoperability. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, (pp. 404-409). Miami, FL: IEEE. 10.1109/SmartGridComm.2015.7436334
- Cintuglu, M. H., Youssef, T., & Mohammed, O. A. (2018). Development and Application of a Real-Time Testbed for Multiagent System Interoperability: A Case Study on Hierarchical Microgrid Control. *IEEE Transactions on Smart Grid*, 9(3), 1759–1768. doi:10.1109/TSG.2016.2599265
- Dagdeviren, O., Korkmaz, I., Tekbacak, F., & Erciyes, K. (2011). A Survey of Agent Technologies for Wireless Sensor Networks. *IETE Technical Review*, 28(2), 168–184. doi:10.4103/0256-4602.72509

- Dutt, N., Jantsch, A., & Sarma, S. (2016). Toward Smart Embedded Systems: A Self-aware System-on-Chip (SoC) Perspective. *ACM Transactions on Embedded Computing Systems*, 22-22:27.
- Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497. doi:10.1016/j.jare.2014.02.006 PMID:25685517
- Elmangoush, A., Steinke, R., Al-Hezmi, A., & Magedanz, T. (Feb 2014). On the usage of standardised M2M platforms for Smart Energy management. *The International Conference on Information Networking 2014 (ICOIN2014)*, 79-84. 10.1109/ICOIN.2014.6799669
- Energy Independence and Security Act of 2007. (2007). Retrieved from <https://www.gpo.gov>
- Erol-Kantarci, M., & Mouftah, H. T. (2015). Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues. *IEEE Communications Surveys and Tutorials*, 17(1), 179–197. doi:10.1109/COMST.2014.2341600
- Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., & Han, Z. (2017). Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid. *IEEE Systems Journal*, 11(3), 1644–1652. doi:10.1109/JSYST.2014.2341597
- Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart Grid- The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, 14, 944-980. doi:10.1109/SURV.2011.101911.00087
- Farhangi, H. (2010). The path of the smart grid. *IEEE Power & Energy Magazine*, 8(1), 18–28. doi:10.1109/MPE.2009.934876
- Giraldo, J., Cardenas, A., & Quijano, N. (2017). Integrity Attacks on Real-Time Pricing in Smart Grids: Impact and Countermeasures. *IEEE Transactions on Smart Grid*, 8(5), 2249–2257. doi:10.1109/TSG.2016.2521339
- Glesner, M., & Philipp, F. (2013). Embedded Systems Design for Smart System Integration. *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 32-33. 10.1109/ISVLSI.2013.6654611
- Gungor, V. C., Sahin, D., Kocak, T., & Ergut, S. (2011). Smart grid technologies: communication technologies and standards. *IEEE transactions*.
- Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013, February). A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Transactions on Industrial Informatics*, 9(1), 28–42. doi:10.1109/TII.2012.2218253
- He, D., Kumar, N., & Lee, J.-H. (2015). Privacy-preserving data aggregation scheme against internal attackers in smart grids. *Wireless Networks*, 22. doi:10.1007/11276-015-0983-3
- IEEE Std 2030-2011. (2011). *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*. Retrieved from <http://ieeexplore.ieee.org/stampPDF/getPDF.jsp?arnumber=6018239>
- IETF. (2010). *Internet Key Exchange Protocol Version 2 (IKEv2)*. Retrieved from <https://tools.ietf.org/html/rfc5996>

- IETF. (2012). *Datagram Transport Layer Security Version 1.2*. Retrieved from <https://tools.ietf.org/html/rfc6347>
- Kabalci, Y. (2016). A survey on smart metering and smart grid communication. *Renewable & Sustainable Energy Reviews*, 57, 302–318. doi:10.1016/j.rser.2015.12.114
- Kahrobaee, S., Rajabzadeh, R., Soh, L.-K., & Asgarpour, S. (2013). A Multiagent Modeling and Investigation of Smart Homes With Power Generation, Storage, and Trading Features. *IEEE Transactions on Smart Grid*, 4(2), 659–668. doi:10.1109/TSG.2012.2215349
- Khan, A. A., Rehmani, M. H., & Reisslein, M. (2016). Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols. *IEEE Communications Surveys Tutorials*, 18, 860–898. doi:10.1109/COMST.2015.2481722
- Khan, R. H., & Khan, J. Y. (2013). A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network. *Computer Networks*, 57(3), 825–845. doi:10.1016/j.comnet.2012.11.002
- Korzun, D. G., & Gurtov, I. N. (2015). Service Intelligence and Communication Security for Ambient Assisted Living. *International Journal of Embedded and Real-Time Communication Systems*, 6(1), 76–100. doi:10.4018/IJERTCS.2015010104
- Li, Z., Wang, Z., Tournier, J.-C., Peterson, W., Li, W., & Wang, Y. (2010). A Unified Solution for Advanced Metering Infrastructure Integration with a Distribution Management System. In *First IEEE International Conference on Smart Grid Communications* (ss. 566–571). Gaithersburg, VA: IEEE. 10.1109/SMARTGRID.2010.5621998
- Liang, H., Choi, B. J., Zhuang, W., Shen, X., Awad, A. S., & Abdr, A. (2012). Multiagent coordination in microgrids via wireless networks. *IEEE Wireless Communications*, 19(3), 14–22. doi:10.1109/MWC.2012.6231155
- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017, October). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 4(5), 1125–1142. doi:10.1109/JIOT.2017.2683200
- Liu, Y., Cheng, C., Gu, T., Jiang, T., & Li, X. (2016). A Lightweight Authenticated Communication Scheme for Smart Grid. *IEEE Sensors Journal*, 16. doi:10.1109/jsen.2015.2489258
- Ma, R., Chen, H.-H., Huang, Y.-R., & Meng, W. (2013). Smart Grid Communication: Its Challenges and Opportunities. *IEEE Transactions on Smart Grid*, 4(1), 36–46. doi:10.1109/TSG.2012.2225851
- Mahmood, K., Chaudhry, S. A., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. K. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81, 557–565. doi:10.1016/j.future.2017.05.002
- Mármol, F., Sorge, C., Ugus, O., & Pérez, G. (2012). Do not snoop my habits: Preserving privacy in the smart grid. *IEEE Communications Magazine*, 50(5), 166–172. doi:10.1109/MCOM.2012.6194398
- Mendel, J. (2017). Smart Grid Cyber Security Challenges: Overview and Classification. *e-mentor*, 2017. doi:10.15219/em68.1282

- Nafi, N. S., Ahmed, K., Gregory, M. A., & Datta, M. (2016, October). A Survey of Smart Grid Architectures, Applications, Benefits and Standardization. *Journal of Network and Computer Applications*, 76, 1–21. doi:10.1016/j.jnca.2016.10.003
- National Institute of Standards and Technology. (2014). *NIST Framework and Roadmap for Smart Grid Interoperability Standards (Release 3.0)*. US Department of Commerce.
- Ozay, M., Esnaola, I., Yarman Vural, F. T., Kulkarni, S. R., & Poor, H. V. (2016). Machine Learning Methods for Attack Detection in the Smart Grid. *IEEE Transactions on Neural Networks and Learning Systems*, 27(8), 1773–1786. doi:10.1109/TNNLS.2015.2404803 PMID:25807571
- Punmiya, R., & Choe, S. (2019). Energy Theft Detection Using Gradient Boosting Theft Detector With Feature Engineering-Based Preprocessing. *IEEE Transactions on Smart Grid*, 10(2), 2326–2329. doi:10.1109/TSG.2019.2892595
- Rasheed, M. B., Javaid, N., Hussain, S. M., Akbar, M., & Khan, Z. A. (2017). Multiagent Control System for Residential Energy Management under Real Time Pricing Environment. In *IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, (pp. 120-125). Taipei: IEEE.
- Rwegasira, D. S., Ben Dhaou, I. S., Kondoro, A., Anagnostou, A., Kelati, A., Naiman, S., ... Tenhunen, H. (2019). A Demand-Response Scheme Using Multi-Agent System for Smart DC Microgrid. *International Journal of Embedded and Real-Time Communication Systems*, 10(1), 48–68. doi:10.4018/IJERTCS.2019010103
- Sekhvatmanesh, H., & Cherkaoui, R. (2019). Distribution Network Restoration in a Multiagent Framework Using a Convex OPF Model. *IEEE Transactions on Smart Grid*, 10(3), 2618–2628. doi:10.1109/TSG.2018.2805922
- Sendin, A., Sanchez-Fornie, M. A., Berganza, I., Simon, J., & Urrutia, I. (2016). *Telecommunication Networks for the Smart Grid*. Norwood, MA: Artech House.
- Shawon, M. H., Muyeen, S. M., Ghosh, A., Islam, S. M., & Baptista, M. S. (2019). Multi-Agent Systems in ICT Enabled Smart Grid: A Status Update on Technology Framework and Applications. *IEEE Access: Practical Innovations, Open Solutions*, 7, 97959–97973. doi:10.1109/ACCESS.2019.2929577
- Sule, R., Katti, R. S., & Kavasseri, R. G. (2012). *A variable length fast Message Authentication Code for secure communication in smart grids*. IEEE. doi:10.1109/PESGM.2012.6345622
- Wan, L., Zhang, Z., & Wang, J. (2019). Demonstrability of Narrowband Internet of Things technology in advanced metering infrastructure. *EURASIP Journal on Wireless Communications and Networking*, (1): 1–12.
- Wan, L., Zhang, Z., & Wang, J. (2019, January). Demonstrability of Narrowband Internet of Things technology in advanced metering infrastructure. *EURASIP Journal on Wireless Communications and Networking*, 2019(1), 2–12. doi:10.1186/13638-018-1323-y
- Wickelgren, I. J. (1996, September). Local-area networks go wireless. *IEEE Spectrum*, 33(9), 34–40. doi:10.1109/6.535256
- Wooldridge, M. (2009). *An Introduction to MultiAgent Systems* (2nd ed.). West Sussex, UK: Wiley.

- Wu, Q., Feng, J., Tang, W., & Fitch, J. (2005). Multi-agent Based Substation Automation Systems. In *IEEE Power Engineering Society General Meeting*, (pp. 1048-1049). San Francisco, CA: IEEE.
- Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials*, 14, 998-1010.
- Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys and Tutorials*, 15(1), 5–20. doi:10.1109/SURV.2012.021312.00034
- Yu, R., Zhang, Y., Gjessing, S., Yuen, C., Xie, S., & Guizani, M. (2011, September). Cognitive radio based hierarchical communications infrastructure for smart grid. *IEEE Network*, 25(5), 6–14. doi:10.1109/MNET.2011.6033030
- Zhabelova, G., & Vyatkin, V. (2012). Multiagent Smart Grid Automation Architecture Based on IEC 61850/61499 Intelligent Logical Nodes. *IEEE Transactions on Industrial Electronics*, 59(5), 2351–2362. doi:10.1109/TIE.2011.2167891