Table of Contents

International Journal of Embedded and Real-Time Communication Systems

Volume 8 • Issue 2 • July-December-2017 • ISSN: 1947-3176 • eISSN: 1947-3184

An official publication of the Information Resources Management Association

Research Articles

COPYRIGHT

The *International Journal of Embedded and Real-Time Communication Systems* is indexed or listed in the following: ACM Digital Library; Bacon's Media Directory; Cabell's Directories; DBLP; Google Scholar; INSPEC; JournalTOCs; Library & Information Science Abstracts (LISA); MediaFinder; SCOPUS; The Standard Periodical Directory; Ulrich's Periodicals Directory

International Journal of Embedded and Real-Time Communication Systems
Volume 8 • Issue 2 • July-December 2017

Communication and Security Technologies for Smart Grid

Imed Ben Dhaou, Qassim University, Buraidah, Saudi Arabia & University of Monastir, Monastir, Tunisia

Aron Kondoro, Royal Institute of Technology, Stockholm, Sweden & University of Dar es Salaam, Dar es Salaam, Tanzania

Amleset Kelati, Royal Institute of Technology, Stockholm, Sweden & University of Turku, Turku, Finland

Diana Severine Rwegasira, Royal Institute of Technology, Stockholm, Sweden &University of Turku, Turku, Finland.

Shililiandumi Naiman, University of Dar es Salaam, Dar es Salaam, Tanzania

Nerey H. Mvungi, University of Dar es Salaam, Dar es Salaam, Tanzania

Hannu Tenhunen, Royal Institute of Technology, Stockholm, Sweden & University of Turku, Turku, Finland

ABSTRACT

The smart grid is a new paradigm that aims to modernize the legacy power grid. It is based on the integration of ICT technologies, embedded system, sensors, renewable energy and advanced algorithms for management and optimization. The smart grid is a system of systems in which communication technology plays a vital role. Safe operations of the smart grid need a careful design of the communication protocols, cryptographic schemes, and computing technology. In this article, the authors describe current communication technologies, recently proposed algorithms, protocols, and architectures for securing smart grid communication network. They analyzed in a unifying approach the three principles pillars of smart-gird: Sensors, communication technologies, and security. Finally, the authors elaborate open issues in the smart-grid communication network

KEYWORDS

Cyber Security, Information and Communication Technology, SCADA Systems, Sensors, Smart Grid

1. 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.

DOI: 10.4018/IJERTCS.2017070103

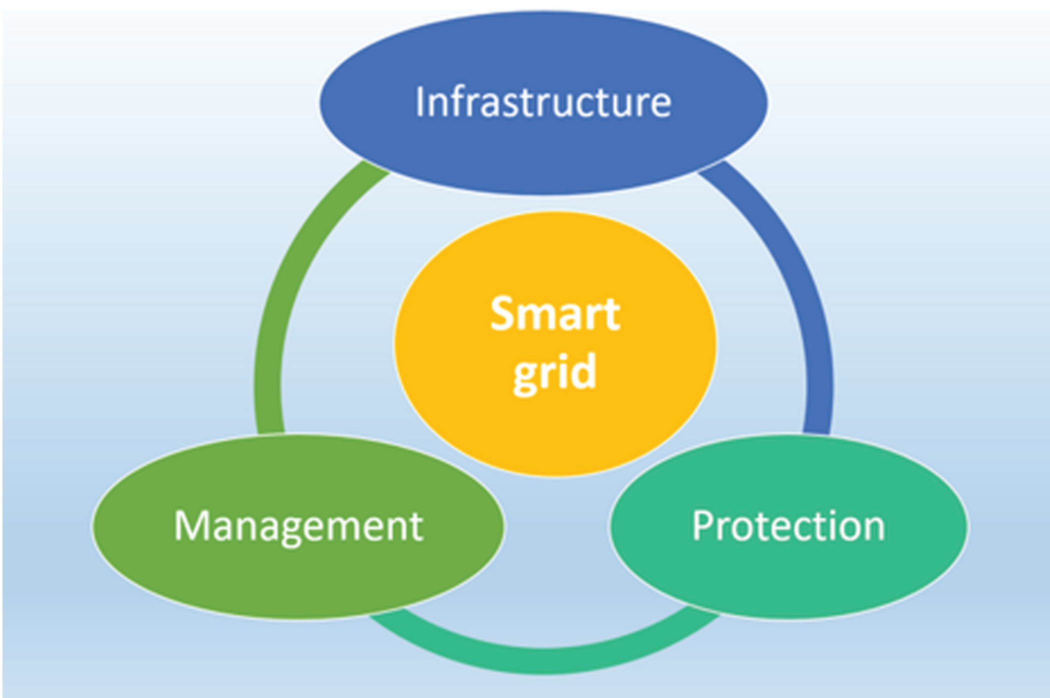
As explained (Korzun & Gurtov, 2015) in (Dutt, Jantsch, & Sarma, 2016) and in (Glesner & Philipp, 2013), smart system should take intelligent decision, has a mechanism for situation awarness, elastic, proactive, etc. The enabling technologies for smart system are determined by the intended functionality. As stated in (Glesner & Philipp, 2013), control and cybersecurity are the cornerstones for smart grid. The recent trend in the process automation is the deployment of sensors for data collection, actuators for control and multi-agent system for solving complex problem.

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.

Communications 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 the confidentiality of the consumers, to protect the data against eavesdropping and to prevent embedded systems, used along the smart grid, from running malicious software. The authors of (Yan, Qian, Sharif, & Tipper, 2012)

Figure 1. Smart grid ingredients proposed in (Fang, Misra, Xue, & Yang, 2012)



wrapped up the cyber security demands and surveyed the solutions for cyber security elaborated prior to the publication date of their report.

To increase the reliability of the grid and to integrate advanced control and monitoring operations, smart grid will include a variety of smart interconnected sensors. Smart grid sensors render the implementation of a multitude of applications such as situation awareness, fast healing, advanced demand-response schemes, and the monitoring of electrical equipment (voltage transformers, circuit breakers, power cables, arrestors, etc.)

This paper describes state of the art published techniques, schemes, and algorithms in communication technology, cyber-security and wireless sensor networks for the smart grid. It highlights the important latest trends in these aspects of smart grid technologies. Many previous surveys have been done individually on the communication technologies, security and wireless sensor networks enabling the smart grid. However, to the best of our knowledge, there are no surveys that considered these aspects together, and analyzed how they relate to each other. The main contributions of this paper are to provide a holistic overview of communication, security and sensor networks technologies powering the smart grid, highlight recent developments in each aspect and how they affect each other. In addition, the paper also describes recent developments that have occurred since previous surveys were done. The paper is organized as follows: Section 2 summarizes the latest communication protocols and architectures proposed for wide-area network (WAN), neighboring area network (NAN), and home area network (HAN). Section 3 discusses contemporary cryptographic algorithms and protocols for smart grid (key-management, tamper resistance devices, network, and system). Section 4 sums up the latest research results in the design of wireless sensor networks for the smart grid. Finally, section 5 summarizes and provides open issues in the covered areas.

2. COMMUNICATION TECHNOLOGIES

Data communication is a key enabler for the smart grid. Various factors determine the communication technology. These factors include environment, coverage area, data-rate, security, and latency.

2.1. Network Classifications

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, 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 design of a suitable communication architecture. For instance, home appliances are placed close to each other, which make 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 is a potential winner as a standard for home energy system, however, recently 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 the authors of (Erol-Kantarci & Mouftah, 2015) added field area networks (FAN) and argued that the topology of FAN is similar to NAN.

Table 1. Preferred communication for HAN, NAN and WAN

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

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 select further the communication architecture based on the QoS requirements, cost, and the environments. For instance, 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 five 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-layer communication network architecture. The core network covers the generation and transmission domains, the wide area network covers the distribution network, and the private network that operates in the customer domain.

(Ma R., 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 the 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 as 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.

2.2. Communication Technologies for NAN and WAN

The wide area network in smart grid is used to ensure data communication between HANs and the utility company. It can also be used to connect the substations to the control center. Both WAN and NAN can be implemented using similar technologies. Figure 2 shows typical applications engendered by WAN (Gobena, Durai, Birkner, Pothamsetty, & Varakantam, 2011).

Table 2 summarizes the latency and bandwidth requirements for smart grid services reported by (Gobena, Durai, Birkner, Pothamsetty, & Varakantam, 2011). The WAN for a smart grid can be private or commercial, the former is solely owned by the utility company. The table shows further the preferred type of communication (private or commercial) for each service (Martin & Schmidt, 2014).

The comparison between private and public WAN for smart grid favors the former, furthermore (Martin & Schmidt, 2014) suggests a few directions to address the shortcomings of private networks. However, a sparkling choice in WAN is to use virtual private networks.

In the sequel, we will describe communication technologies and protocols for WAN proposed from 2014 onwards.

Using PLC as communication technologies in AMI, (Sanz, Pinero, Idiago, Esteban, & Garcia, 2014) argued that the deployment of a data concentrator in every transformer substation in case the subnetwork contains a low number of meters is an inefficient solution. They devised a new PLC AMI configuration using a higher frequency and reported real-life evaluation of the PLC. The results showed that the attenuation is inversely proportional to the PLC frequency.

Figure 2. Domains of WAN in smart grid

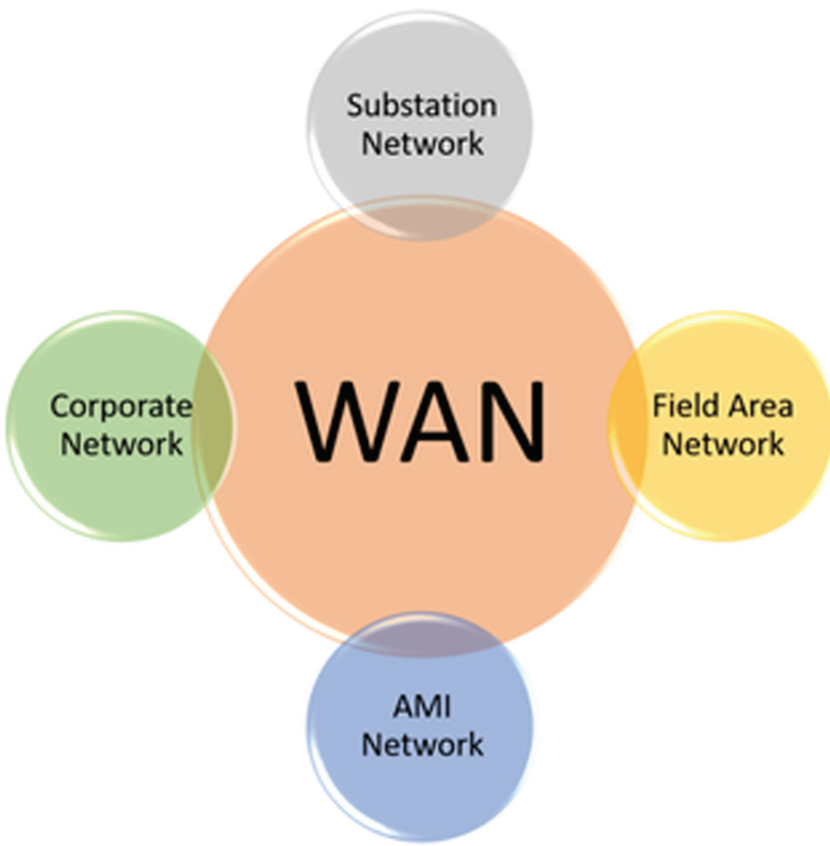


Table 2. QoS for typical WAN applications

Substation				
Service	**Latency**	**Bandwidth**	**main drivers**	**Preferred network**
Synchrophasor	25-100 ms	2-5 Mbps	PMUs	private
Physical security	2 sec	4Mbps	Surveillance cameras	private
SCADA	2-4 sec	10-30 Kbps	number of points	private
AMI				
Connects and disconnects	5 sec	500 Kbps	Grid status	private
Meter Readings	variable	10 Kbps / meter	number of meters	private
Distribution				
FLIR	2-4 sec	10-30 Kbps	circuit complexity	private
Volt/ var optimization	25-100 ms	2-5 Mbps	feeders	private
Asset management	2 sec	5 Mbps	number of assets	private
Workforce access	150 ms	250 Kbps	cameras	commercial
Corporate				
Business Video	250 ms	10-150 Mbps	cameras	commercial
IP Telephony	150 ms	1-5 Mbps	employees	commercial
Wireless	1 sec	variable	employees	commercial
IP Radio	200 ms	250 Kbps	field employees	commercial

Green communication using cellular networks is an attractive research area that aims to guarantee QoS requirements at the lowest possible energy consumption. The reader who is interested in the application of green communication and data centers for the smart grid is advised to read (Erol-Kantarci & Mouftah, 2015). There are hardware and software solutions that can be used at the base-station to reduce the energy consumption per call. Some of these techniques are using a low-power amplifier, sleep-mode techniques, adaptive coverage area, multi-hop relaying, the integration of renewable energy resources, and so forth.

To address the issues raised due to the growing concern of base-station power consumption and the increasing number of cellular subscribers (dual-sim smartphones, tablets, wireless internet, and so forth), (Lee & Choi, 2014) formulated a mixed integer nonlinear programming problem that seeks to reduce the energy consumption for multi-hop cellular networks. The solution accounts for the spectrum, energy storage, routing, and link scheduling.

Software defined network, SDN, is a new communication paradigm that is based on the publisher-subscribe concept (Nunes, Mendonca, Nguyen, Obraczka, & Turletti, 2014). To address the complexity of network managements in the smart grid, (Kim, He, Thottan, & Deshpande, 2014) elaborated an SDN architecture for the utility network. The architecture supports self-configuration, scalability, and security. The SDN is based on a ramification of the IEEE 802.1Q standard and has been demonstrated using Openflow.

(Saputro, Akkaya, & Guvenc, 2015) argued that communication at the various smart grid segments (HAN, NAN, WAN) has been well studied and investigated. Their work has focused on resolving the inter-networking issues between WAN and HAN. They proposed a hybrid communication architecture that uses LTE to build a wide area network and IEEE 802.11s mesh network to construct a NAN. To ensure privacy and direct access to a smart meter, the researchers suggested a layer for network address translation. The layer was designed for the gateway with the task to ensure end-to-end communication protocol, seamless communication, and to preserve privacy.

To address the problem of unconnected smart meters, (Sha, Alatrash, & Wang, 2016) used an overlay architecture that consists of a WiMAX network to build FAN and a commercial fiber-optic to connect the smart meters to the data center.

The smart city is a new vision for future cities that is based on the heavy integration of ICT in every corner that affects citizens in their daily life (transportation, education, electricity, environment, health care, shopping, communication, public services, and the like). The Internet of Things, IoT, is the vehicle for the development of the smart city and the creation of pervasive applications (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014). Starting from the big picture of the smart city, (Filho, Filho, & Moreli, 2016) assert that smart grid should be approached from the smart city standpoint to create a convergent communication platform. The authors further compared two popular open IoT standards for the smart city: RF mesh and LoRaWAN. Both standards are capable of building private and public networks. The authors concluded that LoRaWAN is the technology of choice for building three smart grid networks (HAN, NAN, and WAN) as the standard supports three classes of devices. Table 3 summarizes the smart grid applications that can be engendered by each class of devices. However, for advanced distribution automation, the authors discounted LoRaWAN and suggested to use other alternative communication technologies like WiMAX and LTE.

2.3. Network Technologies for HAN

The Home Area Network, HAN, is a categorization of all communication technologies that enable smart grid applications in the customer domain part of the power grid. It is characterized by technologies that facilitate the communication between components such as smart meters, smart appliances, and energy management systems, EMS. This allows the realization of applications such as home automation, demand response, the integration of local renewable resources, the reduction of energy costs and the reduction of individual carbon footprints.

Due to the nature of components existing in the customer domain of the power grid, the communication requirements and characteristics of HANs are unique. The communication technologies used have a relatively shorter range compared to the ones used in NAN and WAN. This is due to the close proximity of components found in this domain. These components are also resource constrained. They exist in devices that are typically low-powered with minimal storage and computational abilities. As such, communication protocols that have been employed tend to be lightweight in terms of power usage and processing capabilities.

In addition to considering all communication technologies in the customer domain as one homogeneous network, previous studies have further divided the technologies into three more categories (Kuzlu, Pipattanasomporn, & Rahman, 2014). In addition to the Smart Home Area Network (SHAN), there are also Building Area Networks (BANs) and Industrial Area Networks (IANs). These correspond to the different types of customer premises in which they are implemented. This can be either an individual home, a residential building area or an Industrial setting. The characteristics and features of the communication technologies in these categories differ from each other, due to the different application requirements that exist. Recent studies have highlighted this distinction more by focusing on the unique challenges of each of the sub-categories

Table 3. Application of LoRaWAN in smart grid

Class	Services
A	street light, AMI, assets management
B	AMI, substation automation
C	SCADA

2.3.1. SHAN

The main goal of the communication technologies in this area, in the context of the smart grid, is to facilitate the concept of smart homes (Zhou, et al., 2016). This refers to the automation of the different energy components inside a home, in order to manage and control energy use. This includes smart appliances and smart meters that are able to communicate together and coordinate their functions using a communication infrastructure. This is also facilitated by smart home management systems (SHEMs) that integrate all components together, and provide an interface for customers, for monitoring and control purposes (Nanda & Panigrahi, 2016).

Due to the proliferation of the concept of the Internet of Things (IoT), the communication architecture and infrastructure in this category has been dominated by these technologies. Authors in (Stojkoska & Trivodaliev, 2017) describe a novel communication architecture for smart homes based IoT. This architecture is articulated around the cloud technology that connects smart IoT-based appliances, management systems, and third-party analysis tools. These appliances collect and send information directly to the cloud. They also receive commands directly through the communication platform provided by the cloud. In addition, the cloud also provides data storage and processing facilities. Private companies have also recently introduced their own unique communication technologies for their products in this area (Feiler, 2016). As a consequence of this communication architecture, one of the main challenges has been the explosion of data, as more and more devices collect and send energy-related data (Song, Zhou, & Zhu, 2013). Various research efforts have gone into techniques to manage this situation (Diamantoulakis, Kapinas, & Karagiannidis, 2015). However, this remains as an open issue with the need for more innovative solutions (Hu & Vasilakos, 2016).

2.3.2. BAN

Building Area Networks, consist of communication technologies that facilitate the newly emerging concept of smart buildings, and in a broader way smart city. Smart buildings are modern versions of residential buildings with automated energy management systems. Important functions that are supported include demand response, outage management, remote metering and the integration of distributed renewable energy resources. The communication technologies are focused on efficiently supporting these functions.

There are previous studies (Kuzlu, Pipattanasomporn, & Rahman, 2016) that have also looked into and reviewed BAN communication technologies for smart buildings. (Ndjiongue, Ferreira, & Shongwe, 2016) proposed a new communication protocol in the physical layer that combines power line communications (PLC) and visible light communications (VLC). The new technique was able to achieve a much higher throughput for reliable communication especially in inter-building use cases.

(Zhang & Baillieul, 2016) proposed a new communication protocol based on packeted load control messages for smart buildings. The authors developed two new communication protocols based on two scenarios: when there is complete information from sensors in the environment, and in constrained environments where binary information is carried.

(Nguyen, Nguyen, Cuong, & Nguyen, 2016) designed a new wireless-based network for a smart building that transmitted data in the 868 MHz frequency range. The network utilizes a hierarchical architecture with coordinators on each floor of the building, collecting data, and forwarding it upwards through a gateway to a remote server. The gateway and the remote server are linked through the 3G network. This architecture, with the low frequency of transmission, was able to implement a reliable smart building network with low cost and low power consumption.

2.3.3. IAN

In the industrial setting, one of the main concerns is the use of heavy equipment that consumes a lot of power, usually a big portion of that generated in the grid. Therefore, important applications in the context of the grid include demand response (Taqqali & Abdulaziz, 2010), load control (Koutsopoulos

& Tassiulas, 2011) and load scheduling (Ma J., Chen, Song, & Li, 2016). The Industrial Area Network (IAN) is a collection of communication technologies, architecture, and algorithms that support these functions.

(Ding & Hong, 2013) proposed a generic demand response model for industrial facilities that can easily help a facility shave off power consumption during peak demand without adversely affecting operations. The model's communication infrastructure is divided into two main parts: the utility side and the Industrial demand side. The utility gateway/meter acts as the bridge between these two main parts, passing messages and commands back and forth. One unique feature of this model is the inclusion of an energy management agent (EMA) which is a conceptual entity that represents a specific industrial task. This includes a monitoring component that measures consumption and control functions for that specific task.

(Wang, Wang, Sun, Guo, & Wu, 2016) proposed a new energy efficient communication system based on IoT technology. The authors also proposed two new novel communication protocols; sleep and wake up scheduling protocols that automatically schedule sleep and wake cycles of communicating nodes, and thus lower energy consumption.

On the other hand, (Wei, Hong, & Alam, 2016) introduced a new communication strategy based on IoT that improves the connectivity of energy-related nodes in industrial facilities. Based on the TCP/IP network model, the authors selected appropriate open lightweight protocols in each layer to facilitate efficient communication. This helps standardization efforts and promotes interoperability. The strategy is also demonstrated to reduce peak energy use in a simulated industrial environment.

2.4. Emerging Technologies for Distributed Intelligence: Peer-to-Peer Computing, IP/MPLS, and Fog Computing

To manage and control the operations of the various assets and equipment within the smart-grid, several techniques from the industrial control system, ICS, have been promoted to create an autonomous and self-healing smart-grid. Distributed intelligence, DI, is a paradigm shift in ICS that enables the integration of large-scale systems (Mahalik, 2003).

Recently, several authors showed the effectiveness of DI in to achieve the objectives of smart-grid. The essential components to create DI are smart nodes and communication technologies. The smart node should have the ability to make a local decision and to cooperate with similar nodes to achieve a global objective. A multi-agent system is one supporting technologies for creating distributed intelligence.

Distributed intelligence in the smart grid has gained momentum (Mues, Alvarez, Espinoza, & Garbajosa, 2011) (Werbos, 2011) as it has enabled a multitude of applications such as feeder automation (Baker & Meisinger, 2011), volt-var control (Ibrahim & Salama, 2015), fault localization and isolation (Ghorbani, Choudhry, & Feliachi, 2013), the interoperability in microgrid (Vukojevic, Laval, & Handley, 2015), seamless integration of smart meter (Vyatkin, Zhabelova, Yang, McComas, & Chouinard, 2012), distributed protection (Yang, Zhabelova, Vyatkin, Nair, & Apostolov, 2012), and control of wind energy conversion system (Moness & Moustafa, 2016).

A couple of communication technologies support the distributed intelligence in the energy sector. On top of that, peer-to-peer computing has been widely accepted both in industry and in academia. (Campos, Matos, Pereira, & Rua, 2014) devised a service-oriented architecture to solve device heterogeneity and interoperability while guaranteeing both reliability and scalability. The peer-to-peer communication is based on the gossip protocol. Web technology has been adopted for the communication between constrained devices and mainframes. In industry, a number of proprietaries and open standard peer-to-peer communication platforms have been proposed. The commercial system of (S&C electric company, 2017) has been devised to build peer-to-peer communication for distributed intelligence in feeder automation. The system operates in ISM band, deploys 128-AES for data encryption, supports over the air configuration, uses frequency hopping spread spectrum technology with 4-GFSK modulation, etc. Other companies such as Siemens and ABB have constructed a peer-to-peer communication network for substation automation in compliance with the IEC 61850 standard (Siemens, 2017) (ABB, 2017).

IP/MPLS is a standard that was designed to, but not limited to, enable ATM and IP integration, prioritize traffic, accommodate different levels of QoS, and guarantee data security. In smart-grid, a proof of concept for teleprotection using secure IP/MPLS has been demonstrated (Blair et al., 2016).

As part of the efforts to reduce latency and delays in the transmission and processing of real-time data for critical smart grid applications, a new paradigm known as fog computing has emerged (Yi, Hao, Qin, & Li, 2015). This new architecture takes advantage of cloud computing technologies while bringing the computing processes closer to the edge of the network. This allows the scalability of large sensor networks without sacrificing response times of critical data exchanges. (Al Faruque & Vatanparvar, 2016) described a novel energy management system that relies on fog computing to provide a scalable solution for controlling energy production and consumption in a microgrid. An architecture that depends on low powered devices found in customer homes allows creating a system that can handle data from a large number of smart devices in a fast and efficient way. This is demonstrated by home and microgrid level energy management systems that were successfully implemented.

2.5. Discussions

Communication technology is an important aspect to the realization of smart grid and its assorted services. There are wide varieties of communication technologies that can be used at the various areas in the smart-grid architecture. These areas are identified as WAN and HAN. In each area, a number of private and commercial solutions exist. Each communication architecture has its drawbacks and advantages. For instance, public cellular communication technologies (WiMAX, LTE, and UMTS) are affordable for the utility company, however, the latency of these technologies, as well as the security, prohibit the adoption of these technologies in critical services like distributed intelligence and SCADA.

The challenges in designing secure and efficient HAN are significantly lower than for WAN. Privacy is one critical feature that the HAN should guarantee. The existing solutions for the realizations of HAN include ZigBee, WLAN, LoRaWAN, and 6LoWPAN.

3. SECURITY AND PRIVACY FOR SMART GRIDS

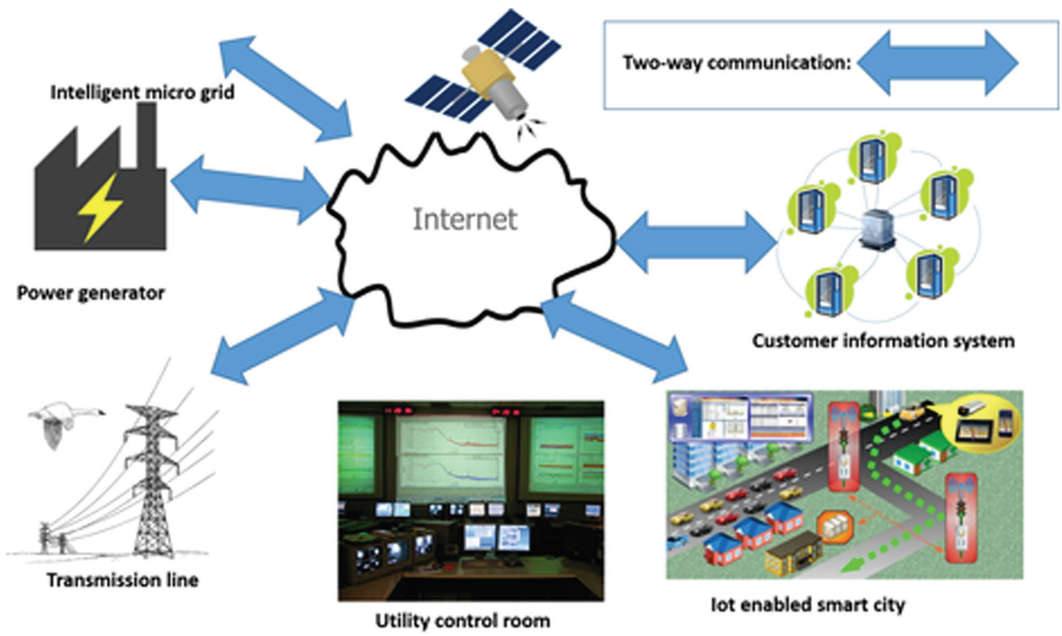
According to the National Institute of Standards and Technology, NIST, a smart grid is composed of four major segments: energy production and distribution, communication infrastructure, information technology, and industrial control system (NIST Special Publication 1108, 2014). Figure 3 depicts these four segments.

Security for the operations of the smart grid has been identified as a vital requirement by NIST. The three ICT pillars for the smart grid (communication, information technology, and industrial control system) should be protected against known security threats. Because of its widespread geographic area, the diversity of equipment, the proliferation of stakeholders and the wide-spectrum of operation environments, NIST has proposed an N-tier and overlay security architecture. The architecture covers the following areas: device, cryptography and key management, system, and network (The Smart Grid Interoperability Panel, 2010).

3.1. Key Management

(Kim, Kolesnikov, Kim, & Thottan, 2011) analyzed the communication requirements for the smart grid using an IP-based network and proposed a scalable, lightweight and secure transport protocol, SSTP. The protocol overcomes the weakness present in current transport layer protocols (stream control transmission protocol and transmission control protocol). The SSTP uses a symmetric-key algorithm for authentication and privacy. SSTP is designed for asymmetric security requirements in which the node keys are derived, at the server side, using a master key and a pseudo-random function

Figure 3. Smart-grid segments



generator. The Diffie-Hellman key exchange protocol is used to establish an SSTP connection between a utility server and a node.

Motivated by the lack of veracious, secure and scalable communication infrastructure for the smart grid, (Kim, Lee, Atkinson, Kim, & Thottan, 2012) proposed a secure data-centric application extensible, SeDax, platform. SeDax supports end-to-end security and uses RSA and AES cryptosystems for authentication and encryption. The X509 certificate is used to authenticate SeDax nodes. The topic-group authentication messages are encrypted using AES and its scheme is identical to SSTP.

(Dan, Lui, Tabassum, Zhu, & Nahrstedt, 2013) devised lightweight and scalable security protocols for the establishment of shared keys between measurement devices and power system operators via unsecure data-collectors.

Using the security requirements for smart meters (SMs) in advanced metering infrastructure reported in (Cleveland, 2008), (Liu, Chen, Zhu, Zhang, & He, 2013) proposed a key management scheme (KMS) suitable for resource constraint devices and accounts for three communication modes: unicast, multicast and broadcast. The authors used the key graph algorithm to build the KMS. Finally, yet importantly, the KMS is designed for both simple and complex AMI applications. However (Wan, Wang, Yang, & Shi, 2014) asserted that KMS described is unscalable and vulnerable to desynchronization attack. Afterwards, the authors devised a scalable key management scheme, SKM, using identity-based encryption (IBE) and key-tree architecture.

(Yu, Arifuzzaman, Wen, Zhang, & Sato, 2015) elaborated an AMI architecture using information centric networking (ICN-AMI). The architecture aims to reduce traffic congestion and to guarantee secure operation. Inspired from (Liu, Chen, Zhu, Zhang, & He, 2013), the authors further devised a KMS for the ICN-AMI.

3.2. Tamper Resistant Device

Electricity theft represents a major challenge to utility companies and has a profound effect on energy cost, utility revenue, and reliability of the grid. As pointed out by (Smith, 2004), a malicious consumer can steal electricity using a variety of ways such as meter tampering, unpaid bills, irregular payment and illegal electricity connection. The latter is a life-threatening practice. To address electricity theft and blackouts, the smart grid should integrate a secure hardware and software system.

To protect the smart meter gateway from ICT attacks (Detken, Genzel, Rudolph, & Jahnke, 2014), proposed a trusted core network architecture. The network uses a trusted platform module, a trusted neighborhood discovery protocol, and a trustworthy boot process. The driving forces behind the development of the security solution are the "chameleon" malware and the security standards elaborated by the German Federal Office for Information Security for the smart meter gateway.

3.3. Network and System

Advanced metering infrastructure (AMI) is an IoT architecture that connects consumer side smart-meters to the utility meter data management system. AMI is the corner stone for the realization of smart grid applications like dynamic pricing, demand-response scheme, load balancing, and so forth. The security of the AMI at the various levels (software, hardware, communication, and system) is critical for a trustworthy system. (Yan Y., Qian, Sharif, & Tipper, 2013) emphasized that the prevailing cryptographic schemes do not meet the security requirements for AMI networks. Subsequently, the authors elaborated an integrated authentication and confidentiality, IAC, protocol that has three processes: (1) authentication, (2) data confidentiality, and (3) control message confidentiality. (Fan, et al., 2014) identified the weakness of the IAC protocol and advocated a cryptographic protocol with auto-correcting capability that eliminates a suspicious meter. The protocol was designed for a wireless sensor network deployed to monitor the transmission line. The authors further used low-energy encryption and authentication schemes.

(Ye, Qian, & Hu, 2014) questioned the security strength of the IAC protocol and identified six security holes. Further, they elaborated an AMI protocol that addresses the shortcomings of the IAC protocol. However, the authors' scheme does not detect intrusion.

3.4. Discussions

Security in the smart grid is a complex and evolving issue. Security architecture, protocols, and primitives are shaped by multiples factors such as smart grid applications, communication protocols, geographic locations, and implementation constraints. Security and privacy of smart grid can benefit from developments in key areas such as wireless sensor network, trusted platform module, network, database, crypto analysis, IoT, cryptographic algorithms, data security, web-design, and cloud computing. Most existing security solutions aim to address the following issues: smart-meter authentication, security protocols for advanced metering infrastructure, secure demand-response scheme, homomorphic encryption, lightweight authentication protocols, a secure vehicle to grid communication, and interoperable security architecture.

4. WIRELESS SENSOR NETWORKS FOR THE SMART GRID

Sensors are the cornerstone for advanced smart grid applications like distributed generation, situation awareness, demand-response schemes, dynamic line rating, and energy management. The wireless sensor network has been deployed at the energy production units, the transmission and distribution side, business sector, customer premises, service provider, and operator. ZigBee and wirelessHART are two popular WSN technologies used in smart-grid (Liu, 2012).

(Mossé & Gadola, 2012) elaborated a WSN platform to control the conversion of wind energy according to the load. (Mabusela, Kruger, Silva, & Hancke, 2015) used a WSN to control solar thermal power plants. The control and real-time monitoring of PV park using WSN were the focus of (Moreno-Garcia, et al., 2015).

A practical and low-cost WSN using ZigBee technology has been proposed in (Vo, Nguyen, Nguyen, Le, & Huynh, 2013). The system comprises low cost smart power outlets that work both as sensors and as actuators. These outlets are connected to router nodes using a mesh network. A ZigBee coordinator is deployed to control and maintain the network. The energy management software is implemented on a mini-web server. Figure 4 depicts the low-cost WSN system for home energy management proposed in (Vo, Nguyen, Nguyen, Le, & Huynh, 2013). The results show that the system has a delay less than 300ms for a distance shorter than 40m. For higher distances, the delay increases drastically due to the increased packet error rate.

In the utility grid, the transmission line has some special electrical properties that determine its capacity, commonly known as *ampacity* (Farzaneh, Farokhi, & Chisholm, 2013). There exist two popular standards for the determination of the ampacity for the overhead conductors used for power transmission. These industrial standards are IEEE and CIGRE (Schmidt, 1999). To increase the efficiency of the grid and to maximize the energy flow, a dynamic line rating (DLR) process has been proposed as an alternative to static line rating (Yang, Lambert, & Divan, 2007). DLR depends on the electrical properties of the overhead conductor, ambient temperature, conductor heat, and geographic location. Currently, advanced utility companies deploy smart sensors to evaluate the ampacity of the transmission line. Figure 5 depicts a commercial sensor used to monitor a 35kV transmission line. The sensor is a Linux-powered embedded system that uses EM energy for energy harvesting. The sensor uses a GPS signal to append the measured data with the location and supports secure Bluetooth for short-range communication. For long-range communication, the mote has a multi-standards radio interface (LTE/4G, 3G, 2G, GPRS/GSM, CDMA fallback, L+G Gridstream, and Silver Spring Networks). The management of the sensors and data-analyses is done at the utility data center.

The study reported in (Fateh, Govindarasu, & Ajjarapu, 2013), showed that a WSN in combination with wireless and wired communication technology is a cost-efficient solution for the monitoring of a transmission line. The authors further described algorithms to optimally place the cellular network

Figure 4. ZigBee based home energy management system proposed by (Vo, Nguyen, Nguyen, Le, & Huynh, 2013)

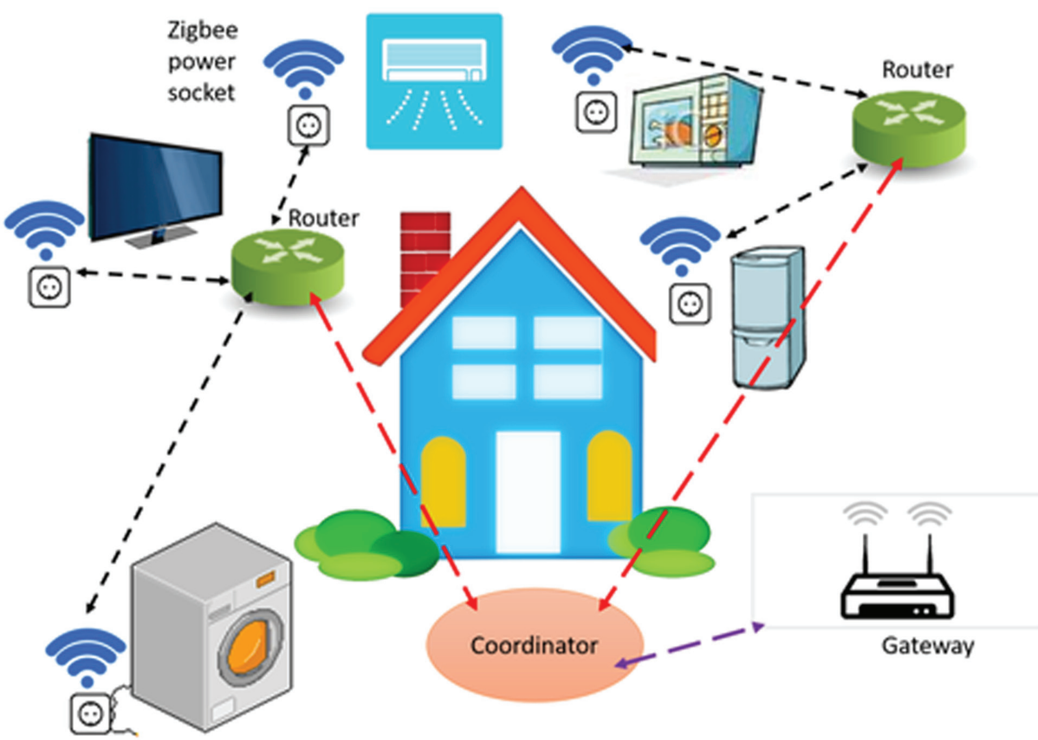


Figure 5. A commercial sensor for transmission line monitoring (Sentient Energy, 2017)

to optimize the cost while satisfying latency and throughout requirements. They further showed the existent technology enables the monitoring of a transmission line using a WSN.

Smart grid sensors and other devices, such as smart meters, can monitor the power consumption of home appliances and facilitate the scheduling of non-critical loads so as to reduce the cost and avoid the peak times (Yang, Lambert, & Divan, 2007).

The smart grid sensor is also the enabling technology for distributed monitoring of the electricity demand and response. The distributed monitoring platform can detect, for instance, equipment failures, blackouts, and power outages in the distribution system.

The new generation of distributed monitoring platforms consists of smart grid sensors with flexible communication modules that perform measuring operations. The measures include electric field strength, fault current, load current, power factors, phase angles, voltage sag, wire temperature, surges and harmonics of the distribution system. A smart grid sensor network uses real-time data to monitor the overhead transformers in the substation, checks the health of vital circuits and schedules maintenance work (Salazar-Llinas, Ginart, & Restrepo, 2014).

WSN is also used for monitoring the load level, controlling the distributed switches, for powering the meter, etc. It can also predict and notify of a potential pending failure before it occurs. A WSN offers plenty of advantages like cost reduction of the grid operation, improving the system up time and reliability (Paoletti & Herman, 2015).

A WSN adds reliability and self-healing characteristics to the smart grid electricity (Gungor, Lu, & Hancke, 2010). The process of automation can be operated on either the generation, transmission or the utilization part of the system. In a WSN enabled smart-grid most equipment failures and damages can be monitored and controlled with devices such as wireless automatic meter reading (WAMR).

The study by (Sood, Fischer, Eklund, & Brown, 2009) mentioned the challenges on how to apply the sensor nodes in the implementation. (McDaniel & McLaughlin, 2009) and (Glaser, 2004) explained that a WSN can be applied in smart grid environments, IoT, Machine to Machine and the communication network.

4.1. WSN Routings in Smart Grid

Routing is an important design factor that determines the efficiency, scalability, and robustness of the WSN. The popular metrics for WSN routing include, but are not limited to, latency, energy efficiency, network lifetime, goodput, scalability, security, coverage, and connectivity (Yamunadevi, Vairam, Kalaiarasan, & Vidya, 2012) (Sangwan, Singh, & Sawant, 2016).

Energy consumption is one important aspect that WSN routing protocols try to optimize. One of the main constraints of a WSN is access to abundant energy (Titouna, Aliouat, & Gueroui, 2016). Sensor devices are typically low power devices that are designed to operate using an energy storage system or energy harvesting. As such, a lot of research has gone into designing energy-efficient routing protocols for WSNs (Sarkar & Senthil Murugan, 2016). There are several approaches that have been used to achieve this (Ari, Yenke, Labraoui, Damakoa, & Gueroui, 2016), inspired by the biological phenomenon of honeybees designed a cluster-based routing mechanism that is energy efficient. By mimicking the fast and efficient clustering mechanisms of artificial bees, the authors were able to design an improved routing protocol that is better performance wise, while still efficient in terms of energy consumption. The authors of (Kumar & Kumar, 2016) proposed a position based routing protocol that achieved energy efficiency by trying to balance the energy consumption of individual sensor nodes across the whole network. They did these using selected parameters such as the remaining sensor energy, the distance between the nodes from the destination and so on. Other authors (Rani, Malhotra, Talwar, & Ahmed, 2017) (Mohemed, Saleh, Abdelrazzak, & Samra, 2016) have also proposed energy-efficient routing protocols for WSN for different use-cases. In the smart grid arena, the RPL routing protocol has been investigated in the context of advanced metering infrastructure (Ancillotti, Bruno, & Conti, 2013). A few enhancements such as auto-configuration, a multi-channel operation have been added to the RPL for AMI (Kulkarni, Gormus, Fan, & Motz, 2011).

A key performance measure related to the energy consumption of a WSN is the network lifetime. Lifetime is the period in which all sensors operational. The death time is the instant of time in which one or more sensor nodes runs out of power. Since WSN, routing protocols consume a considerable amount of power, one of the key challenges that remains is optimizing network lifetime. The goal is to maximize this value as much as possible. An important parameter is used to evaluate the effectiveness of new approaches used for routing protocols. (Chatterjee & Mukherjee, 2014) proposed a novel WSN routing protocol that tried to maximize network lifetime by using a new approach. The WSN was divided into tree based density-varied clusters with a higher density of nodes in the higher levels of the network. This enabled the authors to optimize power usage in the higher traffic levels and provide reliability. (Guo, Yao, Song, Hu, & Liu, 2015) also proposed new routing mechanisms that use sleep mode approach in order to maximize the network lifetime of a WSN. In the context of the smart grid, several routing schemes to extend WSN lifetime have been proposed. The authors considered a routing scheme that accounts for the charging status, the remaining energy, and the transmission power consumption of the nodes. Packet-size optimization combined with transmission power control has been shown as an effective solution to maximize WSN lifetime (Kurt, Yildiz, Yigit, Tavli, & Gungor, 2017).

4.2. Energy Harvesting for WSN

One of the main challenges in WSN is to sustain the power supply at the node. To this end, energy harvesting is an enabling technology, whereby the sensor scavenges power from ambient sources. The most popular sources for energy harvesting are electromagnetic, solar cells, piezoelectric, acoustic, and thermal. Energy harvesting, EH, for WSN in the smart grid is an active research field. The selection of the harvester circuits is determined by factors like cost, location, and application. Most of the recent works on EH (2014-2016) focused on the sensors that are used in the high-voltage domain. (Semedo, Oliveira, & Cardoso, 2014) devised a solar energy harvesting circuit for sensors scattered in high-voltage disconnected switches. The harvested energy is stored in supercapacitor cells. Energy harvesting for sensors deployed along AC lines has its own design bottlenecks because of the low frequency of the EM field (50-60 Hz). To address the problem, a number of schemes have been proposed. J. Han et al., devised a nonintrusive energy harvester circuit using cantilever-structured magneto electric composite (Jinchi, et al., 2015). The experiments showed that the double cell harvester can generate a power of 9.40 mW at 40 A. The work reported in (Moghe, Iyer, Lambert, & Divan, 2015), elaborated an energy harvester for medium and high-voltage, using an electric field. The circuit used two parallel plates to form a storage capacitor. The circuit was able to generate 17 mW using 35-kV AC line. Energy scavenging circuit reported in (Hosseinimehr & Tabesh, 2016) uses miniaturized linear permanent magnet synchronous generator to harvest energy from EM field that surrounds the AC line carrying high-voltage. The results showed that the circuit has a power density of 3.2 mW/kA.

4.3. Discussions

Wireless sensor network is a vital technology for designing robust, secure, self-healing and efficient grid. WSNs have been deployed at the energy generation site, the transmission and distribution side, and consumer premises. The technologies for building WSN are diverse which create an interoperability problem. Middleware is an effective solution that can help to remedy the problem. The processing capabilities and the battery management of the sensor add another dimension to the problem.

5. SUMMARY AND OPEN ISSUES

Smart grid technology is an emerging area of multidisciplinary research. ICT technologies and real-time embedded systems are key enabler for the realization of self-healing, efficient, green and secure smart grid. Recent works in communication technologies have gone in interoperability, secure aggregation, network analyses, self-configuring network, improvements of PLC enabled communication, green communication, and the integration of IoT with the smart grid. However, there are still some open issues that need further investigations. These issues, in general, can be categorized into three main aspects: security/privacy, efficiency, and interoperability.

Security and privacy are still hot issues that continue to affect the underlying communication technologies. These issues have become more prominent as the Internet of Things (IoT) technology has become the backbone technology for the smart grid. IoT devices are vulnerable to cyber-attacks and are used to form bot nets to conduct Distributed Denial of Service Attacks (DDoS). Research into security mechanisms that are lightweight is still an open issue that needs to be tackled.

Due to the stringent communication requirements of smart grid functions and applications, efficiency is an important feature across all aspects of the communication infrastructure and technologies. A number of issues are still open for further research. One area, in particular, is concerned with spectrum utilization. Power line communication (PLC), which is one of the preferred communication technologies, still has to be fully utilized in terms of bandwidth capacity. Research into new techniques such as multi-armed bandit channel selection requires further investigation. Due to the power constraints of different nodes of a smart grid system, a new energy efficient communication protocol has to be investigated further. There are already some interesting proposal and research directions in this area. For smart grid applications that involve complex communication operations, end-to-end latency is still also an open problem. Other open issues related to efficiency include better network traffic characterization mechanisms, which would allow more efficient use of available communication infrastructure, low-cost communication infrastructure, and interference-free communication protocols that minimize packet loss and increase bandwidth efficiency.

The new direction in smart sensor technology is the development of low cost, low maintenance and self-powered sensors to assist realization of a flexible monitoring system. This new type of sensor is referred to as a smart stick-on sensor, which addresses the shortcomings of the current smart sensor technology. The open issues in WSN include the miniaturization of sensors, lightweight protocols, middleware design, interoperability, scalability, healing, energy harvesting, low-power communication protocols, and security.

ACKNOWLEDGMENT

The Swedish government through the SIDA project supports this work. The authors thank the following people: Cleverson Takiguch from S&C electric company for his valuable comments and suggestions to improve the content of the paper and Christine Mwase from Dar es Salam for her effort to improve the paper.

REFERENCES

ABB. (2017). *ABB company*. Retrieved from http://new.abb.com/substation-automation

Al Faruque, M. A., & Vatanparvar, K. (2016, April). Energy Management-as-a-Service Over Fog Computing Platform. *IEEE Internet of Things Journal*, *3*(2), 161–169. doi:10.1109/JIOT.2015.2471260

Ancillotti, E., Bruno, R., & Conti, M. (2013, January). The role of the RPL routing protocol for smart grid communications. *IEEE Communications Magazine*, *51*(1), 75–83. doi:10.1109/MCOM.2013.6400442

Ancillotti, E., Bruno, R., & Conti, M. (2013, November). 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

Anzar, M., Nadeem, J., & Sohail, R. (2015, January). A review of wireless communications for smart grid. *Renewable & Sustainable Energy Reviews*, *41*, 248–260. doi:10.1016/j.rser.2014.08.036

Ari, A. A., Yenke, B. O., Labraoui, N., Damakoa, I., & Gueroui, A. (2016, July). A power efficient cluster-based routing algorithm for wireless sensor networks: Honeybees swarm intelligence based approach. *Journal of Network and Computer Applications*, *69*, 77–97. doi:10.1016/j.jnca.2016.04.020

Baker, J., & Meisinger, M. (2011, December). Experience with a distributed-intelligence, self-healing solution for medium-voltage feeders on the Isle of Wight. In *Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, (pp. 1-4). doi:10.1109/ISGTEurope.2011.6162646

Blair, S. M., Booth, C. D., Valck, B. D., Verhulst, D., Kirasack, C., Wong, K. Y., & Lakshminarayanan, S. (2016, March). Validating secure and reliable IP/MPLS communications for current differential protection. In *Proceedings of the 13th International Conference on Development in Power System Protection 2016 (DPSP)* (pp. 1-6). doi:10.1049/cp.2016.0070

Campos, F., Matos, M., Pereira, J., & Rua, D. (2014, September). A peer-to-peer service architecture for the Smart Grid. In *Proceedings of the 14-th IEEE International Conference on Peer-to-Peer Computing* (pp. 1-5). IEEE. doi:10.1109/P2P.2014.6934315

Chatterjee, A., & Mukherjee, D. (2014). Reliable multipath wireless sensor network routing protocol scheme for network lifetime maximization. In *Proceedings of the 2014 2nd International Conference on Business and Information Management (ICBIM)* (pp. 64-68). IEEE.

Cleveland, F. M. (2008, July). Cyber security issues for Advanced Metering Infrastructure (AMI). In *Proceedings of the Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century* (pp. 1-5). IEEE. doi:10.1109/PES.2008.4596535

Dan, G., Lui, K.-S., Tabassum, R., Zhu, Q., & Nahrstedt, K. (2013, October). SELINDA: A secure, scalable and light-weight data collection protocol for smart grids. In *Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 480-485). doi:10.1109/SmartGridComm.2013.6688004

Detken, K. O., Genzel, C. H., Rudolph, C., & Jahnke, M. (2014, September). Integrity protection in a smart grid environment for wireless access of smart meters. In *Proceedings of the 2014 2nd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems* (pp. 79-86). doi:10.1109/IDAACS-SWS.2014.6954628

Diamantoulakis, P. D., Kapinas, V. M., & Karagiannidis, G. K. (2015). Big Data Analytics for Dynamic Energy Management in Smart Grids. *Big Data Research*, *2*(3), 94–101. doi:10.1016/j.bdr.2015.03.003

Ding, Y., & Hong, S. H. (2013). A model of demand response energy management system in industrial facilities. In *Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm* (pp. 241-246). IEEE. doi:10.1109/SmartGridComm.2013.6687964

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*, *15*(2), 22.

Elmangoush, A., Steinke, R., Al-Hezmi, A., & Magedanz, T. (2014, February). On the usage of standardised M2M platforms for Smart Energy management. In *Proceedings of the International Conference on Information Networking 2014 (ICOIN2014)* (pp. 79-84). doi: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

Fan, S., Ye, F., Guo, J., Liang, Y., Xu, G., Zhang, X., & Qian, Y. (2014, August). A security protocol for wireless sensor networks designed for monitoring smart grid transmission lines. In *Proceedings of the 2014 23rd International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-7). doi:10.1109/ICCCN.2014.6911789

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Fourth). Smart Grid- The New and Improved Power Grid: A Survey. *IEEE Communications Surveys and Tutorials*, *14*(4), 944–980. doi:10.1109/SURV.2011.101911.00087

Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18–28. doi:10.1109/MPE.2009.934876

Farzaneh, M., Farokhi, S., & Chisholm, W. A. (2013). *Electrical design of overhead power transmission lines* (1st ed.). McGraw-Hill.

Fateh, B., Govindarasu, M., & Ajjarapu, V. (2013, June). Wireless Network Design for Transmission Line Monitoring in Smart Grid. *IEEE Transactions on Smart Grid*, *4*(2), 1076–1086. doi:10.1109/TSG.2013.2241796

Feiler, J. (2016). Working with HomeKit Accessories. In *Learn Apple HomeKit on iOS* (pp. 51–71). Berkeley, CA: Apress. doi:10.1007/978-1-4842-1527-2_5

Filho, H. G., Filho, J. P., & Moreli, V. L. (2016, September). The adequacy of LoRaWAN on smart grids: A comparison with RF mesh technology. In *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2)* (pp. 1-6). doi:10.1109/ISC2.2016.7580783

Ghorbani, J., Choudhry, M. A., & Feliachi, A. (2013, February). Fault location and isolation using multi agent systems in power distribution systems with distributed generation sources. In *Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-6). doi:10.1109/ISGT.2013.6497805

Glaser, S. D. (2004). Some real-world applications of wireless sensor nodes. In *Proceedings of SPIE Symposium on Smart Structures and Materials* (pp. 344-355). doi:10.1117/12.539089

Glesner, M., & Philipp, F. (2013). Embedded Systems Design for Smart System Integration. In *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (pp. 32-33). doi:10.1109/ISVLSI.2013.6654611

Gobena, Y., Durai, A., Birkner, M., Pothamsetty, V., & Varakantam, V. (2011, March). Practical architecture considerations for Smart Grid WAN network. In *Proceedings of the 2011 IEEE/PES power systems conference and exposition* (pp. 1-6). doi:10.1109/PSCE.2011.5772481

Gungor, V. C., Lu, B., & Hancke, G. P. (2010). Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Transactions on Industrial Electronics*, *57*(10), 3557–3564. doi:10.1109/TIE.2009.2039455

Gungor, V. C., Sahin, D., Kocak, T., & Ergut, S. (2011). Smart grid technologies: communication technologies and standards. *IEEE transactions on Industrial Informatics*.

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

Guo, J., Yao, J., Song, T., Hu, J., & Liu, M. (2015, Dec). A routing algorithm to long lifetime network for the intelligent power distribution network in smart grid. In *Proceedings of the 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (pp. 1077-1082). IEEE. doi:10.1109/IAEAC.2015.7428724

Hosseinimehr, T., & Tabesh, A. (2016, August). Magnetic Field Energy Harvesting from AC Lines for Powering Wireless Sensor Nodes in Smart Grids. *IEEE Transactions on Industrial Electronics*, *63*, 4947–4954. doi:10.1109/TIE.2016.2546846

Hu, J., & Vasilakos, A. V. (2016, September). Energy Big Data Analytics and Security: Challenges and Opportunities. *IEEE Transactions on Smart Grid*, *7*(5), 2423–2436. doi:10.1109/TSG.2016.2563461

Ibrahim, M., & Salama, M. M. (2015). Smart distribution system volt/VAR control using distributed intelligence and wireless communication. *IET Generation, Transmission Distribution*, *9*(4), 307–318. doi:10.1049/iet-gtd.2014.0513

Jinchi, H., Jun, H., Yang, Y., & Zhongxu, W. (2015, July). A nonintrusive power supply design for self-powered sensor networks in the smart grid by scavenging energy from AC power line. *IEEE Transactions on Industrial Electronics*, *62*(7), 4398–4407. doi:10.1109/TIE.2014.2383992

Kabalci, Y. (2016, May). A survey on smart metering and smart grid communication. *Renewable & Sustainable Energy Reviews*, *57*, 302–318. doi:10.1016/j.rser.2015.12.114

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 and Tutorials*, *18*(1), 860–898. doi:10.1109/COMST.2015.2481722

Khan, R. H., & Khan, J. Y. (2013, February). 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

Kim, Y. J., He, K., Thottan, M., & Deshpande, J. G. (2014, November). Virtualized and self-configurable utility communications enabled by software-defined networks. In *Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 416-421). doi:10.1109/SmartGridComm.2014.7007682

Kim, Y. J., Kolesnikov, V., Kim, H., & Thottan, M. (2011, Oct). SSTP: A scalable and secure transport protocol for smart grid data collection. In *Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 161-166). doi:10.1109/SmartGridComm.2011.6102310

Kim, Y. J., Lee, J., Atkinson, G., Kim, H., & Thottan, M. (2012, July). SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications. *IEEE Journal on Selected Areas in Communications*, *30*(6), 1119–1136. doi:10.1109/JSAC.2012.120710

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

Koutsopoulos, I., & Tassiulas, L. (2011). Challenges in demand load control for the smart grid. *IEEE Network*, *25*(5), 16–21. doi:10.1109/MNET.2011.6033031

Kulkarni, P., Gormus, S., Fan, Z., & Motz, B. (2011, June). A self-organising mesh networking solution based on enhanced RPL for smart metering communications. In *Proceedings of the 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* (pp. 1-6). doi:10.1109/WoWMoM.2011.5986178

Kumar, V., & Kumar, S. (2016, December). Energy balanced position-based routing for lifetime maximization of wireless sensor networks. *Ad Hoc Networks*, *52*, 117–129. doi:10.1016/j.adhoc.2016.08.006

Kurt, S., Yildiz, H. U., Yigit, M., Tavli, B., & Gungor, V. C. (2017, March). Packet Size Optimization in Wireless Sensor Networks for Smart Grid Applications. *IEEE Transactions on Industrial Electronics*, *64*(3), 2392–2401. doi:10.1109/TIE.2016.2619319

Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, *67*, 74–88. doi:10.1016/j.comnet.2014.03.029

Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2016, January). Review of communication technologies for smart homes/building applications. In Proceedings of the 2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA) (pp. 1-6). IEEE.

Lee, J. Y., & Choi, S. G. (2014, Feb). Linear programming based hourly peak load shaving method at home area. In *Proceedings of the 16th International Conference on Advanced Communication Technology* (pp. 310-313). doi:10.1109/ICACT.2014.6778971

Liu, N., Chen, J., Zhu, L., Zhang, J., & He, Y. (2013, October). A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid. *IEEE Transactions on Industrial Electronics*, *60*(10), 4746–4756. doi:10.1109/TIE.2012.2216237

Liu, Y. (2012). Wireless sensor network applications in smart grid: recent trends and challenges. *International Journal of Distributed Sensor Networks*, *8*(9), 492819. doi:10.1155/2012/492819

Ma, J., Chen, H., Song, L., & Li, Y. (2016, March). Residential Load Scheduling in Smart Grid: A Cost Efficiency Perspective. *IEEE Transactions on Smart Grid*, *7*, 1–1.

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

Mabusela, K., Kruger, C. P., Silva, B. J., & Hancke, G. P. (2015, September). Design of a wireless heliostat system. *AFRICON*, *2015*, 1–5. doi:10.1109/AFRCON.2015.7332011

Mahalik, N. P. (2003). Fieldbus Technology: Industrial Network Standards for Real-Time Distributed Control (1st ed.). Springer-Verlag Berlin Heidelberg.

Martin, M., & Schmidt, R. A. (2014, May 31). *Communications: The smart grid enabling technology*. SmartGrid.gov. Retrieved from https://www.smartgrid.gov/files/NRECA_DOE_Communications_1.pdf

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, *7*(3), 75–77. doi:10.1109/MSP.2009.76

Moghe, R., Iyer, A. R., Lambert, F. C., & Divan, D. (2015, March). A Low-Cost Electric Field Energy Harvester for an MV/HV Asset-Monitoring Smart Sensor. *IEEE Transactions on Industry Applications*, *51*(2), 1828–1836. doi:10.1109/TIA.2014.2354741

Mohemed, R. E., Saleh, A. I., Abdelrazzak, M., & Samra, A. S. (2016, December). Energy-efficient routing protocols for solving energy hole problem in wireless sensor networks. *Computer Networks*.

Moness, M., & Moustafa, A. M. (2016, April). A Survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy. *IEEE Internet of Things Journal*, *3*(2), 134–145. doi:10.1109/JIOT.2015.2478381

Moreno-Garcia, I. M., Pallares-Lopez, V., Gonzalez-Redondo, M., Lopez-Lopez, J., Varo-Martinez, M., & Santiago, I. (2015, March). Implementation of a real time monitoring system for a grid-connected PV park. In *Proceedings of the 2015 IEEE International Conference on Industrial Technology (ICIT)* (pp. 2915-2920). doi:10.1109/ICIT.2015.7125528

Mossé, D., & Gadola, G. (2012, June). Controlling wind harvesting with wireless sensor networks. In *Proceedings of the 2012 International Green Computing Conference (IGCC)* (pp. 1-6). doi:10.1109/IGCC.2012.6322285

Mues, M. O., Alvarez, A., Espinoza, A., & Garbajosa, J. (2011, July). Towards a distributed intelligent ICT architecture for the smart grid. In *Proceedings of the 2011 9th IEEE International Conference on Industrial Informatics* (pp. 745-749). doi:10.1109/INDIN.2011.6034985

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

Nanda, A. K., & Panigrahi, C. K. (2016, July). Review on smart home energy management. *International Journal of Ambient Energy*, *37*(5), 541–546. doi:10.1080/01430750.2015.1004107

Ndjiongue, A. R., Ferreira, H. C., & Shongwe, T. (2016). Inter-building PLC-VLC integration based on PSK and CSK techniques. In *Proceedings of the 2016 International Symposium on Power Line Communications and its Applications (ISPLC)* (pp. 31-36). IEEE. doi:10.1109/ISPLC.2016.7476254

Nguyen, L.-L., Nguyen, M.-T., Cuong, L. Q., & Nguyen, T.-D. (2016, January). On the design of wireless Smart Grid network for an apartment building based on 868 MHz low power wireless SoC. In *Proceedings of the 2015 International Conference on Advanced Technologies for Communications (ATC)* (pp. 456-461). IEEE.

Nunes, B. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Communications Surveys and Tutorials*, *16*(3), 1617–1634. doi:10.1109/SURV.2014.012214.00180

Paoletti, G. J., & Herman, G. (2015). Monitoring of electrical equipment failure indicators and zero-planned outages: Past, present and future maintenance practices. In *Proceedings of the IEEE Conference Record of Annual Pulp and Paper Industry Technical Conference*. doi:10.1109/PPIC.2015.7165712

Rani, S., Malhotra, J., Talwar, R., & Ahmed, S. H. (2017, January). Energy Efficient Chain Based Routing Protocol for Underwater Wireless Sensor Networks. *Journal of Network and Computer Applications*.

Salazar-Llinas, A., Ginart, A., & Restrepo, C. (2014). Observer based sensor fault tolerant for grid tied - Solar inverters. In *Proceedings of the IEEE Green Technologies Conference* (pp. 69-74). doi:10.1109/GREENTECH.2014.16

Sangwan, A., Singh, R., & Sawant, P. (2016, April). Coverage and connectivity preserving routing in wireless sensor networks: A new approach. In *Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 503-509). doi:10.1109/CCAA.2016.7813771

Sanz, A., Pinero, P. J., Idiago, J. M., Esteban, S., & Garcia, J. I. (2014, Nov). Narrowband power line communications evaluation in complex distribution networks. In *Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 266-271). doi:10.1109/SmartGridComm.2014.7007657

Saputro, N., Akkaya, K., & Guvenc, I. (2015, October). Privacy-aware communication protocol for hybrid IEEE 802.11s/LTE Smart Grid architectures. In *Proceedings of the 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)* (pp. 905-911). doi:10.1109/LCNW.2015.7365945

Sarkar, A., & Senthil Murugan, T. (2016, December). Routing protocols for wireless sensor networks: What the literature says? *Alexandria Engineering Journal*, *55*(4), 3173–3183. doi:10.1016/j.aej.2016.08.003

S&C electric company. (2017). *S&C electric company*. Retrieved from Solutions for Self-Healing Grids: https://www.sandc.com/en/solutions/self-healing-grids/

Schmidt, N. P. (1999, October). Comparison between IEEE and CIGRE ampacity standards. *IEEE Transactions on Power Delivery*, *14*(4), 1555–1559. doi:10.1109/61.796253

Semedo, S. M., Oliveira, J. E., & Cardoso, F. J. (2014, June). Remote monitoring of high-voltage disconnect switches in electrical distribution substations. In *Proceedings of the 2014 IEEE 23rd International Symposium on Industrial Electronics (ISIE)* (pp. 2060-2064). doi:10.1109/ISIE.2014.6864934

Sentient Energy. (2017). *MM3 Intelligent Sensor*. Retrieved from Sentient Energy: http://www.sentient-energy.com/mm3-intelligent-sensor/

Sha, K., Alatrash, N., & Wang, Z. (2016). A Secure and Efficient Framework to Read Isolated Smart Grid Devices. *IEEE Transactions on Smart Grid*. doi:10.1109/TSG.2016.2526045

Siemens. (2017). *Substation Automation*.

Smith, T. B. (2004). Electricity theft: A comparative analysis. *Energy Policy*, *32*(18), 2067–2076. doi:10.1016/S0301-4215(03)00182-4

Song, Y., Zhou, G., & Zhu, Y. (2013). Present status and challenges of big data processing in smart grid. *Power System Technology*, *37*, 927–935.

Sood, V. K., Fischer, D., Eklund, J. M., & Brown, T. (2009). Developing a communication infrastructure for the smart grid. In *Proceedings of the 2009 IEEE Electrical Power and Energy Conference*. doi:10.1109/EPEC.2009.5420809

IEEE Std. 2030-2011. (2011, January). *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

Stojkoska, B. L., & Trivodaliev, K. V. (2017, January). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454–1464. doi:10.1016/j.jclepro.2016.10.006

Taqqali, W. M., & Abdulaziz, N. (2010, December). Smart Grid and demand response technology. In *Proceedings of the 2010 IEEE International Energy Conference (ENERGYCON 2010)* (pp. 710-715). IEEE. doi:10.1109/ENERGYCON.2010.5771773

The Smart Grid Interoperability Panel. (2010). *Introduction to NISTIR 7628 guidelines for smart grid cybersecurity*. U.S. Department of Energy.

Titouna, C., Aliouat, M., & Gueroui, M. (2016). FDS: Fault detection scheme for wireless sensor networks. *Wireless Personal Communications*, *86*(2), 549–562. doi:10.1007/s11277-015-2944-7

US Department of Commerce. (2014). NIST Special Publication 1108.

Vo, M. T., Nguyen, M. T., Nguyen, T. D., Le, C. T., & Huynh, H. T. (2013, Oct). Towards residential smart grid: A practical design of wireless sensor network and Mini-Web server based low cost home energy monitoring system. In *Proceedings of the 2013 International Conference on Advanced Technologies for Communications (ATC 2013)* (pp. 540-545). doi:10.1109/ATC.2013.6698174

Vukojevic, A., Laval, S., & Handley, J. (2015, Feb). An integrated utility microgrid test site ecosystem optimized by an open interoperable distributed intelligence platform. In *Proceedings of the 2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. doi:10.1109/ISGT.2015.7131852

Vyatkin, V., Zhabelova, G., Yang, C. W., McComas, D., & Chouinard, J. (2012, September). Intelligent IEC 61850/61499 logical nodes for smart metering. In *Proceedings of the 2012 IEEE Energy Conversion Congress and Exposition (ECCE)* (pp. 1220-1227). doi:10.1109/ECCE.2012.6342677

Wan, Z., Wang, G., Yang, Y., & Shi, S. (2014, December). SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids. *IEEE Transactions on Industrial Electronics*, *61*(12), 7055–7066. doi:10.1109/TIE.2014.2331014

Wang, K., Wang, Y., Sun, Y., Guo, S., & Wu, J. (2016). Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective. *IEEE Communications Magazine*, *54*(12), 48–54. doi:10.1109/MCOM.2016.1600399CM

Wei, M., Hong, S. H., & Alam, M. (2016, February). An IoT-based energy-management platform for industrial facilities. *Applied Energy*, *164*, 607–619. doi:10.1016/j.apenergy.2015.11.107

Werbos, P. J. (2011, August). Computational Intelligence for the Smart Grid-History, Challenges, and Opportunities. *IEEE Computational Intelligence Magazine*, *6*(3), 14–21. doi:10.1109/MCI.2011.941587

Wickelgren, I. J. (1996, September). Local-area networks go wireless. *IEEE Spectrum*, *33*(9), 34–40. doi:10.1109/6.535256

Yamunadevi, S. P., Vairam, T., Kalaiarasan, C., & Vidya, G. (2012, March). Efficient comparison of multipath routing protocols in WSN. In *Proceedings of the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)* (pp. 807-811). doi:10.1109/ICCEET.2012.6203845

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

Yang, C. W., Zhabelova, G., Vyatkin, V., Nair, N. K., & Apostolov, A. (2012, July). Smart Grid automation: Distributed protection application with IEC61850/IEC61499. In *Proceedings of the IEEE 10th International Conference on Industrial Informatics* (pp. 1067-1072). doi:10.1109/INDIN.2012.6301145

Yang, Y., Lambert, F., & Divan, D. (2007). A survey on technologies for implementing sensor networks for power delivery systems. In *Proceedings of the EEE Power Engineering Society General Meeting* (pp. 1-8). doi:10.1109/PES.2007.386289

Ye, F., Qian, Y., & Hu, R. Q. (2014, Dec). A security protocol for advanced metering infrastructure in smart grid. In *Proceedings of the 2014 IEEE Global Communications Conference* (pp. 649-654). doi:10.1109/GLOCOM.2014.7036881

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015, Nov). Fog Computing: Platform and Applications. In *Proceedings of the 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)* (pp. 73-78). doi:10.1109/HotWeb.2015.22

Yu, K., Arifuzzaman, M., Wen, Z., Zhang, D., & Sato, T. (2015, August). A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid. *IEEE Transactions on Instrumentation and Measurement*, *64*(8), 2072–2085. doi:10.1109/TIM.2015.2444238

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

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014, February). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, *1*(1), 22–32. doi:10.1109/JIOT.2014.2306328

Zhang, B., & Baillieul, J. (2016). Control and Communication Protocols Based on Packetized Direct Load Control in Smart Building Microgrids. *Proceedings of the IEEE*, *104*(4), 837–857. doi:10.1109/JPROC.2016.2520759

Zhou, B., Li, W., Chan, K. W., Cao, Y., Kuang, Y., Liu, X., & Wang, X. (2016, August). Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable & Sustainable Energy Reviews*, *61*, 30–40. doi:10.1016/j.rser.2016.03.047

Imed Saad Ben Dhaou (S'97-M'02, SM'2011) received a Master's degree in Electrical Engineering from the Tampere University of Technology, Tampere, Finland, and the PhD degree from the Royal Institute of Technology, Stockholm, Sweden, in 1997, and 2002, respectively. He has authored and co-authored more than 30 journals, book chapters, technical reports and conference papers in these areas. Dr. Ben Dhaou received the Best Paper Award from the 1997 Finnish Symposium on Signal Processing and a travel grant from the PhD forum at DAC, Los Angeles in 2000. Since September 2014, Dr. Ben Dhaou has been serving as editor to the microelectronics journal, Elsevier. He was the Guest Editor for the special issue of on-chip signaling in deep-submicron technology, Journal of Analog Integrated Circuits and Signal Processing. Dr. Ben Dhaou is a member of the following IEEE communities: Internet of Things, Smart Cities, Big Data, Rebooting Computing, Cybersecurity, Software Defined Networks, Cloud Computing. He is also a member of IEEE Council on RFID.

Aron Kondoro received his Master of Science degree in Information and Communication Systems Security from the Royal Institute of Technology (KTH - Sweden) in 2012 and Bachelor of Science in Computer Science from the University of Dar-es-Salaam in 2007. He is an Assistant Lecturer in the Computer Science and Engineering (CSE) Department at the University of Dar-es-Salaam (UDSM), Tanzania. Currently, he is a PhD student at KTH/UDSM doing research in using smart grid technologies to design and implement more efficient, reliable and autonomous solar-driven microgrids for off-grid rural communities. His other research and consultancy activities are focused on analyzing ICT systems security and using mobile technologies to design applications for educational and financial use-cases.

Amleset Kelati received the MS degree in Electronics Engineering from the Universidad Central de las villas, Santa Clara, in 1986, MS degree in Electrical Engineering specialization System on chip Design and with specialization Digital communication Systems and Technology from KTH Institute of Technology, Stockholm in 2005 and from Chalmers University of Technology, Gothenburg, in 2001, respectively. Currently, she is a Research Engineer in the Department of Information and communication technology, KTH Sweden and a PHD student at Department of Information Technology, University of Turku, Finland. She previously held positions at Ericsson, Zarlink, NXP, U-Blox. Her research focuses on ultra-low power RFIC design, low-power integrated circuits for biomedical devices, wireless sensing and DSP feature extraction method for IoT applications and wireless communication in smart sensors application. Amleset has been a Senior IEEE member since May 2016.

Diana Severine Rwegasira received her BSc.in Computer Engineering and.IT at University of Dar es salaam in 2008 and her Msc in Computer science at the University of Eastern Finland, Finland in 2011. She had been involved in teaching and supervising undergraduate students in computer and networking courses for three years. Currently, she is a PhD candidate in a sandwich program between Royal institute of Technology (KTH), Sweden and University of Dar es Salaam (UDSM),Tanzania under iGrid project which deals with Smart grid. She is also a coach at the University of Dar es salaam ICT incubator(UDICTI) which is an ICT pre-incubation programme aimed at grooming students to be innovative and entrepreneurial candidates.

Shililiandumi Naiman received BSc degree in Electrical Engineering (2001), MSc degree in Telecommunication Engineering (2004), and a PhD degree in Telecommunication Engineering in 2015 from the University of Dar es Salaam, Tanzania. He joined the academic staff of the University of Dar es Salaam in 2005 as Assistant Lecturer. Currently he is working in the department of Electronic and Telecommunication Engineering of University of Dar-es-Salaam as a Lecturer. Dr. S. Naiman is a Registered Professional Engineer in Tanzania by Engineer Registration Board (ERB). His research interests include power-line communication, Smart grid, microwave communications, antenna, fiber-optic communication, multimedia communication, digital electronics and signal processing.

Nerey H. Mvungi received a BSc in electrical engineering from the University Dare es Salaam, Dare es Salaam, Tanzania, in 1978. He received the MSc degree in electronics control from Salford University, Salford, UK in 1980 and PhD degree from Leeds University Leeds, UK in 1989. He was with Phillips Center for Technology in Eindhoven, Eindhoven, Netherlands in 1982/83. He has been with the University of Dar es Salaam from April 1978 until September 2008 in various academic and administrative capacities. He has done a number of research and consultancy projects and specialized professional services in Tanzania and beyond. He served in a number of committees outside the University of Dodoma and the University of Dar es Salaam. He is Professor at the College of ICT of the University of Dar es Salaam and founding Principal. He was a Professor and founding Principal of the College of Informatics and Virtual Education of the University of Dodoma. His research interest is in control and instrumentation, computer communication and applied electronics, lightning protection, rural access, power quality aspects, and remote monitoring and control of energy consumption. He is a Consulting Engineer in Tanzania (CEng), member IET(TZ), AMSTS, Member ICAE. He received the 2010 IBM Faculty Award, TCRA 2013 Award, 2015-2020 Sida Award, PI for Overall Winner of the 2016 UDSM Research Week.

Hannu Tenhunen received the Diploma Engineer degree in electrical engineering and computer sciences from Helsinki University of Technology, Helsinki, Finland, in 1982 and PhD degree in microelectronics from Cornell University, Ithaca, NY, in 1986. During 1978–1982, he was with Electron Physics Laboratory, Helsinki University of Technology. From 1983 to 1985, he was with Cornell University as a Fulbright Scholar. From September 1985, he was with the Signal Processing Laboratory, Tampere University of Technology, Finland, as an Associate Professor. He was also a Coordinator of the National Microelectronics Program of Finland during 1987–1991. Since January 1992, he has been with Royal Institute of Technology, Sweden, where he is a Chair Professor in electronic system design. His current research interests are VLSI circuits and systems for autonomic and smart systems and IoT. He has been actively involved in several EU programs on VLSI/system-on-a-chip. He was education director of European Institute of Innovation and Technology EIT Digital. He has published over 675 reviewed publications and holds 9 international patents in areas relevant to this project.

Call for Articles

International Journal of Embedded and Real-Time Communication Systems

Volume 8 • Issue 2 • July-December 2017 • ISSN: 1947-3176 • eISSN: 1947-3184
An official publication of the Information Resources Management Association

MISSION

The mission of the **International Journal of Embedded and Real-Time Communication Systems (IJERTCS)** is to disseminate recent advancements and innovations in this interdisciplinary research area for field researchers, practitioners, scientists, academicians, students, and IT professionals. IJERTCS focuses on overcoming challenges involved in the rapid development of embedded communication systems towards feature-rich multimedia computers.

COVERAGE AND MAJOR TOPICS

The topics of interest in this journal include, but are not limited to:
Asynchronous and synchronous circuit techniques • Design methods • Embedded networks (built-in networks in embedded communication devices) • Emerging new topics • Fault-tolerant hardware and software technologies • Formal design and verification methods • Hardware and software solutions for protocol processing • Hardware and software solutions for real-time systems • Hardware platforms and technologies • Hardware/software co-design • Modeling and verification methods • On-chip communication in SoC and NoC • OWA (open wireless architecture) • Platform-based design • Real-time computing • Reconfigurable systems • Security issues and technology • Single-chip SDR (software defined radio) solutions • Software design • Testing techniques

ALL INQUIRIES REGARDING IJERTCS SHOULD BE DIRECTED TO THE ATTENTION OF:

Sergey Balandin, Editor-in-Chief • IJERTCS@igi-global.com

ALL MANUSCRIPT SUBMISSIONS TO IJERTCS SHOULD BE SENT THROUGH THE ONLINE SUBMISSION SYSTEM:

http://www.igi-global.com/authorseditors/titlesubmission/newproject.aspx

IDEAS FOR SPECIAL THEME ISSUES MAY BE SUBMITTED TO THE EDITOR(S)-IN-CHIEF

PLEASE RECOMMEND THIS PUBLICATION TO YOUR LIBRARIAN

For a convenient easy-to-use library recommendation form, please visit:
http://www.igi-global.com/IJERTCS