Sustainable Cities and Society 53 (2020) 101957

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues

Pradeep K. Khatua[a,*], Vigna K. Ramachandaramurthy[a], Padmanathan Kasinathan[b], Jia Ying Yong[a], Jagadeesh Pasupuleti[a], Arul Rajagopalan[c]

[a] Institute of Power Engineering, Department of Electrical Power Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia
[b] Department of Electrical and Electronics Engineering, Agni College of Technology, Thalambur, Chennai, Tamilnadu, India
[c] School of Electrical Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, Tamilnadu, India

ARTICLE INFO

Keywords:
Internet of things
Data protocols
Wireless communication protocols
Energy systems

ABSTRACT

The availability of renewable energy sources along with the advancement of sensing and communication technologies has resulted in the sustainable operation of modern energy systems. An intelligent grid system is the integration of sensors and actuators, which enables the system to connect and exchange energy-related data from renewable sources to a computer system and end-users in a communication network. This data can be monitored in real-time with the help of the Internet of Things (IoT). However, several challenges exist in IoT, such as security, bandwidth management, interfacing interoperability, connectivity, packet loss, and data processing. In this paper, the key challenges and outstanding issues with the IoT when incorporated with energy systems are reviewed. The objective of this paper is to assess the suitability of different data transfer and communication protocols of IoT for deployment in the modern grid system. Moreover, several wireless IoT communication technologies are compared for their suitability in the multilayer network architecture and applications of energy systems.

1. Introduction

Any technological advancement must be accompanied by an investigation of the social aspects of stakeholder impacts (government, private, industry, planner, developer, utility, and people community) and their resilience. The concepts of society–sustainability–cities and their interconnections were discussed in (Padmanathan et al., 2019), which promote an integrated method by considering social, economic, technical, and environmental aspects to make cities smarter and sustainable. Energy supply that is reliable, efficient, and has less carbon emissions is one of the primary requirements for smart cities (Batty et al., 2012).

The conventional electric service structure is continuously changing with increased penetration of renewable energy sources. This evolution has been described as a modernized grid, future grid, and future utility. It emphasizes the need to establish an intelligent grid that can be controlled and monitored in real time to provide a safe, reliable, resilient, and secure service and to empower users to participate actively and profit from diverse market services and opportunities. A few years ago, the Internet of Things (IoT) concept was developed for communication by exploring radio frequency identification. The functionalities of IoT are sensing, communication, and taking automatic desired action according to the sensed data without any human interaction. It can be applied in several domains, such as retail, animal farming, transportation, home automation, agriculture, smart cities, healthcare, factories, and electrical grids. IoT can be a platform for renewable sources, specifically, for real-time monitoring of energy-related information. A comprehensive overview of smart and sustainable cities with the integration of IoT (Orlhac, 2019) is illustrated in Fig. 1. IoT facilitates the necessary building elements for smart cities, such as information acquisition, management, and processing, to handle some applications (Silva, Khan, & Han, 2018).

Several key technologies basically help IoT survive, such as data assignation, information collection, processing, computation, and analysis. These technologies in turn create challenges, such as security, bandwidth management, interfacing interoperability, connectivity, and data processing. IoT nodes are prone to attacks and security breaches. Given that IoT systems are detail-intensive, significant data are frozen through the network, thereby potentially exposing the privacy of individuals of organizations to risk. Thus, the data should be secured in communication networks to avoid unauthorized access. The components of the IoT network are sensors, local networks, and backhaul

* Corresponding author.
E-mail address: pradeep.khatua86@gmail.com (P.K. Khatua).

https://doi.org/10.1016/j.scs.2019.101957
Received 16 April 2019; Received in revised form 5 September 2019; Accepted 13 November 2019
Available online 16 November 2019

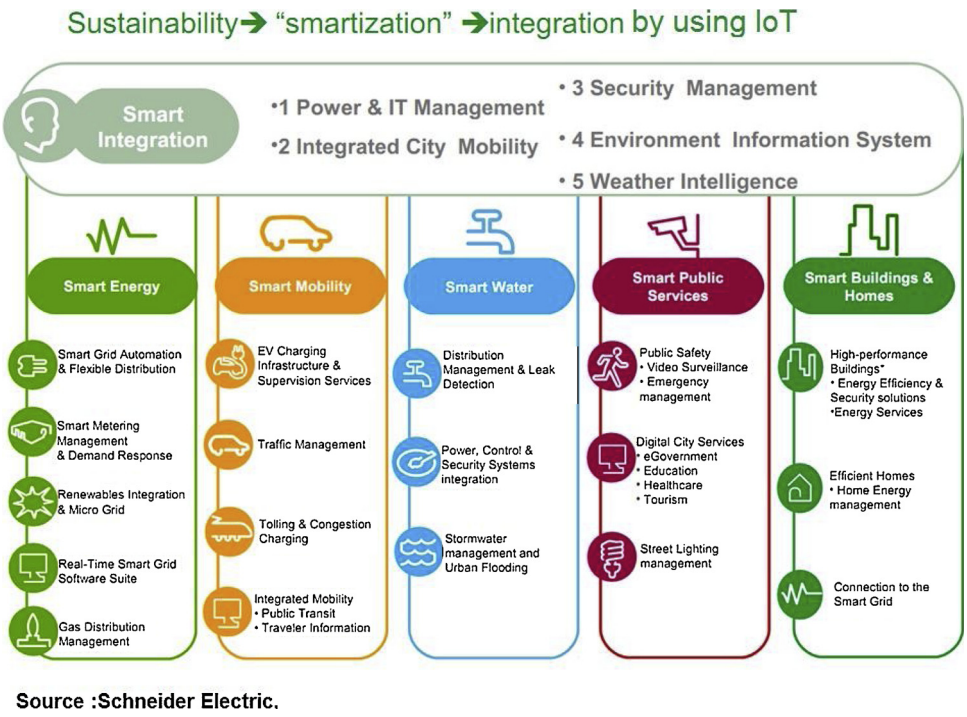

Fig. 1. Sustainability-cities-IoT interconnection methodology (Orlhac, 2019).

networks. A tremendous amount of information is communicated between these components, thereby requiring significant bandwidth. Effective bandwidth utilization should be considered in IoT application in energy systems. The interfacing interoperability in IoT is the device interfacing issue, which arises when the device of one vendor communicates with the device of another vendor that is not running on the same stack or not following the same standard. Hence, in IoT, a handshake needs to be established between several devices, different protocols, and algorithms. Connectivity between networks plays a vital role in facilitating intelligent energy system implementation and handling objects by providing bidirectional conversations between a utility and end users. The complexity of an energy system is directly linked to the problems in establishing its communication interface because many parameters and demands must be considered.

The Internet of Energy (IoE) is the expansion of IoT into distributed energy systems. Typically, an IoE infrastructure consists of smart grid components, such as distributed sources, storage systems, loads, smart meters, and equipment such as circuit breakers, digital relays, and transformers. It empowers the interconnection and peer-to-peer (P2P) transaction of energy. The basic goal of IoE is to fetch and assemble data from individual grid edge components across the available infrastructure to all other grid management contributors simply and quickly.

Stable operation of voltage and frequency, control of reactive and active power, and stored energy management are the expected characteristics of the energy system (Vasquez, Guerrero, miret, castilla, & garci´a de vicun, 2010). The factors in developing and deploying microgrid along with the existing conventional grid can be categorized as economic benefits, integration of clean energy, and energy security (Hirsch, Parag, & Guerrero, 2018). The microgrid decision support tool was developed in (Husein & Chung, 2018) to evaluate all system cash flows in the economic model and to analyze energy usage in the performance model, which decreases energy price by 42 % and emissions by 15 % in a university campus. The authors in (Amrr, Alam, Jamil Asghar, & Ahmad, 2018) proposed two switching schemes for effective utilization of solar energy where a standalone and grid-connected system are combined. The control strategy hierarchy can be divided into three levels: primary level (physical smart devices/sensors, inverters), secondary (electrical and environmental variables), and tertiary (power flow management and optimization algorithm). Different functions of conventional microgrid hierarchical control strategy were reviewed and proposed for IoT-aided home-scale microgrid with renewable energy resources to facilitate the combination of IoT with the microgrid EMS (Guan, Vasquez, & Guerrero, 2017).

The developed simulation model in (Raju, Gokulakrishnan, Muthukumar, Jagannathan, & Morais, 2017) was based on the Java agent development environment (JADE) for progressive and efficient energy management. It contains five potentiometers (two solar PV, battery, load, and grid) for sensing and transmits to the cloud by using a web server (Thingspeak). Arduino receives the data coded by JADE to implement a multi-agent system. The fault detection and the connection or disconnection of the distributed generation system to and from the microgrid are performed by the central protection center (CPC) (Majee & Gnana Swathika, 2017). This paper developed an automated CPC with the help of IoT, which can control the grid regularly for the detection and rectification of faults. Faults were rectified by either finding the shortest path from the faulted bus to the main grid or isolating the faulted bus. An IoT-based smart energy management platform (Ku, Park, & Choi, 2017) was developed by collecting energy data, managing energy demand response, and sharing/trading energy to maximize energy efficiency. To provide energy information services, the platform installed a boiler heat controller, intelligent lighting switch, and provided remote service over the Internet.

The increased and flexible demands of distributed energy resources (DERs) require a more resilient and transactive grid. A transactive grid concept was introduced in (Moslehi & Ranjit Kumar, 2019) as a nested set of virtual microgrids where each can act as a market to support structured and P2P exchanges at all levels in the nested hierarchical market. For both normal and emergency conditions that utilize exchanges of transactive energy, the proposed vision facilitates the realization of a more resilient grid. The load limiter proposed in (Kul & Şen, 2017) can shut down overcurrent devices with the help of IoT to protect the load balance across the grid. It can also eliminate standby energy by disconnecting the standby device from the central software through the cloud. The author in (Lezama, Palominos, guez-Gonzalez, Farinelli, & Munoz de Cote, 2017) proposed an architecture of an IoT-based microgrid to design the long-term optimization scheduling

difficulty as the distributed constraint optimization problem (DCOP). The proposed decentralized architecture treats the problem as a DCOP by considering synchronous branch and bound, asynchronous forward bounding, distributed pseudo-tree optimization procedure (DPOP), and memory-bounded DPOP. Although many researchers have implemented IoT-enabled microgrid systems, only a few of them considered issues such as security, bandwidth, and interoperability, which will be discussed in the next sections.

The objective of this paper is to review the crucial challenges and outstanding issues involved in integrating IoT with energy sources and to compare different data protocols and various wireless communication protocols of IoT. The role of IoT wireless communication protocols in a modernized grid system is evaluated and assessed for their suitability for deployment in the multilayer network architecture of energy systems.

The rest of this paper is structured as follows: Section 2 provides an overview of the critical challenges and issues of IoT application in energy systems. Section 3 describes different types of data protocol. Section 4 explains the communication protocol of IoT. Section 5 describes future recommendations for the suitability of IoT wireless communication technologies for energy systems. Section 6 presents the conclusion.

2. Challenges of IoT application in energy systems

The deployment of IoT in renewable sources integrates information and communication technology in the whole chain of energy with several kinds of embedded devices, sensors, and actuators. IoT extends the range of the Internet to reach the devices deployed on the energy system through standardized communication protocols. However, the implementation of IoT in energy systems comes with its own set of hurdles, such as security, bandwidth management, interfacing interoperability, connectivity, packet loss, and data processing.

2.1. Security issue

The added IoT dimension to the renewable energy sources introduces new security issues and challenges that were not present in the conventional power grid. Security challenges and issues could hamper the deployment of IoT-enabled energy systems by end users. The most critical security problems faced by IoT-enabled energy systems are briefly described in this subsection. Given the wide distribution of IoT devices and the hidden nature of the information that is acquired and carried by IoT nodes, security has become a primary hurdle, which includes issues such as authentication, authorization and access control, privacy, and secure architecture (Conti, Dehghantanha, Franke, & Watson, 2018) (Fig. 2).

IoT-enabled energy systems are based on cyber systems and thus face different security issues.

- **Access control and authorization:** Several devices or objects, such as field-deployed sensors and actuators in distribution substations, should be configured and monitored remotely. An attacker or an angry employee may access and manipulate information, which results in power outages or damaging physical assets such as transformers. The encryption algorithm used in (Pramudita et al., 2017) was the elliptic curve cryptography (ECC) algorithm and the hash function utilized was the secure hash algorithm (SHA 256). Raspberry Pi with Python language and socket communication are used for communication media.
- **Confidentiality and data integrity:** Confidentiality of communicated and stored data ensures accessibility only to the intended recipients. Data integrity ensures that the received data were not modified in the communication path. Ensuring confidentiality for data transmission in IoT networks is difficult because low-end devices are resource-constrained. Approaches such as encoding or ciphers can efficiently mitigate the confidentiality burden of transmitting IoT nodes (Trappe et al., 2015). The authors in (Pramudita et al., 2017) developed a secure line transmission path for microgrid applications where the system can authenticate by using the digital signature plan and assigning a unique ID to all gateways to maintain message confidentiality and data integrity.
- **Authentication:** This is the capability of a communicating device or object in a microgrid system to ensure its identity. A large number of IoT objects such as sensors are deployed in a highly distributed manner, thus making objects difficult to manage. For example, a sensor that is actually in a different location may register itself and claim to be in another location (Liu et al., 2017). The authentication challenges of IoT devices involve device recognition and verification of its association with other devices by correct topological addresses.
- **Privacy:** The threat of information leakage is aggravated when local IoT networks are integrated with the global Internet for monitoring and communicating in the real world. Several organizations may access confidential information over the Internet when the information is communicated through the Internet. In the case of energy systems, smart meters, and smart appliances in residential houses may provide more knowledge than energy consumption can. This information can harm the privacy of customers, such as their location—that is, whether they are home or not—and habits such as sleeping time or wake-up time. The authors in (Sun et al., 2017) proposed the concept of novel dummy location privacy-preserving (DLP) algorithm by analyzing several privacy requirements of different users and computational costs for efficiently preserving users' position secrecy. The DLP algorithm selects the optimal dummy areas by estimating that the opponent may utilize some side information and makes several choices for several secrecy provisions of several customers.

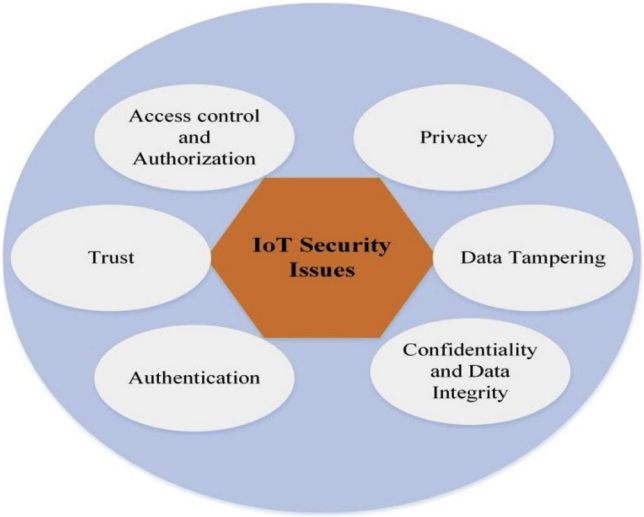

Fig. 2. Important IoT security issues.

Privacy problems can be categorized into two main categories. The first is user-centric privacy, which explains the privacy problems associated with the sensing technologies that collect data about individuals within their monitoring area without them being aware of the situation. The second is network-centric privacy, which can be of two types: (i). content-oriented privacy, which includes aggregated data privacy and query privacy and (ii) context-oriented privacy, which includes temporal, identity, and location privacy (Lopez et al., 2017).

- **Trust:** Microgrid devices or objects could be managed by several entities such as the grid operator for sensors and smart meters and

customers for smart appliances. These devices cannot communicate with each other without the establishment of minimal trust. Establishment of trust between devices owned by several entities is an important issue in large-scale networks (Bekara, 2014).

- **Data tampering:** An attacker can modify communicated data such as prior dynamic price information by turning peak period energy consumption prices into the lowest prices, thereby leading to overload on the power network and increasing the energy consumption of households. In the case of distributed state estimation, the information reliability of microgrid depends on the security of neighboring microgrids. Energy transaction systems in the networked microgrids of an IoT infrastructure may contain additional smart devices. The security of transacted information in each device is critical because false data injection may lead to cascaded failures and probably a blackout in a wide area. An attack detection algorithm based on convergence properties and a mitigation algorithm based on consensus of beliefs were proposed to prevent false injection (Vukovic and Dán, 2014). A trust-based diffusion algorithm based on adaptive combination policy was implemented by excluding misconducting nodes from the infrastructure for secure state estimation (Cintuglu & Ishchenko, 2019).

The implementation of privacy and security backgrounds results in a functionality problem given that an IoT solution combines several components: user interface elements, embedded tools, cloud computing for data processing, tool control, and many others. A lightweight security solution that provides a solution for the authentication and permission mechanism even if an untrusted cloud is adapted for data processing and transmission was proposed in (Chifor, Bica, Patriciu, & Pop, 2018). It designs a federated permission concept, which is sufficient for a cloud solution that regulates the IoT node with the customer's consent. The security clarification described in this work may be combined in an existing software and hardware structure, needing lower expenses from the customer side. User-centric IoT was described as a system that associates objects and services with a primary effect on customers or through real circumstances (Akatyev & James, 2019). A unique categorization scheme was proposed for various IoT objects that almost approximates real-world situations.

A precise unified authentication concept, end-to-end authentication, principal agreement mechanism, public key infrastructure (PKI), wireless PKI, secure routing, and interruption detection should be established for several standards of interface structures (Alaba, Othman, Hashem, & Alotaibi, 2017). The authors in (Khan & Salah, 2018) categorized security threats into three types with regard to the deployment of IoT devices: low-level, medium-level, and high-level security concerns. The authors also discussed blockchain technology, which has been anticipated by the industry and research society as a disruptive technology that is assured to perform an essential function in regulating, controlling, and, most importantly, guarding IoT objects. Secure IoT was proposed in (Teixeira, Pereira, Wong, Nogueira, & Oliveira, 2019) to represent a concept of tainted flow analysis that determines which memory accesses need to be shielded during butter overflow attacks. For secure energy trading in different situations of industrial IoT such as vehicle-to-grid (V2 G), energy harvesting networks, and microgrids, a centralized energy blockchain based on consortium blockchain technology, was presented (Li et al., 2019). The IoT layers can be categorized into perception, network, and application layers in terms of security perspective. Several existing security mechanisms for these layers are summarized in Fig. 3. A detailed analysis of IoT-related security mechanisms in recently published research articles is presented in Table 1.

2.2. Bandwidth management

To deploy IoT in local microgrids, a large number of sensors have to be installed and a significant amount of information is communicated over 24 h for 365 days. Connecting all objects to the Internet is difficult because doing so would be expensive in terms of computation and bandwidth usage. To utilize the IoT system within smart microgrid systems, technologies such as sensor, communication, and data mining technologies should be considered because IoT devices have restricted features such as bandwidth, thus making IoT an inferior way to communicate all unregulated information. Information fusion technologies can be exploited to exchange valuable information (Shakerighadi, Anvari-Moghaddam, Vasquez, & Guerrero, 2018).

Narrowband IoT (NB-IoT) is the latest Long-Term Evolution (LTE) standard accredited by the Third Generation Partner Project (3 GPP) as one of the low-power wide area solutions to accomplish the goals of broad coverage, less power consumption, and cheap and bulky combination. A combination of characteristics, such as synchronization series, random access preface, telecast channel, and control channel, are transformed to be recognized with the LTE blueprint although NB-IoT reuses most LTE principles, such as orthogonal frequency division multiplexing type of modulation in downlink, single carrier frequency division multiple access in uplink, channel coding, rate matching, and interleaving (Xu et al., 2018). The bandwidth of some IoT protocols is listed in Table 2.

2.3. Interfacing interoperability

Interoperability is the feature of a product whose interfaces are completely understood to work with other products in terms of implementation or access without any restrictions. Interoperability can be categorized into user and device interoperability, as mentioned in Fig. 4.

Interoperability is required to fulfill certain objectives, such as the following:

- Physical objects can interact with other physical objects to share information.
- Any object can communicate with other objects at anytime from anywhere.
- Machine-to-machine (M2M), device-to-device (D2D), and device-to-machine communication.
- Smooth device integration with IoT networks.

Therefore, the energy system needs to be adequate to survive with heterogeneity to interact with grid patterns in an interoperable way. An energy system consists of heterogeneous energy resources, in which an EMS is responsible for interfacing interoperability (Vaccaro, Popov, Villacci, & Terzija, 2011). The authors in (Lee, Shi, Gadh, & Kim, 2016) proposed a microgrid platform that fulfills the interoperability criteria by interfacing energy services.

2.4. Connectivity issue

Connecting IoT devices to the network of millions of users simultaneously is an important issue for energy systems. The global Internet includes heterogeneous networks such as cellular networks, slow or fast connectivity, proxy servers or gateways, and firewalls, all of which can disrupt connectivity. Reliable bidirectional signaling is necessary for routing data between IoT devices to establish connectivity. Knowing immediately when the IoT device drops off the network and goes offline is essential.

Packet losses occur particularly because the structure of the distributed filter is interconnected. For microgrids with DERs, a distributed dynamic phase estimation technique was proposed in (Md, Xiang, & Wang, 2018), where the error function is rewritten using the matrix property of the Kronecker product. The authors in (Md, Xiang, Wang, & Jia, 2017) proposed a state estimation and stabilization method for microgrids by considering both input and output packet losses in IoT-enabled grid communication. They also proposed a

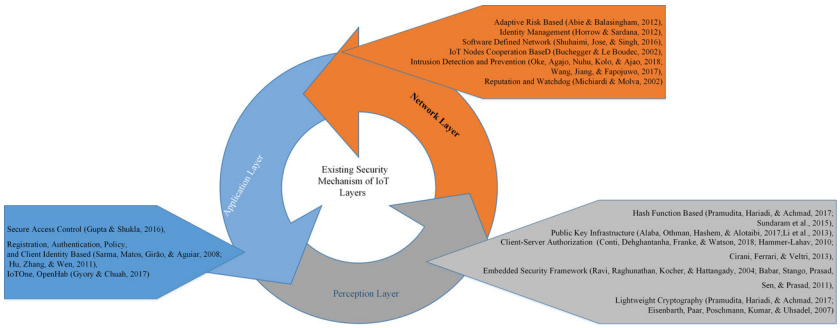

Fig. 3. Security mechanism of IoT layers Hammer-Lahav, 2010; Cirani, Ferrari, & Veltri, 2013; Ravi, Raghunathan, Kocher, & Hattangady, 2004; Babar, Stango, Prasad, Sen, & Prasad, 2011; Eisenbarth, Paar, Poschmann, Kumar, & Uhsadel, 2007; Buchegger & Le Boudec, 2002; Michiardi & Molva, 2002; Gupta & Shukla, 2016; Sarma et al., 2008Sarma, Matos, Girão, & Aguiar, 2008; Hu, Zhang, & Wen, 2011.

semidefinite programming-enabled state feedback controller for IoT-aided grid communication to regulate system states or to stabilize the system states within a short time.

2.5. Packet loss

The EMS is generally responsible for system state estimation to stabilize the grid. Several techniques were introduced in previous literature to estimate the system states, such as least mean squares (LMS), normalized LMS, variable step size-based LMS, artificial intelligence-based, and physical model-based Kalman filter (KF) method. All these methods assume that the communication channels between the distributed sources and the EMS are ideal or lossless. However, in reality, the channels are lossy.

The information signals of microgrid such as measurement or control signals are sometimes lost due to the factors involved in the lossy channel of IoT networks, such as network failure or delays, signal distortion or attenuation, and packet dropouts (Su & Chesi, 2015). A state feedback closed-loop controller based on semidefinite programming approach was proposed in (Md et al., 2017) to stabilize the system states. For optimal estimation of system states, the estimator was developed based on mean squared error (MSE). A modified estimation algorithm over LMS known as LMS fourth was developed to minimize the packet loss in IoT-based microgrid communication channels. This algorithm was named as such because it can minimize the fourth error function with respect to the predicted microgrid states (Md, 2019).

The IoT infrastructure has great potential for wireless power transfer (WPT) systems due to its broad connectivity, advanced sensing, and data processing technology (Lin et al., 2017). The IoT-based communication infrastructure was designed in (Md, Xiang, Wang, Li, & Choi, 2018) for WPT systems by using quantized binary phase shift keying technique. The state of the WPT system was estimated by KF and feedback controller. For WPT system state estimation and stabilization, the states were measured by the sensors in the IoT network. To avoid packet losses in channel coding-based IoT communication infrastructure, the MSE-based algorithm was used along with a semidefinite feedback controller (Md & Xiang, 2018).

2.6. Data processing

Traditional data handling methods are inappropriate for an IoT-based system because the latter deals with a large amount of information or big data. The IoT system should be able to accumulate and analyze data based on present and past information, which is one of the important challenges for IoT devices. Big data mechanisms have become a critical data analytics tool for critical decision making due to the expeditious development of IoT. Big data technologies have been applied in some specific domains, including energy system from many IoT domains by using a conceptual framework (Ge, Bangui, & Buhnova, 2018). A typical application of a cyber-physical system is the modern energy system, which is the combination of interdependent energy system and the communication networks. A localized data processing algorithm can be the solution for big data processing, where the network server and neighbor state are known by the devices to save network bandwidth (Stojmenovic, 2014). The concentrators deployed in field area networks (FANs) are responsible for data aggregation in smart grids (Niyato, Xiao, & Wang, 2011). The concentrator acts as a cluster to receive independent computation information from smart meters, combines them, and communicates the combined information to base station for data aggregation. The authors in (Akusok, Björk, Miche, & Lendasse, 2015) proposed a methodology for efficient utilization of extreme learning machine toolbox to solve the big data problem in terms of overhead reduction and fast file storage. The advanced methods with a specific architecture are required to solve the big data processing problem. Few toolboxes such as the toolbox in MATLAB can be used to deal with a large amount of information (Akusok et al., 2015; Baccarelli, Vinueza Naranjo, Scarpiniti, Shojafar, & Abawajy, 2017).

In modern energy systems, the advanced meter infrastructure (AMI) system is responsible for measurement, collection, and analysis of energy distribution and consumption information. It also establishes communication between the metering device and the utility server. An IoT-enabled smart metering energy system architecture that includes a big data platform was proposed in (Lloret, Tomas, Canovas, & Parra, 2016) for making critical decisions and providing communication in AMI systems.

3. IoT data protocols for energy systems

This section reviews the message transmitting protocols in the IoT session layer. Many Internet protocol applications, including IoT, use user datagram protocol (UDP) or transmission control protocol (TCP) for message transport. Some message distribution functions are common in IoT applications. These functions are also known as session layer or IoT data protocols.

- **Message queue telemetry transport (MQTT):** It is a lightweight message transport protocol used in conjunction with the TCP/IP protocol. MQTT provides connectivity among the middleware with applications on one side and networks with communications on the other side. The clients of this standard do not need to have known each other. The publish/subscribe model is sketched in Fig. 5. The MQTT protocol is an open standard and follows publish and subscribe pattern over TCP. Thus, the translation between HTTP and MQTT protocol is difficult to achieve (Collina, Corazza, & Vanelli-Coralli, 2012). A battery monitoring system was designed as a primary module to observe the operation and reliability of batteries in an IoT-enabled smart microgrid system. The speed of information communication and the authenticity of cloud connection can be increased with the help of the MQTT protocol (Friansa et al., 2017). Certain issues associated with the modern integrated energy storage system (ESS) in a smart grid, such as increased installation expenses and reduced administration performance, were analyzed in (Park, Kang, Choi, Jeon, & Park, 2018). The hardware was configured into a wireless interface based light-emitting diode system, MQTT

Table 1
Recent research on IoT-based security mechanisms.

Security issues	Objective	Advantage	Light weight (length/method)	Simulator/Analytical tool/Algorithm	Benchmark	Ref
Authentication, access control, confidentiality and integrity	Secure line communication for MG applications	Overcome security problems such as data confidentiality and integrity	Y (160 bits)	Raspberry Pi (Python 2.7), ECC, SHA-256	RSA (Rivest–Shamir–Adleman)	Pramudita, Hariadi, & Achmad (2017)
Authentication, trust	Management of IoT networks security from local IoT systems to the global Internet	Provides both IoT middleware and network security	Y (128 bits)	MobilityFirst Architecture (NCRS: Name Certificate & Resolution Service, GNRS: Global Name Resolution Service, IoT-NRS: IoT Name Resolution Service), mbed SSL (Polar SSL), AES Galois/Counter Mode	wolfSSL (CyaSSL)	Liu, Zhao, Li, Zhang, & Trappe (2017)
Privacy	To preserve user's location privacy	Less possibility of disclosing user's actual location and improved computational cost	Y (Adopt greedy method to select dummy locations)	DLP	Dummy location selection	Sun et al. (2017)
Data tampering, Data integrity	To detect and mitigate the attacked region of distributed power system	Faster detection and mitigation of strong attacks	NA	Belief consensus localization	IEEE 118 bus power system	Vukovic & Dán (2014)
Data tampering, Data integrity	Detection and isolation of misconducting nodes for MG networks	Fully distributed solution for prohibiting disobedient nodes in MGs and ensuring lower MSE and faster convergence	NA	Micro SCADA, trust-based diffusion algorithm	Consensus algorithm	Cintuglu & Ishchenko (2019)
Authentication	Secure IoT nodes that are connected to untrusted cloud	Integrable with earlier existing hardware and software infrastructure, Cost-efficient	Y (key length not available)	Fast Identity Online protocol, Kaa cloud platform, CoAP, ECC	EAP-NOOB (Extensible Authentication Protocol-Nimble Out Of Band)	Chifor et al. (2018)
Authentication, Privacy	Secure P2P energy trading in MGs, energy harvesting networks, V2 G	credit-based payment scheme, fast and frequent energy trading	NA	Consortium blockchain technology, Stackelberg game model	Traditional blockchain technology	Li et al. (2019)
Authentication, confidentiality and integrity	Improve security in smart home	Free from weak keys, highly secure, fast, and efficient	Y (128 bits)	Hash function-based, RC 4	RC 5, Skipjack, AES	Sundaram et al. (2015)
Authentication, access control	To overcome security problems at perception layer	Simple security mechanism	N (2048 bits)	PKI security protocol, RSA encryption	TCP/IP	Li et al. (2013)
Privacy	To design a risk-based security framework for IoT to predict and estimate destruction	Improve security level by adjusting dynamic changing states of IoTs	NA	Game theory, Context awareness technique	Case study validation	Abie & Balasingham (2012)
Authentication	To design an identity management framework for cloud-based IoT	Unique identification of cloud-based devices	NA	Publisher-Subscriber approach, Cloud-based IoT	Traditional IoT	Horrow & Sardana, (2012)
Data integrity, trust, privacy	To increase network performance and security in IoT and decrease hardware requirement	Reduced cost and hardware	NA	Software-defined network, cluster head selection process	Traditional devices (switches, routers)	Shuhaimi, Jose, & Singh (2016)
Authentication, confidentiality, and integrity	To develop a multilevel malicious node detection system	Better detection accuracy	NA	MATLAB, Trust value computation algorithm	Conventional encryption	Oke, Agajo, Nuhu, Kolo, & Ajao (2018)
Authentication, confidentiality, and integrity	To develop a protocol layer malicious node detection system	Effective cross-layer attack detection	NA	MATLAB, t-distribution	NBBTE (node behavioral banding belief theory of trust evaluation)	Wang, Jiang, & Fapojuwo (2017)
Authentication, access control	Secure smart things in IoT framework and to overcome limited device compatibility issue	Supports heterogeneous devices, both user- and developer-friendly	NA	Raspberry Pi, IoTOne web application	openHab	Gyory & Chuah (2017)

Table 2
Bandwidth of IoT protocols.

IoT Protocols	Bandwidth
IEEE 802.15.4	2 MHz
Zigbee	3 MHz
Z-Wave	300 kHz/400 kHz
WirelessHART	2 MHz
Sigfox	100 Hz
LoRa	125 kHz
NB-IoT (LTE Cat-NB1)	180 kHz
eMTC (LTE Cat-M1)	1.08 MHz
LTE Cat-1	20 MHz
EC-GSM-IoT	200 kHz

gateway, ESS and ESS controller, an inverter, and single-mode power supply for bidirectional power supply.

- **Constrained application protocol (CoAP):** It is a session layer protocol implemented by the Internet Engineering Task Force to provide a lightweight HTTP interface. CoAP is based on the request–response model between end users. Four messaging modes of this standard based on request–response model are presented in Fig. 6. Client–server interaction is asynchronous over a transport protocol such as UDP.

It is basically designed for M2M applications such as smart energy and home automation. The authors in (Sun & Ansari, 2018) proposed the application of CoAP publish/subscribe to achieve IoT resource caching and demonstrated that caching the IoT devices in the broker is not the better option to conserve the energy of the servers and minimize the mean delay to declare the contents of the devices. As the topology of both CoAP and HTTP is request/response, the mapping in between them is direct. Generally, a small area of IoT protocols such as MQTT and CoAP facilitates the integration of the devices with the Internet (Caballero, Vernet, Zaballos, & Corral, 2018). For smart grid, UDP-based transport protocol such as CoAP can be used, which has the advantages of interoperability with the HTTP protocol (Kayastha, Niyato, Hossain, & Han, 2014).

- **Extensible messaging and presence protocol (XMPP):** XMPP is a data standard that includes open source moment carrier standards, client, and server based on Extensible Markup Language. Different standards such as IEC 61,850 and OpenADR 2.0b have been described for the transmissions between EMS and distribution system operator/aggregator to assure interoperability. XMPP is one of the application layer standards of OpenADR 2.0b and IEC 61,850, because it provides a warning system in which a control mechanism containing information to be observed can transmit a message to a distant object (Okuno et al., 2016). An IoT system based on the requirements of the universal IoT home gateway using XMPP was designed and performed in a testbed for energy management applications in smart grid (Viswanath et al., 2016). The service interface function blocks for XMPP provide the decentralized control applications, which utilize the XMPP protocol to replace all the information related to control in smart grids, accomplished with the cooperation of IEC 61,499 reference models (Veichtlbauer, Parfant, Langthaler, Filip, and Strasser (2016). The advantages and disadvantages of several middleware were identified in (Petersen, Bindner, Poulsen, & You, 2017), which presented better options for web services and XMPP for smart grid applications.
- **Advanced message queuing protocol (AMQP):** It can be considered as the protocol that ensures that data are securely transmitted among applications, organizations, mobile infrastructures, and beyond the cloud. AMQP is also suitable for information communication due to its security feature, because encryption is based on either transport layer service or simple authentication and security layer. An intermediate entity consists of web application and AMQP protocol is stationed in most public buildings of the city to transmit and receive data from hardware components such as smart meters (Rodríguez-Molina, Martínez, Castillejo, & Rubio, 2017).

4. IoT wireless communication protocol for energy system

The connectivity protocols or communication protocols of IoT are reviewed in this section and summarized in Table 3. It includes the physical layer and the media access control layer protocols, which are combined by most IoT standards.

- **Zigbee:** It is a compact-range, low-power, and low-information-speed wireless communication protocol based on the IEEE 802.15.4 protocol, which may be used extensively in home or building

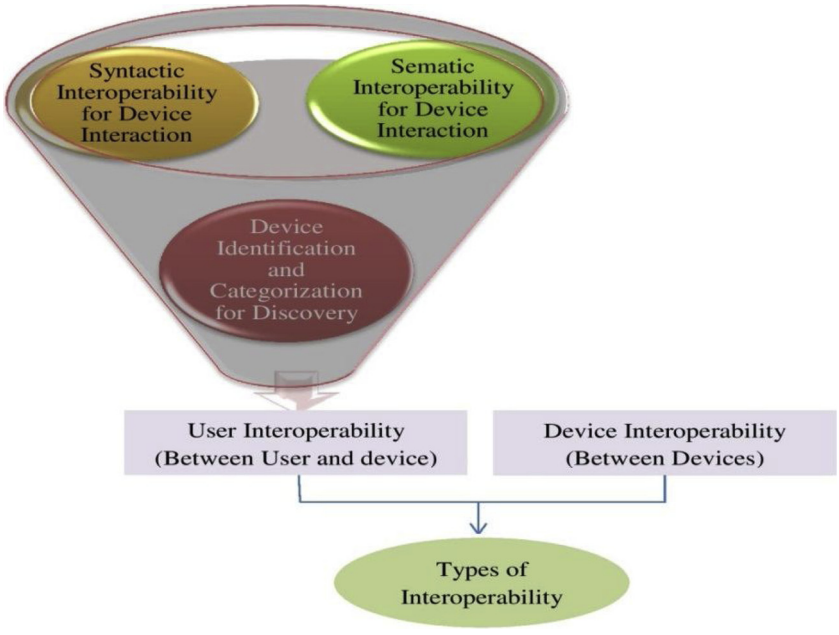

Fig. 4. Types of interoperability.

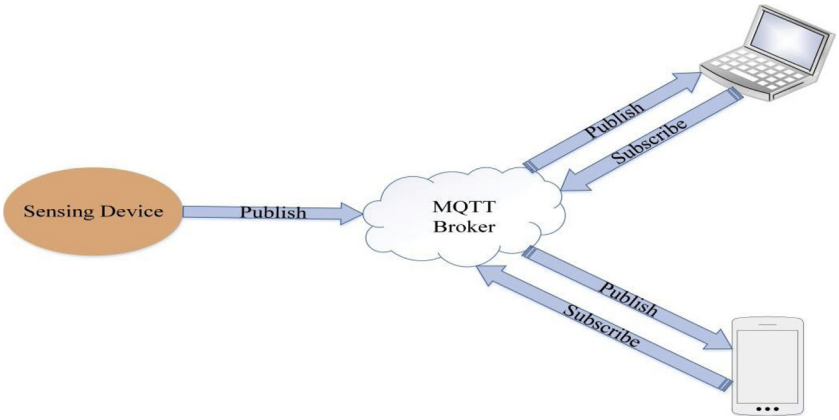

Fig. 5. MQTT publish/subscribe model.

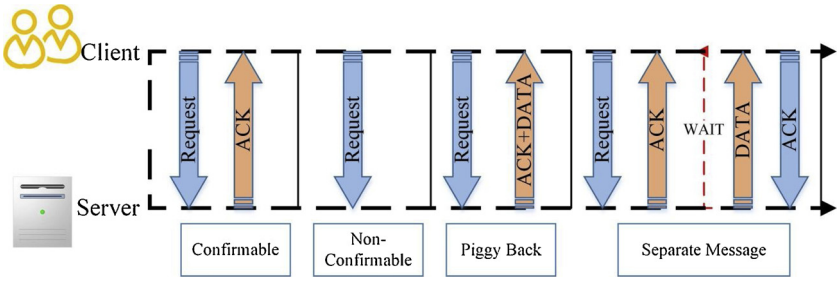

Fig. 6. CoAP messaging modes of the request–response model.

automation, industrial control, healthcare, remote control, and consumer electronics. The applicability of the Zigbee standard for smart grid was investigated by considering the monitoring and regulating information requirement of the smart grid. Zigbee is not limited to home area networks (HANs) only because smart grid AMI, advanced distribution operation, advanced asset management, and advanced transmission operation can implement a comprehensive application area for Zigbee (Zhang, Sun, & Cui, 2010). The authors in (Setiawan, Shahnia, Rajakaruna, & Ghosh, 2015) proposed a Zigbee-based communication system that communicates different electrical parameters such as voltage, frequency, active or reactive power, and circuit breaker status between the local controller and the microgrid central controller.

An efficient Zigbee-based building energy monitoring and control system may be adapted for monitoring of energy consumption and planning for long-term preservation of energy, which is an extension of automated energy storage for building applications (Peng & Qian, 2014). The performance of Zigbee for smart grid applications in HANs, neighborhood area networks (NANs), and wide area networks (WAN) are evaluated; findings showed that Zigbee can be implemented at any certain layer with proper topology (Mulla, Baviskary, Kaziz, & Wagh, 2014). The performance of Zigbee was evaluated for indoor power control room, underground interface transformer vaults, and an outdoor 500 kV substation context concerning energy consumption, end-to-end delay, packet transmission rate, and network throughput (Bilgin & Gungor, 2012).

- **Z-Wave:** It is a low-power wireless communication technology that is generally used for home automation. The major advantages of this

Table 3
Comparison of IoT wireless communication standards.

Standard/ protocol	Frequency	Data rate	Modulation	Range	**Power usage**	**cost**
Zigbee	868 MHz –Europe 915 MHz–USA and Australia 2.4 GHz –Worldwide	20 Kbps 40 Kbps 250 Kbps	BPSK BPSK O-QPSK	10–100 m, 1600 m	Low	Med.
Z-Wave	865.2 MHz–India; 868.1 MHz–Malaysia; 919.8, 921.4 MHz–Australia, Brazil, New Zealand; 868.4,869.85 MHz–EU, Singapore, SA, UAE; 908.4, 916 MHz–USA, Canada, Chile, Mexico	9.6 Kbps 40 Kbps 100 Kbps	FSK FSK GFSK	30 m–indoor, 100 m–outdoor	Low	Med.
Wireless HART	2.4 GHz	250 Kbps	O-QPSK	100 m	Med.	Med.
SigFox	868–868.2 MHz–Europe, 902–928 MHz–rest of the world	10–1000 bps	PSK-UL, GFSK-DL	30–50 km: Rural, 3–10 km: Urban	Low	Med.
LoRa	867–869 MHz–Europe; 902–928 MHz–North America; 470–510, 779–787 MHz–China; 920–925 MHz–Korea, Japan; 865–867 MHz–India	290 bps-50 Kbps	SS Chirp	< 15 km	Low	Med.
NB-IoT eMTC EC-GSM-IoT	Cellular (LTE band)	250 Kbps 1 Mbps 0.47–2 Mbps	QPSK QPSK, 16QAM	< 35 km Several miles Several miles	Med.	High

protocol are its simple structured command and its freedom from interference due to household, low bandwidth, and IP support. Z-wave automatically routes information between several nodes with the help of its controller and slave type devices. (Mahmood, Javaid, & Razzaq, 2015). A Z-wave smart plug was employed to remotely monitor and control the energy expenditure of several devices in the HAN (Tushar et al., 2016). The energy consumption of several devices was monitored in real time and the data were sent instantaneously to the unified home gateway via Z-wave communication protocol.

- **WirelessHART:** It is a multi-hop mesh network-based protocol designed for industrial control and monitoring applications. It uses 128-bit Advanced Encryption Standard (AES) encryption technology for security, Direct Sequence Spread Spectrum, and Time Division Multiple Access technique, in which 10 ms time slots are allotted to the nodes. The devices connected to this communication protocol should have routing capability because it does not give any directive about the configuration of the network by a network manager (Chhaya, Sharma, Bhagwatikar, & Kumar, 2017). An industry infrastructure demonstration system for demand response in smart grids was developed by using WirelessHART and International Society of Automation (ISA) 100.11a standard protocols (Alam et al., 2014).
- **ISA 100.11a:** The ISA 100.11a is mainly designed for large-scale industrial plants to support native and tunneled application layers. It supports twin data security schemes at each node. The data link layer encrypts each hop and the transport layer secures P2P communication. ISA 100.11a can establish the communication path used for sensors installed in power plants to monitor generation systems (Liu, 2012).
- **LoRa and Sigfox:** These wide-range, low-power-consumption information communication protocols are widely applied in IoT systems due to the availability of free licensed frequency range. Ultra-narrowband technology was used in the Sigfox protocol for long-distance data transmission (Reynders, Meert, & Pollin, 2016). Long range (LoRa) can be used for bidirectional communication and for grid monitoring. Sigfox and LoRa are generally similar, except Sigfox requires more network density than LoRa (Lauridsen et al., 2017). Sigfox is extensively used in isolated devices that require the transfer of an inadequate amount of information (Sundaram, Ramnath, Prasanth, & Varsha Sundaram, 2015).
- **Cellular:** Cellular networks can establish a wide area communication path between several IoT devices of the distribution grid because of its licensed frequency bands, wide area coverage, high data rate, high system reliability, and low latency. The transition of the mobile cellular technology from 2 G, 3 G, 4 G, and toward 5 G is giving rise to a powerful communication platform for data sensing, communication, storage, and processing. The emerging mobile cellular interface of 5 G along with its M2M communication progression and the idea of mobile edge computing enable a distributed monitoring and control environment in smart grids (Cosovic, Tsitsimelis, Vukobratovic, Matamoros, & Antón-Haro, 2017). The 3 GPP standard provides radio interface enhancements for machine-type communication (MTC), which have been adopted recently in the 3 GPP LTE Release 13. Three techniques were introduced in this release for MTC services: enhanced MTC (eMTC), NB-IoT, and extended-coverage GSM IoT (EC-GSM-IoT). These techniques offer fast uplink access and reduced LTE scheduling period and processing time.

A latency reduction mechanism can also be achieved by the semi-persistent scheduling protocol, which is based on conditional transmission and data availability. It is currently under discussion for 3 GPP Release 14 standards (Qi, Quddus, Imran, & Fazolli, 2015). Cellular communication protocols establish a promising communication path within NANs for the accomplishment of the smart grid between other available dilemmas. LTE D2D will enable applications such as distributed microgrid management, active demand response services, and automation of smart substation in future because these are not realizable with current cellular technology (Kalalas, Thrybom, & Alonso-Zarate, 2016).

The IPV6-based low-power wireless personal area network (6LoWPAN) can be used for small devices with limited processing. It is a combination of the IEEE 802.15.4 standard and IPV6 and is used for low-power lossy networks. A demand response-based EMS that includes energy storage, monitoring, and control systems and a PV panel was proposed in (Wei, Hong, & Alam, 2016) for industrial users with the help of the 6LoWPAN-based wireless communication protocol.

5. Future paths for the suitability of IoT wireless communication technologies of energy systems

The wireless IoT connectivity technologies are compared and represented in Table 2. The communication infrastructure in the energy system can be categorized into three architecture layers: HAN/building area network (BAN)/industrial area network (IAN), NAN/FAN, and WAN. All the layers along with data rate, communication range, and the possible IoT communication protocols of respective layers based on

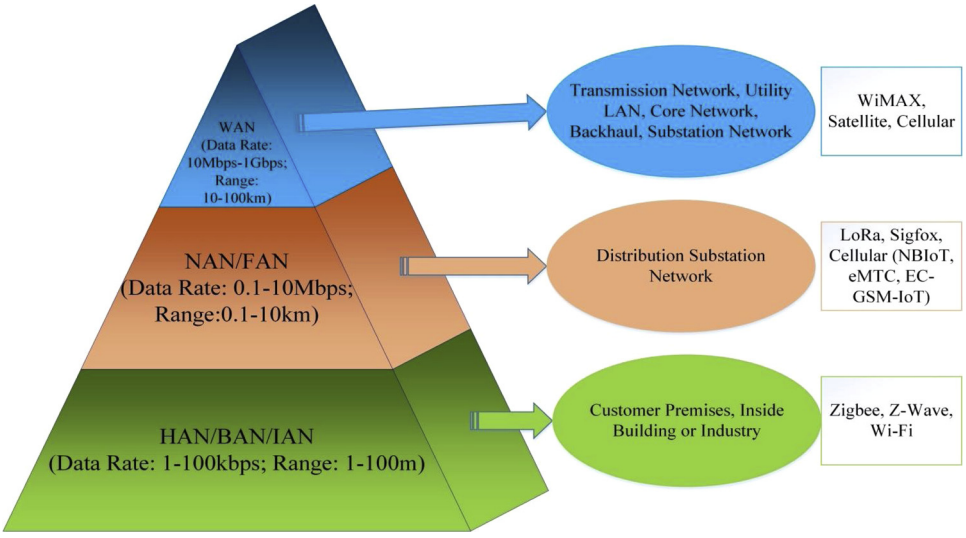

Fig. 7. Multilayer communication architecture of energy system.

Table 4
Wireless communication standards requirement for different applications.

Applications in modern energy system	IoT wireless communication protocols					
	Zigbee	Z-Wave	LoRa	NB-IoT	WiMAX	Satellite
Home automation	√	√	X	X	X	X
On-demand/multi-interval meter reading	X	X	X	√	√	X
Load/demand response management	X	X	√	√	√	X
RTP/CPP/TOU pricing	X	X	√	√	√	X
Grid-to-vehicle (G2V)	X	X	√	√	√	X
Vehicle-to-grid (V2 G)	X	X	√	√	√	X
Distribution energy resources	X	X	√	X	√	X
Distribution automation	X	X	X	X	√	X
Synchrophasor measurement	X	X	X	X	√	X
Long-haul communication for data aggregation	X	X	X	X	√	√

Table 3 are presented in Fig. 7.

A HAN is a dedicated network that connects various household devices such as smart appliances to the energy system via a smart metering system. It uses the IPV4 addressing scheme and contains a turnkey reference system design to control and monitor networks. A network architecture like HAN/BAN/IAN may establish the communication path between end users and NAN/FAN architecture. BAN and IAN are considered more complicated networks than HAN because these may combine specialized local area network, control devices, and building management software. The main connectivity requirements are less power consumption, optimum cost, and secure transmission for services such as demand response, real-time price, load control, and information message. Generally, these services require a data rate of less than 100 kbps and a coverage range of up to 100 m. Thus, wireless communication protocols such as Zigbee, Z-wave, and WiFi are the most suitable protocols for this network layer.

The NAN/FAN is basically a distribution substation network that facilitates the communication flow between HAN and the utility grid. The main design requirements for the NAN/FAN architecture are reliability, scalability, real-time capability, security, throughput, and economy. It may support services such as distribution automation, load management, and other customer related applications. The coverage area for this type of network is between 100 m to 10 km, and the required data rate is typically 100 kbps to 10 Mbps. Low-power WAN wireless protocols such as LoRa, Sigfox, and 3 GPP-based cellular protocols such as NB-IoT, eMTC, and EC-GSM-IoT may be used in this type of network layer.

WAN enables a communication link for the core network and covers remote ranges from the control center to NAN. Real-time computations are obtained at the transmission network and transferred to the controller when a controller is located at a distance from the transmission network through WANs. It provides the communication with distribution and automation devices, phasor measurement unit, and remote terminal unit for services such as demand response, load management, and field device automation. Cellular, WiMAX, and satellite communication protocols may be suitable for this type of network due to the high data rate and wide geographical area coverage.

Several applications of modern energy systems have certain requirements for communication. The modern energy system applications belong to the three-layer network architecture, as presented in Fig. 7, and can thus be compared with IoT wireless communication standards based on data rate and coverage area presented in Table 3. Some applications with the required IoT wireless communication protocols are summarized in Table 4.

The 6LoWPAN wireless communication standards can be utilized more to implement real-time energy management systems, including ones for renewable sources such as solar panels and wind turbines, by taking the advantages of IPV6 integrated with IEEE 802.15.4.

6. Conclusion

The IoT technology enables the connectivity of many objects from anywhere at any time. It helps energy systems in monitoring, computing, and controlling the grid through IoT objects such as sensors and actuators. The connectivity, automation, and tracking of IoT objects improve several network functions during utilization, distribution, transmission, and power generation of the energy system. Furthermore, IoE can help countries manage their energy demand by enabling generating stations to generate more electricity during peak times and less during times with low consumption requirements. The adoption of this technology may help countries prevent power blackouts.

Several challenges and issues, such as security, interoperability, efficient bandwidth utilization, connectivity issue, and big data processing, are presented in this paper. An IoT-aided energy system may generate a large amount of information; thus, the suitability of some existing IoT-supported devices message protocols and wireless connectivity or communication protocols is assessed. This paper reviewed important applications of the current IoT connectivity standard infrastructure, including non-cellular LPWA standards such as LoRa, Sigfox, and cellular LPWA or 3 GPP technologies such as NB-IoT, eMTC, and EC-GSM-IoT. The suitability of the wireless communication standards of IoT in the multilayer network architecture and several applications of energy system was outlined. A sustainable IoT-based energy system still faces many serious and unavoidable challenges and issues. To enhance related knowledge and provide guidance for future research, we outlined some identified issues and options for refinement.

Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

Abie, H., & Balasingham, I. (2012). Risk-based adaptive security for smart IoT in eHealth. *Proceedings of the 7th International Conference on Body Area Networks, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)* (pp. 269–275).

Akatyev, N., & James, J. I. (2019). Evidence identification in IoT networks based on threat assessment. *Future Generation Computer Systems, 93*, 814–821.

Akusok, A., Björk, K.-M., Miche, Y., & Lendasse, A. (2015). High-performance extreme learning machines: A complete toolbox for big data applications. *IEEE Access, 3*, 1011–1025.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.

Alam, M., Kim, J., Li, Y.i-C., Hong, S. H.o., Li, X., & Aidong, X. (2014). Implementation of wireless industrial networks for industrial smart grids. *International Conference on Advances in Energy Conversion Technologies (ICAECT)*.

Amrr, S. M., Alam, M. S., Jamil Asghar, M. S., & Ahmad, F. (2018). Low cost residential microgrid system based home to grid (H2G) back up power management. *Sustainable Cities and Society, 36*, 204–214.

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (IoT). *2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*.

Baccarelli, E., Vinueza Naranjo, P. G., Scarpiniti, M., Shojafar, M., & Abawajy, J. H. (2017). Fog of everything: Energy-efficient networked computing architectures, research challenges, and a case study. *IEEE Access, 5*, 9882–9910.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. *The European Physical Journal Special Topics, 214*, 481–518.

Bekara, C. (2014). Security issues and challenges for the IoT based smart grid. *Procedia Computer Science, 34*, 532–537.

Bilgin, B. E., & Gungor, V. C. (2012). Performance evaluations of ZigBee in different smart grid environments. *Computer Networks, 56*, 2196–2205.

Buchegger, S., & Le Boudec, J.-Y. (2002). Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness In Dynamic Ad-hoc NeTworks). *Proceedings*

of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (pp. 226–236).
Caballero, V., Vernet, D., Zaballos, A., & Corral, G. (2018). Prototyping a web-of-energy architecture for smart integration of sensor networks in smart grids domain. *Sensors, 18*(400), 1–25.
Chhaya, L., Sharma, P., Bhagwatikar, G., & Kumar, A. (2017). Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. In: *Electronics, 6*(5), 1–22.
Chifor, B.-C., Bica, I., Patriciu, V.-V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems, 86*, 740–749.
Cintuglu, M. H., & Ishchenko, D. (2019). Secure distributed state estimation for networked microgrids. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2019.2902793.
Cirani, S., Ferrari, G., & Veltri, L. (2013). Enforcing security mechanisms in the IP-Based internet of things: An algorithmic overview. *Algorithms, 6*, 197–226.
Collina, M., Corazza, G. E., & Vanelli-Coralli, A. (2012). Introducing the QEST broker: Scaling the IoT by bridging MQTT and REST. *23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*.
Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.
Cosovic, M., Tsitsimelis, A., Vukobratovic, D., Matamoros, J., & Antón-Haro, C. (2017). 5G mobile cellular networks: Enabling distributed state estimation for smart grids. *IEEE Communications Magazine, 55*(10), 62–69.
Eisenbarth, T., Paar, C., Poschmann, A., Kumar, S., & Uhsadel, L. (2007). A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers, 24*(6), 522–533.
Friansa, K., Haq, I. N., Santi, B. M., Kurniadi, D., Leksono, E., & Yuliarto, B. (2017). Development of battery monitoring system in smart microgrid based on internet of things (IoT). *Procedia Engineering, 170*, 482–487.
Ge, M., Bangui, H., & Buhnova, B. (2018). Big data for internet of things: A survey. *Future Generation Computer Systems, 87*, 601–614.
Guan, Y., Vasquez, J. C., & Guerrero, J. M. (2017). An enhanced hierarchical control strategy for the internet of things-based home scale microgrid. *IEEE 26th International Symposium on Industrial Electronics (ISIE)*.
Gupta, K. K., & Shukla, S. (2016). Internet of things: Security challenges for next generation networks. *1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)*.
Gyory, N., & Chuah, M. (2017). IoTOne: Integrated platform for heterogeneous IoT devices. *International Conference on Computing, Networking and Communications (ICNC)*.
Hammer-Lahav, E. (2010). The OAuth 1.0 protocol. *Internet Engineering Task Force (IETF)*.
Hirsch, A., Parag, Y., & Guerrero, J. (2018). Microgrids: A review of technologies, key drivers, and outstanding issues. *Renewable and Sustainable Energy Reviews, 90*, 402–411.
Horrow, S., & Sardana, A. (2012). Identity management framework for Cloud based internet of things. *Proceedings of the First International Conference on Security of Internet of Things* (pp. 200–203).
Hu, C., Zhang, J., & Wen, Q. (2011). An identity-based personal location system with protected privacy in IOT. *4th IEEE International Conference on Broadband Network and Multimedia Technology*.
Husein, M., & Chung, I.-Y. (2018). Optimal design and financial feasibility of a university campus microgrid considering renewable energy incentives. *Applied Energy, 25*, 273–289.
Kalalas, C., Thrybom, L., & Alonso-Zarate, J. (2016). Cellular communications for smart grid neighborhood area networks: A Survey. *IEEE Access: Practical Innovations, Open Solutions, 4*, 1469–1493.
Kayastha, N., Niyato, D., Hossain, E., & Han, Z. (2014). Smart grid sensor data collection, communication, and networking: A tutorial. *Wireless Communications and Mobile Computing, 14*, 1055–1087.
Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.
Ku, T.-Y., Park, W.-K.i, & Choi, H. (2017). IoT energy management platform for MicroGrid. *IEEE 7th International Conference on Power and Energy Systems (ICPES)*.
Kul, B., & Şen, M. (2017). Energy saving IoT-based advanced load limiter. In: *Proc. XXVI International Scientific Conference Electronics-ET2017*.
Lauridsen, M., Nguyen, H., Vejlgaard, B., Kovacs, I. Z., Mogensen, P., & Sorensen, M. (2017). Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area. *IEEE 85th Vehicular Technology Conference (VTC Spring)*.
Lee, E.-K., Shi, W., Gadh, R., & Kim, W. (2016). Design and implementation of a microgrid energy management system. *Sustainability, 8*(1143), 1–19.
Lezama, F., Palominos, J., guez-Gonzalez, A. Y. R., Farinelli, A., & Munoz de Cote, E. (2017). Optimal scheduling of on/off cycles: A decentralized IoT-Microgrid Approach. *Applications for future Internet, 179*, 79–90.
Li, Z., Yin, X., Geng, Z., Zhang, H., Li, P., Sun, Y., et al. (2013). Research on PKI-like protocol for the internet of things. *Fifth Conference on Measuring Technology and Mechatronics Automation*.
Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2019). Consortium Blockchain for secure energy trading in Industrial IoT. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2017.2786307.
Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*(5), 1125–1142.
Liu, Y. (2012). Wireless sensor network applications in smart grid: Recent trends and challenges. *International Journal of Distributed Sensor Networks, 2012*, 1–8.
Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A security framework for the internet of things in the future internet architecture. *Future Internet, 9*(27).
Lloret, J., Tomas, J., Canovas, A., & Parra, L. (2016). An integrated IoT architecture for smart metering. *IEEE Communications Magazine, 54*(12), 50–57.
Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the internet of things. *Future Generation Computer Systems, 75*, 46–57.
Mahmood, A., Javaid, N., & Razzaq, S. (2015). A review of wireless communications for smart grid. *Renewable and Sustainable Energy Reviews, 41*, 248–260.
Majee, A., & Gnana Swathika, O. V. (2017). IoT based reconfiguration of microgrids through an automated Central protection Centre. *International Conference on Power and Embedded Drive Control (ICPEDC)*.
Md, M. R., & Xiang, W. (2018). IoT communications network for wireless power transfer system state estimation and stabilization. *IEEE Internet of Things Journal, 5*(5), 4142–4150.
Md, M. R., Xiang, W., Wang, E., & Jia, M. (2017). IoT infrastructure and potential application to smart grid communications. *IEEE Global Communication Conference (GLOBECOM 2017)*.
Md, M. R., Xiang, W., & Wang, E. (2018). IoT-based state estimation for microgrids. *IEEE Internet of Things Journal, 5*(2), 1345–1346.
Md, M. R., Xiang, W., Wang, E., Li, X., & Choi, B. J. (2018). Internet of things infrastructure for wireless power transfer systems. *IEEE Access : Practical Innovations, Open Solutions, 6*, 19295–19303.
Md, M. R. (2019). Least mean square fourth based microgrid state estimation algorithm using the internet of things technology. *PloS One, 12*(5), e0176099.
Michiardi, P., & Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Advanced Communications and Multimedia Security, 100*, 107–121.
Moslehi, K., & Ranjit Kumar, A. B. (2019). Autonomous resilient grids in an IoT landscape vision for a nested transactive grid. *IEEE Transactions on Power Systems*. https://doi.org/10.1109/TPWRS.2018.2810134.
Mulla, A. Y., Baviskary, J. J., Kaziz, F. S., & Wagh, S. R. (2014). Implementation of ZigBee/802.15.4 in smart grid communication and analysis of power consumption: A case study. *Annual IEEE India Conference (INDICON)*.
Niyato, D., Xiao, L., & Wang, P. (2011). Machine-to-machine communications for home energy management system in smart grid. *IEEE Communications Magazine, 49*(4), 53–59.
Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G., & Ajao, L. A. (2018). Two layers trust based intrusion prevention system for wireless sensor networks. *Advances in Electrical and Telecommunication Engineering, 1*, 23–29.
Okuno, Y., Arai, Y., Hoshi, Y., Henmi, H., Otani, T., & Ohba, E. (2016). XMPP-based energy management system architecture for communications systems. *IEEE International Telecommunications Energy Conference (INTELEC)*.
Orlhac, M. (2019). *Sustainable cities–Making cities smarter*. Norway: International Student Energy Summit (ISES 2013). https://www.slideshare.net/studentenergy/ises-2013-day-3-michel-orlhac-vice-president-schneiderelectric-sustainable-cities.
Padmanathan, K., Govindarajan, U., Ramachandaramurthy, V. K., Rajagopalan, A., Pachaivannan, N., Sowmmiya, U., et al. (2019). A sociocultural study on solar photovoltaic energy system in India: Stratification and policy implication. *Journal of Cleaner Production, 216*, 461–481.
Park, S., Kang, B., Choi, M.-in, Jeon, S., & Park, S. (2018). A micro-distributed ess-based smart LED streetlight system for intelligent demand management of the micro-grid. *Sustainable Cities and Society, 39*, 801–813.
Peng, C., & Qian, K. (2014). Development and application of a ZigBee-Based building energy monitoring and control system. *Thee Scientific World Journal, 2014*, 1–13.
Petersen, B., Bindner, H., Poulsen, B., & You, S. (2017). Smart grid communication comparison: Distributed control middleware and serialization comparison for the internet of things. *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*.
Pramudita, R., Hariadi, F. I., & Achmad, A. S. (2017). Development of IoT authentication mechanisms for microgrid applications. *2017 International Symposium on Electronics and Smart Devices (ISESD)*.
Qi, Y., Quddus, A. U., Imran, M. A., & Fazolli, R. T. (2015). Semi-persistent RRC protocol for machine-type communication devices in LTE networks. *IEEE Access : Practical Innovations, Open Solutions, 3*, 864–874.
Raju, L., Gokulakrishnan, S., Muthukumar, P. R., Jagannathan, S., & Morais, A. A. (2017). IOT based Autonomous demand Side management of a micro-grid using arduino and multi agent system. *International Conference on Power and Embedded Drive Control (ICPEDC)*.
Ravi, S., Raghunathan, A., Kocher, P., & Hattangady, S. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems, 3*(3), 461–491.
Reynders, B., Meert, W., & Pollin, S. (2016). Range and coexistence analysis of long range unlicensed communication. *23rd International Conference on Telecommunications (ICT)*.
Rodríguez-Molina, J., Martínez, J.-F., Castillejo, P., & Rubio, G. (2017). Development of middleware applied to microgrids by means of an open source enterprise service bus. *Energies, 10*(172), 1–50.
Sarma, A., Matos, A., Girão, J., & Aguiar, R. L. (2008). Virtual identity framework for telecom infrastructures. *Wireless Personal Communications, 45*(4), 521–543.
Setiawan, M. A., Shahnia, F., Rajakaruna, S., & Ghosh, A. (2015). ZigBee-based communication system for data transfer within future microgrids. *IEEE Transactions on Smart Grid, 6*(5), 2343–2355.
Shakerighadi, B., Anvari-Moghaddam, A., Vasquez, J. C., & Guerrero, J. M. (2018). Internet of things for modern energy systems: State-of-the-art, challenges, and open issues. *Energies, 11*(1252), 1–23.
Shuhaimi, F. A. L., Jose, M., & Singh, A. V. (2016). Software defined network as solution to overcome security challenges in IoT. *5th International Conference on Reliability,*

Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).
Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society, 38*, 697–713.
Stojmenovic, I. (2014). Machine-to-Machine Communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. *IEEE Internet of Things Journal, 1*(2), 122–128.
Su, L., & Chesi, G. (2015). *On the robust stability of Uncertain discrete-Time networked control systems over fading channels.* Chicago, USA: American Control Conference (ACC) July.
Sun, X., & Ansari, N. (2018). Dynamic resource caching in the IoT application layer for smart cities. *IEEE Internet of Things Journal, 5*(2), 606–613.
Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., et al. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *Journal of Network and Computer Applications, 89*, 3–13.
Sundaram, B. V., Ramnath, M., Prasanth, M., & Varsha Sundaram, J. (2015). Encryption and hash based security in internet of things. *3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*.
Teixeira, F. A., Pereira, F. M. Q., Wong, H.-C., Nogueira, J. M. S., & Oliveira, L. B. (2019). SIoT: Securing Internet of Things through distributed systems analysis. *Future Generation Computer Systems, 92*, 1172–1186.
Trappe, W., Howard, R., & Moore, R. S. (2015). Low-energy security: Limits and opportunities in the internet of things. *IEEE Security & Privacy, 13*(1), 14–21.
Tushar, W., Yuen, C., Chai, B., Huang, S., Wood, K. L., Kerk, S. G., et al. (2016). Smart grid testbed for demand focused energy management in end user environments. *IEEE Wireless Communications, 23*(6), 70–80.
Vaccaro, A., Popov, M., Villacci, D., & Terzija, V. (2011). An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification. *IEEE Proceedings, 99*(1), 119–132.
Vasquez, J., Guerrero, J. M., miret, J., castilla, M., & garci´a de vicun, L. (2010). Hierarchical control of intelligent microgrids. *IEEE Industrial Electronics Magazine* (pp. 23–29).
Veichtlbauer, A., Parfant, M., Langthaler, O., Filip, P. A., & Strasser, T. (2016). *Evaluating XMPP communication in IEC 61499-based distributed energy applications.* Berlin, Germany, Sep..
Viswanath, S. K., Yuen, C., Tushar, W., Li, W.-T., Wen, C.-K., Kun, H., et al. (2016). System design of the internet of things for residential smart grid. *IEEE Wireless Communications, 23*(5), 90–98.
Vukovic, O., & Dán, G. (2014). Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks. *IEEE Journal on Selected Areas in Communications, 32*(7), 1500–1508.
Wang, J., Jiang, S., & Fapojuwo, A. O. (2017). A protocol layer trust-based intrusion detection scheme for wireless sensor networks. *Sensors, 17*(1227).
Wei, M., Hong, S. H., & Alam, M. (2016). An IoT-based energy-management platform for industrial facilities. *Applied Energy, 164*, 607–619.
Xu, J., Yao, J., Wang, L., Ming, Z., Wu, K., & Chen, L. (2018). Narrowband internet of things: Evolutions, technologies and open issues. *IEEE Internet of Things Journal, 5*(3), 1449–1462.
Zhang, Q., Sun, Y., & Cui, Z. (2010). Application and analysis of ZigBee technology for smart grid. *International Conference on Computer and Information Application (ICCIA)* (pp. 171–174).