IEEE
INTERNET OF THINGS JOURNAL
IEEE Xplore Digital Library
http://ieeexplore.ieee.org/Xplore

Review of Internet of Things (IoT) in Electric Power and Energy Systems

Guneet Bedi, *Graduate Student Member, IEEE*, Ganesh Kumar Venayagamoorthy, *Senior Member, IEEE*, Rajendra Singh, *Fellow, IEEE*, Richard Brooks, *Senior Member, IEEE*, and Kuang-Ching Wang, *Member, IEEE*

***Abstract*— A transformation is underway in electric power and energy systems (EPESs) to provide clean distributed energy for sustainable global economic growth. Internet of Things (IoT) is at the forefront of this transformation imparting capabilities, such as real-time monitoring, situational awareness and intelligence, control, and cyber security to transform the existing EPES into intelligent cyber-enabled EPES, which is more efficient, secure, reliable, resilient, and sustainable. Additionally, digitizing the electric power ecosystem using IoT improves asset visibility, optimal management of distributed generation, eliminates energy wastage, and create savings. IoT has a significant impact on EPESs and offers several opportunities for growth and development. There are several challenges with the deployment of IoT for EPESs. Viable solutions need to be developed to overcome these challenges to ensure continued growth of IoT for EPESs. The advancements in computational intelligence capabilities can evolve an intelligent IoT system by emulating biological nervous systems with cognitive computation, streaming and distributed analytics including at the edge and device levels. This review paper provides an assessment of the role, impact and challenges of IoT in transforming electric power and energy systems.**

***Index Terms*— Challenges of IoT, Computational Intelligence, Communications, Networking, and Security for IoT, Impact of IoT, Intelligent Power and Energy Systems, Internet of Things, Sensors and Devices for IoT, Services and Applications for IoT, Smart Home, SmartPark**

I. INTRODUCTION

WHILE the last half century was dominated by the communication revolution, the next several decades will be dominated by electric power and energy systems (EPESs). Since the global economic crisis of 2008, energy has started to dominate the market landscape [1]. However, the emergence of a real transformation in EPESs started in December 2015 with the adoption of the climate change agreement at the Paris UN Climate Change Conference (COP21) [2]. The transformation in EPESs emphasizes increasing efficiency and improving the reliability of electric power network operations, energy conservation, renewable sources of distributed power generation, and reduction of carbon emissions [2]. The major drivers of this transformation are shown in Fig. 1.

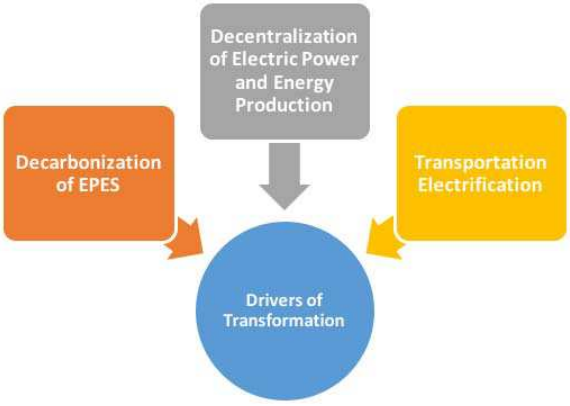


Fig. 1. Major drivers of the transformation in electric power industry.

Driven by the cost reduction of batteries for electric vehicles (EVs) (Fig. 2) [3], it is expected that in the next 3-4 years, the cost of battery storage will be less than hydroelectric storage (~$100/kWh). Therefore, a major shift towards new infrastructure based on photovoltaic (PV) and battery for electricity supply has already started.

Internet of Things (IoT) imparts networked connectivity to everyday objects in the physical world. All physical entities on earth (e.g. goods, buildings, appliances, machines, vehicles, plants, animals, and human beings) are the "Things" in IoT [4, 5].

IoT can transform EPESs by providing a sustainable solution, viz. a dynamic stochastic energy management system (DS-EMS) (Fig. 3), which is both intelligent and cyber-enabled, to meet the growing demands of access to affordable, clean and sustainable energy. The goal of DS-EMS is to maximize revenue generation, minimize energy costs, and reduce carbon emissions by optimizing the electric power flow in a way that minimum power is drawn from the power grid and maximum power is supplied to the power grid. The dependence on the power grid for meeting the energy demands of a user can be reduced by employing distributed energy resources including renewable energy resources (e.g. solar and

This paper was originally submitted for review on May 2, 2017. This work is supported in part by the US National Science Foundation (NSF) under grant #1312260 and the Duke Energy Distinguished Professor Endowment Fund. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF and Duke Energy Foundation.

Guneet Bedi is with the Real-Time Power and Intelligent Systems Laboratory, Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634 USA (email: gbedi@clemson.edu).

Ganesh Kumar Venayagamoorthy is with the Real-Time Power and Intelligent Systems Laboratory, Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634 USA, and also with the School of Engineering, University of KwaZulu–Natal, Durban 4041, South Africa (e-mail: gkumar@ieee.org).

Rajendra Singh is with the Real-Time Power and Intelligent Systems Laboratory, Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634 USA (email: srajend@clemson.edu).

Richard Brooks is with the Real-Time Power and Intelligent Systems Laboratory, Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634 USA (email: rrb@acm.org).

Kuang-Ching Wang is with the Real-Time Power and Intelligent Systems Laboratory, Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634 USA (email: kwang@clemson.edu).

Digital Object Identifier: 10.1109/JIOT.2018.2802704

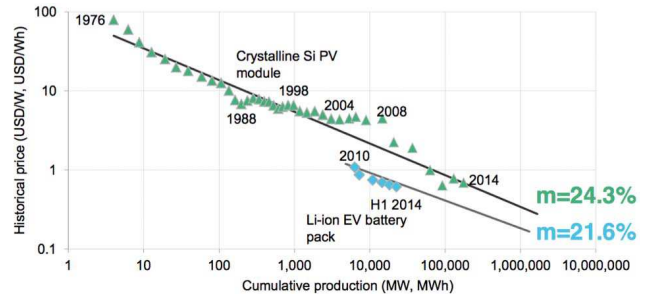


Fig. 2. Continuously reducing costs of crystalline Si PV module and Li-ion EV battery pack [3].

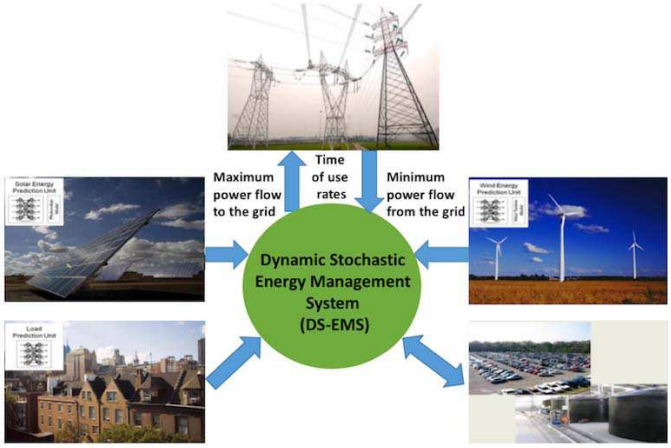


Fig. 3. Dynamic Stochastic Energy Management System (DS-EMS) [6].

wind) and batteries to meet the bulk of the energy needs. Once the energy needs are satisfied, any excess generation form these distributed energy resources can be supplied to the power grid. The electric power exchanges to-and-from the grid are done based on time of use rates. With IoT, EPESs will become more efficient, reliable, secure, cost-effective, resilient, and sustainable [6].

IoT also imparts real-time feedback capabilities to the utilities which function to better serve customers through enhanced monitoring and control functionalities [4]. This is the reason that utilities are among the largest IoT market and will be the third-largest industry by expenditure in IoT products and services, with more than $69 billion already spent worldwide [7]. The adoption of IoT in EPESs is also favored by the significant reduction of costs associated with sensors, bandwidth, processing, and memory/storage [8].

IoT presents numerous opportunities in EPESs having a significant societal, economic, and environmental impact, eventually moving towards the vision of a smarter cities and world.

The main contributions of this review paper are as follows (Fig. 4):

- Highlighting the limitations associated with the current electric power and energy systems
- Discussing the role of IoT in transforming the traditional electric power networks into intelligent power networks
- Providing an extensive review of IoT-based electric power and energy systems applications and services
- Providing a survey and technical assessment of smart home applications IoT sensors
- Highlighting the economic, societal, and environmental impact of IoT in electric power and energy systems
- Providing extensive insights into communications, networking, and security for IoT-based electric power and energy systems
- Enumerating the constraints associated with IoT deployment in electric power and energy systems and recommending solutions to overcome them

The rest of the paper is organized as follows: Section II provides an assessment of the current state of the electric power network and the importance of IoT in moving towards an intelligent electric power network. Section III briefly touches upon the economic, societal, and environmental impacts of IoT enabled electric power networks. Section IV discusses some of the challenges associated with IoT and lists recommended solutions in overcoming these challenges. Section V describes a real-world application example of IoT in EPESs. The conclusion of the paper is included in the last section.

II. Role of IoT for Intelligent Electric Power Networks

EPESs are comprised of generation, transmission and distribution (T&D) networks and their customers (residential, commercial, and industrial) (Fig. 5) [9].

EPESs are currently facing numerous limitations including balancing the fuel mix, reliability of power delivery and quality, asset level visibility, identifying new revenue sources, aging workforce and knowledge capture, and technology integration [10]. The fuel mix for power generation is becoming more diverse and flexible comprising of centralized generation (fossil fuels and nuclear), distributed generation (renewables), and energy storage. Balancing this fuel mix is critical for maximizing cost-effectiveness and energy output of the EPES. The diversity of fuel mix coupled with multiplicity of moving parts with different incentives and priorities increases the energy value chain complexity. This degrades the reliability and quality of power delivery if left unmonitored. Therefore, it is imperative to have asset level visibility through which system operators can continuously monitor all EPES assets' state and performance in real-time to assess demand and supply and their responsiveness to price signals. The traditional revenue model for EPES where volumetric tariff was used to compensate utilities is becoming suboptimal. New revenue sources that correctly value and allocate investment cost and other efforts need to be identified for future EPESs. Such revenue models will induce players to add value to EPESs through actions and information provision by adequately compensating investment and incentivizing innovative experimentation. Population aging presents the challenge of skills, knowledge, and experience shortage resulting from prospective simultaneous retirement of a large number of experienced workers. Digital innovations (collaboration, communication, and digital memory creation) are needed to capture the knowledge and experience of the senior workers, incorporate it in the

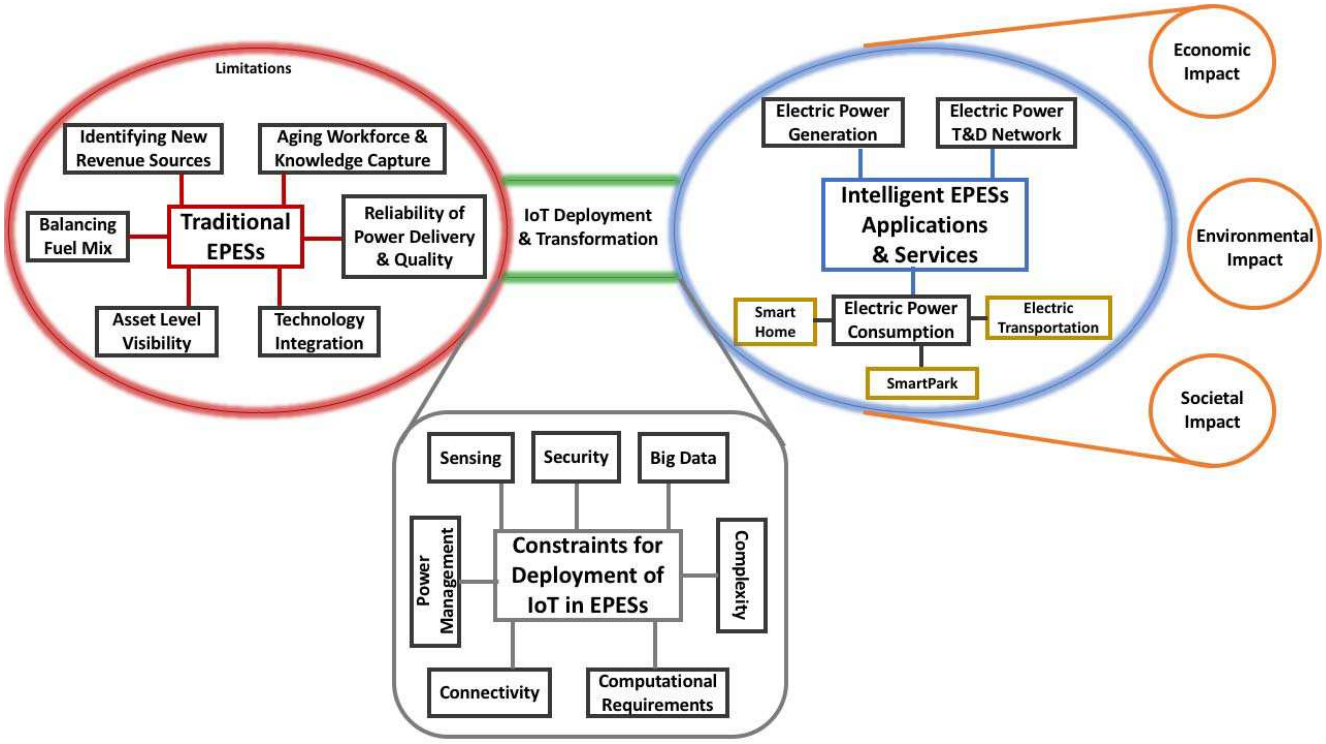


Fig. 4. Integration of all the phases presented in the paper.

companies' institutional memory, and make it accessible to the new workforce. With the advent of IoT, smart machines, and big data, the traditionally separate information technology (IT) and operations technology (OT) now need to be integrated to develop a new information-driven infrastructure for enhancing productivity using data.

To overcome these challenges, existing unidirectional EPESs are transforming into bidirectional intelligent electric power networks. "The intelligent power network is an automated, flexible, intelligent, robust, and consumer-centric network that supports bidirectional flow of electricity and data. Energy storage plays a key-role in making bidirectional power flow feasible enabling active customer participation in selling/buying power. Intelligent power network is the integration of cyber-secure technologies, intelligent device communications and high-penetration distributed energy generation across all elements of electricity generation, transmission, distribution and consumption that creates a resilient, reliable, safe and sustainable energy delivery network. It has self-healing and intelligent measurement and control capabilities. It also imparts real-time power network monitoring capabilities for better failure prediction/diagnosis to identify irregularities/weak points in a timely manner [6]." The intelligent electric power networks have several advantages including increased energy efficiency, reduced cost, better demand supply response, and reduced T&D losses [6, 11].

IoT has been an integral part of the transformation towards intelligent electric power networks. Examples of IoT technologies that are currently employed in intelligent electric power networks include advanced metering infrastructure (AMI) and supervisory control and data acquisition (SCADA) [12, 13]. There are several benefits of deploying IoT in intelligent electric power networks:

- Enhanced reliability, resiliency, adaptability, and energy efficiency [6]
- Reduced number of communication protocols [14-16]
- Networked operation and enhanced information operation capabilities [17]
- Improved control over home appliances [18]
- Enable on-demand information access and end-to-end service provisioning [18]
- Improved sensing capabilities [19]
- Enhanced scalability and interoperability [20]
- Reduced damages from natural disasters [21]
- Reduced physical attacks (e.g. substation break-ins [22]) on EPESs by continuously monitoring the electric power network's physical assets in real-time.

Realizing the full potential of IoT is critical to enhance the flexibility, asset management, operations, and reliability of intelligent electric power networks. To enhance the resiliency of electric power networks, it is essential to account for fluctuations introduced by decentralized generation from distributed energy resources (DER) integration [23]. Smart inverters are a potential IoT solution to overcome this challenge. To enhance the enablement of electric power networks, IoT devices and technologies such as advanced distribution management system (ADMS) collect, analyze, and disseminate data to all electric power network stakeholders (e.g. customers, utilities and regulators). Insights gained from these data enable stakeholders to make more informed optimization decisions, resulting in efficient utilization of electric power network

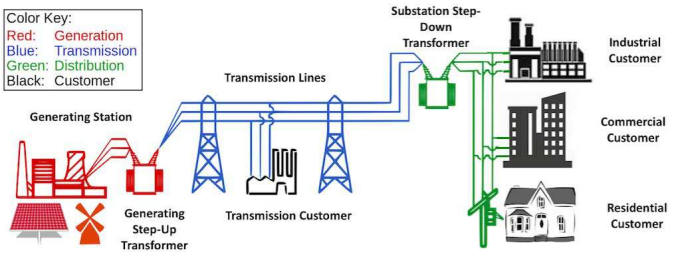


Fig. 5. Power and energy system (extended version of Figure 2.1 from [9]).

resources and more efficient network operations [13].

The benefits associated with digitizing intelligent electric power networks across generation, T&D networks, and consumption with IoT are discussed below.

A. Digitizing Electric Power Generation

DER generation will dominate the new electric power generation infrastructure. IoT can improve DER generation efficiency and therefore must be deployed across all power generation phases, viz. power plant portfolio design, siting, operations, maintenance, and optimization. Additionally, deploying IoT in power generation guarantees reliable, affordable, and safe access to power [10].

For optimal balancing of the generation portfolio of power plants and intelligent EPES operation, it is important to collect data in real-time from both the transmission and distribution electric power network assets. This subsequently needs to be analyzed to perform load forecasts, state predictions and distributed control of the EPES [10]. This data can be collected using IoT devices, such as smart meters, intelligent feeders, micro phasor measurement units (PMUs) and PMUs [24].

The location of power plants is especially important for renewable power plants, where power generation output can fluctuate depending on parameters such as clouds related solar intensity fluctuations (for solar power plants) and wind patterns (for wind power plants). IoT software solutions to account for such fluctuations include cloud computation, advanced load, and weather simulation algorithms. IoT hardware solutions include trackers, modular turbines and power storage [10].

IoT technologies use cloud-based advanced analytics as well as a holistic information technology (IT) and operations technology (OT) perspective to provide real-time insights into power plant operations, thereby improving visibility across all power plant asset. This helps in ensuring optimal power plant operations, sustainable generation portfolios, and predictive/timely maintenance [10]. An example of digitized power generation is the Digital Twin/Virtual Power Plant, developed by General Electric (GE) using Predix – a cloud-based IoT platform [25].

B. Digitizing Electric Power T&D Network

Existing electric power T&D network faces a number of challenges including delayed outage response times, power losses, data thefts, and DER integration. Digitizing the existing electric power T&D network with IoT can alleviate these challenges. IoT imparts intelligent monitoring and control capabilities to existing electric power T&D networks, which enable T&D operators to proactively respond to power outages, address customer concerns, and better account for DER integration. Additionally, IoT can help reduce power losses and data thefts during transmission and distribution by adjusting electrical parameters (voltage, current, power, and phase) in real-time and by tracking the source of theft, respectively. Electric power T&D networks can more efficiently and reliably ensure optimal power delivery with IoT. Examples of IoT devices and technologies in electric power T&D networks include smart meters, smart inverters, ADMS, and distribution electric power network sensors [10].

C. Digitizing Electric Power Consumption

IoT devices and technologies (e.g. IoT sensors) are the key drivers contributing to the growth of microgrids/nanogrids, smart homes with intelligent loads (IoT enabled loads), electric transportation and distributed energy storage systems. As a result of this growth, customer roles are evolving. Customers are now able to generate power locally from renewable sources to meet their needs and can participate in power exchanges with the electric power network. Intelligent loads utilize IoT sensors to provide customers with meaningful power generation and usage data that helps them utilize power more efficiently, reduce power wastage, and control costs. Distributed energy storage systems are advantageous over centralized storage systems in terms of having greater flexibility, better control, scalability, and enhanced reliability [26]. Distributed energy storage systems, such as battery and EVs, are critical to account for any fluctuations in power generation from renewable sources. If the generation falls below the demand, battery/EV can supplement the shortage. Alternatively, excess generation from renewable sources can be stored in battery/EV or it can be supplied to the electric power network. Examples of scenarios where customers are able to participate in power exchanges with the electric power network include smart home environment (Fig. 6) [27] and SmartParks (Fig. 7) [28]. Innovative pricing schemes [29] and strategic business models need to be implemented by the utilities to extract maximum benefit from these scenarios [6, 10].

1) Smart Home Environment: A smart home environment (Fig. 8) is comprised of a number of IoT sensors and actuators (e.g. pressure sensor, lighting sensor, motion sensor, temperature sensor, and humidity sensor); a computational system that includes wireless communication technologies (e.g. Zigbee, Bluetooth, Wi-Fi, and IPv6), control systems (e.g. remote control, smartphone, and tablet), and computation system; and visualizations (both remote and in-house). This imparts sense-making, decision-making, and adaptation capabilities to different home appliances present in the smart home [30]. The key enablers of smart home power system include advanced IoT sensor technology, better wireless connectivity, smaller device size, cheaper price, high volume manufacturing, enhanced computing capabilities, and improved control systems.

IoT sensors offer several benefits when deployed in a smart home environment. They help minimize energy wastage,

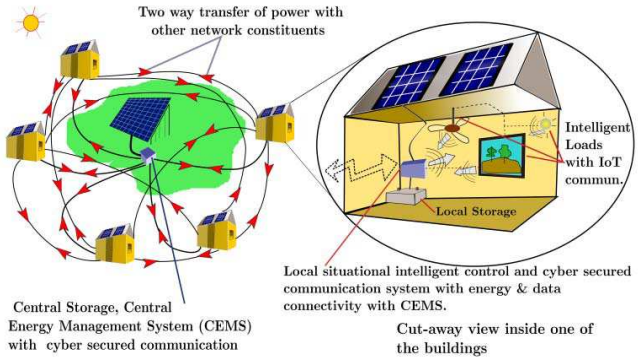


Fig. 6. Smart home with intelligent loads [27].

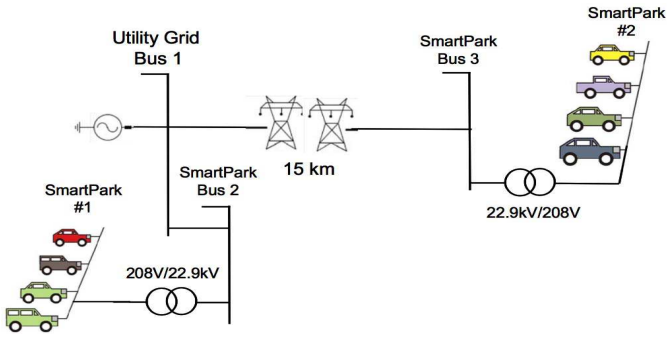


Fig. 7. SmartParks connected to the electric power network [28].

reduce costs, actively monitor home environment, reduces the risk to harmful environmental exposures such as carbon monoxide and smoke, and make home life more convenient and comfortable [31-34]. The different types of IoT sensors are listed below:

a) IoT Smart Home Occupancy Sensors: With IoT smart home occupancy sensors, the homeowners can monitor all movements in and around the house, thereby helping to protect the house from criminals and vandals. These sensors also reduce energy waste by controlling lighting in an area dependent on its occupancy. The different types of IoT smart home occupancy sensors include motion sensors, open/close sensors, and perimeter sensors [36-38].

- Motion sensors: These sensors monitor movements inside the house. With motion sensors, the homeowners can detect unexpected movements in the house, monitor pets and kids to ensure they stay away from "off-limit" areas, and detect the presence or absence of people in a particular area and control the lights to turn on/off accordingly [36, 38]. Examples of motion sensors include passive infrared sensors, microwave sensors, ultrasonic sensors, area reflective sensors, dual sensors, video sensors, wireless sensors, vibration sensors, and pet immune sensors [39].
- Open/close sensors: These sensors monitor the opening or closing of cabinets, doors, and windows. Open/close sensors can also automatically turn on the lights when a door is opened [36, 38]. Examples of open/close sensors include glassbreak sensors, passive infrared sensors, and door and window sensors [39, 40].
- Perimeter sensors: These sensors provide the extra layer of security by detecting any vehicles or persons approaching the house [36, 38]. Examples of perimeter sensors include active infrared sensors, capacitance sensors, vibration sensors, radar sensors, fence sensors, driveway sensors, and electric field sensors [40].

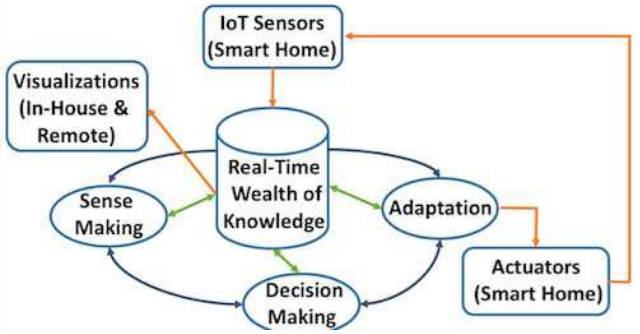


Fig. 8. Smart home environment (extended version of Figure 1 from [65])

b) IoT Smart Home Environmental Sensors: The homeowners can create a comfortable living environment inside the house with IoT smart home environment sensors [36]. IoT smart home environmental sensors include temperature and humidity sensors, leak and water sensors, smoke and air sensors, and light sensors [38].

- Temperature and humidity sensors: These sensors monitor unexpected changes in heating, cooling, and the amount of water vapor inside the house. Temperature and humidity sensors also reduce energy waste by turning off the cooling or heating in an area where there is no person present [36]. Examples of temperature sensors include resistive temperature devices, thermometers, thermocouples, infrared sensors, bimetallic devices, silicon diode, and change-of-state sensors [41]. Examples of humidity sensors include resistive sensors and capacitive sensors [42].
- Leak and water sensors: These sensors alert the homeowners as soon as a leak is detected, thereby helping to prevent damaging floods that can be costly to repair [36]. Examples of leak and water sensors include under carpet leak detectors, rope-style sensors, spot leak detectors, and hydroscopic tape-based sensors [43].
- Smoke and air sensors: These sensors monitor the air quality inside the house. With smoke and air sensors, the homeowners can detect the presence of smoke, carbon monoxide or any other harmful gas in the house [36]. This would in turn help the homeowners to take corrective measures before any serious harm happens to anyone residing in the house. Examples of smoke and air sensors include photoelectric sensors, ionization sensors, dual sensors, aspirating sensors, projected beam sensors, video sensors, and heat sensors [44].
- Light sensors: These sensors monitor the lighting levels inside the house. Light sensors automatically adjust the

lighting inside the house depending on the ambient natural lighting from the sun [36]. This helps enhance the lifetime of the light bulbs and reduce energy wastage. Examples of light sensors include photo-junction sensors, photoconductive sensors, and photovoltaic sensors [45].

c) IoT Smart Home Power Monitors: IoT smart home power monitors keep track of the amount of energy used by each home appliance or any other device inside the house [36]. Using these power monitors, the homeowners can be more conscious of their energy usage, adjust their energy usage behaviors to cut down costs and reduce energy wastage, and ensure that all home appliances and other devices operate efficiently and not consume too much power. There are four types of power monitors including readout and history monitors (e.g. Wattvision power monitor), instant readout monitors (e.g. Blue Line PowerCost monitor), plug in monitors (e.g. Kill a Watt EZ electricity monitor), and circuit by circuit measurement monitors with both history tracking and instant readout capabilities (e.g. eMonitor) [46].

d) Other IoT Smart Home Sensors: Some of the other IoT smart home sensors that are currently on market and have not been listed above include the following [36, 37]:

- Dry contact sensors: Detect contact between two wired contact points
- Smart plugs: Enable homeowners to turn on/off the home appliances or other home devices remotely using their smartphones
- Current transformers: Monitor the electricity flow inside the house
- AC/DC voltage sensors: Determine the powered state of equipment and alert the homeowners if voltage levels exceed the device ratings
- Power synching sensors: Create customized triggers in response to changing state of the plugged-in device (e.g. the homeowner can have the TV set the lighting level in the room when turned on)
- Smart home monitoring kits: IoT smart home monitoring kits are made by incorporating some of the above-mentioned IoT sensors in a single package. These kits provide the homeowners with a more advanced and affordable way to monitor and stay connected to their house from anywhere and at all times. Further, the functionality of these kits can be enhanced by connecting other compatible peripherals (cameras, alarms, and other IoT sensors).

Fig. 9 shows different types of IoT sensors with their leading suppliers, which are currently on the market for smart home applications [36-37]. A technical assessment of IoT sensors for smart home environment is provided below:

a) Technology Nodes for IoT Integrated Circuits (ICs): IoT ICs for smart home power systems include IoT sensors, analog to digital converters, digital processing, and radio frequency (RF) network connection. Currently, these ICs employ the 45nm/65nm-node (Node-3). In the next five years, it is estimated that the technology nodes for IoT ICs will vary depending on low, medium, or high-end smart home power system applications [47].

Minimizing cost and power consumption are at the forefront in designing IoT ICs for low-end smart home power system applications (e.g. connected LED lighting, security sensors, and connected smoke detectors). These ICs will employ the 55nm/40nm ultra low power and leakage technology node with the microcontroller (MCU) power of ∼50 dhrystone million instructions per second (DMIPs). Additional technological features for these applications will include integrated security features, eFlash or magnetoresistive random-access memory, power management unit, and integrated radios based on bluetooth low energy (BLE) and low-rate wireless personal area networks (802.15.4) [47].

Minimizing dynamic power while maximizing battery life is a key concept in designing IoT ICs for mid-end smart home power system applications (e.g. smart meters). These ICs will employ the 40nm, 28nm, and 22nm technology nodes with the MCU power of ∼300 DMIPs. Additional technological features for these applications will include several wireless low power wide area network protocols including LPWAN, BLE/802.15.4, and Wi Fi; wired communication protocols including power line communication (PLC), and ethernet; and more integrated security features [47].

Similarly, minimizing dynamic power while maximizing battery life is also a key concept in designing IoT ICs for high-end smart home power system applications (e.g. learning thermostats and home monitoring/security cameras). These ICs will employ the 22nm, 14nm, and 7nm technology nodes with the MCU power of ∼2000 DMIPs. Additional technological features for these applications will include strongest security features, human machine interface with high-resolution graphics and displays, and wireless connectivity including BLE, Wi Fi, and cellular [47].

b) IoT Sensor Design, Modeling, and Testing Technologies: In the past, sensors were designed by considering the electrical and physical boundaries as separate entities. Today, IoT sensors have integrated the electrical and the physical boundaries and are therefore designed using co-design methodologies, co-optimization techniques, and multi-domain (microelectromechanical system (MEMS), digital, analog, and RF) analysis [47].

Standardized MEMS models based on finite element analysis are available for modeling IoT sensors. These models employ reduced-order modeling and can be used to simulate IoT sensors at the system-level [47].

IoT sensors undergo complicated test cycles using various test equipment to ensure their adequate performance under different operating conditions. Increasing the number of test cycles and amount of equipment lead to better test results, but it also increases the test time and cost. IEEE 1687 IP plug-and-play standard minimizes test times through quick mapping of vendor-provided operational and initialization data to the IoT sensor [48]. It is necessary to test IoT sensor performance at near-threshold or sub-threshold voltage levels to account for process variations and non-linear transistor characteristics. However, the sub-threshold voltage level tests may result in the sensor operation overshooting the process corners. One way to prevent this overshooting is by "over-designing" the IoT sensor with a very conservative design sign-off criteria. Alternatively,

higher levels of manufacturing tests must be performed on the IoT sensor that would further increase the cost [47].

c) IoT Sensor Reliability and Power Requirement: A few ways to improve the IoT sensor reliability include lowering current densities and operating the IoT sensor at cooler temperatures. Improved IoT sensor reliability comes with an additional cost. The product life-cycle is directly proportional to and is an excellent measure of IoT sensor reliability. Consumer wearables and smartphones require very short product life-cycles (around 1-3 years). The IoT sensors for such applications are cheaper and less reliable. Other consumer applications including smart appliances in smart home power systems require longer product life-cycles (around 3-5 years). The IoT sensors for such applications are slightly expensive and more reliable. Industrial applications including infrastructure (bridges, buildings, and pipelines) monitoring require much longer product life-cycles (around 10-20 years). The IoT sensors for such applications are very expensive and most reliable [47].

To improve power consumption efficiency, IoT sensors employ many technologies (e.g. power-save mode, discontinuous reception, and fully depleted silicon on insulator), standards (e.g. Unified Power Format 3.0 (IEEE Standard 1801-2015) [49]), softwares (e.g. dynamic voltage and frequency scaling, power and voltage islands, and clock frequency adjustment based on the chip load), and energy harvesting solutions (e.g. light, heat, RF, and vibration) [50].

d) IoT Sensor Interoperability and Form-Factor: Interoperability is essential to integrate multiple IoT sensors in a smart home environment and to ensure their seamless operation. Developing comprehensive standards is critical to achieve interoperability to increase the penetration of IoT sensors in smart home power systems. 5G is one such comprehensive standard (currently under development) for improving communication efficiency, reducing costs, increasing network bandwidths, and extending coverage [47].

IoT devices are application-centric, i.e. if built for one application, they cannot be used for any other application. For example, one cannot use the IoT devices built for smart homes with other commercial, industrial, or medical applications. The IoT devices differ from one application to another regarding power requirements, form-factor levels, and the user-interface designs; however, the underlying component technologies and IoT sensors may be the same. A generalized device design (one device for different applications) is avoided as it introduces sub-optimality [47].

2) Electric Transportation and SmartPark: Electric transportation is becoming an essential part of the global automotive industry providing environmental, economic, and energy security benefits. Governments around the world are urging the automobile manufacturers to develop more EVs and are providing incentives to the citizens for buying the EVs. Navigant Research has estimated the global light duty EV market to increase from 2.7 million vehicle sales in 2014 to 6.4 million in 2023 [51]. Integrating EVs into the electric utility grid facilitates both vehicle-to-grid (V2G) and grid-to-vehicle (G2V) applications owing to the bidirectional nature of the power flows between the EVs and the grid [52]. Several electric grid services can be availed from EVs including regulation, spinning reserve, load leveling, storage for renewable sources, demand-response, and revenue generation through power transactions with the electric utility grid (e.g. SmartParks). There are also a few associated challenges with integrating EVs into the electric utility grid, such as variable prices of power transactions at different times and large power swings. Intelligent scheduling is required for the charging and discharging of EVs to overcome these challenges [28, 53].

A SmartPark is made up of a fleet of plug-in (gridable) vehicles (plug-in hybrid electric vehicles and EVs) performing V2G power transactions. Fig. 7 shows two SmartParks connected to the utility grid through a step-up transformer. Each SmartPark can have hundreds of vehicles that can participate in power transactions with the grid. SmartParks provide several grid services including load-peak shaving, maximum utilization of renewable sources of energy, minimizing cost of energy, and reducing emissions. Major challenges associated with numerous distributed SmartParks include grid stability and cyber-security. To overcome these challenges, intelligent computing in conjunction with advanced control and protection is needed [28].

III. Impact of IoT on Electric Power and Energy Systems

In this section, economic, environmental, and societal impact of IoT on EPESs is discussed.

A. Economic Impact of IoT on Electric Power and Energy Systems

McKinsey Global Institute has estimated that by 2025, the economic impact of IoT for energy and power systems will be in the range of $200 billion to $500 billion [54]. Cisco Systems, Inc. has estimated that between 2013 and 2022, the net profit accrued from IoT deployment in EPESs will be $757 billion [55]. GE has estimated significant revenue gains from digitization of EPESs: $230 million from new combined cycle gas plants, $100 million from new wind farms, and $50 million from existing combined cycle gas plants [10]. Frost & Sullivan reported that approximately 37 million smart meters were shipped in the United States between 2011 and 2014 [56].

The market for IoT sensors for EPESs is undergoing a favorable progression as well and offers numerous opportunities for growth and development. Driven by reduction in cost and energy per sensor, IoT sensors are now becoming more popular for industrial and consumer applications [57]. Transparency Market Research has estimated the increase in global market for IoT sensors from $9 billion in 2012 up to $21.60 billion by 2019, growing at a compound annual growth rate (CAGR) of 12.2 percent (Fig. 10) [58].

ABI Research has estimated an increase in the market value of enterprise IoT analytics from $4.2 billion in 2014 to $23 billion by 2020, indicating the increasing investment in IoT analytics [59].

While there are considerable opportunities for increased revenue in EPESs, these impressive statistics must be balanced with the costly investments companies must make

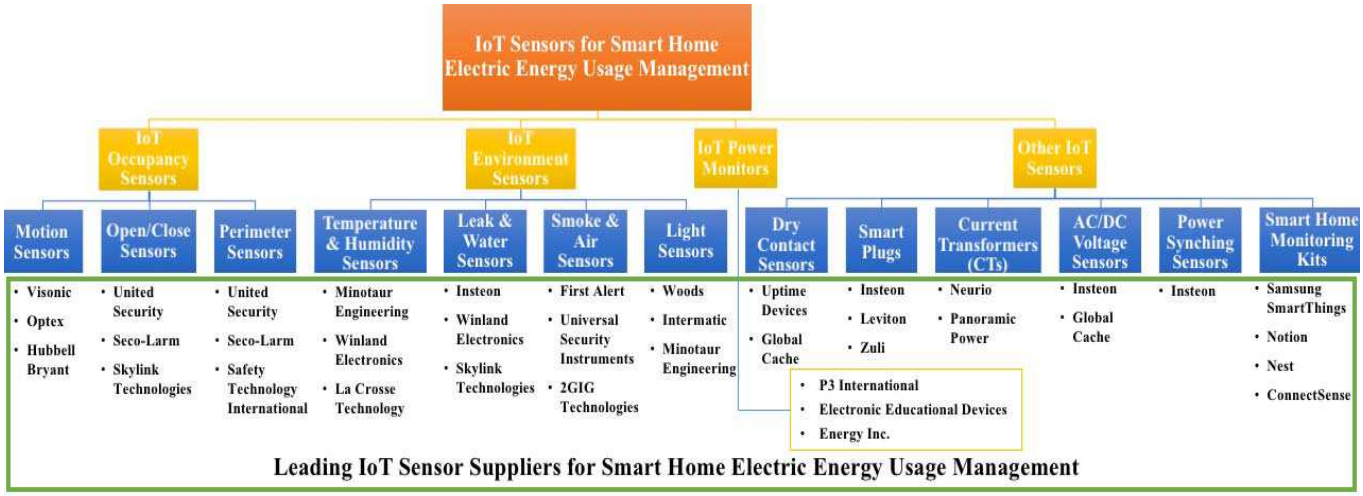


Fig. 9. Different types of IoT sensors, with their leading suppliers, which are currently on the market for smart home electric energy usage management.

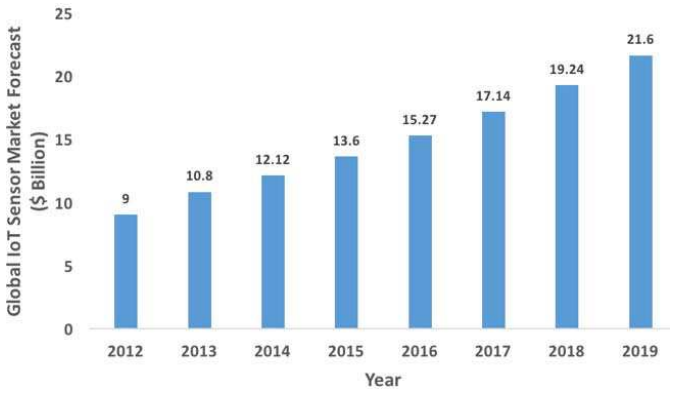


Fig. 10. Global IoT sensor market forecast ($ billion) (adapted from [58]).

upfront when employing novel IoT devices and technologies. Nevertheless, the surplus generated will outweigh the initial expenses. Additionally, IoT technologies can be deployed in existing devices and infrastructures, further minimizing expenses.

Currently there are some barriers to the market entry of IoT devices and technologies including connectivity, cyber security, big data handling, individual privacy, sustainable low cost power resources, and sensors that are inexpensive, efficient, and reliable [6]. Viable solutions are needed to overcome these barriers to ensure the continued growth of IoT for EPESs.

B. Environmental Impact of IoT on Electric Power and Energy Systems

With IoT deployed in EPESs, power is utilized more efficiently. Also, control systems are optimized for maximum power absorption from renewable sources (solar and wind) [5]. This has a positive impact on the environment in terms of less energy waste and reduced carbon dioxide (CO_2) emissions [60]. By 2020, 2 Gigatons annual decrease in CO_2 emissions is expected [61].

C. Societal Impact of IoT on Electric Power and Energy Systems

As world's population continues to grow, it becomes increasingly necessary for its inhabitants to care for the available resources. With rising living standards globally, health, convenience, and comfort have become personal priorities. IoT can meet all of these needs and desires through its abilities to sense, collect, transmit, analyze, and distribute big data.

To meet these demands, organizations and institutions will deploy IoT EPESs, leading to increased energy efficiency and greater control and auditing capabilities. With greater amounts of personal data collected from smart meters to decrease energy waste (e.g. energy usage data and user movements and activities tracking data), personal security could be jeopardized if the meter is hacked. For instance, a hacker could determine if a user is home or not or if a child at home alone.

While there are cyber-security and privacy risks associated with IoT deployment in EPESs, there are overwhelming societal benefits including lifestyle convenience, public safety, energy conservation, expense reduction, and a healthy living environment [62]. Individuals and corporations must decide the optimal use of the technology for their needs based on these tradeoffs [6, 63].

IoT deployment cannot be pushed onto the society and expected to be readily accepted. People like to take responsibility for their well-being. Considering the numerous benefits of the deployment of IoT technology, a lot of people might be willing to try it out. But there will be some people who will resist this technology, even after being aware of its benefits. For them, IoT technology might not be the need of the hour, or they might just fear the unknown. Additionally, the competition between nations to excel at IoT device manufacturing and technology development makes it difficult for a company to establish a base in a foreign country and utilize its resources. An instance of this was reported recently in [64] where GE launched its digital foundry in Shanghai and is facing tough competition from the Chinese local firms. In any case, people's choices must be respected, and they should not be forced down

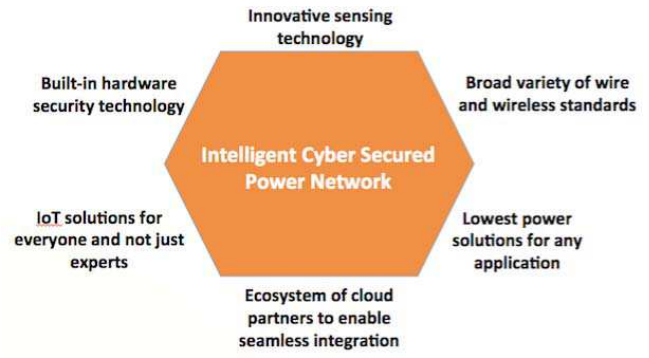


Fig. 11. Technological innovations for intelligent cyber-secured electric power networks [4].

a path that makes them uncomfortable.

IV. Constraints for Deployment of IoT in Electric Power and Energy Systems

Deploying IoT in EPESs has several advantages, but some associated challenges exist. These challenges include sensing, connectivity, power management, big data, computation, complexity, and security [4]. Technological innovations are necessary to overcome these challenges and achieve the vision of an intelligent cyber-secured electric power network (Fig. 11).

A. Sensing Challenges and Recommended Solutions

Advancements in sensor technology have resulted in IoT sensors becoming more powerful, cheaper and smaller in size. This, in turn, has led to their large scale deployment in EPESs. IoT sensors currently on the market lack some critical features viz. situational intelligence, efficient power management, and enhanced cyber security, which must be incorporated into future IoT sensors to enhance their functionalities [23].

Near-future situational intelligence can be implemented by integrating historical IoT sensor data with IoT sensor data obtained in real time. Benefits of implementing near-future situational intelligence in IoT sensors include security and stability limit prediction with contingency analysis, load and generation forecasting, cyber security, and real-time/predictive visualizations [65]. For efficient power management, solutions include using arrays of low-accuracy sensor modules with subsequent data fusion to generate high-accuracy information, employing energy harvesting solutions (e.g. light, heat, RF, and vibration) to prolong battery life (discussed in sub-section C below), and using digital circuits to design low power sensor nodes [19].

Cyber security solutions include embedding hardware security features, adding more layers of security, and advanced virtualization, which are discussed in detail in sub-section G below [66-68].

The various ongoing research initiatives directed towards improving the existing IoT sensor functionality include:

- Developing smart control algorithms to improve IoT sensors power, fault tolerance, and bandwidth [69]
- Employing fuzzy logic and statistical outlier detection algorithm (e.g. FindCBLOF) to better detect abnormal sensor events [70, 71]
- Integrating robust communication technologies (e.g. PLC) with IoT sensor networks to resolve communication network issues (wireless interferences, packet losses, and transmission errors) [72]
- Using service-based proxy frameworks to resolve interoperability challenges between IoT sensors and heterogeneous devices [73]
- Integrating gesture recognition and brain-computer interface with IoT sensors to better monitor the physically impaired and elderly [74, 75]
- Implementing energy harvesting technologies in IoT sensors to do away with batteries [76]
- Reducing the complexity of programming platforms for IoT sensor network to enable average users program them as required [77]
- Employing aggregation-based data privacy preserving protocols to secure the IoT sensor data [78]
- Using context-aware computing to better understand the IoT sensor data [79]
- Virtualizing the IoT sensor infrastructure and making it available for use by multiple applications [80]
- Analysis of privacy and cyber security risks in IoT devices and softwares for smart home automation system [81, 82]
- Advancements in detection technologies to counter cyber attacks [82, 83]

B. Connectivity Challenges and Recommended Solutions

1) Need for Comprehensive Connectivity Standards for IoT: There are many connectivity standards for IoT applications that can broadly be classified into three categories: service-related, communications-related, and data-related [84]. The service-related connectivity standards provide definitions for common services to support IoT applications. They provide definitions for common capabilities, their respective access interfaces, and the protocols employed over these interfaces in a manner that enables different IoT applications to gain access to these capabilities across protocol stacks developed by different standard organizations (e.g. International Telecommunication Union [85], European Telecommunication Standards Institute [86], oneM2M [87]). Additionally, the service-related connectivity standards develop access-independent interface standards (e.g. [88] by Telecommunications Industry Association), addresses carrier portability matters (e.g. [89] by ATIS), and network security concerns (e.g. [89] by ATIS) for IoT applications. The communications-related connectivity standards provide definitions for efficient communication mechanisms for supporting IoT applications. They provide application guidelines to fit the operation of particular standards, like Transport Layer Security, in an IoT setting (e.g. [90, 91] by Internet Engineering Task Force (IETF)). They also define additional protocols, like RPL (pronounced “ripple”) routing protocol for 6LowPAN, to fill gaps in the protocol solution set for IoT (e.g. [92] by IETF). They also provide support

for multiple vertical application domains (e.g. [93] by IEEE). The data-related connectivity standards provide definitions for generic mechanisms for supporting versatile data usage and interoperable data exchange in IoT applications. They provide technology-independent interfaces for generic data definition and access (e.g. [94] by Open Geospatial Consortium, and [95] by Object Management Group). Additionally, they provide flexible mechanisms for defining object identity information and exchanging this information with other administrative domains (e.g. [96, 97] by OASIS, [84]).

Interoperability between all the different standards available for IoT applications is critical to support the integration of different types of data generated from a variety of sources. Interoperability enables the IoT devices to support the curation, provenance and exposure of data to third party applications enabling rapid innovations in the application and service ecosystems [84, 98].

Without interoperability, there will be challenges with data representation formats, data dissemination mechanisms, and data management platforms. For EPESs, the diverse physical and virtual assets can no longer remain disparate entities. They must be interoperable entities across IoT applications. These challenges along with the continuously increasing number of IoT devices demand the development and implementation of comprehensive connectivity standards that will be critical in achieving interoperability and seamless transitions between the physical and virtual domains of IoT [84, 98].

With the emerging 5G cellular communication standard, low-cost and efficient communication with increased network coverage and bandwidths are expected to support a sheer scale of IoT devices, the continuously increasing multimedia applications, and an exponential increase in wireless data [99].

2) Coexistence Challenge and Recommended Solutions: IoT applications in EPESs utilize several connectivity protocols (e.g. Wi-Fi, Bluetooth, ZigBee, and BLE) for data transmission [100, 101]. Such heterogeneous connectivity scenarios are faced with the coexistence challenge – interferences resulting from interaction between wireless connectivity protocols that share the same (2.4GHz) frequency band. These interferences significantly degrade the network's quality of service [100].

A solution for overcoming the coexistence challenges is with wireless convergence modules since they can handle multiple connectivity protocols simultaneously using advanced coexistence algorithms. Fig. 12(a) shows a home automation scenario where the wireless convergence module handles different connectivity protocols, enabling data transfer between IoT sensors and the cloud. An example of a wireless convergence module is Redpine RS9113, which supports the heterogeneous connectivity scenarios of IoT and addresses coexistence challenges through its innovative coexistence algorithms (Fig. 12(b) and Fig. 12(c)) [100]. Other solutions for overcoming the coexistence challenge include fair channel assignment [102] and dynamic licensed spectrum sharing [103]. The fair channel assignment approaches ensure fair allocation of radio resources to links or flows to achieve seamless transmission [102]. The dynamic licensed spectrum sharing approaches allow mobile operators to make use of

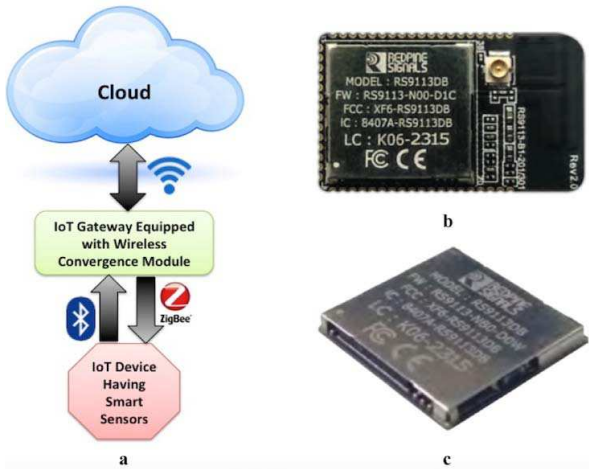


Fig. 12. (a) Application of wireless convergence module in a home automation scenario [4], (b) Redpine RS9113 module with built-in antenna [100], and (c) Redpine RS9113 module without built-in antenna [100].

underutilized licensed spectrum bands based on service level agreements [103].

C. Power Management Challenges and Recommended Solutions

Incorporating power management is critical for an IoT device to perform its designated functions. Based on the position and functionality of IoT devices in EPESs, their power collection methods vary. This makes it challenging to incorporate power management in IoT devices.

The recommended solutions to overcome the power management challenge in IoT devices are discussed below.

1) Energy Harvesting System: IoT devices in EPESs may be installed in locations that are not easily accessible (hazardous, toxic, or hard-to-reach areas) making grid connection or battery replacement a complex and expensive approach to power these devices. In such scenarios, an energy harvesting system can be a promising alternative to prolong the lifetime of the IoT device and reduce their dependency on the grid or battery [104].

The energy harvesting system comprises of three components: energy source, harvesting architecture, and load (sink for the harvested energy) [105]. An energy source is the source of energy to be harvested. The energy sources that are present in the surrounding environment are called ambient energy sources, for example solar, wind and vibrations. Energy may also be harvested using body movements of humans and is called human power. Human power can be active or passive depending on whether the body movements are controllable by the user or not. Examples of active human power include finger motions and footfalls; and examples of passive human power include exhalation, breathing, and blood pressure. In general, energy sources can either be controllable or non-controllable. Controllable energy sources can be harvested as needed. There is no need to predict energy availability before harvesting them. Examples of controllable energy sources include finger motions and footfalls. Non-controllable energy sources must

be harvested whenever they are available. Prediction models are needed for non-controllable energy sources to forecast their availability to plan the next recharge cycle. Examples of non-controllable energy sources include (solar, wind, and vibrations) [105]. Out of all the different energy sources, solar energy emerges as the most promising harvestable energy source due to the following reasons [104]:

- Solar energy is freely available and easily accessible energy source
- The amount of energy harvested from solar is 24mW/cm2
- It is uncontrollable but predictable
- Solar panels can be made small enough to fit the form factor of wireless IoT sensor nodes

A harvesting architecture is a mechanism to collect and convert ambient energy to electrical energy. It either harvests the source energy for just-in-time use (harvest-use architecture) or stores the harvested source energy for future use (harvest-store-use architecture). The energy conversion mechanism in the energy harvesting architecture depends on the energy source being harvested. For example, solar panels are used to convert solar energy into electrical energy; piezoelectric elements are used to convert mechanical energy sources such as walking, paddling, pushing buttons/keys, into electrical energy; and rotors and turbines are used to convert wind energy into electrical energy [105].

Employing energy harvesting systems exclusively to power IoT devices that have low-energy requirements can make these devices truly portable and self-sustaining in addition to helping reduce the carbon footprint [104, 105]. Studies have shown that an energy harvesting system has the potential to prolong the lifetime of low-power IoT sensor nodes when deployed in randomly distributed multi-hop topology and uniformly distributed ring topology [106]. Although energy harvesting systems offer promising benefits, they also have the following associated drawbacks [104]:

- The random and intermittent nature of the renewable sources of energy (e.g. solar and wind) for energy harvesting systems makes it challenging to provide a stable power source to the IoT devices.
- RF Energy harvesting systems have very low efficiencies (around 16.3 percent [107]).

Therefore, there is a need to overcome these drawbacks for successful deployment of ambient energy harvesting solutions to power the IoT devices. A solution to account for the intermittent nature of renewable sources of energy is to employ storage technologies (e.g. NiMH batteries, Li-ion batteries, and supercapacitors) to store the harvested energy [105].

2) Energy-Efficient Communication Networks: Energy consumption in communication networks is increasing at a tremendous rate, which is attributed to the rapid rise in the number of IoT devices with networking capabilities and the progressive growth of information and communication technology. Therefore, effective power management solutions need to be developed to overcome this issue. Energy-efficient communication networks for EPESs can be achieved by incorporating power management in both peripheral (e.g. IoT sensor nodes and smartphones) and access (e.g. base stations, switches, and routers) network equipment of the communication network. This section discusses the energy-efficient communication techniques for wireless, wired, optical, and optical-wireless communication networks [108].

a) Energy-Efficient Wireless Communication Networks : Applications of wireless communication networks in EPESs include meter data collection, demand management, substation monitoring and protection, and power line monitoring and protection. Cellular networks including 3G, 4G, 5G (yet to be launched), WiMAX, ZigBee, and Wi-Fi are utilized in wireless communication. The metric for energy efficiency in wireless networks is "bits-per-joule" and is a measure of throughput with regards to unit energy consumption [108]. The following power management solutions can be incorporated in wireless communication networks to make them energy-efficient:

- Employing the relaying technique using mobile relays between IoT entities that are geographically spread (wide area networks (WANs)), resulting in shorter transmission range requiring low transmission power [109, 110]
- Using the cooperative communication technique for IoT entities that have different channel conditions (channel diversity) [109]
- Placing the base station (BS) in sleep mode during low traffic volume since they account for 60–80% of the whole power consumption in a wireless network [111, 112]
- Using the coordinated multi-point technology for WAN applications, where the function of the base station is separated into baseband unit and remote radio unit parts. By doing so, the distance between the user and antennas decreases, resulting in reduced system transmission power consumption [113].
- Adoption of the power saving mode by IEEE 802.11 standards that allow the wireless nodes to go into sleep mode when they are neither receiving nor transmitting [114]
- Employing networks like ZigBee [115] and ultra-low power Wi-Fi [116], which are inherently energy efficient, for home area network
- Connecting IoT devices in mesh topology to improve power efficiency and communication capability [117]
- Using radio frequency energy harvesting to power the wireless communication networks [118]
- Deploying turbo codes in energy-constrained wireless communication applications can help decrease RF bandwidth requirements and/or increase information bit rates significantly, without having to increase the transmission energy consumption [119].

b) Energy-Efficient Wired Communication Networks: Applications of wired communication networks in EPESs include load control and remote metering. PLC and Energy Efficient Ethernet (EEE) are utilized in wired communication [108]. The following power management solutions can be incorporated in wired communication networks to make them energy-efficient:

- Incorporating spectrum sensing scheme in PLC to reduce its power consumption [120, 121]

- Incorporating green resource allocation scheme in PLC that optimizes data allocation to the available channels [122]
- Adoption of the power saving mode by HomePlug Alliance (PLC standard for Smart Grid applications) within its Green PHY 1.1 definition [123]
- Employing low-power cycles in EEE with periodic refresh intervals to maintain the transmitter-receiver alignment and save energy [124]

c) Energy-Efficient Optical Communication Networks: An application of optical communication networks in EPESs is the information flow between independent system operators in distant regions. Fiber optical communication networks offer several advantages including high speed, large bandwidth, and a high degree of reliability. These networks follow a hierarchical organization consisting of core (providing coverage ranging from a few hundred to a few thousand kilometers), metro (providing coverage ranging from a few tens to a few hundred kilometers) and access (providing coverage ranging over a few kilometers) domains [108]. The following power management solutions can be incorporated in optical communication networks to make them energy-efficient:

- Turning off the network equipment (e.g. switches, line cards or the links) that is in its idle state during low traffic volume [125, 126]
- Employing lightpath bypass technique over lightpath non-bypass technique to provision survivable demands with minimized power consumption in IP-over-WDM networks [127, 128]
- Incorporating techniques like multi-path selection [129], multi-granular switching [130], and energy-aware routing [131] to save energy
- Employing energy-efficient access technologies such as passive optical networks [132], Ethernet passive optical networks [133, 134], long-reach passive optical networks [135], and point to point optical networks [132]

d) Energy-Efficient Optical-Wireless Communication Networks: Optical-wireless communication networks, commonly known as fiber-wireless (Fi-Wi) communication networks, combine the ubiquity, coverage and flexibility of wireless communication networks with the speed and the reliability of optical communication networks. To make the optical-wireless communication networks energy-efficient, the optical network unit (ONU) module of a joint ONU-BS node can be placed in sleep mode during low traffic volumes. In this case only the BS module from the joint ONU-BS node handles data forwarding to the peers [108, 136].

D. Big Data Challenges and Recommended Solutions in Support of IoT Deployment in Power and Energy Systems

Thousands of IoT devices connected across EPESs generate large amounts of data (or big data), making it challenging to store, track, analyze, capture, cure, search, share, transfer, secure, visualize, and interpret the generated data [137]. It is challenging to process big data using traditional data processing applications due to the following unique characteristics that are associated with big data [138]:

- Large volume/quantity of generated data
- Variety in the type of generated data
- Different velocity/speed of data generation
- Variation in the veracity/quality of source data
- Data inconsistency/variability

Big data must be transformed to actionable/intelligent information, knowledge, and understanding to extract value from it. Understanding is a process by which individuals attach meaning to an experience. Understanding of what matters must be a priority, especially for critical operations. Additionally, understanding must be gained from a shared view due to the interconnected (spatial and temporal) nature of the electric power grid dynamics [65].

A recommended solution to overcome big data storage and processing challenge is Apache Hadoop – an open-source software framework. Hadoop utilizes large clusters of commodity servers to enable distributed processing of big data. Hadoop has a number of advantages including hardware infrastructure scalability, cost efficiency, data type flexibility, and fault tolerance, which makes it a leading candidate for storing, managing, and processing big data [138]. Another recommended solution to overcome the big data handling and storage challenge involves a collaborative effort from all leading cloud providers to develop a new IoT cloud ecosystem [137].

E. IoT Computational Requirements and Capabilities

As compared to human brain, IoT infrastructure is not that complicated. In a human brain, there are 100 billion neurons with each neuron connected to 10,000 other neurons [139]. Imparting computational capabilities to the IoT devices and the network-edge devices (e.g. gateways and routers) have resulted in a paradigm shift from connected/networked IoT devices to intelligent IoT devices.

The advancements in computational intelligence capabilities can evolve an intelligent IoT system by emulating biological nervous systems with cognitive computation, streaming and distributed analytics including at the edge and device levels. Cognitive computation emulates biological thinking, analysis, and strategy, serving as a learning mechanism for the entire IoT ecosystem. It can identify patterns from large and diverse data sequences in real-time by weighing the incoming data against the long-term information and making strong decisions. Several companies such as Intel and CognitiveScale are exploring intelligent interactions by combining sensors, contextual data, and cognitive computing to drive new strategies for various industries including home automation, healthcare, and traffic management. Streaming analytics mimics the biological spinal cord by controlling the reflex actions that do not need extensive computations to make decisions in real time. It weighs the incoming analytical data with historical information in real time to make quick decisions (very low latency). The decision making with streaming analytics is much faster than batch processing large amounts of data. There are several cloud solutions (e.g. Amazon Kineses and Azure Streaming Analytics) and cloud-based, open source or on-premise applications (e.g. Apache Spark and Apache Storm)

that support streaming analytics. Edge and device computation mimics biological nerves and neurons that filter the incoming data, retain the data that can be processed locally in the edge devices (impacting only a small part of the IoT ecosystem), and forward the remaining data to be processed in the cloud (impacting a larger part of the IoT ecosystem). An example of a small and inexpensive edge computing device is Raspberry Pi [140, 141].

The number of IoT devices and applications are continuously growing leading to a significant increase in IoT data volume. ABI Research has estimated the IoT data volume to grow from 233 exabytes in 2014 to 1.6 zettabytes in 2020 [59]. The different IoT devices and applications generating real-time data are dispersed over large geographical areas and support a variety of use cases and domains. A centralized computation and storage solution (e.g. cloud) for real-time heterogeneous IoT data is not ideal. IoT applications have strict requirements like high throughput during short time periods, very low latency, and prompt decision making based on real-time data analytics, which cloud computation cannot satisfy. With all the IoT devices and applications sending service requests to the cloud, it would be challenging to serve these requests in real-time resulting in inefficient service-provisioning and increased latency. Additionally, IoT ecosystems are constrained in terms of low power communications, scarce energy, and lossy communications, which necessitates localized computation and storage solutions for processing, analyzing, and storing IoT data [142-146].

Two approaches for overcoming the IoT data computation challenge are discussed below viz. fog computing and IoT data footprint reduction methods. Deploying these solutions in the IoT ecosystem will drive the EPES operations using hard evidence and statistical probabilities rather than relying on soft opinions and intuitions.

1) Fog Computing: The term fog computing was coined by Cisco Systems, Inc. in 2012 [147]. Fog computing is a distributed computing infrastructure that provides computational and storage capabilities to the network devices located at different levels in the IoT hierarchy viz. endpoint level, gateway/server level, and cloud level [142].

Fog computing is based on the principle of edge computing where IoT application service requests, requiring low latency, support for mobility, and real-time data analysis with decision making abilities (e.g. smart grid, smart traffic monitoring, and smart parking), are processed locally within the fog computing devices (e.g. gateways, routers, and access points). Alternatively, the requests that demand extensive analysis involving historical data-sets, or semi-permanent and permanent storage (e.g. social media data, photos, videos, medical history, and data backups), are forwarded to the cloud by the fog computing devices [142].

Therefore, fog computing and cloud computing are not competing computation technologies, but are instead complementary. Together they support the IoT applications' real-time and low latency service requests at the network edge, as well as applications requiring complex analysis and long-term data storage in the cloud [142, 145, 146].

The following are the advantages of employing fog computing in the IoT ecosystem. Many of these advantages are a result of the proximity of fog computing devices to consumers, their dense geographical distribution, and mobility support [143, 148]:

- Refining the generated IoT data by distributing it among the edge devices [59]
- Lowering latency and saving bandwidth by processing IoT applications' service requests at the network edge [59, 143]
- Improving availability through local storage and analytics [59]
- Providing location awareness, improved quality of service, heterogeneity support, fault tolerance, scalability, and reliability [148]
- Reducing network traffic by increasing the operational size of the network [149]
- Maximizing security and compliance by encrypting critical data packets at the source [59]
- Saving both time and cost of transmitting the locally generated IoT data to the cloud over the Internet (high latency network) [150]
- Optimizing the total cost of ownership by reducing the connectivity costs and increasing the lifetime of battery-operated IoT devices [59]

Although there are several advantages, associated challenges with fog computing also exist:

- Handling data generated from dissimilar sources because of different protocols and data formats [149]
- Cyber attacks (e.g. node-compromised attack and man-in-the-middle attack) and privacy concerns (e.g. data protection and data management issues) [150]
- The unpredictability of the computational availability of the edge devices [151]

Several fog computing techniques have been proposed to overcome these challenges including software defined network and network functions virtualization [148], schema-less database record [149], task execution by idle edge resources [151], and smart shadow technique [152].

2) IoT Data Footprint Reduction Methods: As mentioned before, centralized computation and storage are not ideal for IoT applications. The increased IoT data velocity and volume from the growing scale of IoT devices can elevate the stress on the communication network resources to a point where resource starvation occurs. Therefore, it is critical to minimize the traffic inserted into the communication network. One way to reduce the data traffic is by appropriately distributing the data between the network elements based on their computation capabilities and available resources. Another way to reduce the IoT data footprint is dimensionality reduction method. This method relies on the global awareness and knowledge of the IoT ecosystem for eliminating redundancy and filtering out the noise from IoT data packets. The drawback with the dimensionality reduction method is that it does not address the impact of IoT data exchanges on the communication network. Data filtering methods are used to address the impact of IoT data exchanges at an operational level. These methods are distributed throughout the communication infrastructure,

monitoring the IoT data in transit for significant events. Once a significant event is detected, data filtering methods label them with critical local information (e.g. network load) resulting in a more efficient treatment for these events at the operational level. The IoT data footprint on the communication networks can be further reduced by employing both data filtering and data processing methods within the same IoT node [149].

F. Complexity Challenges and Recommended Solutions

The expansion of network infrastructure due to the wide penetration of IoT devices has resulted in increased network size, heterogeneity (different vendors providing services, equipment, and applications), and complexity [153, 154]. For a lot of these devices, networked connectivity is a brand new feature. To continue this trend of adding more IoT devices with networked connectivity that seamlessly integrate with EPESs, IoT device design and development must be simplified [101, 137]. Further, the wireless capabilities must be encapsulated and instead easier to understand reference designs, modules, and on-chip connectivity stack and development environment must be provided [137].

The traditional approaches for network optimization, configuration, and troubleshooting are cumbersome, error-prone, and have proved to be inefficient in resolving the complexity issue [153]. For example, autonomous system based approaches have resulted in suboptimal performance, local optimization methods have resulted in conflicting operations, and the lack of inbuilt programmability, flexibility, and support has resulted in service interruptions while implementing new ideas [155-157]. Additionally, the development, implementation, and testing of new methods for network optimization, configuration, and troubleshooting takes several years before they can be deployed, which may render them useless [158, 159]. A promising solution to manage the growing network complexity is software-defined networking (SDN) [153, 154].

The Open Networking Foundation defines SDN as "an emerging network architecture where network control is decoupled from forwarding and is directly programmable [160]." SDN decouples the control plane from the data plane. The data plane includes devices such as routers and switches that follow the controller rules to perform packet forwarding. The control plane includes controllers that oversee the network operations and provide a platform for the implementation of different network services and applications. The main advantage of SDN is that it offers the rapid implementation and deployment of innovative solutions (e.g., network security, network virtualization, and green networking) in the form of software. Additionally, SDN uses the cross-layer information and global network view in the logical centralization of feedback control to make better decisions. Therefore, SDN provides enhanced network configuration, improved network performance, and higher network flexibility to accommodate innovative architectures and operations [153].

Although SDN provides many benefits to overcome the complexity issue, it also has some associated challenges including SDN interoperability issues with legacy network devices, performance and privacy concerns with centralized control, and lack of experts for technical support. Additionally, the shift from traditional networking to SDN can be disruptive [153].

G. Security Challenges and Recommended Solutions

"A cyber security vulnerability is a weakness in a computing system that can result in harm to the system or its operation, especially when this weakness is exploited by a hostile actor or is present in conjunction with particular events or circumstances [161]." Consider the hypothetical threat where an adversary can steal information or take down servers, which could disrupt power network operations [162]. Cyber security is a potential issue for EPES modernization. Recent cyber attacks on IoT devices include the distributed denial of service (DDoS) attack on Dyn's managed domain name system infrastructure using Mirai botnet affecting over 100,000 endpoints [163], ransomware for smart thermostats that lock the user out and demand bitcoins to release the thermostat [164], Bluetooth smart locks that are easily hacked [165], DoS attacks by a lightbulb that froze the controls of the entire smart home [166], and the ease by which a neighbor was able to unlock the resident's front door smart lock, connected over Apple HomeKit, and gained entry into the house by simply issuing the unlock voice command to Siri [167].

Security solutions developed for IT computer systems will typically be inappropriate for EPESs. The attack incident taxonomy used by Computer Emergency Response Team (CERT) to describe security incidents is shown in Fig. 13 [168]. This taxonomy provides uniform terminology and useful framework to the security research community. Incidents consist of a set of attacks that are executed to achieve the desired objectives. Attacks produce unauthorized results by using tools to exploit system/network vulnerabilities. An attack consists of a sequence of events.

Fig. 14 shows a modified attack taxonomy that adapts this approach to the EPES network. As before, attackers use tools to exploit the vulnerabilities of the IoT devices in EPESs and launch attacks against targets to obtain unauthorized results.

There are four general classes of attacks for the integrity, availability, confidentiality, access control, authentication, and nonrepudiation security aspects [169, 193]:

- Interruption: Asset availability is disrupted
- Interception: Unauthorized asset access
- Modification: Unauthorized asset tampering
- Fabrication: Fictitious asset creation

Security solutions are needed to overcome these risks and protect the IoT devices, networks, and sensitive data from security breaches and unauthorized access. Discussed below are some of the security challenges and recommended solutions for IoT devices in EPESs [170].

1) Interruption Attacks: An interruption attack includes both hardware-based DoS attack or sabotage and software-based DoS attack [171].

a) Sabotage and Countermeasures: IoT device hardware or infrastructure sabotage (e.g. cutting a cable or inflicting damage to a physical IoT device) result in the disconnection of the device from the network. Examples of sabotage in

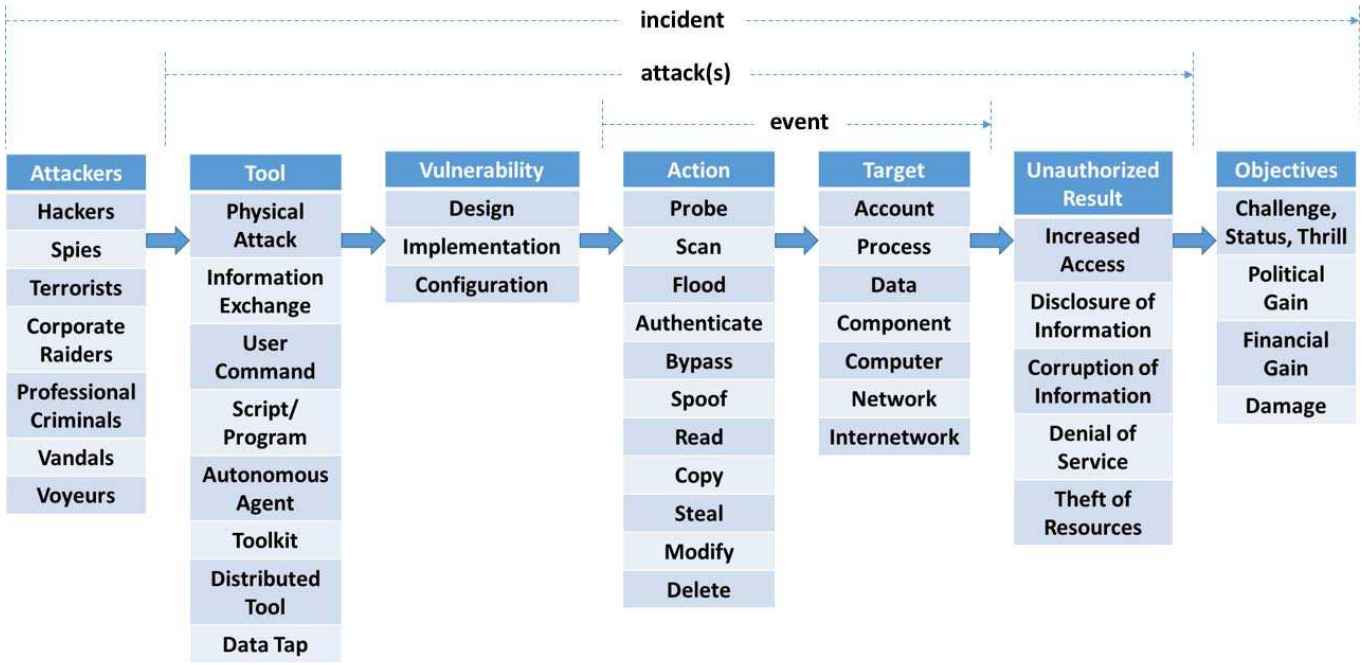


Fig. 13. Attack taxonomy by CERT [168].

the EPES include cutting a network connection between the PMU and phasor data concentrator (PDC), PDCs and a Super PDC, or inflicting physical damage to PMUs and smart meters [172-175]. Power stations are susceptible to sabotage as well. An example includes the sniper attack on the California power station where 17 giant transformers funneling power to Silicon Valley were knocked out [176]. Nuclear power plants are also vulnerable to sabotage by terrorist attacks. A study conducted by the National Academy of Sciences projected a high risk of ground or air assault to nuclear power plants, which could result in a core meltdown and failure of the containment infrastructure releasing a large amount of radioactive substances [177, 178]. Sabotage of nuclear power plants can potentially have a long-lasting and devastating effect on the environment, public health, and economy. These attacks can be reduced by limiting access to critical IoT infrastructure.

b) DoS Attacks and Countermeasures: In DoS attacks, the attacker compromises several machines (or zombies) and consumes network resources, which overloads the bandwidth of the target and results in slowed or dropped legitimate traffic (also known as distributed DoS (DDoS)). For instance, DoS attacks on EPES devices (e.g. PMUs and smart meters) relying on the real-time measurement data cause delayed or lost measurements from these devices. This results in inaccurate predictions of the transmission system status, delayed resolution of power system complications, or complete failure of network measurement devices. Other examples of DoS attacks include network layer attacks, transport layer attacks, Local Area Network Denial attacks, and teardrop attacks [179]. In teardrop attacks, the attackers transmit fragmented packets to a target. Due to a bug in TCP/IP fragmentation reassembly, the target is not able to reassemble the received packets resulting in overlapping packets, which crash the target network device [180]. DoS attacks have the capability to inflict serious damage to the EPES and therefore, must be reduced by using network security techniques such as air gapped network, anomaly detection approaches, big pipes, and traffic filtering.

An air gapped network is a network security technique that physically isolates a secure computer network from other insecure networks (e.g. public Internet or an insecure local area network). It eliminates any communication with the machines not connected to the local segment. However, there is a drawback to this technique in terms of the high costs associated with building separate network infrastructures for the EPES.

Anomaly detection approaches are used to detect DoS attacks on EPES networks. Experimental results have shown that the detection performance is inversely proportional to the network utilization. Also, the optimal detection parameters have a strong dependence on the network utilization [181].

Big pipes are large bandwidth network connections that can absorb attack traffic to mitigate the DoS attack on the EPES. However, there is a drawback to this technique in terms of the high costs associated with it.

A less expensive approach to mitigate DoS attacks on EPES networks is traffic filtering. This approach utilizes distributed or redundant infrastructure to redirect attack traffic [182]. However, there are a couple of drawbacks with this technique including the lack of documentation to support the claim of filtering DoS traffic from normal traffic and the difficulty of employing this technique, especially with large traffic volume [171-173, 178, 182-187].

2) Interception Attacks: An interception attack gains access to the information that is traversing the network between EPES devices (e.g. between PMU and PDC). These attacks can either be passive or active. Two types of interception attacks, packet

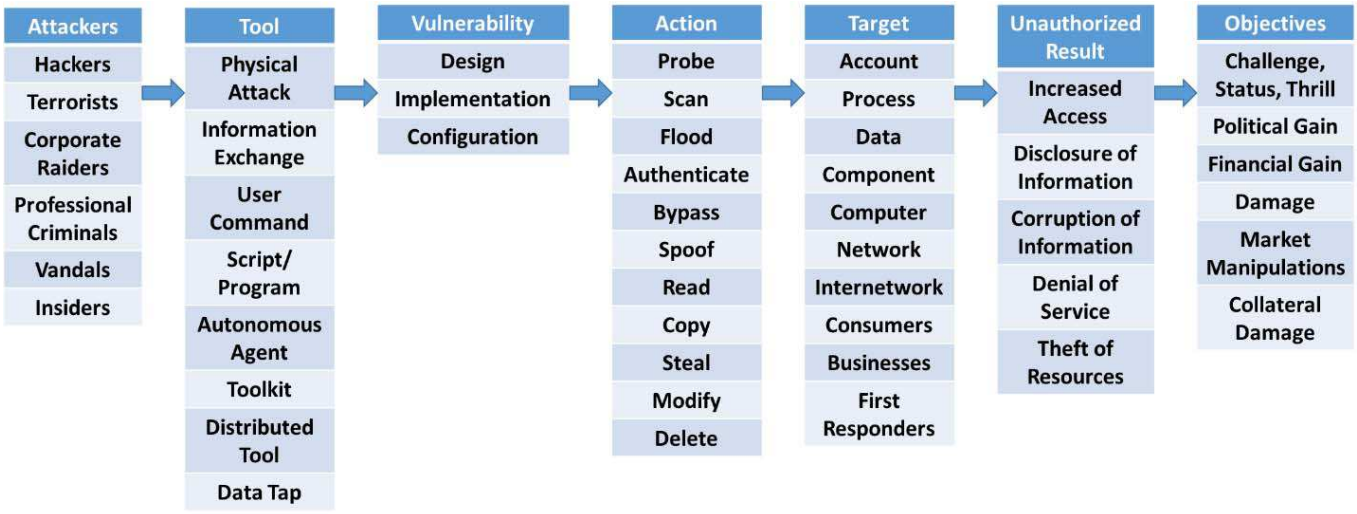


Fig. 14. Modified attack taxonomy for EPES networks.

sniffing and side channel attacks, are discussed below [181].

a) Packet Sniffing and Countermeasures: Attackers can gain access to the contents of the PMU or smart meter Transmission Control Protocol (TCP)/Internet Protocol (IP) packets that are sent across the EPES network using software programs such as Wireshark [171]. This is known as packet analysis or packet sniffing. In the absence of encryption, the attacker can see and harvest all the sensitive information in the data packet. An instance of packet sniffing was reported in [186], where the authors used Wireshark to analyze the network traffic in a synchrophasor network.

Packet sniffing can be mitigated by using a security gateway that sends packets through a virtual private network (VPN) tunnel, which is created by embedding an IP tunnel (with encryption) within the normal IP network payload. The encryption hides the data from the attackers, making the network private, in addition to being virtual [186]. The communications between VPNs are secured using the Transport Layer Security (TLS) protocol. The connections between different parties on the EPES network are secured using the X.509 certificates, which first authenticate users and subsequently exchange symmetric keys. However, there is a possibility that the X.509 certificates are compromised or are issued in error [173]. An instance of compromised certificates was reported in [188], where an imposter tricked VeriSign in to issuing two certificates for Microsoft. Although using VPN tunnels provide EPES network security, they have associated implementation and design errors. For example, an attack on a VPN tunnel was reported in [173], where the Heartbleed bug was discovered in the OpenSSL cryptography library leaving around half a million supposedly secure web servers vulnerable to cyber attacks. Therefore, it is essential to verify the security of VPN tunnels during their implementation [173, 178, 186, 189]. Using pre-shared keys is usually effective. Also, Secure Sockets Layer certificates or TLS certificates, which are generated by a common root of trust controlled by a trusted entity, can be used.

b) Side Channel Attacks and Countermeasures: From the above discussion, even though VPN encryption provides security for network connections, side-channel attacks are still possible. In side-channel attacks, sensitive information can be extracted by observing implementation artifacts [170, 190]. An example side-channel attack is in [180], where the protocol information was extracted by using a timing side-channel vulnerability for secure shell – a cryptographic network protocol [191]. Other instances of side channel attacks were reported in [192] and [193], where the authors indicated the possibility to identify VPN-encrypted PMU measurement sessions allowing attackers to reroute, delay, or drop data packets [192], and analyze VPN power consumption [193]. This could severely degrade the EPES monitoring as the attacker can stop parts of the system's feedback control and hide inefficiencies or instabilities in the EPES.

To counter side channel attacks on EPES, the communication channel bandwidth could be saturated to disallow any new patterns to emerge. However, this approach has an extreme resource requirement and can only be used in extreme cases [194]. Additionally, the detection of saturated channels, which can potentially be side channels, helps mitigate side channel attacks in EPES. Also, building a separate infrastructure for EPES device communications can help resolve side channel attacks, but it is an expensive approach [192].

3) Modification Attacks: Modification attacks exploit security vulnerabilities in EPESs for corrupting, highjacking, or altering a legitimate process. Examples of modification attacks include man-in-the-middle (MITM) attack and Structured Query Language (SQL) injection [170].

a) MITM Attacks and Countermeasures: In MITM attacks, the attacker poses as the legitimate target to both the legitimate client and server during the protocol session. In other words, if A and B are communicating with each other, the intruder I disguises itself as B in front of A and as A in front of B, thereby replacing the AB link with two links AI and IB [170]. MITM attack in an EPES network splits the PMU-PDC communication link with two links PMU-I

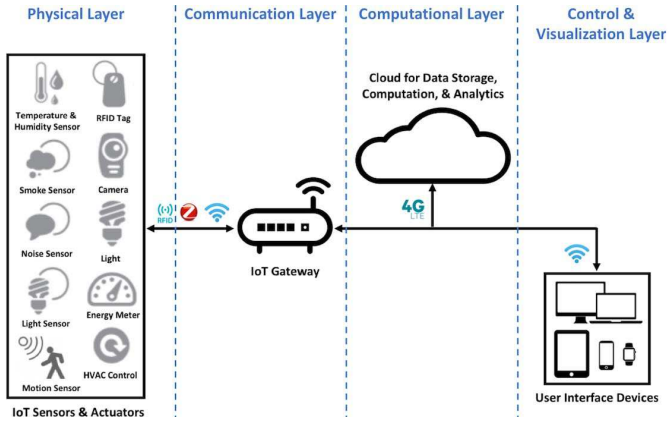


Fig. 15. Layered architecture of applying IoT in a smart building environment.

and I-PDC. Some of the MITM attack methods include route table poisoning, modified packet source and destinations, and compromised certificates [170]. An instance of compromised certificate of Hypertext Transfer Protocol (HTTP) over TLS (HTTPS) connection was reported in [195], where the authors used fake certificates to initiate a MITM attack. PMU communications with PDC in a EPES network uses X.509 certificates for authentication, which can be compromised making PMU-PDC communication vulnerable to a MITM attack.

To counter the MITM attacks, the network traffic should be encrypted using security gateways [190]. The security gateway creates a VPN tunnel (unsecure network) connecting two secure networks. To ensure that the sensitive data is protected when passing through the VPN tunnel, the security gateway encrypts the data at the source and decrypts the data at the target. This encryption is typically done in hardware and can be efficient. Security gateways support EPES communications and interoperability by employing the Internet Protocol Security (IPsec) protocol. IPsec secures the communication link by ensuring that the data stays authentic, unaltered, and confidential throughout the communication process [190]. Additionally, to mitigate MITM attacks, both the system client and server need to be authenticated [189]. TLS protocols have in-built public key cryptography mechanisms that can promptly detect and correct any errors to avoid the occurrence of MITM attacks [171-173, 178, 184, 189, 196].

b) SQL Injection and Countermeasures: In SQL injection, the attacker alters the database by inserting new script commands [170]. Smart meters continuously send energy usage data to the utilities and the users, which is stored in a database. The SQL injection occurs if the queries formulated by the user are not properly validated before inclusion in the SQL query [197]. This attack can send malicious queries to the database management system to add, delete, or modify the database contents and take control of the system. This can disrupt the EPES operations as the attacker can indicate a normal operation state even when it's not, which might eventually result in an outage.

SQL injection on EPES networks can be mitigated by using measures including input type checking, positive pattern matching, penetration testing, static code checking, limiting database access to remote users, and avoiding dynamic SQL use [198, 199]. In input type checking, the characters that can be abused, like ";", are filtered out by the programmer to avoid any malformed input. This is not simple; authors in [200] have shown that most existing tools for sanitizing inputs have errors. In positive pattern matching, the user input is matched with the format of a good input. In penetration testing, SQL injection is attempted on the interface to ensure that these attacks are properly detected. In static code checking, the program is checked for correctness using code checking tools. Limiting database access to remote users means that the remote users should have limited rights on the database and all their inputs should go through an application program interface (API). Dynamic SQL use should be avoided and user inputs should be forced to use static templates and existing tables [173, 198, 199].

4) Fabrication Attacks: In fabrication attacks, the attacker creates a fictitious asset on the EPES network that transmits fabricated data across the network, which may be accepted by other network assets if not properly authenticated. Data spoofing – a type of fabrication attack is discussed below [170].

Data Spoofing and Countermeasures: The accuracy of data in the EPES network is critical for its efficient and reliable operation. In data spoofing, fabricated (inaccurate) data is injected into the control centers. An instance of data spoofing on EPES network was reported in [187], where the authors injected fabricated data (voltage, current, frequency, or GPS time stamp data) into the system. Another instance of a data spoofing was reported in [201], where the authors injected a fabricated GPS time stamp data into the system for measurements. Data spoofing severely degrade the EPES operation, stability, security, and reliability, which may result in an outage.

To counter data spoofing, the authors in [172] advise using a single data feed. Additionally, multiple/redundant EPES devices (smart meters or PMUs) can be used to monitor the same electrical transmission bus to reduce data spoofing [174]. Other approaches to mitigate data spoofing include collaboration among GPS receivers to efficiently detect any spoofing [202] and synchronizing measurements using the network time protocol (NTP) across different locations in real time [203]. A combination of NTP and GPS is recommended to limit the modification of timestamps through GPS spoofing [168, 172-174, 178, 184, 186, 201].

Table I provides a summary of the challenges and proposed solutions for IoT deployment in EPESs.

V. Building Automation – A Real-World Application Example of IoT in Electric Power and Energy Systems

In current building environments, there exists problems including inefficient energy management, wasted energy resources, and expensive energy costs. IoT-enabled building automation can overcome these challenges and improve operational efficiency and productivity gains thereby boosting the bottom line by providing building managers full visibility,

TABLE I
SUMMARY OF CHALLENGES AND PROPOSED SOLUTIONS FOR IOT DEPLOYMENT IN EPESS

IoT Challenges for Deployment in EPESs	Proposed Solution Mechanisms	Related Work References
Sensing Current IoT sensors lack the following critical features: • Situational intelligence • Efficient power management • Enhanced cyber security	**Sensing** • Integrating historical IoT sensor data with real time data • Using arrays of low accuracy sensor modules with subsequent data fusion to generate high-accuracy information • Embedding hardware security features, adding more security layers, and advanced virtualization	[19], [23], [65-83]
Connectivity • Lack of interoperability between all the different standards for IoT • Coexistence challenge	**Connectivity** • Comprehensive connectivity standards (e.g. 5G) • Wireless convergence modules, fair channel assignments, and dynamic licensed spectrum sharing	[84], [98-103]
Power management • Difficult to incorporate power management in IoT devices due to variations in power collection methods	**Power management** • Energy harvesting systems deployed in randomly distributed multi-hop topology and uniformly distributed ring topology • Energy-efficient wireless, wired, optical, and optical-wireless communication networks	[104-106], [108-136]
Big data • Difficult to store, track, analyze, capture, cure, search, share, transfer, secure, visualize, and interpret the generated data	**Big data** • Apache Hadoop – an open-source software framework • New IoT cloud ecosystem	[137], [138]
IoT Data Computation • Centralized computation and storage solution is not ideal for real-time heterogeneous IoT data and results in inefficient service-provisioning and increased latency • IoT ecosystems are constrained in terms of low power communications, scarce energy, and lossy communications	**IoT Data Computation** • Localized computation and storage solutions for processing, analyzing, and storing IoT data • Fog computing • IoT data footprint reduction methods (e.g. dimensionality reduction and data filtering)	[59], [142-146], [148-152]
Complexity • Increased network size from wide penetration of IoT devices • Increased heterogeneity from different vendors providing services, equipment, and applications	**Complexity** • Simplification of IoT device design and development • Encapsulation of wireless capabilities • Providing easier to understand reference designs, modules, and on-chip connectivity stack and development environment • Software-defined networking (SDN)	[101], [137], [153-160]
Security • Sabotage • DoS attacks • Packet sniffing • Side channel attacks • MITM attacks • SQL injection • Data spoofing	**Security** • Limiting access to critical IoT infrastructure • Using air gapped network, anomaly detection approaches, big pipes, and traffic filtering • Using security gateway that sends packets through a VPN tunnel • Saturating communication channel bandwidth, detection of saturated channels, and building a separate infrastructure for EPES device communications • Encryption of network traffic using security gateways, and authentication of both the system client and server • Using input type checking, positive pattern matching, penetration testing, static code checking, limiting database access to remote users, and avoiding dynamic SQL use • Using single data feed, using multiple/redundant EPES devices to monitor the same electrical transmission bus, collaboration among GPS receivers, and synchronizing measurements using NTP across different locations in real time	[66-68], [161-203]

flexibility, and control of all building assets. Fig. 15 shows a reference model that describes the layered architecture of applying IoT in a smart building environment. This model can be adapted for any IoT application in EPESs.

The architecture shown in Fig. 15 includes four layers viz. physical layer, communication layer, computational layer, and control and visualization layer. The physical layer comprises of IoT sensors (e.g. temperature and humidity sensor, motion sensor, and light sensor) and IoT actuators (e.g. light controller and HVAC controller). IoT sensors monitor the smart building environment and assets' operation state. The operational data is transmitted to the communication layer using some communication technology (e.g. ZigBee, WiFi, and RFID). The communication layer comprises of IoT gateway that receives

the operational data and transmits it to computational layer (using 4G) and control and visualization layer (using WiFi). The computational layer comprises of the cloud for storing, computing, and analyzing the operational data to generate actionable information. This information is also transmitted to the control and visualization layer via IoT gateway. The control and visualization layer includes user interface devices (e.g. tablet, desktop computer, laptop, smart phone, and smart watch) that perform three tasks: (1) generate visualizations using the operational data from IoT sensors, (2) generate control parameters using the actionable information from the cloud, and (3) transmit the generated control parameters to IoT actuators in the physical layer via IoT gateway. The smart building assets are regulated based on the control parameters to improve both their energy and operation efficiencies.

VI. Conclusions

Important role of IoT in transforming EPESs was presented in this paper. Digitizing the electric power ecosystem using IoT helps to better account for DER integration; reduce energy wastage; generate savings; and improve the efficiency, reliability, resiliency, security, and sustainability of the electric power networks. The role of IoT sensors for smart home scenario was also presented in this paper, wherein a detailed assessment of the technical parameters of IoT sensors was provided. Additionally, IoT sensors that are currently on the market were surveyed.

IoT for EPESs presents an exciting area of innovative growth and development and has a significant impact on the economy, society, and environment; in terms of increased revenue in EPESs, reduced CO_2 emissions, lifestyle convenience, public safety, energy conservation, expense reduction, and a healthy living environment.

Apart from the numerous advantages of IoT for EPESs, it also has some associated challenges, viz. sensing, connectivity, power management, big data, computation, complexity, and security. To ensure continued growth of IoT for EPESs, it is essential to develop viable solutions to handle its growing complexity. Some of the recommended solutions were reviewed in the paper.

A potential direction to handle complexity of future IoT can be inspired from brain computing (with 100 billion neurons in a human brain, where each neuron is connected to 10,000 other neurons). Computational intelligence is the future to handling complexity in artificial systems.

References

[1] B. Gokay, "The 2008 World Economic Crisis: Global Shifts and Faultlines," Global Research, February 2009, http://www.globalresearch.ca/the-2008-world-economic-crisis-global-shifts-and-faultlines/12283

[2] "Paris Agreement", PARIS2015 UN Climate Change Conference COP21•CMP11, December 2015, http://ec.europa.eu/clima/policies/international/negotiations/paris/index_en.htm

[3] M. Liebreich, "Lithium-ion EV battery experience curve compared with solar PV experience curve", Bloomberg New Energy Finance Summit 2015, April 2015, https://data.bloomberglp.com/bnef/sites/4/2015/04/Final-keynote_ML.pdf

[4] G. Bedi, G. K. Venayagamoorthy and R. Singh, "Navigating the challenges of Internet of Things (IoT) for power and energy systems," 2016 Clemson University Power Systems Conference (PSC), Clemson, SC, 2016, pp. 1-5

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015

[6] G. Bedi, G. K. Venayagamoorthy and R. Singh, " Towards an Intelligent Power Network with Internet of Things (IoT)," accepted for publication in Intelligent Systems Conference 2017

[7] R. Bigliani, J-F. Segalotto and G. Gallotti, "Shaping a New Battleground in the IoT Era: Highlights from the 2016 IDC Pan–European Utilities Executive Summit," IDC Energy Insights, June 2016, https://www.ericsson.com/res/narratives/docs/industries/iot-utilities-era-new-battleground-idc-summit-report-2016.pdf

[8] S. Jankowski, J. Covello, H. Bellini, J. Ritchie, and D. Costa, "The Internet of Things: Making sense of the next mega-trend", Goldman Sachs IoT Primer Report, September 2014, http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf

[9] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," U.S.-Canada Power System Outage Task Force, April 2004, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[10] M. Annunziata, G. Bell, R. Buch, S. Patel, and N. Sanyal, "Powering the Future: Leading the Digital Transformation of the Power Industry", GE Power Digital Solutions, 2016, https://www.gepower.com/content/dam/gepower-pw/global/en_US/documents/industrial%20internet%20and%20big%20data/powering-the-future-whitepaper.pdf

[11] X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012

[12] S. Jain, Vinoth Kumar N., A. Paventhan, V. Kumar Chinnaiyan, V. Arnachalam and Pradish M., "Survey on smart grid technologies- smart metering, IoT and EMS," Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on, Bhopal, 2014, pp. 1-6

[13] R. Young, J.McCue, and C. Grant, "The power is on: How IoT technology is driving energy innovation", Deloitte Center for Energy Solutions Report, January 2016, http://dupress.com/articles/internet-of-things-iot-in-electric-power-industry/

[14] Al-Ali, A.R. and Aburukba, R., "Role of Internet of Things in the Smart Grid Technology" Journal of Computer and Communications, 3, 229-233, (2015)

[15] L. Li, H. Xiaoguang, C. Ke and H. Ketai, "The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid," 2011 6th IEEE Conference on Industrial Electronics and Applications, Beijing, 2011, pp. 789-793

[16] Chakib Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", Procedia Computer Science, Volume 34, 2014, pp. 532-537

[17] Miao Yun and Bu Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," Advances in Energy Engineering (ICAEE), 2010 International Conference on, Beijing, 2010, pp. 69-72.

[18] J. Gubbi et al., "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems 29, 1645–1660, (2013)

[19] J. Liu, X. Li, X. Chen, Y. Zhen and L. Zeng, "Applications of Internet of Things on smart grid in China," Advanced Communication Technology (ICACT), 2011 13th International Conference on, Seoul, 2011, pp. 13-17

[20] N. Bui, A. P. Castellani, P. Casari and M. Zorzi, "The internet of energy: a web-enabled smart grid system," in IEEE Network, vol. 26, no. 4, pp. 39-45, July-August 2012

[21] Q. Ou, Y. Zhen, X. Li, Y. Zhang and L. Zeng, "Application of Internet of Things in Smart Grid Power Transmission," Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2012 Third FTRA International Conference on, Vancouver, BC, 2012, pp. 96-100

[22] R. Smith, "How America Could Go Dark," http://www.wsj.com/articles/how-america-could-go-dark-1468423254, Washington Street Journal, July 2016

[23] Electric Power Research Institute (EPRI), "Contributions of Supply and Demand Resources to Required Power System Reliability Services", May 2015, http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002006400

[24] R. Gore and S. P. Valsan, "Big Data challenges in smart Grid IoT (WAMS) deployment," 2016 8th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, 2016, pp. 1-6

[25] GE Reports, "The Digital Power Plant: Bridging the intelligence gap between people and machines," https://www.ge.com/digital/sites/default/files/GE-Digital-Power-Plant-Brochure.pdf

[26] D. Lounsbury, "Weighing the Advantages of Distributed and Centralized Energy Storage," Renewable Energy World, April 2015, http://www.renewableenergyworld.com/articles/2015/04/weighing-the-advantages-of-distributed-energy-storage-and-centralized-energy-storage.html

[27] A. A. Asif, R. Singh, and G. K. Venayagamoorthy, "Ultra-Low Cost and Solar Storm Secured Local DC Electricity to Address Climate Change Challenges for All Economies", 2016 Clemson University Power Systems Conference (PSC), Clemson, SC, USA, 2016

[28] G. K. Venayagamoorthy, P. Mitra, K. Corzine and C. Huston, "Real-time modeling of distributed plug-in vehicles for V2G transactions," 2009 IEEE Energy Conversion Congress and Exposition, San Jose, CA, 2009, pp. 3937-3941

[29] J. S. Vardakas, N. Zorba and C. V. Verikoukis, "A Survey on Demand Response Programs in Smart Grids: Pricing Methods and Optimization Algorithms," in IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 152-178, Firstquarter 2015

[30] Y. K. Chen, "Challenges and opportunities of internet of things," 17th Asia and South Pacific Design Automation Conference, Sydney, NSW, 2012, pp. 383-388

[31] D. Partynski and S. G. M. Koo, "Integration of Smart Sensor Networks into Internet of Things: Challenges and Applications," Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, Beijing, 2013, pp. 1162-1167

[32] S. D. T. Kelly, N. K. Suryadevara and S. C. Mukhopadhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes," IEEE Sensors Journal, vol. 13, no. 10, pp. 3846-3853, Oct. 2013

[33] J. Pan, R. Jain and S. Paul, "A Survey of Energy Efficiency in Buildings and Microgrids using Networking Technologies," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1709-1731, Third Quarter 2014

[34] J. Shah and B. Mishra, "Customized IoT enabled Wireless Sensing and Monitoring Platform for Smart Buildings," 3rd International Conference on Innovations in Automation and Mechatronics Engineering 2016, ICIAME 2016 05-06 February, 2016, Volume 23, 2016, Pages 256-263

[35] G. Bedi, G. K. Venayagamoorthy and R. Singh, " Internet of Things (IoT) Sensors for Smart Home Electric Energy Usage Management," accepted for publication in 2016 IEEE International Conference on Information and Automation for Sustainability

[36] "Sensors & Security", http://www.smarthome.com/sensors-security.html, last accessed 06/14/2016

[37] "Wireless Home Sensor Systems", http://postscapes.com/home-wireless-sensor-systems, last accessed 06/14/2016

[38] W. Lee, S. Cho, P. Chu, H. Vu, S. Helal, W. Song, Y.-S. Jeong, and K. Cho, "Automatic agent generation for IoT-based smart house simulator," Neurocomputing, Available online 8 June 2016, (http://www.sciencedirect.com/science/article/pii/S092523121630580X)

[39] "The Beginner's Guide to Motion Sensors," by SafeWise, 2013, http://www.safewise.com/resources/motion-sensor-guide

[40] "Perimeter Security Sensor Technologies Handbook," by Defense Advanced Research Projects Agency (DARPA) and The National Institute of Justice (NIJ), July 1998, https://www.ncjrs.gov/pdffiles1/Digitization/206415NCJRS.pdf

[41] "The Seven Basic Types of Temperature Sensors," by Water & Wastes Digest, December 2000, http://www.wwdmag.com/water/seven-basic-types-temperature-sensors

[42] D. K. Roveti, "Choosing a Humidity Sensor: A Review of Three Technologies," Sensors Online, July 2001, http://www.sensorsmag.com/sensors/humidity-moisture/choosing-a-humidity-sensor-a-review-three-technologies-840

[43] "Water Detection Sensors: Types and Applications," by Network Technologies Incorporated, September 2013, http://www.networktechinc.com/blog/water-detection-sensors-types-and-applications/303/

[44] "Types of Smoke Alarms and Detectors," by Grainger, https://www.grainger.com/content/qt-types-smoke-alarms-detectors-366, last accessed 11/04/2016

[45] C. Mathas, "Light Sensors: An Overview," Digi-Key Electronics, September 2012, http://www.digikey.com/en/articles/techzone/2012/sep/light-sensors-an-overview

[46] "Energy Monitoring," by Green Step, http://www.greensteptoday.com/energy-monitoring, last accessed 11/04/2016

[47] Ed Korczynski, "IoT demands: Are we ready?", Solid State Technology, June 2016, pp. 19-23

[48] S. Pateras, "Dreaming of plug-and-play IP," http://electroiq.com/blog/2012/12/dreaming-of-plug-and-play-ip/, Solid State Technology, last accessed 07/15/2016

[49] "1801-2015 - IEEE Standard for Design and Verification of Low-Power, Energy-Aware Electronic Systems," https://standards.ieee.org/findstds/standard/1801-2015.html, last accessed 09/04/2016

[50] E. Sperling, "What's Important For IoT—Power, Performance Or Integration?," Semiconductor Engineering, August 2016, http://semiengineering.com/whats-important-for-iot-power-performance-or-integration/

[51] "Sales of Light Duty Electric Vehicles Are Expected To Reach 6.4 Million Annually by 2023" by Navigant Research, https://www.navigantresearch.com/newsroom/sales-of-light-duty-electric-vehicles-are-expected-to-reach-6-4-million-annually-by-2023, January 2015

[52] W. Kempton, J. Tomicì, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," Journal of Power Sources, Volume 166 Issue 2, 15 April 2007, Pages 549-566

[53] Hutson, Chris M., Venayagamoorthy, Ganesh K., Corzine, Keith A. "Intelligent Scheduling of Hybrid and Electric Vehicle Storage Capacity in a Parking Lot for Profit Maximization in Grid Power Transactions" IEEE Energy 2030, 2008, 17-18 November 2008

[54] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, "Disruptive technologies: Advances that will transform life, business, and the global economy", McKinsey Global Institute, May 2013, http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies

[55] J. Bradley, J. Barbier, D. Handler, "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience", Cisco Systems, Inc, 2013, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf

[56] AT&T and the Utilities, "An insight into best practice enablers in the U.S. utility sector," http://www.m2mnow.biz/2015/07/08/34626-m2m-now- magazine-july-august-2015-edition/, M2M Now Magazine, July-August 2015

[57] "The Evolution of Wireless Sensor Networks" by Silicon Laboratories, Inc., 2013, http://www.silabs.com/Support%20Documents/TechnicalDocs/evolution-of-wireless-sensor-networks.pdf

[58] "Smart/Intelligent Sensors Market-Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2013-2019" by Transparency Market Research, April 2014, http://www.transparencymarketresearch.com/smart-intelligent-sensor-market.html

[59] A. Markkanen, "Competitive Edge from Edge Intelligence IoT Analytics Today and in 2020," ABI Research, May 2015, https://www.thingworx.com/wp-content/uploads/2016/05/WP_abi-research_iot-analytics-today-and-in-2020_EN.pdf

[60] R. Hledik, "How Green Is the Smart Grid?", The Electricity Journal, Volume 22, Issue 3, April 2009, Pages 29-41

[61] M. Cullinen, "Machine to Machine technologies: Unlocking the potential of a $1 trillion industry", AT&T Carbon War Room Research Report, February 2013, http://carbonwarroom.com/sites/default/files/reports/M2M%20Technologies%20%28Carbon%20War%20Room%29.pdf

[62] "Clean Power Plan Saves Nearly $40 Billion On Health, Too," http://cleantechnica.com/2016/07/15/clean-power-plan-saves-nearly-40-billion-health/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IM-cleantechnica+%28CleanTechnica%29, CleanTechnica, July 2016

[63] "The Societal Impact of the Internet of Things", BCS-OII Forum Report, March 2013 BCS-OII Forum Report, March 2013, https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf

[64] "China aims to lead the world in connecting the factory," http://www.economist.com/news/business/21702487-china-aims-lead-world-connecting-factory-great-convergence, The great convergence | The Economist, July 2016

[65] G. K. Venayagamoorthy, "Dynamic, Stochastic, Computational, and Scalable Technologies for Smart Grids," in IEEE Computational Intelligence Magazine, vol. 6, no. 3, pp. 22-35, Aug. 2011

[66] A. Jha and S. M C, "Security considerations for Internet of Things", http://www.lnttechservices.com/media/30090/whitepaper_security-considerations-for-internet-of-things.pdf, L&T Technology Services, 2014

[67] "IC Industry Waking Up To Security", http://semiengineering.com/ic-industry-waking-up-to-security/, last accessed 06/15/2016

[68] "Cyber Defense: Businesses Need Effective Security Partnerships to Stop Advanced Attacks" Bloomberg Businessweek, July 2016

[69] P. K. Choubey, S. Pateria, A. Saxena, Vaisakh Punnekkattu Chirayil SB, K. K. Jha and Sharana Basaiah PM, "Power efficient, bandwidth optimized and fault tolerant sensor management for IOT in Smart Home," Advance Computing Conference (IACC), 2015 IEEE International, Banglore, 2015, pp. 366-370

[70] M. Usman, V. Muthukkumarasamy and X. W. Wu, "Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic," in IEEE Transactions on Consumer Electronics, vol. 61, no. 2, pp. 197-205, May 2015

[71] J. Ye, G. Stevenson and S. Dobson, "Fault detection for binary sensors in smart home environments," Pervasive Computing and Communications (PerCom), 2015 IEEE International Conference on, St. Louis, MO, 2015, pp. 20-28

[72] M. Li and H. J. Lin, "Design and Implementation of Smart Home Control Systems Based on Wireless Sensor Networks and Power Line Communications," in IEEE Transactions on Industrial Electronics, vol. 62, no. 7, pp. 4430-4442, July 2015

[73] Y. Tao, X. Xu and X. Wang, "Service-Based Interactive Proxy for Sensor Networks in Smart Home: An Implementation of Home Service Bus," Digital Home (ICDH), 2014 5th International Conference on, Guangzhou, 2014, pp. 237-241

[74] V. Tulceanu, "A Matter of Trust: Smart Home System Relying on Logic, BCI, and Sensor Agents," 2015 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), Timisoara, 2015, pp. 177-180

[75] Q. Wan, Y. Li, C. Li and R. Pal, "Gesture recognition for smart home applications using portable radar sensors," 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Chicago, IL, 2014, pp. 6414-6417

[76] P. Györke and B. Pataki, "Energy harvesting wireless sensors for smart home applications," 2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, Pisa, 2015, pp. 1757-1762

[77] M. Á Serna, C. J. Sreenan and S. Fedor, "A visual programming framework for wireless sensor networks in smart home applications," Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on, Singapore, 2015, pp. 1-6

[78] A. Alami, L. Benhlima and S. Bah, "An overview of privacy preserving techniques in smart home Wireless Sensor Networks," 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA), Rabat, 2015, pp. 1-4

[79] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 414-454, First Quarter 2014

[80] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow and P. Polakos, "Wireless sensor network virtualization: A survey," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 553-576, Firstquarter 2016

[81] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system, Future Generation Computer Systems," Volume 56, March 2016, Pages 719-733, (http://www.sciencedirect.com/science/article/pii/S0167739X15002812)

[82] Y. Liu and S. Hu, "Chapter 10 - Smart home scheduling and cybersecurity: fundamentals," In Smart Cities and Homes, edited by Mohammad S. Obaidat and Petros Nicopolitidis, Morgan Kaufmann, Boston, 2016, Pages 191-217, (http://www.sciencedirect.com/science/article/pii/B9780128034545000109)

[83] Y. Liu, S. Hu, J. Wu, Y. Shi, Y. Jin, Y. Hu and X. Li, "Chapter 9 - Smart home cybersecurity considering the integration of renewable energy," In Smart Cities and Homes, edited by Mohammad S. Obaidat and Petros Nicopolitidis, Morgan Kaufmann, Boston, 2016, Pages 173-189, (http://www.sciencedirect.com/science/article/pii/B9780128034545000092)

[84] V. Gazis, "A Survey of Standards for Machine to Machine (M2M) and the Internet of Things (IoT)," in IEEE Communications Surveys & Tutorials, vol.PP, no.99, pp.1-1

[85] ITU-T, Focus Group on M2M Service Layer, ITU-T Std., http://www.itu.int/en/ITU-T/focusgroups/m2m/Pages/default.aspx, last accessed 07/30/2016

[86] ETSI, TS 102 689; Machine-to-Machine communications (M2M); M2M service requirements Release 2, European Telecommunications Standards Institute (ETSI) Std., 2013, http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=38384, last accessed 07/30/2016

[87] oneM2M Partners, oneM2M Partnership Agreement, http://www.onem2m.org/docs/oneM2M_Partnership_Agreement.pdf, Std., July 2012

[88] TIA, TIA-4940.005: Smart Device Communications Reference Architecture, Telecommunications Industry Association Std., 2012, http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-4940, last accessed 07/30/2016

[89] ATIS, Assessments and Recommendations, ATIS Std., 2013, http://atis.org/M2M/index.asp, last accessed 07/30/2016

[90] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFCs 5746, 5878, 6176, http://www.ietf.org/rfc/rfc5246.txt, last accessed 07/30/2016

[91] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347 (Proposed Standard), Internet Engineering Task Force, Jan. 2012, http://www.ietf.org/rfc/rfc6347.txt, last accessed 07/30/2016

[92] P. Thubert, "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)," RFC 6552 (Proposed Standard), Internet Engineering Task Force, Mar. 2012, http://www.ietf.org/rfc/rfc6552.txt, last accessed 07/30/2016

[93] IEEE 802.24 Vertical Applications TAG, Institute of Electrical and Electronics Engineers (IEEE) Std., 2014, http://www.ieee802.org/24/, last accessed 07/30/2016

[94] OGC, Sensor Web Enablement Architecture, Open Geospatial Consortium Std., http://portal.opengeospatial.org/, last accessed 07/30/2016

[95] OMG, Data Distribution Service (DDS), Object Management Group TS, 2005, http://www.omg.org/spec/DDS/, last accessed 07/30/2016

[96] OASIS, Extensible Resource Identifier (XRI) Version 2.0, OASIS Std., 2005, http://docs.oasis-open.org/xri/xri/V2.0/xri-syntax-V2.0-cd-01.pdf, last accessed 07/30/2016

[97] OASIS, Extensible Resource Descriptor (XRD) Version 1.0, OASIS Std., 2010, http://docs.oasis-open.org/xri/xrd/v1.0/cd02/xrd-1.0-cd02.html, last accessed 07/30/2016

[98] M. R. Palattella et al., "Standardized Protocol Stack for the Internet of (Important) Things," in IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389-1406, Third Quarter 2013

[99] M. Agiwal; A. Roy; N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol.PP, no.99, pp.1-1

[100] N. Venkatesh, "Ensuring Coexistence of IoT Wireless Protocols Using a Convergence Module to Avoid Contention", Embedded Innovator, 12th Edition, 2015

[101] J. Chase, "The Evolution of the Internet of Things", http://www.ti.com/lit/ml/swrb028/swrb028.pdf, Texas Instruments, September 2013

[102] H. SHI, R. V. Prasad, E. Onur and I. G. M. M. Niemegeers, "Fairness in Wireless Networks:Issues, Measures and Challenges," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 5-24, First Quarter 2014

[103] R. H. Tehrani; S. Vahid; D. Triantafyllopoulou; H. Lee; K. Moessner, "Licensed Spectrum Sharing Schemes for Mobile Operators: A Survey and Outlook," in IEEE Communications Surveys & Tutorials, vol.PP, no.99, pp.1-1

[104] M. L. Ku, W. Li, Y. Chen and K. J. Ray Liu, "Advances in Energy Harvesting Communications: Past, Present, and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1384-1412, Secondquarter 2016

[105] S. Sudevalayam and P. Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications," in IEEE Communications Surveys & Tutorials, vol. 13, no. 3, pp. 443-461, Third Quarter 2011

[106] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," IEEE Commun. Mag., vol. 53, no. 6, pp. 102–108, Jun. 2015

[107] A. Sample and J. R. Smith, "Experimental results with two wireless power transfer systems," Proceedings of the 4th international conference on Radio and wireless symposium, pp. 16-18, Jan. 2009

[108] M. Erol-Kantarci and H. T. Mouftah, "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 179-197, Firstquarter 2015

[109] D. Feng, C. Jiang, G. Lim, L. J. Cimini, G. Feng and G. Y. Li, "A survey of energy-efficient wireless communications," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 167-178, First Quarter 2013

[110] G. Y. Li et al., "Energy-efficient wireless communications: tutorial, survey, and open issues," in IEEE Wireless Communications, vol. 18, no. 6, pp. 28-35, December 2011

[111] M. A. Marsan, L. Chiaraviglio, D. Ciullo, and M. Meo, "Optimal energy savings in cellular access networks," in Proc. IEEE ICC Workshops, 2009, pp. 1–5.

[112] J. Gong, S. Zhou, Z. Niu, and P. Yang, "Traffic-aware base station sleeping in dense cellular networks," in Proc. IWQoS, 2010, pp. 1–2.

[113] C. Zhang, T. Zhang, Z. Zeng, L. Cuthbert, and L. Xiao, "Optimal locations of remote radio units in comp systems for energy efficiency," in Proc. IEEE VTC–Fall, 2010, pp. 1–5.

[114] G. Gur and F. Alagoz, "Green wireless communications via cognitive dimension: An overview," IEEE Netw., vol. 25, no. 2, pp. 50–56, Mar./Apr. 2011

[115] M. Erol-Kantarci and H. T. Mouftah, "Wireless sensor networks for cost- efficient residential energy management in the smart grid," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 314–325, Jun. 2011.

[116] L. Li, X. Hu, C. Ke, and K. He, "The applications of WiFi-based wireless sensor network in Internet of things and smart grid," in Proc. IEEE ICIEA, Jun. 2011, pp. 789–793

[117] D. Bandyopadhyay and J. Sen, "Internet of Things - Applications and Challenges in Technology and Standardization", Springer International Journal of Wireless Personal Communications, Vol. 58, No. 1, pp. 49 – 69, May 2011

[118] X. Lu, P. Wang, D. Niyato, D. I. Kim and Z. Han, "Wireless Networks With RF Energy Harvesting: A Contemporary Survey," in IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 757-789, Secondquarter 2015

[119] M. F. Brejza, L. Li, R. G. Maunder, B. M. Al-Hashimi, C. Berrou and L. Hanzo, "20 Years of Turbo Coding and Energy-Aware Design Guidelines for Energy-Constrained Wireless Applications," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 8-28, Firstquarter 2016

[120] H. Sun, A. Nallanathan, and J. Jiang, "Improving the energy efficiency of power line communications by spectrum sensing," in Proc. Int. Conf. Adv. Comput., Commun. Informat., 2012, pp. 758–762

[121] H. Sun, A. Nallanathan, N. Zhao, and C. Wang, "Green data transmission in power line communications," in Proc. IEEE GLOBECOM, Dec. 3–7, 2012, pp. 3702, 3706

[122] A. Hamini, J. Baudais, and J. Helard, "Green resource allocation for powerline communications," in Proc. IEEE ISPLC Appl., Apr. 3–6, 2011, pp. 393, 398

[123] HomePlug Green PHY 1.1 Specification, "HomePlug Alliance," Portland, OR, USA, 2012, http://www.homeplug.org/tech/whitepapers/HomePlug_Green_PHY_whitepaper_121003.pdf, last accessed 07/30/2016

[124] K. Christensen et al., "IEEE 802.3az: the road to energy efficient ethernet," IEEE Commun. Mag., vol. 48, no. 11, pp. 50–56, Nov. 2010

[125] L. Chiaraviglio, M. Mellia, and F. Neri, "Reducing power consumption in backbone networks," in Proc. IEEE ICC, Dresden, Germany, Jun. 2009, pp. 1–6

[126] F. Idzikowski, S. Orlowski, C. Raack, H. Woesner, and A. Wolisz, "Saving energy in IP-over-WDM networks by switching off line cards in low-demand scenarios," in Proc. Conf. ONDM, Kyoto, Japan, Feb. 2010, pp. 1–6

[127] G. Shen and R. S. Tucker, "Energy-minimized design for IP over WDM networks," IEEE/OSA J. Opt. Commun. Netw., vol. 1, no. 1, pp. 176–186, Jun. 2009

[128] B. Kantarci and H. T. Mouftah, "Greening the availability design of optical WDM networks," in Proc. IEEE GLOBECOM—Workshop Green Commun., Dec. 2010, pp. 1417–1421

[129] B. G. Bathula and J. M. H. Elmirghani, "Green networks: Energy efficient design for optical networks," in Proc. IFIP Int. Conf. Wireless Opt. Commun. Netw., Apr. 28–30, 2009, pp. 1–5

[130] N. Naas, B. Kantarci, and H. T. Mouftah, "Energy-efficient realistic design and planning of optical backbone with multi-granular switching," in Proc. ICTON, Jul. 2012, pp. 1–4

[131] J. Chabarek et al., "Power awareness in network design and routing," in Proc. IEEE INFOCOM, 2008, pp. 1130–1138

[132] J. Baliga, R. Ayre, K. Hinton, and R. Tucker, "Energy consumption in wired and wireless access networks," IEEE Commun. Mag., vol. 49, no. 6, pp. 70–77, Jun. 2011

[133] M. Maier, "Fiber-wireless sensor networks (FI-WSNs) for smart grids," in Proc. 13th IEEE ICTON, Jun. 2011, pp. 1–4.

[134] N. Zaker, B. Kantarci, M. Erol-Kantarci and H. T. Mouftah, "Quality-of-service-aware fiber wireless sensor network gateway design for the smart grid," 2013 IEEE International Conference on Communications Workshops (ICC), Budapest, 2013, pp. 863-867

[135] D. P. Van, M. P. I. Dias, K. Kondepu, L. Valcarenghi, P. Castoldi and E. Wong, "Energy-efficient dynamic bandwidth allocation for long-reach passive optical networks," Optical Fibre Technology, 2014 OptoElectronics and Communication Conference and Australian Conference on, Melbourne, VIC, 2014, pp. 999-1001

[136] J. Liu, H. Guo, H. Nishiyama, H. Ujikawa, K. Suzuki and N. Kato, "New Perspectives on Future Smart FiWi Networks: Scalability, Reliability, and Energy Efficiency," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1045-1072, Secondquarter 2016

[137] "The Internet of Things: Opportunities & Challenges", http://www.ti.com/ww/en/internet_of_things/pdf/14-09-17-IoTforCap.pdf, Texas Instruments

[138] H. Hu, Y. Wen, T. S. Chua and X. Li, "Toward Scalable Systems for Big Data Analytics: A Technology Tutorial," in IEEE Access, vol. 2, no., pp. 652-687, 2014

[139] "Neurons and Synapses," http://www.human-memory.net/brain_neurons.html, last accessed 09/04/2016

[140] M. Trevathan, "Why the IoT Ecosystem Is Like the Nervous System," Internet of Things Institute, http://www.ioti.com/iot-strategy/why-iot-ecosystem-nervous-system, July 2016

[141] K. Ashton, "The Internet of Things is Becoming a Nervous System," https://www.theintelligenceofthings.com/article/the-internet-or-things-is-becoming-a-new-nervous-system/, last accessed 08/04/2016

[142] S. Sarkar; S. Chatterjee; S. Misra, "Assessment of the Suitability of Fog Computing in the Context of Internet of Things," in IEEE Transactions on Cloud Computing, vol.PP, no.99, pp.1-1

[143] S. K. Datta, C. Bonnet and J. Haerri, "Fog Computing architecture to enable consumer centric Internet of Things services," 2015 International Symposium on Consumer Electronics (ISCE), Madrid, 2015, pp. 1-2

[144] A. Bader, H. Ghazzai, A. Kadri and M. S. Alouini, "Front-end intelligence for large-scale application-oriented internet-of-things," in IEEE Access, vol. 4, no., pp. 3257-3272, 2016

[145] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero and M. Nemirovsky, "Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing," 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, 2014, pp. 325-329

[146] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: a green computing paradigm to support IoT applications," in IET Networks, vol. 5, no. 2, pp. 23-29, 3 2016

[147] "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," http://newsroom.cisco.com/release/1334100/Cisco-Delivers-Vision-of-Fog-Computing-to-Accelerate-Value-from-Billions-of-Connected-Devices-utm-medium-rss, January 2014

[148] O. Salman, I. Elhajj, A. Kayssi and A. Chehab, "Edge computing enabling the Internet of Things," Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, Milan, 2015, pp. 603-608

[149] V. Gazis, A. Leonardi, K. Mathioudakis, K. Sasloglou, P. Kikiras and R. Sudhaakar, "Components of fog computing in an industrial internet of things context," Sensing, Communication, and Networking - Workshops (SECON Workshops), 2015 12th Annual IEEE International Conference on, Seattle, WA, 2015, pp. 1-6

[150] K. Lee, D. Kim, D. Ha, U. Rajput and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," Network of the Future (NOF), 2015 6th International Conference on the, Montreal, QC, 2015, pp. 1-3

[151] S. Dey, A. Mukherjee, H. S. Paul and A. Pal, "Challenges of Using Edge Devices in IoT Computation Grids," Parallel and Distributed Systems (ICPADS), 2013 International Conference on, Seoul, 2013, pp. 564-569

[152] D. R. d. Vasconcelos, R. M. d. C. Andrade and J. N. d. Souza, "Smart Shadow – An Autonomous Availability Computation Resource Allocation Platform for Internet of Things in the Fog Computing Environment," 2015 International Conference on Distributed Computing in Sensor Systems, Fortaleza, 2015, pp. 216-217

[153] W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, "A Survey on Software-Defined Networking," in IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 27-51, Firstquarter 2015

[154] B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617-1634, Third Quarter 2014

[155] H. Xie, Y. Yang, A. Krishnamurthy, Y. Liu, and A. Silberschatz, "P4p: Provider portal for applications," ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 4, pp. 351–362, Aug. 2008

[156] T.-Y. Huang, N. Handigol, B. Heller, N. McKeown, and R. Johari, "Con- fused, timid, and unstable: Picking a video streaming rate is hard," in Proc. ACM Conf. Internet Meas. Conf., 2012, pp. 225–238

[157] X. Chen, Z. M. Mao, and J. Van Der Merwe, "ShadowNet: A platform for rapid and safe network evolution," in Proc. Conf. USENIX Annu. Tech. Conf., 2009, p. 3.

[158] R. Perlman, "Rbridges: Transparent routing," in Proc. 23rd Annu. Joint Conf. IEEE INFOCOM, 2004, vol. 2, pp. 1211–1218.

[159] R. Perlman, D. Eastlake, III, S. Gai, D. Dutt, and A. Ghanwani, Routing bridges (RBridges): Base Protocol Specification, Jul. 2011, RFC 6325, http://tools.ietf.org/rfc/rfc6325.txt, last accessed 07/30/2016

[160] "Software-defined networking: The new norm for networks," Palo Alto, CA, USA, White Paper, Apr. 2012, https://www.opennetworking.org/images/stories/downloads/white- papers/wp-sdn-newnorm.pdf, last accessed 07/30/2016

[161] "Vulnerability Analysis of Energy Delivery Control Systems" by Idaho National Laboratory, September 2011, http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems%202011.pdf

[162] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014

[163] S. Hilton, "Dyn Analysis Summary of Friday October 21 Attack," http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/, October 2016

[164] C. Doctorow, "Proof-of-concept ransomware for smart thermostats demoed at Defcon," Boingboing, August 2016, http://boingboing.net/2016/08/08/proof-of-concept-ransomware-fo.html

[165] M. Frauenfelder, "75 percent of Bluetooth smart locks can be hacked," Boingboing, August 2016, http://boingboing.net/2016/08/08/75-percent-of-bluetooth-smart.html

[166] K. Hill, "This guy's light bulb performed a DoS attack on his entire smart house," Fusion, March 2015, http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/

[167] "How A Few Words To Siri Unlocked A Man's Front Door And Exposed A Major Security Flaw In Apple's HomeKit," Forbes, September 2016, http://www.forbes.com/sites/aarontilley/2016/09/21/apple-homekit-siri-security/#f5fa4b6e8a3d

[168] J.D. Howard and T.A. Longstaff, "A Common Language for Computer Security Incidents," Sandia National Laboratories, October 1998, http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf

[169] W. Stallings, "Network and Internetwork Security," Prentice Hall, Upper Saddle River, NJ, 1995

[170] R.R. Brooks, S. Sander, J. Deng, and J. Taiber, "Automotive Security Concerns: Challenges and State of the Art of Automotive System Security," IEEE Vehicular Technology Magazine, June 2009

[171] C. Beasley, X. Zhong, J. Deng, R. Brooks and G. K. Venayagamoorthy, "A survey of electric power synchrophasor network cyber security," IEEE PES Innovative Smart Grid Technologies, Europe, Istanbul, 2014, pp. 1-5

[172] S. Muthyala, "Communication security for smart grid distribution networks," ISU, Proj. Rep. 2013

[173] H. Lin, et al., "A study of communication and power system infrastructure interdependence on PMU-based wide area monitoring and protection," Power and Energy Society General Meeting, San Diego, CA, 2012 IEEE , pp.1-7, 22-26 July 2012

[174] R. Brooks, Introduction to Computer and Network Security Navigating Shades of Gray. Boca Raton: Taylor & Francis Group, LLC, 2014

[175] T. Baumeister, "Literature review on smart grid cyber security." in Proc. University of Hawaii at Manoa, Tech. Rep. December 2010

[176] R. Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," The Wall Street Journal, February 2014, http://www.wsj.com/articles/SB10001424052702304851104579359141941621778

[177] "Nuclear Security," http://www.ucsusa.org/nuclear-power/nuclear-plant-security#.WIEgFlMrJQI, last accessed 01/19/2017

[178] "Defending against Sabotage and Terrorist Attacks," http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nuclear_power/NPWWch3.pdf, last accessed 01/19/2017

[179] T. Morris, et al, "Cyber security testing of substation phasor measurement units and phasor data concentrators." in Proc. The 8th Annual ACM Cyber Security and Information Intelligence Research Workshop (CSIIRW), 2011

[180] "Teardrop Attack," https://security.radware.com/ddos-knowledge-center/ddospedia/teardrop-attack/, last accessed 01/19/2017

[181] I. Ozcelik, Y. Fu, and R. R. Brooks, "DoS detection is easier now," Research and Educational Experiment Workshop (GREE), 2013

[182] "Deflect," https://equalit.ie/portfolio/deflect, last accessed 09/04/2016

[183] S. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," Communications Surveys & Tutorials, IEEE, vol. 15, no. 4, pp. 2046- 2069, Fourth Quarter 2013

[184] Y. Ye, et al., "A Survey on Cyber Security for Smart Grid Communications," Communications Surveys & Tutorials, IEEE , vol.14, no.4, pp.998-1010, Fourth Quarter 2012

[185] W. F. Boyer, and S. A. McBride, "Study of security attributes of smart grid systems–current cyber security issues," INL, USDOE, Battelle Energy Alliance LLC., Rep INL/EXT-09-15500, Apr. 2009

[186] J. Stewart, et al., "Synchrophasor security practices." in Proc. 14th Annual Georgia Tech Fault and Disturbance Analysis Conf. Atlanta, GA, 2011

[187] S. Siddharth, A. Hahn, and M. Govindarasu. "Cyber–physical system security for the electric power grid." Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, 2012

[188] R. Lemos, "Microsoft warns of hijacked certificates," CNET Tech Industry, January 2002, https://www.cnet.com/news/microsoft-warns-of-hijacked-certificates/

[189] R. Oppliger, R. Hauser, and D. Basin, "SSL/TLS session-aware user authentication." Computer, vol. 41, no. 3, pp. 59-65, 2008

[190] X. Zhong, A. Ahmadi, R. Brooks, G. K. Venayagamoorthy, L. Yu and Y. Fu, "Side channel analysis of multiple PMU data in electric power systems," Power Systems Conference (PSC), 2015 Clemson University, Clemson, SC, 2015, pp. 1-6

[191] H. Bhanu, et al., "Side-channel analysis for detecting protocol tunneling," Advances in Internet of Things, Vol. 1 No. 2, 2011, pp. 13- 26.

[192] C. Beasley, Electric power synchrophasor network cyber security vulnerabilities, MS Dissertation, Dept. of Electrical and Computer Engineering, Clemson University, 2014

[193] R. R. Brooks, Disruptive security technologies with mobile code and peer-to-peer networks, CRC Press, Boca Raton, FLA, 2005

[194] Y. Guan, et al., "Netcamo: camouflaging network traffic for QoS- guaranteed mission critical applications," Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, vol. 31, no. 4, July 2001, pp. 253-265

[195] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attacks to the HTTPS protocol." Security & Privacy, IEEE, vol. 7, no. 1, pp. 78-81, 2009

[196] S. D'Antonio, L. Coppolino, I. A. Elia, and V. Formicola, "Security issues of a phasor data concentrator for smart grid infrastructure." in Proc. 13th European Workshop on Dependable Computing, Pisa, Italy, ACM, pp. 3, 2011

[197] G. J. W. Halfond, and A. Orso. "AMNESIA: analysis and monitoring for neutralizing SQL-injection attacks." in Proc. 20th IEEE/ACM international Conference on Automated software engineering. ACM, pp. 174, 2005

[198] K. Deltchev, "New Web 2.0 Attacks," Bachelor's Thesis, Ruhr-University of Bochum, February 2010, http://www.slideshare.net/test2v/new-web-20-attacks

[199] "Tutorial on Defending Against SQL Injection Attacks," Oracle, http://download.oracle.com/oll/tutorials/SQLInjection/index.htm, last accessed 01/19/2017

[200] P. Hooimeijer, B. Livshits, D. Molnar, P. Saxena, and M. Veanes, "Fast and Precise Sanitizer Analysis with BEK," Proceedings of the 20th USENIX conference on Security, SEC'11, pages 1-1, Berkeley, CA, 2011, http://www.msr-waypoint.com/en-us/um/people/livshits/papers/pdf/usenixsec11a.pdf

[201] D. P. Shepard, T. E. Humphreys, and A. A. Fansler. "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks." International Journal of Critical Infrastructure Protection, vol. 5 issues 3, 2012, pp. 146-153

[202] D. Yu, et al., "Short paper: detection of GPS spoofing attacks in power grids," Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks. ACM, 2014.

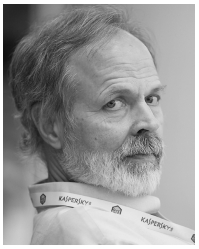
[203] S. Cui, et al., "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," Signal Processing Magazine, IEEE, vol.29, no.5, pp.106-115, Sept. 2012

O riginally from India, **Guneet Bedi** is a Ph.D. candidate in the Department of Electrical and Computer Engineering (ECE) at Clemson University, researching Internet of Things applications in Electric Power and Energy Systems. Guneet received his B.E. in Electronics and Telecommunication from University of Pune, India (2011) and his M.S. in Electrical Engineering from Clemson University (2014). While in the ECE program, Guneet has worked as a graduate research, teaching, instructional, and grading assistant as well as a mentor for K-12 and undergraduate science enrichment programs. Guneet has published several peer-reviewed papers and has presented his research at a number of conferences. He has also served as a reviewer for IEEE Internet of Things journal and Elsevier Computers and Security journal. Besides his academic pursuits, Guneet has served as the President of Graduate Student Government, President of International Student Association, and the Vice-President of Clemson Indian Students' Association. Guneet played on Clemson's water polo club team for two successive years and is a graduate student member of the Omicron Delta Kappa national level leadership honor society and the Institute of Electrical and Electronics Engineers. During his time at Clemson, Guneet has been honored with awards for his outstanding scholarship, leadership, teaching, and service.

G. Kumar Venayagamoorthy is currently the Duke Energy Distinguished Professor of Power Engineering and a Professor of Electrical and Computer Engineering and Automotive Engineering with Clemson University, Clemson, SC, USA. He is also the Founder and Director of the Real-Time Power and Intelligent Systems Laboratory (http://rtpis.org) with Clemson University. He is an Honorary Professor with the School of Engineering, University of KwaZulu–Natal, Durban, South Africa. Dr. Venayagamoorthy's interests are in the research, development and innovation of advanced computational methods for smart grid operations, including intelligent sensing and monitoring, power system optimization, stability and control, and signal processing. He has published $\sim$ 500 refereed technical articles. His publications are cited $\sim$14,000 times with a h-index of 59. Dr. Venayagamoorthy has been involved $\sim$ 70 sponsored projects in excess of $10 million. He has received several awards from IEEE and other professional societies and institutions for his contributions to field of electrical and electronic engineering.

Dr. Venayagamoorthy is involved in the leadership and organization of many conferences including the General Chair of the Power System Conference (Clemson, SC, USA) since 2013, and Pioneer and Chair/co-Chair of the IEEE Symposium of Computational Intelligence Applications in Smart Grid (CIASG) since 2011. He is currently the Chair of the IEEE PES Working Group on Intelligent Control Systems, and the Founder and Chair of IEEE Computational Intelligence Society (CIS) Task Force on Smart Grid. Dr. Venayagamoorthy is a Senior Member of the IEEE and International Neural Network Society, and a Fellow of the IET (UK), and the SAIEE (South Africa). He has served as an Editor/Guest Editor of several IEEE and Elsevier journal.

Rajendra Singh is D. Houser Banks professor in the Holcombe Department of Electrical and Computer Engineering and Automotive Engineering at Clemson University (CU). He is also the Director of Center for Nanoelectronics at CU. He left India in 1973 and during the energy crisis of 1973 decided to do Ph.D. dissertation in the area of Silicon Solar Cells. In the last 43 years, he has contributed and witnessed the growth of photovoltaic and semiconductor industries. With proven success in operations, project/program leadership, R&D, product/process commercialization, and start-ups, Dr. Singh is a leading technologist with the focused goal of eradication of energy poverty and poverty of under privileged people all over the world. He is fellow of IEEE, SPIE, ASM and AAAS. Dr. Singh has received a number of international awards. In 2014, he was honored by US President Barack Obama as a White House "Champion of Change for Solar Deployment" for his leadership in advancing solar energy with photovoltaics technology.



Dr. Richard R. Brooks got his BA from Johns Hopkins University in Mathematical Sciences and PhD in Computer Science from Louisiana State University. He was head of the Penn State ARL distributed systems department for 7 years and is now a professor of Computer Engineering at Clemson. Dr. Brooks' network security research projects have included funding from NSF (analyzing denial of service), DoE (authentication and authorization), BMW Corporation (penetration testing), NIST (standards definition), AFOSR (timing side-channels) and the US State Department (creating anonymous communications tools). He finds attacks that disable security measures by working at a different level of the protocol stack. His Internet freedom work involves interactions with at risk populations working for freedom of expression.

Kuang-Ching Wang received the B.S. and M.S. degrees from National Taiwan University, Taipei, Taiwan, in 1997 and 1999, respectively, and the M.S. and Ph.D. degrees from the University of Wisconsin–Madison, Madison, WI, USA, in 2001 and 2003, respectively, all in electrical engineering. Since 2004, he has been with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, USA, where he is currently Professor and Networking CTO. His research concerns assurance of network communication quality of service, with a present focus on software defined networking and future cloud computing systems.