



**Michigan
Technological
University**

Michigan Technological University
Digital Commons @ Michigan Tech

Michigan Tech Publications

12-1-2020

A low-cost secure iot mechanism for monitoring and controlling polygeneration microgrids

Josué Martínez-Martínez
Universidad Ana G. Méndez

Diego Aponte-Roa
Universidad Ana G. Méndez

Idalides Vergara-Laurens
Universidad Ana G. Méndez

Wayne Weaver
Michigan Technological University, wwweaver@mtu.edu

Follow this and additional works at: <https://digitalcommons.mtu.edu/michigantech-p>



Part of the [Mechanical Engineering Commons](#)

Recommended Citation

Martínez-Martínez, J., Aponte-Roa, D., Vergara-Laurens, I., & Weaver, W. (2020). A low-cost secure iot mechanism for monitoring and controlling polygeneration microgrids. *Applied Sciences (Switzerland)*, 10(23), 1-14. <http://doi.org/10.3390/app10238354>
Retrieved from: <https://digitalcommons.mtu.edu/michigantech-p/14345>




Follow this and additional works at: <https://digitalcommons.mtu.edu/michigantech-p>



Part of the [Mechanical Engineering Commons](#)

Article

A Low-Cost Secure IoT Mechanism for Monitoring and Controlling Polygeneration Microgrids

Josué Martínez-Martínez ¹, Diego Aponte-Roa ^{1,*}, Idalides Vergara-Laurens ¹
and Wayne W. Weaver ²

¹ Electrical and Computer Engineering Department, Ana G. Méndez University, Gurabo 00778, Puerto Rico; jmartinez718@email.uagm.edu (J.M.-M.); ivergara@uagm.edu (I.V.-L.)

² Mechanical Engineering Department, Michigan Technological University, Houghton, MI 49931, USA; wwweaver@mtu.edu

* Correspondence: aponted1@uagm.edu; Tel.: +1-787-806-8053

Received: 30 September 2020; Accepted: 28 October 2020; Published: 24 November 2020



Abstract: The use of Internet-connected devices at homes has increased to monitor energy consumption. Furthermore, renewable energy sources have also increased, reducing electricity bills. However, the high cost of the equipment limits the use of these technologies. This paper presents a low-cost secured-distributed Internet of Things (IoT) system to monitor and control devices connected in a polygeneration microgrid, as a combined power system for local loads with renewable sources. The proposed mechanism includes a Wireless Sensor Actuator Networked Control System that links network nodes using the IEEE 802.15.4 standard. The Internet communication enables the monitor and control of devices using a mobile application to increase the efficiency. In addition, security mechanisms are implemented at several levels including the authentication, encryption, and decryption of the transmitted data. Furthermore, a firewall and a network intrusion detection-and-prevention program are implemented to increase the system protection against cyber-attack. The feasibility of the proposed solution was demonstrated using a DC microgrid test bench consisting of a diverse range of renewable energy sources and loads.

Keywords: IoT; cyber-physical system; renewable energy; microgrid; polygeneration

1. Introduction

According to the United States Energy Information Administration (EIA), over \$370 billion has been spent annually in recent years on electricity generation. Roughly 48% (\$177.6 billion) of the total generation was spent in the residential sector [1]. To increase the efficiency in energy consumption, data acquisition equipment such as smart meters, smart plugs, and many other sensors are commonly used. Although Home Energy Management System (HEMS) are anticipated as one of the promising technologies to fulfill the demand for energy saving, thus far it has only had limited implementation because the high initial equipment cost [2] and the lack of optimal managing software because the power consumption pattern of residence is too diverse to find an optimal power management for each home [3]. A HEMS works by placing sensors at different appliances and/or devices that reads their energy consumption. By scheduling major household appliances, residents can reduce their electricity bills [4–6]. In several cases, the sensors are connected to the Internet reporting the data to the owner. The extension of the Internet connectivity into physical devices is named the Internet of Things (IoT), defined by the Institute of Electrical and Electronics Engineers (IEEE) as a network of items embedded with sensors that are connected to the Internet [7].

Monitoring applications can provide valuable information about your home from the actual status to a detailed history. This technology can provide the services, information, communication, and data

analysis anytime, as long there is a connection to the Internet, to tackle the energy consumption along with augmentation of the modern home living experience [8–10]. In addition, the integration of renewable energy sources (RESs) in distributed generation (DG), with proper control systems, have proven a lower electric bills in the residential sector [11]. In addition, the usage of RESs reduces carbon dioxide emissions by 1925 million metric tons in 2015, or roughly 36.5% of the total of all sectors in the United States [12]. However, the integration of RESs presents challenges in power quality, cost, power availability, location of RESs resource, and power forecast, among others [12]. Therefore, the integration of an IoT monitoring systems would improves the network performance to make a more resilient and efficient cyber-physical system. Since this environment is connected to the Internet, it needs to be protected from security threats. As shown in [13], the scheme has to fulfill three requirements:

1. Confidentiality concerns the protection of data, such that only approved users can access the data.
2. Authentication means checking that the data have not been altered and that the data can be confirmed by the claimed author to have been sent.
3. Access refers to only allowing suitably authorized users to access data, communications network, and computing resources and ensuring that those authorized users are not prevented from such access.

This paper presents a cyber-physical system consisting of a low-cost secure IoT mechanism for monitoring and controlling appliances/devices connected in a polygeneration microgrid. The hardware of the system was implemented using low-cost commercial off-the-shelf items, while the software was developed using free and open source resources. The IoT control scheme is comprised of a Wireless Sensor and Actuator Networked Control System (WSANCS) which implements a star topology with one sink node (S-N) and a set of sensor-actuator nodes (SA-N). The sensor-actuator nodes are an embedded entity composed of a micro-controller, a communication device, and a current/voltage sensor. The sink node is an embedded entity comprised of a micro-controller, a communication device, and a micro-computer. The data gathered by the WSANCS are sent to a cloud database. In addition, a mobile application allows the user to monitor and control the system in real-time. This mobile application retrieves the data from the database through the encrypted Transport Layer Security (TLS) protocol, providing to the system both the energy production and consumption. Finally, the mobile application allows the user to control all the registered electric appliances as well, and, according to the literature, these smart homes applications might achieve around 8% reduction in energy consumption [14,15]. Therefore, the use of these approaches in RES grids might represent a considerable improve in energy efficiency since the energy availability and storage are the bigger constraints in polygeneration microgrids.

This manuscript is organized as follows. Section 2 presents the related work. Section 3 presents the system architecture including the WSANCS architecture and details of the IoT secure architecture. Simulation results and security analysis are discussed in Section 4. Finally, Section 5 presents a summary and future work.

2. Related Work

A microgrid is a group of interconnected loads and distributed energy resources within a defined electrical boundaries [16]. Traditionally, microgrids have been used in remote areas without access to main power grids and can employ various communication technologies to data sharing. In addition, the governments in the U.S., the Asia Pacific region, and the European Union have established supporting policies, demonstration projects, control systems research, and the development of software tools for microgrids. For instance, The U.S. federal government provides investment tax incentives for customers installing microgrid technologies. The incentives cover a wide range of technologies including solar photovoltaics, combined heat and power, and electric vehicles. Some states provide incentive for microgrid projects to supply individual customers

or critical loads such as hospitals, first responders, and water treatment facilities, after natural disasters such as Hurricane Sandy [17]. However, given the intermittency and variability of RES, microgrid customers need mechanisms for controlling power demand depending on power availability. Therefore, the U.S. Department of Energy has identified several core areas for microgrid controls: (1) frequency control; (2) volt/volt-ampere-reactive control; (3) grid-connected-to-islanding transition; (4) islanding-to-grid-connected transition; (5) energy management; (6) protection; (7) ancillary service; (8) black start; and (9) user interface and data management [18].

Wireless Sensor Networks (WSN) are used in area monitoring, threat detection, the domestic sector, health care sector, environmental sector, industrial sector, and the primary sector. A WSN is defined as a self-configured and infrastructure-less wireless network of spatially dispersed sensors dedicated to monitoring and recording physical conditions of the environment [19]. A WSN can have a few to even thousands of nodes, where each node is connected to one or many sensor nodes to cooperatively pass their data across the network to a main location (usually a data center). Each sensor node is typically composed of a radio transceiver with an internal or external antenna, a micro-controller, an electronic circuit interfacing with the sensors and an energy source. WSNs topologies can vary from a simple star topology to a multi-hop wireless mesh topology [20]. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed, and communications bandwidth. Moreover, a WSANCS is composed of a group of distributed sensors and actuators that communicate through wireless link which achieves distributed sensing and executing tasks [21]. This latter scheme allows the distributed control of devices that are spread in a wide area without physical connections between them such as a polygeneration distributed system with several renewable energy sources.

A WSANCS connected to the Internet becomes an IoT system. Coelho [22] illustrated the integration of the IoT for monitoring tasks in the office sector. They showed the convenience of having a monitoring system for conserving energy. A similar application was implemented by Patchava [23], who demonstrated the potentiality of having a smart home monitoring system. However, the use of this communication technology puts at risks the security and privacy of the data. IoT uses the Internet, thus carrying its vulnerabilities. These systems are vulnerable to diverse types of attacks such as denial of services, packet sniffing, and session hijacking to the confidentiality, integrity, and availability of the system, both damaging the system and putting the user to a possible personal risk [24,25]. In [26], Rawlinson described that 70% of the most popular IoT devices have vulnerabilities. Additionally, more than 25 vulnerabilities per device were discovered on average, with a total of 250 security concerns across all products tested. Furthermore, some devices had unsafe user interfaces and/or insecure firmware. Consequently, IoT devices need an efficient and effective protection scheme.

3. The Proposed System Architecture

This section presents the IoT WSANCS architecture implemented in a DC microgrid. The IoT security protection scheme is also introduced.

3.1. The IoT WSANCS Architecture

Figure 1 presents the updated system architecture introduced in [27]. The system consists of two RESs including a micro-wind turbine and a photovoltaic system (PV Array), both with their respective charge controller. It is worth noting that the architecture allows the system to increase the number of RESs as needed. The produced energy is stored in a battery bank. In addition, an inverter and a DC-to-DC converter are required to supply the loads. The WSANCS is composed by two types of nodes: the sensor-actuator nodes (SA-N) and the sink node (S-N).

The SA-N are included in every load of the system while the S-N is responsible for receiving the sensed data, process them, and control the network by sending wireless-control signals to the SA-N. The current and voltage are measured at different points in the microgrid using the SA-N. XBee modules are included in the WSANCS for wireless transmission purposes. Switches are connected to

the Arduino micro-controller to control the loads (turn-on/turn-off) through a digital signal. The SA-N architecture (seen in Figure 2) is composed of a current sensor, an Arduino micro-controller, and a XBee Pro module as end device using the IEEE 802.15.4 protocol [28] to monitor the grid generation and consumption. A voltage sensor is also included to measure the quality of voltage levels at different points in the microgrid.

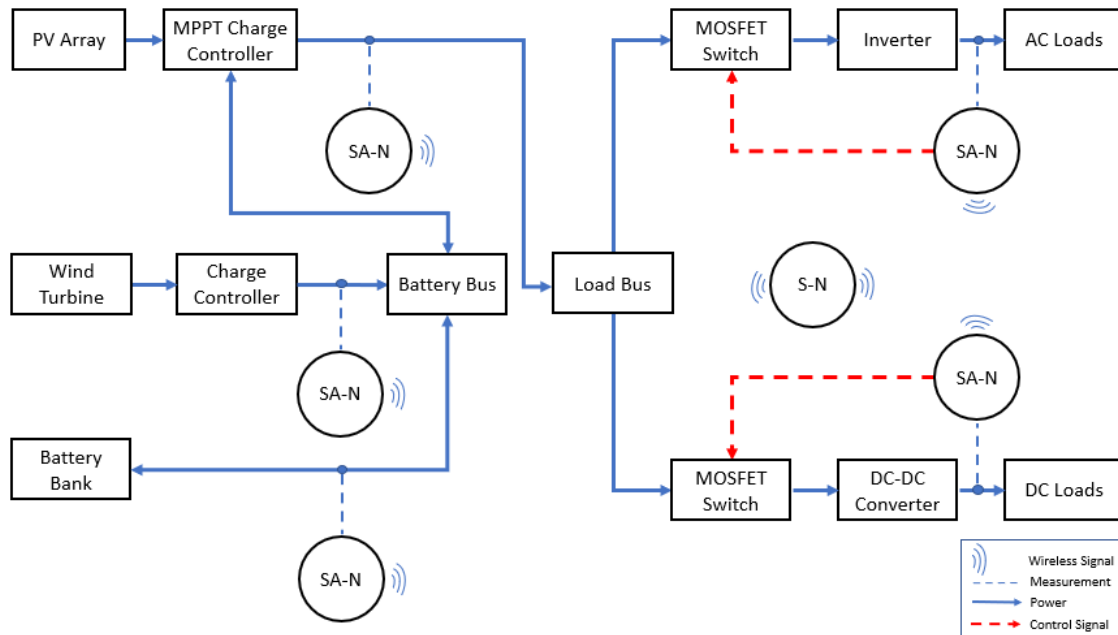


Figure 1. System architecture.

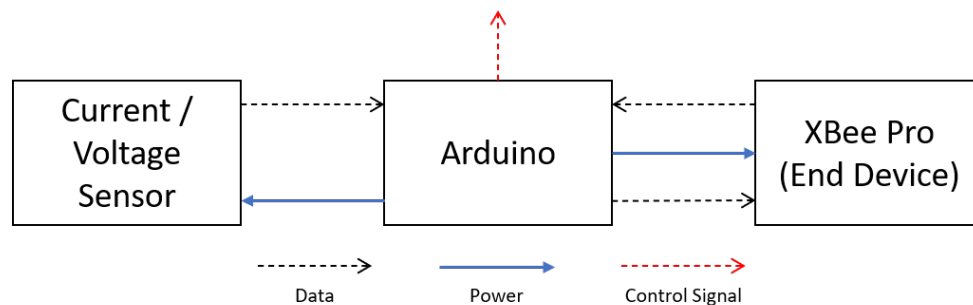


Figure 2. Sensor-actuator node architecture.

The S-N architecture (see Figure 3) includes the XBee coordinator connected to the Arduino 2 MEGA microprocessor for reading the signal of all the sensor nodes, making the necessary calculations, and printing those values to the corresponding serial port. A Raspberry-PI3 B+ (RPI3+) computer collects these values using a Python script to store data in both local and cloud databases using Sqlite3 and Firestore, respectively. This information is accessible for the user through the Android mobile application explained in detail in Section 3.2.3. In addition, the user can send the command to switch the state of the loads connected in the microgrid test bench through the mobile application, and then the S-N will send the signal to the corresponding SA-N to achieve what the user desires.

Since there are different XBees frequently attempting communication, the implemented module includes an acknowledgment scheme that allows the user to verify if data were received and from which device. The system was designed as a centralized coordinator-end device system with a coordinator XBee in the S-N that receives data from the SA-N and delivers them to a RPI3+.

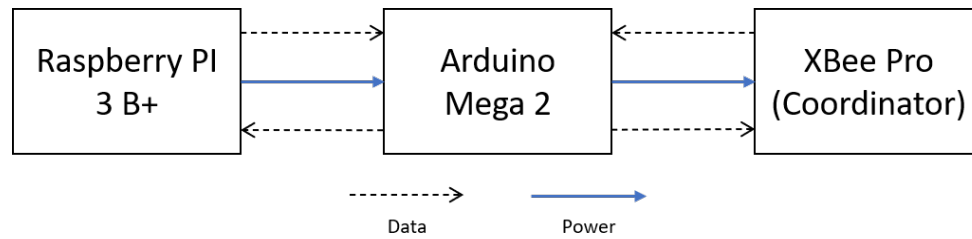


Figure 3. Sink node architecture.

3.1.1. Range and Operation Modes

The maximum distance to transmit data between two XBees was around 60 feet (18.3 m), taking into consideration concrete walls. The XBee's radio modules require 3.3 V with a power-down current $< 10 \mu\text{A}$, a transmit (TX) current of 45 mA, and a receive (RX) current of 50 mA. A consumption of less than 50 μA is expected in sleep mode operation; in this mode, for 1 min, the micro-controller keeps receiving information from the current or voltage sensors. Then, when the XBee wakes up, the acquired power consumption is sent to the sink node.

3.1.2. Network Topology

The WSANCS is implemented using a star topology because of its improved ability to contain errors and their tolerance to proximity and common-mode failures [29–33]. A quantitative comparison of the error-containment capabilities was presented by Barranco [34]. In the proposed topology, each SA-N has a XBee end-device used to connect it to the S-N which has the XBee coordinator. The XBee technology defines a point-to-point (PTP) connection between a coordinator and an end device. The coordinator receives a signal from any SA-N and can route them to the other SA-N. The S-N works as a server and it controls and manages entire function of the network. Some of the advantage of using this topology are:

1. It is easy to locate problems because if an end device fails, it affects only one sensor node.
2. It is easy to extend the network without disturbing the entire WSANCS.
3. It is easy to identify faults and remove nodes in the WSANCS.
4. It provides very high speed of data transfer.

In addition, the S-N is connected to Internet through the RPI3+. This connection allows the system to send and received data to the user's mobile application as well as to upload the sensed data to a cloud database.

3.2. The IoT Security Protection Scheme

Khan in [35] described that the structure of IoT is divided into three main layers: (1) perception; (2) network; and (3) application. The large quantities of data generated by IoT devices, and their sensitive nature, make the IoT a prime target for cyber-attacks [36]. For this reason, the transmitted data are encrypted and authenticated using different protocols to secure the IoT layers [37].

Figure 4 presents the proposed protection for each IoT Layer. In the figure, red is assigned for the WSANCS nodes, blue for protocols, violet for intrusion detection systems, clear blue for databases, green for mobile applications, and orange for authentication measures. The implemented tools for every layer are explained below.

3.2.1. The Perception Layer

The perception layer is similar to the facial skin and five sense organs of the IoT, i.e., it mainly identifies objects and gathering information [38]. In this work, the perception layer is composed of WSANCS mentioned in Section 3.1. To assure data are traveling between the SA-N and the S-N, the IEEE 802.15.4 protocol authenticates the received message with the Media Access Control (MAC) address of the end devices.

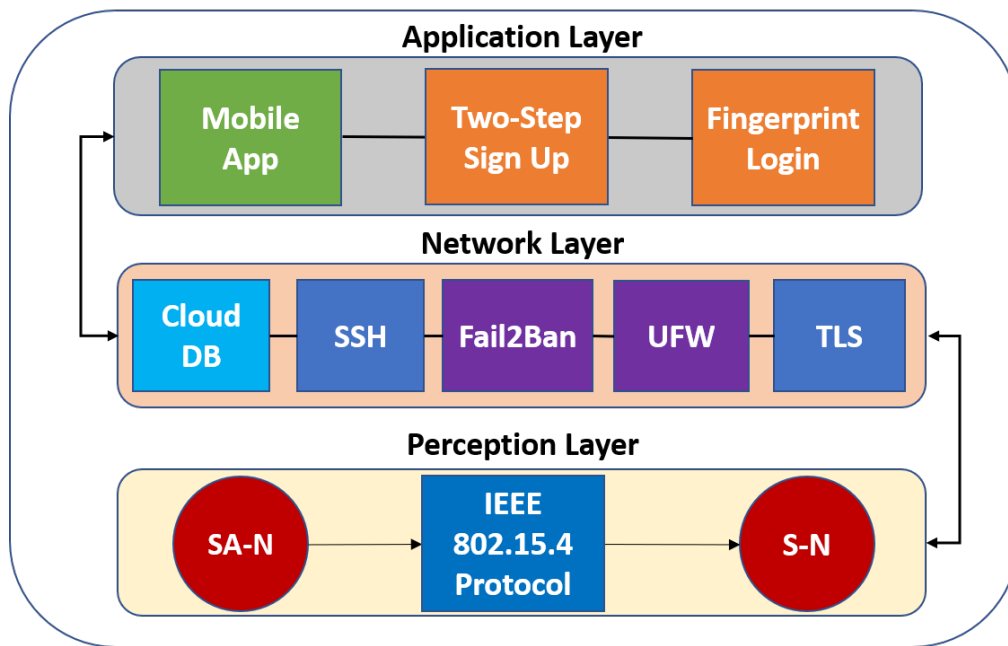


Figure 4. Proposed IoT security protection scheme.

3.2.2. The Network Layer

The network layer is for transmitting and processing data [38]. The network layer in this system includes the S-N. This node receives, processes, decrypts/encrypts data from/to the SA-N, and decrypts/encrypts data from/to the cloud-based database Firestore using the TLS protocol.

The major security threat is related to the access to the Internet. The Uncomplicated Firewall (UFW) is used to protect the RPI3+ against cyber-attacks, monitor network traffic, and block unauthorized traffic according to a defined set of security rules. Fail2Ban is used for intrusion prevention; this framework protects the S-N against brute force attacks and tracks the log files generated in order to detect malicious activity. Similarly, it can inform and update the firewall to avoid further suspicious IP login attempts. OpenSSH is used for providing a secured remote login connection to the RPI3+. This encrypts all traffic (including passwords) in order to prevent spying, hijacking, and other attacks, providing a secure network channel through a client–server architecture. The remote login is implemented using the key-based authentication standard where every authorized user must generate a key and encrypt the key with a passphrase to log on the computer. Finally, the passphrase is implemented in order to protect the user key in case a hacker takes control of the user computer and tries to log into the RPI3+ using the generated key.

3.2.3. The Application Layer

The application layer provides global management of the application based on the object’s information processed in the database [35]. This layer is composed of a monitoring mobile application for Android. The security of this layer comes from all the security implemented in the perception and network layers and the authentication that is implemented in the mobile application to certify that is the user who is accessing the data and not an intruder. The application has a two-step authentication procedure to register a new user and a fingerprint authentication to log-in this user; both dashboards are shown in Section 4 of this paper.

Therefore, a home energy management mobile application for Android is developed. This application retrieves the consumption and generation data from the cloud database which allows the user to track their energy consumption and generation, providing information for scheduling some activities might demand more energy (e.g., use the washing machine when the PV and turbine are

generating more energy). A listener is implemented to refresh the consumption/generation graphs in real-time. In addition, the application lists all the monitored equipment with the option to be switched on and off to avoid energy waste when are being left on and nobody is at home. The user has the option to delete or register a new device by providing basic information about it as well. In addition, the application lists all the monitored equipment with the option to be switched on and off to avoid energy waste when they are left on and nobody is at home.

For security purposes, a two-step sign up verification was implemented with the user cell-phone number. After the sign up, the user has the option to log-in using his fingerprint if desired. Both features are explained in detailed in Section 4.4.1. The application dashboard and some capabilities are shown in Figure 5.

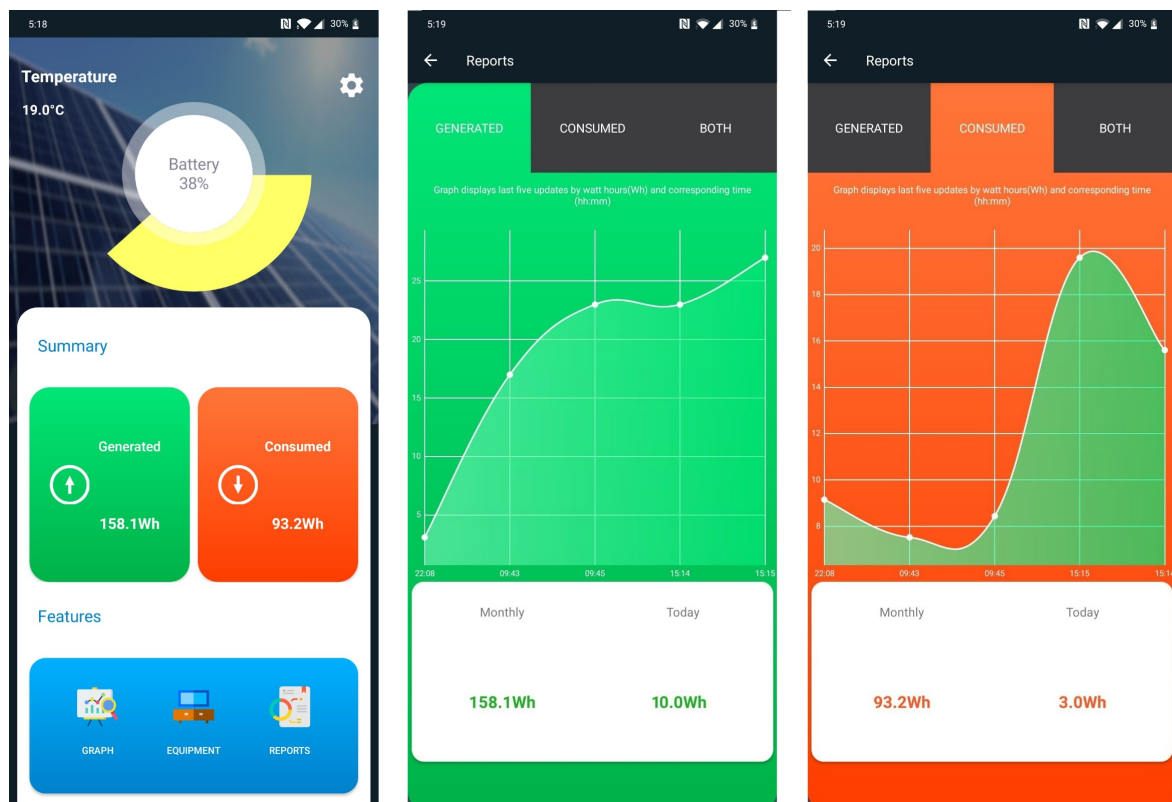


Figure 5. Mobile application capabilities.

Figure 6 shows the application interface listing the devices that the user has registered. The required information to register a new device is presented as well. A threshold value to be aware of an excess of power consumption could be included in order to turn-off the device when the power consumption reaches such threshold.

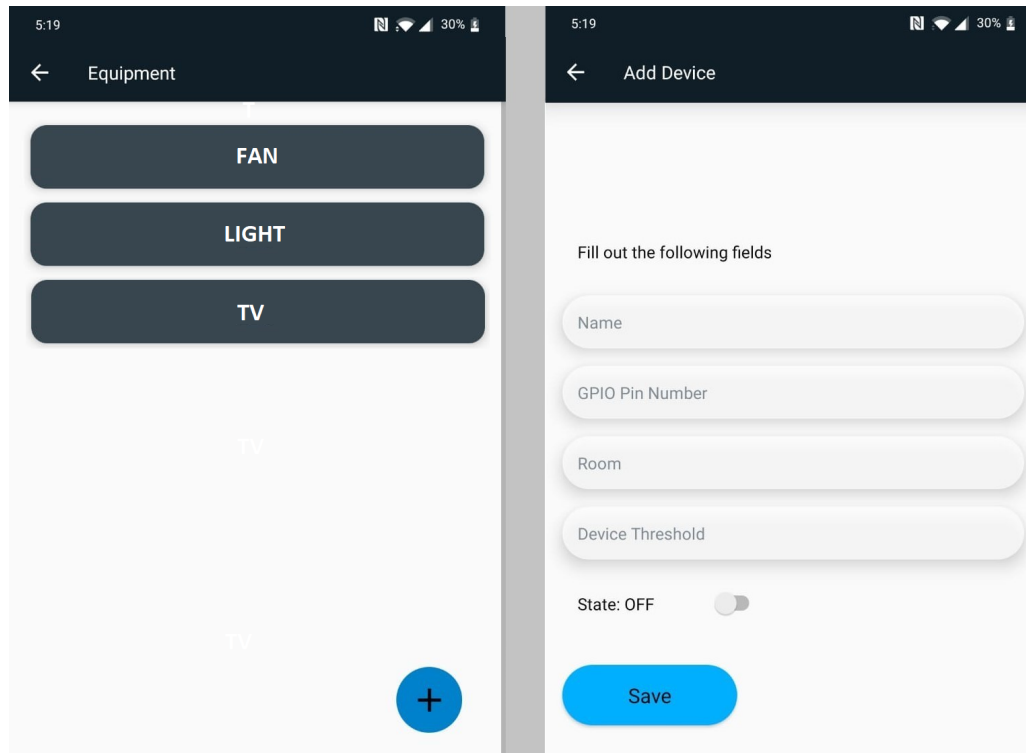


Figure 6. Some equipment options.

4. Results and Discussion

This section provides the simulation results and security analysis implemented in the DC microgrid test bench used as a test platform.

4.1. Microgrid Test-Bed

The proposed system was tested using the updated configuration of a DC microgrid test bench introduced in [27]. The test bed microgrid consists of two RESs including a 400 W micro-wind turbine and a 400 W PV system, each with its respective charge controller. The generated energy is stored in a 12 V deep-cycle battery bank. A 400 W inverter and a DC-to-DC converter were required to supply the loads. Arduino off-the-shelf modules are used to measure currents and voltages at different points in the microgrid, as presented in Figure 1. The WSANCS communication was implemented using the XBee modules. The mosfet switches are connected to the Arduino micro-controller to control the load state (turn-on or turn-off) through a digital signal, as shown in Section 3.

4.2. WSANCS Simulation

The Riverbed Modeler Academic Edition was selected to simulate the data transfer protocol used by the XBees. The simulation used the ZigBee protocol based on the IEEE 802.15.4 standard, and the data link layer worked with the same standard. The star topology presented in Section 3.2.2 was implemented.

To assure that the bidirectional data transfer is between the S-N and the SA-N, two SA-N were simulated. Figure 7 shows the model implemented where the node_0 is the coordinator and the other two nodes are end devices. The results demonstrate that the protocol can send 120 package in 1 min between these three nodes. A total of 1–60 package per minute is estimated for the desired application, which validates that protocol has the transfer capacity required.

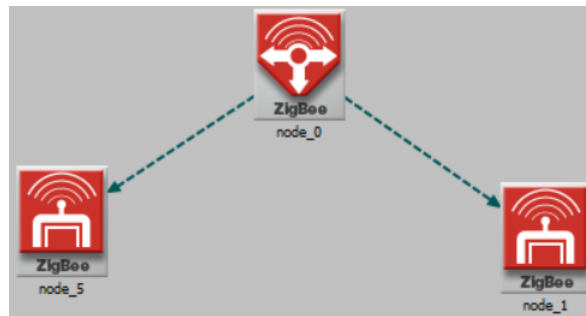


Figure 7. Communication simulation.

4.3. WSNCS Implementation

In a survey conducted by Lim [39], they found that 68.75% of 35 survey respondents occasionally forget to switch off unused appliances while 6.25% of the respondents tend to forget frequently. Besides that, it is also noted that 48.57% (17 respondents) of survey takers find it troublesome to walk to the switch to turn off an appliance, hence 35.29% of the above 17 respondents often leave the appliance turned on. To mitigate this waste of energy, a script was written with a listener to the Firestore database to perform real-time changes in the microgrid through the mobile application. The desired switch state can be uploaded by the user from the application to the cloud database. Then, the listener in the S-N uploads and downloads these changes. Section 3.1.1 mentions that the SA-N only wakes up every 1 min to send data. However, the S-N is able to send an interrupt signal to the SA-N to switch the state of the desired device instantly, after a user requested.

4.4. Security Protection Analysis

4.4.1. Two-Step Verification and Fingerprint

Figure 8 presents the login interface of the mobile application. To achieve a higher level of security, the application contains a two-step verification process to create the user account. In this case, the two-step verification is implemented using the user phone number. Then, the user needs to enter the code that was sent by SMS. The authentication process is using SHA-256 to encrypt and authenticate such process. Log-in via fingerprint capability is available for better security if desired. A reset password interface is included as well. An email with detailed procedure will be received after a request.

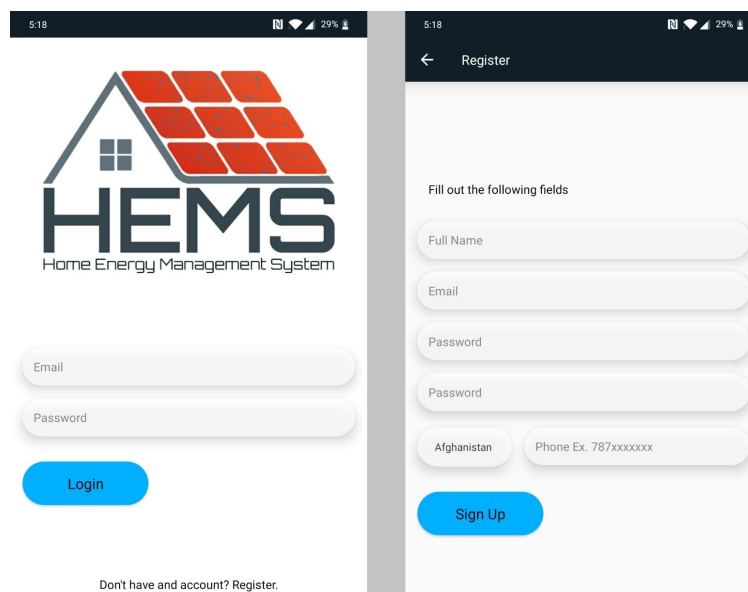


Figure 8. Login interface.

4.4.2. Brute Force Attacks

The penetration test was conducted with the Metasploit software that it is owned by Boston, Massachusetts-based security company Rapid7 [40]. The exploit was successful the first time in the insecure environment, which also has a Secure Shell (SSH) for secure remote login (SRL) but with a common password (e.g., abcdefg). This exploit provides the attacker with access to device management, as shown in Figure 9. There is a constant loop that the hacker can have access all the time. The SSH-key based protocol was used to secure the RPI3+ running Raspbian operating system. However, SSH-key-based protocol does not guarantee that the system will be resistant to such attacks but only those with the key and passphrase will be able to log-in and execute the exploits.

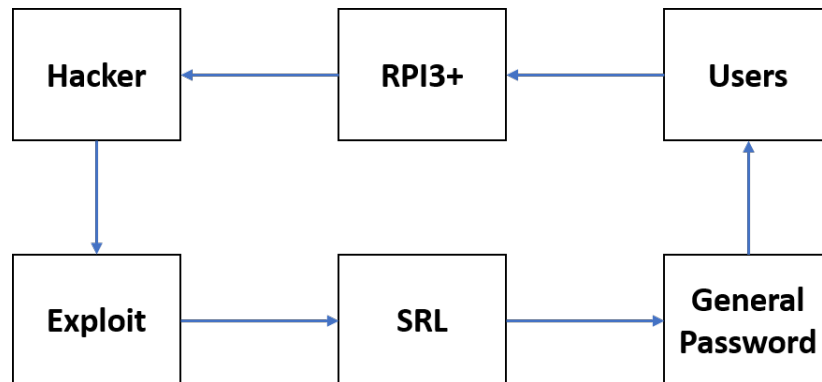


Figure 9. Pen-Test in vulnerable environment.

In addition, another attack was successfully performed because the user inserted the same general passphrase to encrypt the key. Taking into consideration this situation, the Fail2Ban and UFW installation settings were modified as well as the default rules. In addition, the key’s passphrase was changed with numbers and special characters for the strongest one with more than 16 characters. Now, the exploit was run again, but the key’s passphrase was hard to guess and after five tries Fail2Ban banned the IP address updating its Firewall’s IP-Tables for an unlimited period. This procedure is shown in Figure 10. Then, the host files were modified for allowing only the IP address from the authorized users in the system. Thus, only registered user IP address can target and break the machine.

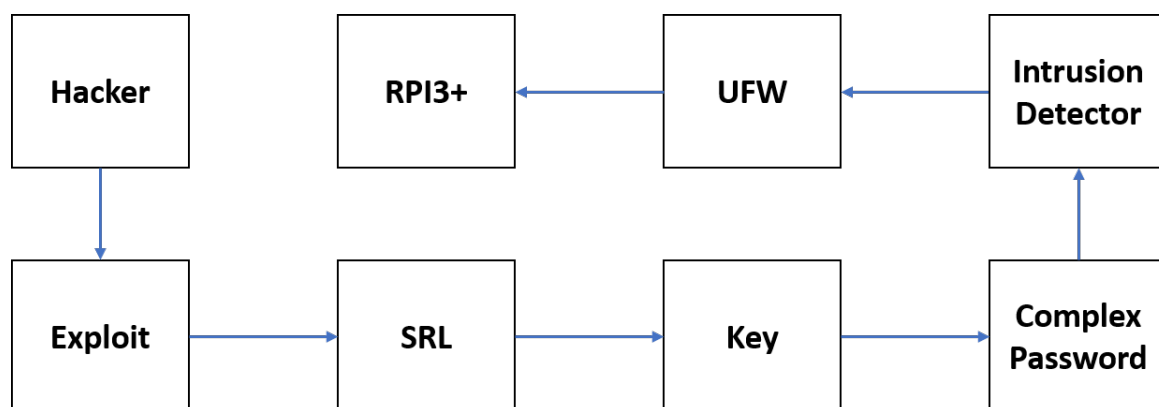


Figure 10. Pen-Test in the proposed scheme.

4.4.3. Denial of Service (DoS) Attacks

Low Orbit Ion Cannon (LOIC) [41] was the mechanism used to strike the RPI3+. One of the DoS attacks requests 530,020 to the server from which 1239 failed in vulnerable environment. A high number in the failed parameter means that the server goes down and does not respond. To mitigate this attack, modifications in the host (.allow and .deny) files and Fail2Ban (.local) rules were made.

After those changes, a total of 44,045 requests were made to the server by the first attack, and only 10 failed. In addition, the request to the server stops when the failed goes to 10 because the Fail2Ban detects and bans the invalid IP address. Then, another threat was carried out, since the Fail2Ban had blocked the IP address, 0 requests were processed and 0 failed, as shown in Figure 11. This indicates the IP address is blocked and can no longer attack or attempt to access the RPI3+.

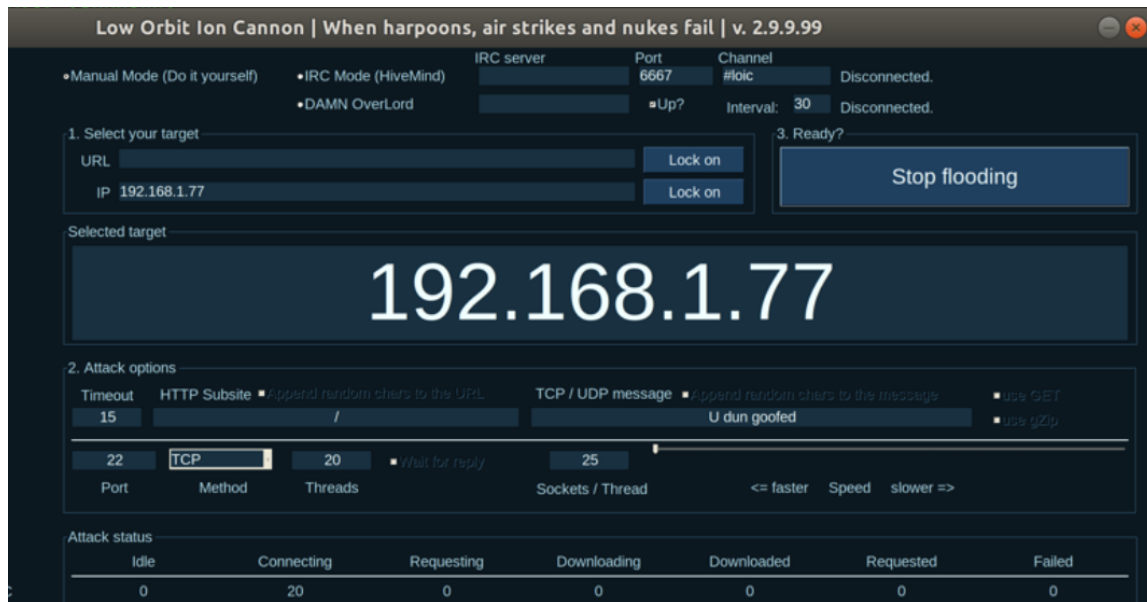


Figure 11. DoS stopped.

The calculated failure rate of our system after some runs of DoS attacks in the vulnerable environment was 0.20% but the CPU was working at 100%. In the case of DDoS attacks, the system can shut down for an amount of time without the proposed scheme in this paper. The failure rate equation used was:

$$F_{rate} = \frac{\sum_{i=1}^n F_i / R_i}{n} (100\%) \quad (1)$$

where F is the failed parameter and R is the requested parameter of the LOIC software.

5. Summary and Future Work

This paper presented a low-cost, secure IoT mechanism for monitoring and controlling appliances/devices in a microgrid with renewable energy sources. The integration of a WSANCS to the microgrid provides real-time access to each device connected to the system for monitoring and control purposes. In addition, a mobile application allows the user to visualize real time power consumption/generation data with a graphical user interface. As soon one of the categories is selected, a graph of the desired measurement is refreshed with the latest desired data, providing updated results. The application alerts the user when a device reaches a power consumption threshold defined by the user.

A control and security analysis was conducted to establish the feasibility of the proposed system. The results demonstrate the systems capabilities in a DC microgrid test bench. Brute force and denial of service attacks were mitigated involving free and open-source software mechanisms in the network layer of the IoT implementation.

Future work includes the increasing the microgrid size and developing an iOS version app to reach more users. In addition, the system can be improved through the use of machine learning algorithms to detect anomalies in the system or a turned-on device without human interaction based on previous data [42].

Author Contributions: Conceptualization, J.M.-M. and D.A.-R.; formal analysis, J.M.-M., D.A.-R., and I.V.-L.; funding acquisition, D.A.-R. and W.W.W.; investigation, J.M.-M. and D.A.-R.; methodology, J.M.-M., D.A.-R., and I.V.-L.; Project administration, J.M.-M. and D.A.-R.; resources, J.M.-M., D.A.-R., and I.V.-L.; software, J.M.-M. and I.V.-L.; supervision, J.M.-M., D.A.-R., and I.V.-L.; validation, J.M.-M., D.A.-R., and I.V.-L.; writing—original draft, J.M.-M. and D.A.-R.; and writing—review and editing, J.M.-M., D.A.-R., I.V.-L., and W.W.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Consortium for Integrating Energy System in Engineering and Science Education (CIESESE), a program supported by the U.S. Energy Department (DE-NA0003330).

Acknowledgments: The authors are grateful for the support of the José Domingo Pérez Engineering School at Ana G. Mendez University, Gurabo Campus, and to the Puerto Rico Energy Center (PREC). In addition, the authors gratefully acknowledge the contributions of the undergraduate students Javier Sanchez, Jorge Cruz, and Shervin Firouzdehghan to this paper.

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

Abbreviations

The following abbreviations are used in this manuscript:

| | |
|--------|---|
| CAN | Controller Area Network |
| DC | Direct Current |
| DG | Distributed Generation |
| MPPT | Maximum Power Point Tracking |
| HEMS | Home Energy Monitoring System |
| IoT | Internet of Things |
| MAC | Media Access Control |
| PTP | Point-to-Point |
| RESs | Renewable Energy Sources |
| RPI3+ | Raspberry Pi 3 B+ |
| SA-N | Sensor-Actuator Nodes |
| S-N | Sink Node |
| TLS | Transport Layer Security |
| UFW | Uncomplicated Firewall |
| WSANCS | Wireless sensor and Actuator Networked Control System |
| WSN | Wireless Sensor Network |

References

1. Electric Sales, Revenue, and Average Price—Energy Information Administration. Available online: https://www.eia.gov/electricity/sales_revenue_price/ (accessed on 2 April 2020).
2. Yoshikawa, T.; Saraya, S. HEMS Assisted by a Sensor Network Having an Efficient Wireless Power Supply. *IEEE Trans. Magn.* **2013**, *49*, 974–977. [[CrossRef](#)]
3. Lee, S.; Park, B. Home Energy Management System for Residential Customer: Present Status and Limitation. *Int. J. Adv. Cult. Technol.* **2018**, *6*, 284–291.
4. Rodriguez-Diaz, E.; Vasquez, J.C.; Guerrero, J.M. Intelligent DC Homes in Future Sustainable Energy Systems: When efficiency and intelligence work together. *IEEE Trans. Consum. Electron.* **2016**, *5*, 74–80. [[CrossRef](#)]
5. Liu, L.; Liu, Y.; Wang, L.; Zomaya, A.; Hu, S. Economical and Balanced Energy Usage in the Smart Home Infrastructure: A Tutorial and New Results. *IEEE Trans. Emerg. Top. Comput.* **2015**, *3*, 556–570. [[CrossRef](#)]
6. Salman, L.; Salman, S.; Jahangirian, S.; Abraham, M.; German, F.; Blair, C.; Krenz, P. Energy efficient IoT-based smart home. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT 2016), Reston, VA, USA, 12–14 December 2016; pp. 526–529.
7. Minerva, R.; Biru, A.; Rotondi, D. Towards a definition of the Internet of things (IoT). *IEEE Internet Initiat.* **2015**, *1*, 1–86.
8. Mandula, K.; Parupalli, R.; Murty, C.A.S.; Magesh, E.; Lunagariya, R. Mobile based home automation using Internet of Things (IoT). In Proceedings of the 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICT), Kumaracoil, India, 18–19 December 2015.

9. Dlamini, N.N.; Johnston, K. The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review. In Proceedings of the 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban, South Africa, 28–29 November 2016.
10. Mahmud, S.; Ahmed, S.; Shikder, K. A Smart Home Automation and Metering System using Internet of Things (IoT). In Proceedings of the 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 10–12 January 2019.
11. Mishra, A.; Irwin, D.; Shenoy, P.; Kurose, J.; Zhu, T. GreenCharge: Managing Renewable Energy in Smart Buildings. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1281–1293. [[CrossRef](#)]
12. Alsaif, K.A. Challenges and Benefits of Integrating the Renewable Energy Technologies into the AC Power System Grid. *AJER* **2017**, *6*, 95–100.
13. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [[CrossRef](#)]
14. Zipperer, A.; Aloise-Young, P.A.; Suryanarayanan, S.; Roche, R.; Earle, L.; Christensen, D.; Bauleo, P.; Zimmerle, D. Electric Energy Management in the Smart Home: Perspectives on Enabling Technologies and Consumer Behavior. *Proc. IEEE* **2013**, *101*, 2397–2408. [[CrossRef](#)]
15. Van Dam, S. Smart Energy Management for Households. Ph.D. Thesis, Delft University of Technology, Delft, The Netherlands, 2013. [[CrossRef](#)]
16. Dan, T.; Merrill, S. The U.S. Department of Energy’s Microgrid Initiative. *Electr. J.* **2012**, *25*, 84–94. [[CrossRef](#)]
17. Wei, F.; Ming, J.; Xu, L.; Yi, B.; Chris, M.; Cheng, Y.; Jian, Y. A review of microgrid development in the United States—A decade of progress on policies, demonstrations, controls, and software tools. *Appl. Energy J.* **2018**, *228*, 1656–1668. [[CrossRef](#)]
18. Ward, B.; Dan, T.; Ross, G.; Steve, G.; Jason, S.; Dhruv, B.; Jim, R. The Advanced Microgrid Integration and Interoperability. February 2014. Available online: <https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2014/141535.pdf> (accessed on 2 April 2020).
19. Bushra, R.; Husain, R.M. Applications of wireless sensor networks for urban areas: A survey. *J. Netw. Comput. Appl.* **2015**, *60*. [[CrossRef](#)]
20. Dargie, W.; Poellabauer, C. *Fundamentals of Wireless Sensor Networks: Theory and Practice*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2010; ISBN 978-0-470-99765-9.
21. Song, Z.; Zhou, X. Research and simulation of wireless sensor and actuator networked control system. In Proceedings of the 2013 25th Chinese Control and Decision Conference (CCDC), Guiyang, China, 25–27 May 2013; pp. 3995–3998.
22. Coelho, S.; Rozario, R.; Sharma, R.; Mehra, M. An IOT Based Smart Cubicle System for Effective Power Usage and Employee Monitoring in Offices. In Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 5 January 2018; pp. 1–6.
23. Patchava, V.; Kandala, H.B.; Babu, P.R. A Smart Home Automation technique with Raspberry Pi using IoT. In Proceedings of the 2015 International Conference on Smart Sensors and Systems (ICSSS), Bangalore, India, 21–23 December 2015; pp. 1–4.
24. Dean, A.; Agyeman, M.O. A Study of the Advances in IoT Security. In Proceedings of the 2018 International Symposium on Computer Science and Intelligent Control (ISCSIC), Stockholm, Sweden, 21–23 September 2018.
25. Medwed, M. IoT Security Challenges and Ways Forward. In Proceedings of the 2016 6th International Workshop on Trustworthy Embedded Devices, Vienna, Austria, 28 October 2016.
26. Rawlinson, K. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. HP Development Company, L.P. 29 July 2014. Available online: <https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676> (accessed on 2 April 2020).
27. Aponte-Roa, D.A.; Martinez, J.B.; Fernandez, X.C.; Weaver, W.W. A Benchtop DC Microgrid for Renewable Energy Sources Integration. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 79–84.
28. Yi, P.; Iwayemi, A.; Zhou, C. Developing ZigBee deployment guideline under wifi interference for smart grid applications. *IEEE Trans. Smart Grid* **2011**, *2*, 110–120. [[CrossRef](#)]
29. Hall, B.; Paulitsch, M.; Driscoll, K.; Sivencrona, H. ESCAPE CAN limitations. *SAE Trans. J. Passeng. Cars Electron. Electr. Syst.* **2008**, *116*, 422–429.

30. Cena, G.; Valenzano, A.; Vitturi, S. Advances in automotive digital communications. *Comput. Stand. Interfaces* **2005**, *27*, 665–678. [[CrossRef](#)]
31. Bauer, G.; Kopetz, H.; Steiner, W. The central guardian approach to enforce fault isolation in the time-triggered architecture. In Proceedings of the 6th ISADS, Pisa, Italy, 9–11 April 2003; pp. 37–44.
32. Navet, N.; Simonot-Lion, Y.S.F.; Wilwert, C. Trends in automotive communication systems. *Proc. IEEE* **2005**, *93*, 1204–1223. [[CrossRef](#)]
33. Zurawski, R. (Ed.) Fault tolerant services for safe in-car embedded systems. In *The Embedded Systems Handbook*; CRC: Boca Raton, FL, USA, 2005.
34. Barranco, M.; Proenza, J.; Almeida, L. Quantitative Comparison of the Error-Containment Capabilities of a Bus and a Star Topology in CAN Networks. *IEEE Trans. Ind. Electron.* **2011**, *58*, 802–813. [[CrossRef](#)]
35. Khan, R.; Khan, S.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17–19 December 2012.
36. Aman, M.N.; Chua, K.C.; Sikdar, B. Secure Data Provenance for the Internet of Things. In Proceedings of the ASIA CCSACM Symposium on Information, Computer and Communications Security, Abu Dhabi, UAE, 2–6 April 2017.
37. Martínez-Martínez, J.; Carvajal-Jiménez, C.; Aponte-Roa, D.A. A Secured IoT Scheme for Microgrids Monitoring. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0986–0990.
38. Wu, M.; Lu, T.; Ling, F.; Sun, J.; Du, H. Research on the Architecture of Internet of Things. In Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010.
39. Lim, S.; Yeap, G. Centralised Smart Home Control System via XBee Transceivers. In Proceedings of the 2011 IEEE Colloquium on Humanities, Science and Engineering Research (CHUSER), Penang, Malaysia, 5–6 December 2011; pp. 327–330.
40. Metasploit-Penetration Testing Software. Available online: <https://www.metasploit.com> (accessed on 2 April 2020).
41. Low Orbit Ion Cannon (LOIC). Available online: <https://www.imperva.com/learn/application-security/low-orbit-ion-cannon/> (accessed on 2 April 2020).
42. De Coninck, E.; Verbelen, T.; Vankeirsbilck, B.; Bohez, S.; Leroux, S.; Simoens, P. DIANNE: Distributed Artificial Neural Networks for the Internet of Things. In Proceedings of the 2nd Workshop on Middleware for Context-Aware Applications in the IoT, Vancouver, BC, Canada, 8 December 2015.

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).