Theory and Practice of Science and Technology
2025, VOL. 6, NO. 2, 78-83
DOI: 10.47297/taposatWSP2633-456916.20250602

Key Technologies and Protocol Comparison in Wired Communication of IoT Gateways in Smart Grids

Yu Cheng

School of Software and Microelectronics, Peking University, Beijing 102600

ABSTRACT

Connect multiple devices like sensors, meters, control systems across the network and act as building blocks for communication in smart grid networks. In this study, the frequently used communication technologies and protocols including for example Ethernet, Power Line Communication (PLC) or fiber optics in the communication of smart grid and Internet of Things (IoT) gateways are evaluated. All of these technologies are pitched in terms of speed, reliability, cost, scalability, and security. The link can be ethernet and fiber optics links providing high speed communication but is relatively expensive or a PLC link can be less expensive but with lesser speed and reliability owing to electric interference. One can also cite security issues such as the shift from privacy and so forth that are important in safeguarding data away from the grid. Neither is new for IoT gateways (known to have similar future-proofing considerations) and scalability as key design dimensions follow suit as organizations need to prepare themselves for new technologies and higher data flows. Ultimately, this work provides guidelines for selecting the appropriate communication technology once the communication requirements of different smart grid applications are ordered in terms of performance, cost, and security trade-offs.

KEYWORDS

IoT gateways, smart grid; communication technologies; interoperability; security

1 Introduction

Smart grids have made it possible to do so by leveraging Internet of Things (IoT) technologies. The integration of IoT provides real-time monitoring and control of various components of the grid, resulting in major enhancements of energy efficiency, reliability, and sustainability. With the proliferation of smart grids and their complexity, reliable and efficient communication systems between grid components becomes imperative. Because of this communication infrastructure, which serves as the backbone of any smart grid, critical data is exchanged for decision-making processes, load balancing, and fault detection[1]. It is one of the essential components of the communication network of the smart grid. They function as intermediaries between the IoT devices and the central control system, allowing for seamless communication across all the layers of the grid.

They are responsible for sensor data collection, local information processing, and remote communication of this information to the central system for analysis and decision-making. The paper is organized as follows. The first section summarizes the most important technologies for wired communication in IoT gateways in smart grids, and their power supply and fiber optic communication.

After that, we address the communication protocols used across smart grid communication, including but not limited to Modbus, DNP3, IEC 61850, etc., alongside their feasibility for smart grid operations. The next section provides an in-depth comparative analysis of these technologies and protocols and discusses implementation challenges. This work concludes with a discussion of future trends and innovations in the area.

2 Overview of Smart Grids and IoT Gateways

Smart grids refer to technology installed in electric networks and systems, such as sensors and monitoring systems which help electricity generation, storage, and consumption. Newer grid systems, known as smart grids, have transformed the one-way communications of the traditional power grid (whereby the utility communicates to the consumer) to a two-way communication system, allowing for data exchange in real-time for all components, from the power generation facilities to the end users of this energy. It has to be based on a network that combines real-time data from multiple sources like IoT devices, smart sensors, and data analytics. This perception of IoT gateways and communication in a smart grid is frequently required as it can combine diverse IoT devices and systems via the network. They can be used to send information to centralized decision makers through data collected by distributed smart meters, sensors, and other hubs [2]. This will ensure interoperability of devices work with different communication protocols, an important aspect in a complex and multi-layered grid ecosystem. Furthermore, these gateways also control network security, data encryption and fault detection operations, ensuring that every communication within the grid is safe and reliable.

3 Key Technologies in Wired Communication for IoT Gateways

3.1 Ethernet-based Communication

Ethernet networks are a well-defined and complex network structure used to transmit larger data over longer distances with little intervention. There are limitations to Ethernet based communication. The primary disadvantage is costly infrastructure investment, particularly in broad-grid areas where considerable distance wiring and hardware may be necessary. Ethernet networks are also vulnerable to physical damage since the technology depends on wired connections that can be affected by other factors in the environment or equipment malfunctions. Despite these limitations, Ethernet's high capacity and reliability provide distinct advantages as a smart grid communication network backbone. Its deterministic clock cycle guarantees the transmission of important information for time-sensitive activities such as load balancing or grid failure detection, stabilizing the grid and ensuring that it operates as effectively as possible.

3.2 Power Line Communication (PLC)

PLC is a novel technique in the Smart grid that enables devices to communicate using existing power lines, offering less expensive communication infrastructure. Unlike traditional communication methods, PLC uses the pre-installed electrical grid for data transmission, eliminating the need for extra wiring or major infrastructure upgrades. This makes PLC highly attractive for retrofitting-wireless/communication networks in situations where it is impractical or cost prohibitive to lay new cable. Pilot PLC is reinforced for process automation & distribution line network to make specific, secure communication, addressing a wide range of grid applications such as smart metering, load management, and remote monitoring of grid components, on long & short distance [3].

PLC, for example, was being utilized in such a way that communication could be provided in regions where other wired technologies like Ethernet or fiber optics may not make sense. It runs with relatively low installation cost and uses the same power lines. But PLC does come with certain limitations. A technology susceptible to noise and electromagnetic interference, the device can degrade in quality with excessive electrical interference, particularly in environments radiated with electromagnetic energy or where the power line quality is low. Also, the data transmission speed may be lower compared to Ethernet and fiber optic solutions, which makes USB less suitable for use where high bandwidth is important. Although PLC has challenges, it is still significant for extending smart grid communication, especially in remote or closely populated regions.

3.3 Fiber Optic Communication

One of the most sophisticated and dependability wired communication technologies utilized in smart grids, specifically, for long-range and high- bandwidth applications is fiber optic communication. In contrast to copper-based systems, fiber optics transfer data as light pulses through glass or plastic fibers, providing considerable data transfer rates with higher bandwidth capabilities. Fiber optics are therefore well suited for applications in smart grids that require real-time data transmission, such as grid monitoring, fault detection, and automated control systems. One of the fiber optic section advantages is capable of transmitting data in large amounts at different wavelength intervals with no or little signal loss and electromagnetic interference.

In terms of fiber optic communication, it is needed especially when there is need for long-distance transmission of data at large capacity for real-time transmission of data between various parts of the power system, such as between substations and between control centers and power plants [4]. Also, it is more secure than other wired technologies because no one can listen to or manipulate the signals. The high initial installation cost and difficulty in laying fiber optic cables, especially in difficult environments, are the main drawback of fiber optics. Nonetheless, the long-term advantages of fiber optic communication, such as its reliability, speed, and ability to handle substantial data traffic, position it as an essential element of contemporary smart grid infrastructure, bolstering the efficiency and resilience of the grid in the process.

4 Communication Protocols for IoT Gateways

4.1 Modbus

Modbus is a widely used communication protocol for industrial applications including smart grids. The implementation of ModBus is very simple and also quite low cost. Being open-source with large support, it becomes a top choice of producers and system integrators. Still, Modbus faces some obstacles, especially those concerned with security and speed that can appear when dealing with sizeable amounts of real-time data. Furthermore, its protocol does not perform encryption and authentication by default, which is a security concern in the modern smart grid scenario.

Despite its weaknesses, the Modbus protocol continues to be an efficient solution for applications where ease of use and reliable message transmission take precedence over complex security mechanisms.

4.2 DNP3

The DNP3 (Distributed Network Protocol), a communication protocol widely used in utilities and industrial control (ICS) systems, is especially common in smart grids. It is specifically tailored for remote monitoring and control of electrical networks including in focuses where data integrity and high reliability are essential. The DNP3 protocol encompasses multiple valuable capabilities including time-stamped data, secure data transmission, and support for point-to-point and multipoint communications. As a result, DNP3 is a very efficient protocol for the purpose of controlling important grid structures, including substations, distribution networks, and power generation plants. The DNP3 protocol is optimized for low-bandwidth, long-distance communications, and is therefore well-suited for use in rural, or remote, areas where connectivity may be limited. DNP3 does require somewhat more complex implementation than say, Modbus, for example, and its higher overhead does make it more resource-intensive. However, the reliability and security features of DNP3 and overall—make it the go to protocol for mission-critical applications, in the smart grid, especially where high availability and resilience is necessary.

4.3 IEC 61850

IEC 61850 is an international standard specifying communication networks and systems in substations, it is often used in smart grids due to its ability to support real-time communication, automation and control. With a protocol focus that enables different devices in substations to seamlessly communicate with each other and the grid, this encompasses protection relays, switchgear, transformers, and other components. IEC 61850: This protocol is targeted towards applications that require high-speed data exchange and complex automation, making it a fundamental element of modern smart grid architecture. It enables horizontal and vertical communication for devices; that is, devices can directly communicate with one another or with central control systems, allowing for flexibility and scalability [5]. A major benefit of IEC 61850 is that it facilitates the transfer of time-coherent information, for example, data for disturbance recording, protective relays, fault clearing and grid control signals, with very low latencies. Indeed, its robustness, security features, and real-time capabilities make it essential for large-scale, high-performance smart grids that require advanced automation and control, despite these shortcomings.

4.4 Zigbee and LoRaWAN

Alternatives such as Zigbee and LoRaWAN come under the umbrella of hybrid protocols that integrate both wired and wireless technologies to provide a comprehensive communication strategy within smart grids. These protocols are useful in situations where entirely wired technologies are not feasible or economical, such as in remote regions or for low-power, battery-operated devices. Zigbee is also a short range wireless protocol for low rate devices, commonly used for IoT applications, whereas LoRaWAN (Long Range Wide Area Network) technology is used for long-range communication while consuming minimal power, hence devices can be connected over a wide geographical area.

Zigbee supports mesh networking for increased coverage; LoRaWAN enables distance over kilometers with a low data rate, so both give you scalability. These characteristics are valuable in smart grids that require communication systems in the range of vast areas with a high density of sensors and units of smart metering and environmental management. Both these protocols face the question of data transfer rates and network interference. Zigbee, for staple, can suffer from congestion in dense environments; LoRaWAN's low data rate might not fit high-bandwidth fates. Zigbee and LoRaWAN both face drawbacks, but both play critical roles in hybrid communication solutions, occupying the space between wired and wire-free technologies in the expanding smart grid ecosystem.

5 Comparison of Technologies and Protocols

5.1 Criteria for Comparison: Speed, Reliability, Cost, Scalability, Security

Choosing the right IoT gateway communication technologies and protocols in smart-grid requires the following limitation. Speed is of the essence for real-time applications, including grid monitoring and fault detection, which require low latency and high data throughput. Reliability guarantees that the communication is smooth, steady, and stable, even with environmental challenges or system failures. Cost is a critical consideration, since smart grid deployments typically require large-scale infrastructure, and affordable solutions are essential for scalability. Due to its development, scalability means that the communication system can accommodate more data traffic and more devices as the smart grid grows [6].

Lastly, as cyberattacks on critical infrastructure become increasingly common, security is paramount to protect sensitive grid data and ensure data integrity across communications. Different communications technology and protocol have strengths and weaknesses in these areas. Ethernet has the advantage of speed and reliability, but the infrastructure expense, particularly over large areas, is high.

5.2 Performance Analysis of Each Technology

From a speed perspective, fibre optic communication is the fastest option, as it has the ability to transfer high data rates with low latency, ideal for high-demand applications in the smart grid. Next comes Ethernet, which provides decent performance and large throughput, but with possible bandwidth limitations in high density locations. Whereas PLC facilitates the cheapest solution, it usual functions at slower speeds, thus not being ideal for data-heavy applications. Conversely, Zigbee and LoRaWAN hybrid protocols, with low-speed, long-range communication capabilities, suit use cases where high bandwidth is not pivotal.

Another consideration is reliability, where fiber optics and ethernet ensures stable, uninterrupted data transfer even in demanding environments. PLC based communication can be affected by electromagnetic interference caused by the power lines which would lead to the degradation of the signal which leads to less reliability. Due to security concerns related to IoT gateway integration, important protocols in this area such as DNP3 and IEC 61850 provide strong encryption and authentication mechanisms to validate that sensitive grid data is only shared with appropriate entities. Ethernet and fiber optics can be secure, but many other protocols and hardware must also be supplemented to provide comprehensive cybersecurity. For low-power use cases, Zigbee and LoRaWAN provide a middle ground with moderate reliability but can be limited with respect to range under certain conditions.

5.3 Strengths and Weaknesses of Each Communication Protocol in IoT Gateway Integration

As a result, every communication protocol has its particular strengths and weaknesses when incorporated in IoT gateways for smart grids. Support for Modbus is also widely available, but the protocol is basic and easy to implement, making it relatively low cost and suitable for simple grid functions, while lacking advanced security features that can limit its use in critical applications. DNP3 is a secure protocol primarily used for remote monitoring and control operations in low-bandwidth or long-distance scenarios. But it's not as simple to implement and requires more resources to set up and maintain possible. However, IEC 61850 is more suitable for faster data exchange in substations, which offers excellent scalability and is capable of supporting advanced grid operations like automation and protection. Ultimately, the choice of communication protocol will depend on the specific needs of the smart grid system, where considerations of speed, reliability, cost, and security need to be balanced.

6 Challenges in Implementing IoT Gateways for Smart Grid Communication

6.1 Interoperability between Different Communication Technologies

Interoperability among different communication technologies is one of the major challenges in the deployments of IoT gateways for smart grid communication. Smart grids are composed of interfacing with many devices such as sensors, meters, and control systems, but also network components with different communication standards. Thus, the IoT gateways need to support multiple protocols simultaneously for the smooth exchange of data between all devices and systems. This is a compatibility issue arising from the convergence of communication technologies such as Ethernet. Every protocol has its demands regarding transmission rates, minimum latency, data formats, formats for error detection and recovery, etc., or simply put, makes life difficult for communications in heterogeneous environments. Those gateways are ELT business cost services fees and needs updates in periods with new standards. A smart grid can only function properly if a well-defined set of procedures are formed that can close the gap between heterogeneous systems. Interoperability acts as a value enhancer—ensuring that data losses do not occur, and the systems are working efficiently and smoothly.

6.2 Security Concerns (Data Privacy, Cyber Threats)

IoT gateways for smart grid communication systems are susceptible to security threats. Because these systems carry sensitive data like grid operations, financial transactions, and customer usage patterns, they are prime targets for cyberattacks. The end users' privacy and the whole Grid network's integrity are in great threat due to the data breaches and unauthorized access. IoT gateways serve as conduits between different devices and networks, making them prime targets for cybercriminals trying to intrude weak spots in the communication framework.

Additionally, data transmissions are often complex, since there are many communication protocols associated with different components of the grid. The protocols can have variable levels of security, which may lead to vulnerabilities. Older protocols like Modbus offer little encryption capacity, whereas more recently developed ones such as IEC 61850 have good features, but their implementation and maintenance requires attention. IoT gateway security approaches encompass data encryption, as well as robust authentication mechanisms, advanced intrusion detection systems, and frequent software updates to address newly discovered vulnerabilities. As cyber threats continue to evolve, it becomes necessary to ensure that these IoT gateways have robust security to protect critical infrastructure and the confidence of users.

6.3 Scalability and Future-Proofing in Smart Grid Networks

IoT gateway must be scalable because smart grids will have an increasing number of devices and they must support the increasing data traffic. As smart meters, sensors, and connected devices proliferate, so, too, will smart grid networks, producing significant amounts of data. Due to the growth, IoT gateways should be designed to scale as this number grows to ensure that the operation is seamless. New technologies involving communication protocols, IoT devices, grid management technologies and others will likely emerge at breakneck speeds due to technological advancement. As a result, IoT Gateways should be flexible in nature, compatible with newer technologies with just a minor Touch up using Integration than redeveloping systems [7]. This means investing in hardware and software solutions that are flexible enough to make future upgrades simple, regardless of how the grid's architecture changes over time. Modular gateway systems may be one way to adapt, upgrading first to higher bandwidth, opening up new capabilities to ensure a better experience. Scalability and future-proofing are key to maintaining smart grid operations while minimizing the need for continual, expensive upgrades to our infrastructure.

6.4 Challenges Related to Cost and Implementation

Cost-related benefit challenges arising from the inclusion of low-cost IoT gateways in smart grid communication networks. Another reason for high IoT Gateway prices is due to most of these IoT Gateways being very expensive at first place as the installation of IoT gateways involves any special hardware or equipment that may be required, special integration with the current infrastructure, and support for various protocols of communication. In addition, these systems could also be expensive — particularly with large networks being forced to spend on periodic updates, troubleshooting, and enhanced security. Once established, smart grid networks pose another challenge in their long-term operational cost. Gateway at the edge of the network is processing growing amounts of data, at a near-exponential rate, with the growth in the number of connected devices. Moreover, post-deployment, continuous support would be required, like software updates and monitoring to ensure security breaches, this accounts for the total associated expense which could act as a limiting factor. Striking a balance between those costs and ensuring that the grid continues to function reliably and securely is a delicate job for grid operators and planners. These may mitigate some of these costs, but using existing infrastructure or developing hybrid communication systems is unlikely to make energy distribution systems as a whole financially viable to operate. However, a significant barrier to the IoT gateways characterisation in smart grid systems lies in performance and cost scalability.

7 Conclusion

The parts that facilitate remote communication are the IoT gateways, which serve as the backbone of the smart grid, allowing devices to interact with one another and allowing real-time communication, control, and data exchange. Ethernet, PLC, fiber optics could be the communication technology etc. It is a decision on the needs of the grid with regard to speed, reliability, cost, and security. With the benefits of Ethernet and fiber, provides very high data transfer and reliability, however the installation cost is high and thus can be a barrier for widespread deployment, particularly in remote or large scale applications. Since we have a lot of various technologies and protocols, interoperability between such systems is a challenge that further establishes the necessity to develop IoT gateways that can process multiple communication standards in parallel. Additionally, security challenges require a response because the original settings of the grid depend on the security of sensitive data from cyber attacks. Security and future-proofing for the exploding demand in smart-grid services become very important in making choices about the IoT communications solutions they choose. Selecting the right communication protocol requires a balance between performance, price, and security. It also requires a long-term scalability approach, which is vital in ensuring that smart grid systems can evolve wit h emerging technologies. By leveraging on such interdependent factors, IoT-based advanced smart grids have enabled utilities to create comprehensive grids capable of servicing the primary sectors of contemporary energy systems.

About the Author

Yu Cheng was born in Baoding City, Hebei Province in 2002. He graduated from Beijing University of Posts and Telecommunications with a Bachelor of Engineering degree. Currently, he is pursuing a major in Engineering (Electronic Information major) at Peking University.

References

[1] Singh, S. V., Khursheed, A., & Alam, Z. (2022). Wired communication technologies and networks for smart grid—A review. Cyber Security in Intelligent Computing and Communications, 183-195.

[2] Emmanuel, M., & Rayudu, R. (2016). Communication technologies for smart grid applications: A survey. Journal of Network and Computer Applications, 74, 133-148.

[3] Ghasempour, A. (2019). Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. Inventions, 4 (1), 22.

[4] León, J. P. A., Santos, C. L. D., Mezher, A. M., Barrera, J. C., Meng, J., & Guerra, E. C. (2023). Exploring the potential, limitations, and future directions of wireless technologies in smart grid networks: A comparative analysis. Computer Networks, 235, 109956.

[5] Chhaya, L., Sharma, P., Kumar, A., & Bhagwatikar, G. (2018). IoT-based implementation of field area network using smart grid communication infrastructure. Smart Cities, 1(1), 176-189.

[6] Ancillotti, E., Bruno, R., & Conti, M. (2013). The role of communication systems in smart grids: Architectures, technical solutions and research challenges. Computer Communications, 36(17-18), 1665-1697.

[7] Abdul Salam, R., Iqbal Ratyal, N., Ahmed, U., Aziz, I., Sajid, M., & Mahmood, A. (2024). An Overview of Recent Wireless Technologies for IoT-Enabled Smart Grids. Journal of Electrical and Computer Engineering, 2024(1), 2568751.