IAES Journal of Electrical and Electronics Engineering
Vol. 10, No. 1, June 2023, pp. 6~11
ISSN: 2338-7432, DOI: 10.11591/jeee.v10i1.pp6-11

Communication architectures for smart electrical plugs: a review of wireless protocols, network connectivity, and remote appliance operation

Tole Sutikno[1], Watra Arsadiando[2], Anggit Pamungkas[2]
[1]Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

Article Info

Article history:

Received Dec 30, 2020
Revised Sep 14, 2021
Accepted Nov 2, 2021

Keywords:

Bluetooth
IoT communication
Matter
Remote appliance control
Smart electrical plugs
Wi-Fi
Zigbee

ABSTRACT

Smart electrical plugs have evolved from simple remotely operated switches into connected devices capable of monitoring electricity consumption and supporting intelligent appliance management. Their effectiveness, however, depends strongly on communication architecture, wireless connectivity, interoperability, and the reliability of remote control. This review examines communication technologies and network architectures relevant to smart electrical plugs, with particular attention to Wi-Fi, Bluetooth, Zigbee, and Matter. It also discusses the roles of gateways, cloud platforms, local controllers, and application-layer messaging protocols in enabling device monitoring and remote appliance operation. Research published up to 2022 is reviewed to compare communication range, network topology, power requirements, data capacity, scalability, and security considerations. The analysis indicates that Wi-Fi is suitable for direct internet connectivity, Bluetooth is useful for local commissioning and short-range control, and Zigbee supports low-power mesh networking. Matter provides an emerging interoperability framework that can operate over supported IP-based network technologies. The review concludes that no single communication technology is optimal for every application, and that reliable smart-plug deployment requires protocol selection based on network conditions, operational requirements, cybersecurity, and interoperability.

This is an open access article under the CC BY-SA license.

1. INTRODUCTION

Smart electrical plugs are increasingly used to connect conventional electrical appliances to digital monitoring and control systems. Their functions may include remote switching, energy measurement, operating-time scheduling, and appliance status reporting. These capabilities depend on reliable communication between the plug, a local network, a management platform, and the user's control interface. Consequently, communication architecture is a fundamental factor determining the performance and usability of smart-plug systems [1], [2].

The growing diversity of wireless technologies creates both opportunities and challenges for smart-plug development. Wi-Fi offers direct connectivity to conventional IP networks, whereas Bluetooth provides convenient short-range communication and Zigbee supports low-power networking among multiple devices. Differences in network topology, communication range, energy consumption, bandwidth, and security influence the suitability of each technology for particular applications [3]-[5]. Interoperability is another concern because products from different manufacturers may use incompatible communication methods or proprietary application interfaces.

This review examines the communication architectures that enable smart electrical plugs to monitor and control connected appliances remotely. It focuses on Wi-Fi, Bluetooth, Zigbee, and the Matter interoperability framework, while also considering gateways, messaging protocols, and cloud-based services. The discussion follows a technical progression from wireless connectivity to network architecture, remote

operation, and implementation challenges. The objective is to provide a comparative basis for selecting communication technologies and designing reliable smart-plug systems.

2. COMMUNICATION ARCHITECTURE OF SMART ELECTRICAL PLUGS

A typical smart-plug communication architecture consists of the electrical switching unit, communication interface, network infrastructure, management platform, and user application. The switching unit receives commands and controls the electrical connection to the appliance, while the communication interface exchanges data with a local controller or network. The management platform processes device status, energy measurements, user commands, and automation rules. This layered structure is consistent with general IoT architectures that separate physical devices, communication networks, gateways, applications, and security functions [1], [6].

Communication can be organized using direct, gateway-based, or cloud-mediated architectures. In a direct architecture, a smartphone or local controller communicates with the smart plug through a supported wireless connection. A gateway-based architecture introduces an intermediary device that manages several plugs and forwards their data to a local server or cloud platform. Cloud-mediated systems allow remote access over the internet, but their operation depends on external connectivity and service availability [6], [7].

The architecture should distinguish between network connectivity and application-level communication. Wireless technologies such as Wi-Fi, Bluetooth, and Zigbee establish the physical and link-layer connections between devices. Application protocols such as MQTT, CoAP, and HTTP define how monitoring data and control commands are exchanged between devices and software services. This distinction is important because two smart plugs may use different wireless technologies while still communicating with the same management platform through a common application interface [8], [9].

3. WIRELESS COMMUNICATION TECHNOLOGIES

3.1. Wi-Fi communication

Wi-Fi is widely used in smart plugs because it can connect directly to existing wireless local area networks and IP-based services. A Wi-Fi smart plug can communicate with a router and subsequently exchange information with a mobile application, local server, or cloud platform. This arrangement reduces the need for a dedicated gateway in installations where compatible wireless infrastructure is already available. Wi-Fi is therefore attractive for individual appliances and small-scale installations requiring straightforward internet connectivity [2], [3].

The principal advantages of Wi-Fi include relatively high data capacity, broad ecosystem support, and direct integration with conventional network services. These characteristics are useful when smart plugs must transmit measurement data frequently or interact with other IP-based applications. However, Wi-Fi devices generally require more communication energy than low-power sensor-network technologies, and large numbers of connected devices can increase network-management demands. Network congestion, access-point coverage, and wireless interference should therefore be considered during deployment [4], [10].

Wi-Fi HaLow, based on IEEE 802.11ah, extends the Wi-Fi family toward lower-power and longer-range IoT applications. Its sub-gigahertz operation and mechanisms for supporting numerous stations make it relevant to distributed monitoring environments. Nevertheless, the availability of compatible hardware and infrastructure must be evaluated before selecting it for smart-plug products. The technology should be viewed as a specialized IoT-oriented Wi-Fi option rather than an automatic replacement for conventional Wi-Fi [10].

3.2. Bluetooth communication

Bluetooth provides short-range wireless connectivity and is particularly useful during smart-plug installation, commissioning, and local operation. A user can configure a compatible plug through a smartphone without initially connecting it to a conventional Wi-Fi network. Bluetooth low energy (BLE) is designed to reduce energy consumption in devices that exchange relatively small amounts of information. These characteristics make Bluetooth suitable for configuration, proximity-based interaction, and selected local-control functions [3], [11].

Bluetooth's main limitation for large smart-plug installations is its network coverage and device-management model. Conventional Bluetooth connections are generally more appropriate for nearby devices than for managing many distributed appliances across a building. BLE mesh extends communication through multiple participating nodes, but its design and operational characteristics differ from a simple point-to-point Bluetooth connection. Designers should therefore distinguish BLE, conventional Bluetooth, and Bluetooth mesh when evaluating smart-plug communication requirements [11], [12].

3.3. Zigbee communication

Zigbee is designed for low-power wireless networking and is commonly associated with sensor and automation applications. It operates over IEEE 802.15.4 physical and medium-access-control foundations and supports network arrangements such as star, tree, and mesh configurations. In a mesh network, selected devices can forward messages for other nodes, extending communication beyond the direct radio range of a central coordinator. This capability makes Zigbee attractive for installations containing multiple smart plugs and other automation devices [5], [13].

Zigbee can reduce dependence on individual Wi-Fi connections and support coordinated communication among numerous low-power devices. Its mesh structure can improve coverage when routing nodes are appropriately distributed throughout the installation. However, a Zigbee smart plug normally requires a compatible coordinator or gateway to communicate with IP-based management platforms. Compatibility between Zigbee profiles, device implementations, and gateway software must also be considered before deployment [5], [6].

3.4. Matter and interoperability

Matter emerged as an interoperability initiative intended to simplify communication among smart-home products from different manufacturers. Its first major specification release, Matter 1.0, appeared in 2022 and established an IP-based application-layer framework for supported smart-home devices. Matter is not a radio technology equivalent to Wi-Fi, Bluetooth, or Zigbee; instead, it provides common application-level behavior over supported network technologies, including Wi-Fi and Thread. BLE is also used in commissioning processes, while Thread provides low-power IPv6 mesh connectivity for suitable devices [6], [14].

For smart plugs, Matter's significance lies in reducing dependence on manufacturer-specific application ecosystems. A compatible plug can potentially be integrated into multiple supported control platforms, subject to certification, device capabilities, and ecosystem support. However, Matter does not automatically make every existing Wi-Fi or Zigbee plug interoperable, and legacy devices may require a compatible bridge or replacement. Its practical value therefore depends on implementation quality, certification, and the availability of compatible controllers and applications [6], [14].

4. COMPARISON OF WIRELESS TECHNOLOGIES

The wireless technologies discussed above differ in their communication range, topology, energy requirements, and integration methods. Table 1 summarizes their general characteristics and typical roles in smart-plug systems. These characteristics are indicative rather than fixed performance guarantees because actual results depend on radio hardware, antenna design, building materials, interference, and network configuration. The comparison is intended to guide technology selection rather than establish a universal ranking [3]-[6], [10], [13].

Table 1. Comparison of communication technologies for smart electrical plugs

Technology	Typical network structure	Main strengths	Main limitations	Potential smart-plug application
Wi-Fi	Infrastructure-based star	Direct IP and internet connectivity; relatively high data capacity	Higher power demand; dependence on access-point coverage	Remote control and monitoring through routers or cloud platforms
Bluetooth / BLE	Point-to-point or star; BLE mesh where supported	Convenient commissioning; low-power BLE operation	Shorter-range local connectivity; device-management constraints	Initial setup and local user interaction
Zigbee	Star, tree, or mesh	Low-power operation; multi-device networking	Requires compatible coordinator or gateway; profile compatibility	Coordinated control of multiple plugs
Matter over Wi-Fi	IP-based infrastructure network	Cross-platform application interoperability	Requires Matter-compatible products and controllers	Remote appliance control across supported ecosystems
Matter over Thread	IPv6 low-power mesh	IP-based interoperability and mesh connectivity	Requires Thread infrastructure, such as a border router	Distributed smart-plug and sensor networks

The comparison indicates that Wi-Fi is convenient when direct internet access is the primary requirement. Zigbee is more attractive when numerous low-power devices must communicate through a coordinated mesh network, while Bluetooth is useful for local setup and proximity-based interaction. Matter

adds a common application framework but does not eliminate the need to select an appropriate underlying network technology. Accordingly, the best architecture may combine several technologies rather than rely on a single wireless protocol [6], [10], [13], [14].

5. NETWORK CONNECTIVITY AND APPLICATION PROTOCOLS

Network connectivity determines how smart plugs exchange information with local controllers and remote services. A local network may provide device discovery, addressing, routing, and communication between the plug and a gateway. Internet connectivity extends these functions to remote applications and cloud platforms, enabling appliance operation from outside the local environment. The architecture must also account for situations in which internet connectivity is unavailable, because essential local switching functions should not necessarily depend on cloud access [6], [7].

Application-layer protocols provide the mechanisms for transmitting measurements and control instructions. MQTT uses a publish–subscribe model in which devices publish messages to topics and authorized clients subscribe to receive relevant information. CoAP provides a lightweight request–response approach intended for constrained devices and networks, whereas HTTP is widely supported by conventional web services. Studies comparing IoT messaging protocols show that their performance varies according to message size, transport mechanisms, security configuration, and network conditions [8], [9], [15].

A practical smart-plug platform may use different communication protocols at different layers. For example, a Zigbee plug can send its status to a gateway, which then forwards the information to a server using MQTT. A Wi-Fi plug may communicate directly with an IP-based service, while a Matter-compatible device may exchange standardized application data through a supported controller. Such arrangements allow heterogeneous devices to participate in a common monitoring and control environment [6], [8], [16].

6. REMOTE APPLIANCE OPERATION AND CONTROL RELIABILITY

Remote appliance operation is one of the most visible functions of smart plugs. A user command may originate from a mobile application, pass through a local controller or cloud platform, and reach the plug through its wireless network. The plug then changes its switching state and returns a status message to confirm the result. Reliable operation therefore requires both command delivery and feedback from the controlled device [2], [7].

Cloud-based control offers convenient access from geographically distant locations, but it introduces dependencies on internet connectivity, server availability, and account authentication. Local control can reduce these dependencies and may provide faster responses within a building. Hybrid architectures combine local automation with remote access, allowing selected functions to remain available when the internet connection is interrupted. The use of gateways and edge processing can further improve local responsiveness and reduce unnecessary cloud communication [6], [7], [17].

Remote switching must also be designed with electrical safety and operational constraints in mind. A communication system should distinguish between a command being transmitted, a command being received, and the actual electrical state of the output. Authentication, access permissions, encrypted communication, and event logging are necessary to reduce unauthorized operation. Smart plugs should not be treated as substitutes for certified circuit protection or safety interlocks, particularly when controlling high-power or safety-critical appliances [16], [18].

7. SECURITY, INTEROPERABILITY, AND IMPLEMENTATION CHALLENGES

Cybersecurity is a major concern because connected plugs provide a network-accessible path to electrical appliances. Weak passwords, insecure firmware, poor authentication, and unencrypted communication may expose devices to unauthorized control. A compromised plug could be switched unexpectedly or used as an entry point into a wider local network. Security therefore needs to be considered throughout device commissioning, communication, software updates, and operational management [16], [18].

Interoperability remains challenging because wireless connectivity alone does not guarantee that different products can exchange meaningful commands. Devices may use different data models, discovery mechanisms, application protocols, and vendor-specific services. Gateways can translate between technologies, but they also introduce additional configuration and maintenance requirements. Matter addresses part of this challenge by defining a common application framework for supported devices, although compatibility still depends on product implementation and certification [6], [14].

Reliability should be evaluated under realistic operating conditions rather than inferred solely from nominal protocol specifications. Building materials, radio interference, network congestion, device density,

and gateway placement can affect communication quality. Remote-control systems should include command acknowledgement, device-state feedback, timeout handling, and safe recovery behavior after network interruptions. These measures are particularly important when smart plugs are deployed in large buildings or used to control appliances whose operation must remain predictable [4], [7], [16].

8. RESEARCH GAPS AND FUTURE DIRECTIONS

Further research is needed to evaluate smart-plug communication technologies under comparable experimental conditions. Studies should measure end-to-end command latency, packet delivery reliability, reconnection time, network scalability, and energy consumption using consistent test environments. Such evaluations should include Wi-Fi, BLE, Zigbee, and Matter-compatible implementations rather than relying only on theoretical protocol comparisons. The resulting evidence would help manufacturers and system integrators select architectures according to measurable operational requirements [4], [10], [13].

Another research direction concerns unified management across heterogeneous communication networks. Future smart-plug platforms could combine local control, cloud access, standardized device models, and secure gateway functions in a modular architecture. Matter may support interoperability among compatible products, while MQTT, CoAP, or other application protocols can connect devices to broader IoT management services where appropriate. Research should also examine long-term software maintenance, backward compatibility, privacy, and resilience against communication failures [6], [8], [14].

9. CONCLUSION

Communication architecture is a central determinant of smart electrical plug functionality, influencing connectivity, remote operation, interoperability, and system reliability. Wi-Fi provides convenient direct IP connectivity, Bluetooth supports local interaction and commissioning, and Zigbee enables low-power mesh networking for multiple devices. Matter, introduced in 2022, adds an application-layer interoperability framework over supported IP-based connectivity technologies. These technologies serve different purposes and should be selected according to installation scale, network conditions, energy requirements, and desired control functions.

Reliable smart-plug deployment requires more than choosing a wireless protocol. It also requires appropriate gateways, application messaging, secure authentication, command acknowledgement, device-state feedback, and local fallback behavior. Hybrid architectures can combine the strengths of different technologies while reducing dependence on a single communication path. Future developments should prioritize experimentally validated interoperability, cybersecurity, and reliable remote appliance operation to support scalable smart-plug applications.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[2] E. Ferro and F. Potortì, "Bluetooth and Wi-Fi wireless protocols: a survey and a comparison," *IEEE Wireless Communications*, vol. 12, no. 1, pp. 12–26, Feb. 2005, doi: 10.1109/MWC.2005.1404569.

[3] C. Gomez and J. Paradells, "Wireless home automation networks: a survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92–101, Jun. 2010, doi: 10.1109/MCOM.2010.5473869.

[4] A. Seferagić, J. Famaey, E. De Poorter, and J. Hoebeke, "Survey on wireless technology trade-offs for the industrial internet of things," *Sensors*, vol. 20, no. 2, p. 488, Jan. 2020, doi: 10.3390/s20020488.

[5] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, May 2007, doi: 10.1016/j.comcom.2006.12.020.

[6] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, "An overview of IoT architectures, technologies, and existing open-source projects," *Internet of Things*, vol. 20, p. 100626, Nov. 2022, doi: 10.1016/j.iot.2022.100626.

[7] A. O. Bang, U. P. Rao, A. Visconti, A. Brighente, and M. Conti, "An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions," *Computers and Security*, vol. 123, p. 102914, Dec. 2022, doi: 10.1016/j.cose.2022.102914.

[8] B. Mishra and A. Kertesz, "The use of MQTT in M2M and IoT systems: a survey," *IEEE Access*, vol. 8, pp. 201071–201086, 2020, doi: 10.1109/ACCESS.2020.3035849.

[9] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for internet of things," *Digital Communications and Networks*, vol. 8, no. 6, pp. 1094–1104, Dec. 2022, doi: 10.1016/j.dcan.2022.03.013.

[10] L. Tian, S. Santi, A. Seferagić, J. Lan, and J. Famaey, "Wi-Fi HaLow for the internet of things: an up-to-date survey on IEEE 802.11ah research," *Journal of Network and Computer Applications*, vol. 182, p. 103036, May 2021, doi: 10.1016/j.jnca.2021.103036.

[11] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, no. 9, pp. 11734–11753, Aug. 2012, doi: 10.3390/s120911734.
[12] A. Seferagic, I. Moerman, E. De Poorter, and J. Hoebeke, "Evaluating the Suitability of IEEE 802.11ah for Low-Latency Time-Critical Control Loops," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7839–7848, Oct. 2019, doi: 10.1109/JIOT.2019.2916579.
[13] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards dbl," *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, May 2007, doi: 10.1016/j.comcom.2006.12.020.
[14] J. S. Lee, Y. W. Su, and C. C. Shen, "A comparative study of wireless protocols: bluetooth, uwb, zigbee, and wi-fi," in *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*, IEEE, 2007, pp. 46–51. doi: 10.1109/IECON.2007.4460126.
[15] D. Thangavel, X. Ma, A. Valera, H. X. Tan, and C. K. Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," in *2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing (ISSNIP)*, IEEE, Apr. 2014, pp. 1–6. doi: 10.1109/ISSNIP.2014.6827678.
[16] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, Jan. 2017, doi: 10.1016/j.jclepro.2016.10.006.
[17] V. Seoane, C. Garcia-Rubio, F. Almenares, and C. Campo, "Performance evaluation of CoAP and MQTT with security support for IoT environments," *Computer Networks*, vol. 197, p. 108338, Oct. 2021, doi: 10.1016/j.comnet.2021.108338.
[18] Z. Laaroussi and O. Novo, "A performance analysis of the security communication in CoAP and MQTT," in *2021 IEEE 18th Annual consumer communications & networking conference (CCNC)*, IEEE, Jan. 2021, pp. 1–6. doi: 10.1109/CCNC49032.2021.9369565.