Micro-Grid Communication Protocols and Standards

Subjects: Engineering, Electrical & Electronic

Contributor: Eyuel Debebe Ayele, Javier Ferreira Gonzalez, Wouter B. Teeuw

A microgrid is a comprehensive system that includes energy storage, different energy sources, and loads within a certain boundary. It functions seamlessly, whether it is linked to, or works independently from, the main electrical grid, ensuring a consistent power supply. Microgrids consist of distributed energy resources (DER) and loads, which may be located in one place or spread throughout an electrical distribution network.

Keywords: microgrid ; energy storage ; energy

1. Introduction

Figure 1 illustrates the typical configuration of a microgrid, showcasing its fundamental elements and linkages to large-scale generation, transmission, and distribution networks.

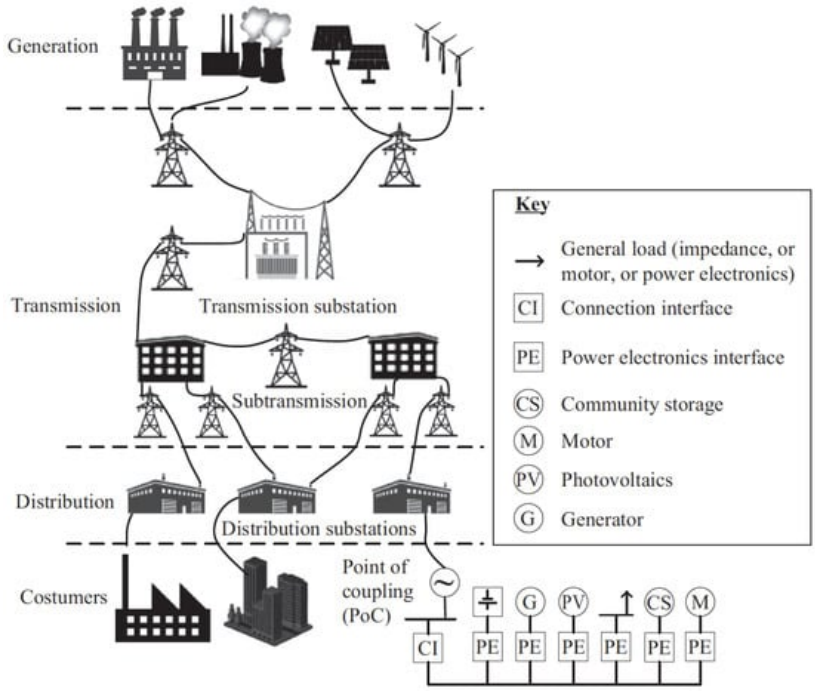

Figure 1. Schematic of a microgrid connected to a distribution network [1].

Microgrids must be able to adjust to different operational contexts, such as being connected to the main power grid, operating autonomously or transitioning between these two states. Multiple microgrids can be integrated into the main power grid, with each acting as a key component of the distribution communication network [1][2]. In island mode, a microgrid works independently, providing electricity only to its internal power requirements. The microgrid's management system interacts with market signals and optimizes features such as peak shaving and frequency regulation. The control system must effectively manage the allocation and utilization of resources, including power production and storage, load management, and ensuring self-sufficient operation [3][4][5].

The illustration in **Figure 1** displays a typical microgrid configuration, which includes energy storage, renewable sources such as wind and solar, a microturbine, and various electrical needs. Renewable distributed energy resources (DERs), such as wind and solar power, offer considerable advantages by replacing fossil fuel energy and reducing pollutants. These systems strive to reduce energy losses across transmission, storage, and secondary electrical networks [1][2]. An automated controller is essential for the efficient operation of the intelligent microgrid, as it guarantees the maintenance of optimal frequency and voltage levels. During island mode, the system's control and management must effectively synchronize its components. The influence of communication technologies in microgrids is contingent on the arrangement

of the network and the particular components involved. Uninterrupted and reliable data transmission is essential for the purpose of real-time monitoring [6][7].

The hierarchical structure of microgrid communication architectures typically consists of three tiers (**Figure 2**) [2][8]. At the top is a central controller that oversees multiple microgrids and the wider smart grid (SG). Energy storage systems (ES) are included to balance loads and enable a smooth transition to islanded operation. Power electronics converters are included to provide improved control and rapid response, allowing for the regulation of varying power consumption by non-essential loads. A local controller (LC) is responsible for managing the state variables of a microgrid, such as phase currents and voltages at the point of common coupling (PCC) [8]. In fact, multiple microgrids can be connected to a single PCC, allowing energy transfer to and from the primary electrical network.

The bottom layer of the microgrid design comprises measuring equipment such as PLCs and safety switches, which regularly track the data flow. The intermediate layer comprises gateway control devices, such as IEDs, whose functions are accountable for immediate processing of information and provisional data retention. The uppermost tier comprises an in-the-cloud platform specifically designed for long-term data storage and performing comprehensive quantitative operations [9][10]. **Figure 2** illustrates the variations in computational energy and connectivity demands across each of the three tiers. This requires the implementation of distinct communication methods for every tier. Specifically, the first two layers use both distributed and centralized versions of the home area network (HAN) [8][11] and the local area network (LAN) [11]. The higher levels, in contrast, utilize the neighborhood area network (NAN) [12] and the wide area network (WAN) [12].

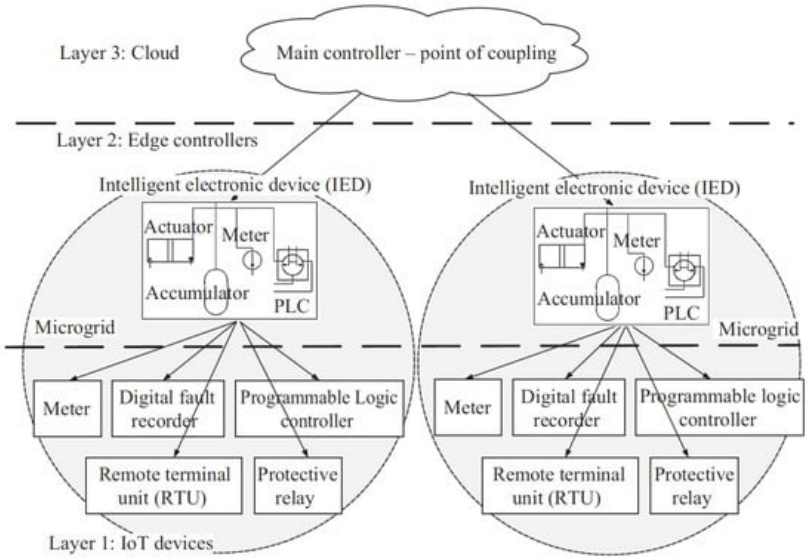

Figure 2. Tri-level communication structure used in microgrid systems [8][11].

Microgrids are a significant development in the distribution of energy. They are defined by their incorporation of energy storage, various energy sources, and loads within specific bounds. Whether operating independently or in tandem with the primary electrical grid, these systems guarantee a reliable power source and demonstrate durability in diverse operational situations [13][14][15]. Nevertheless, despite their increasing ubiquity, there are still significant deficiencies in comprehending and executing efficient cybersecurity measures in these systems, namely in the domain of control communication protocols and standards.

2. Cybersecure Communication in Microgrid

2.1. Cybersecurity Overview

The IEC 62351 standard [16] lays out the security framework for managing grid systems and sharing information about them. **Figure 3** shows an overview of this framework. It demonstrates the link between different cyber security risks and the security requirements necessary to reduce them. These risks are divided into four categories: unauthorized access to data (confidentiality), unauthorized alteration or theft of data (integrity), and non-repudiation, which guarantees responsibility and denies false assertions of action or inaction [16]. Additionally, specific types of attacks, such as listening and service spoofing, are linked to the breaches they can cause in the security requirements, emphasizing the importance of a comprehensive and layered approach to cybersecurity in energy management systems.

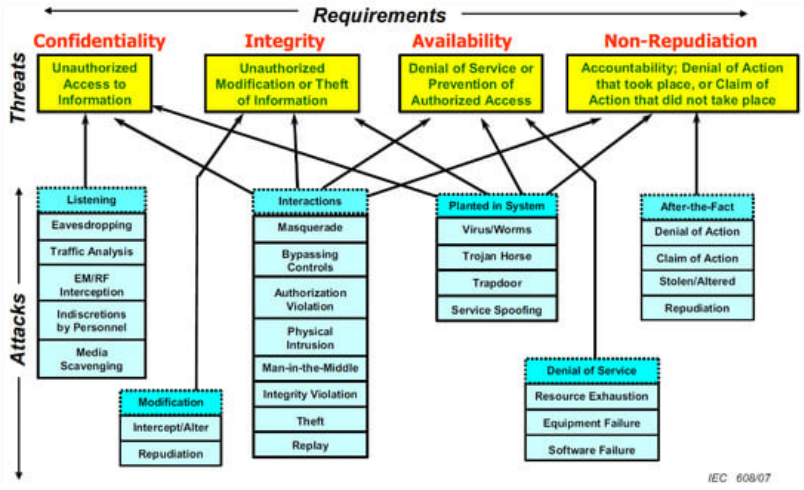

Figure 3. Overview of microgrid security [16].

The architecture shown in **Figure 3** illustrates the security requirements, hazards, and attacks in a microgrid system [16]. The security requirements are categorized into four primary domains: confidentiality, integrity, availability, and non-repudiation. Each criterion is complemented with a roster of specific hazards. An example of a situation where the principle of 'confidentiality' might be violated is via 'unauthorized access to information', which can be achieved using techniques like eavesdropping and interception. Instances of 'unauthorized modification or theft of information', such as masquerade and repudiation, weaken the idea of 'integrity'. 'Availability' refers to the obstruction of allowed access or denial of service, which includes actions like service spoofing and resource depletion [16]. Finally, 'non-repudiation' ensures 'accountability and denial of action' to prevent denial of service attacks and disprove allegations of actions not carried out, as well as mitigate hazards such as repudiation and retrospective denial. Comprehending this comprehensive picture is crucial for developing robust security measures to defend microgrid systems from various cyber threats, ensuring a reliable and secure energy distribution network [16].

2.2. Centralized vs. Distributed Microgrid Communication Networks

A microgrid's communication network may have either a centralized or a hierarchical structure, as illustrated in **Figure 4**. These electrical systems are flexible and resilient, and may be used either in conjunction with the primary power network or autonomously. They can range from small residential setups to larger groups of residences. Centralized and distributed approaches are often employed for network topology in microgrid management. All data in the microgrid network are managed by a centralized system, known as an energy management system. If there is a single issue in this system, it can have a major impact on the entire network. In a distributed system, each microgrid works independently, thus increasing its ability to withstand disruptions and ensuring consistent performance [17].

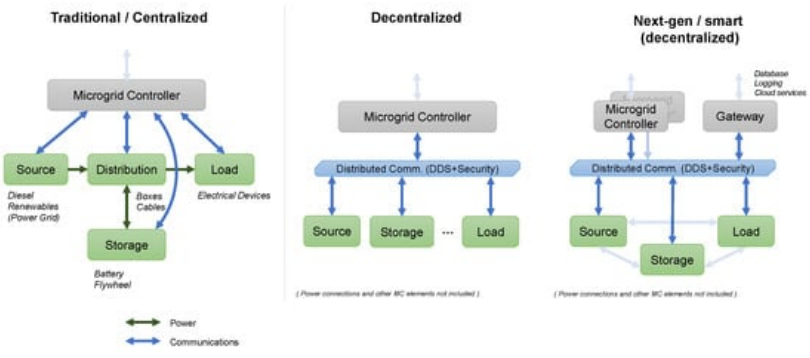

Figure 4. Network topology of microgrid data communication infrastructure.

A centralized microgrid system utilizes a single controller to simplify and consolidate activities, thus decreasing operational conflicts and scheduling issues. On the other hand, decentralized systems allow for the autonomous functioning of multiple devices, leading to a considerable rise in redundancy rates. Microgrids employ a mix of wired and wireless connectivity methods. It is essential to precisely monitor and regulate parameters such as current, voltage, and power at each individual unit through suitable communication lines. This ensures the consolidation of authority and efficient supervision of microgrid components [18]. Effective communication is essential for effectively managing variations in power production and demand, as well as tackling critical distribution operating challenges such as voltage regulation and power flow control. For instance, solar photovoltaic farms may experience sudden changes in power generation due to shifting

cloud cover, while wind farms may experience unexpected power loss. This infrastructure guarantees uninterrupted connection and the smooth exchange of information between all units. In a microgrid, a central controller makes it possible for devices in the central control topology (shown in **Figure 4**) to talk to each other at the same time. Regional central controllers collect information from multiple nodes and relay data towards the central controller. The process of choosing the communication technology or network architecture in a microgrid does not follow a predetermined methodology [19]. The secure and stable operation of the microgrid is heavily dependent on the use of effective communication technologies.

2.3. Cybersecurity Challenges in Microgrid Systems

Efficient microgrids, which combine physical and cyber systems, require dependable and efficient monitoring and administration. However, the integration of these components can create weaknesses in the system, necessitating a particular focus on these issues to ensure a successful deployment and operation of the microgrid. Smart microgrids are composed of complex arrangements, including distributed sensors, actuators, controllers, and power components, all of which require precise and prompt communication coordination. Smart microgrids must address challenges such as ensuring reliable connectivity, enhancing data security, and effectively managing large-scale data processing.

Microgrids are exposed to a variety of attacks, including cyber-attacks that target communication networks, data storage, and software, as well as physical sabotage that can affect equipment, infrastructure, and personnel. Cybersecurity threats can also compromise the privacy, reliability, and accessibility of both IT and industrial automation systems. Fortunately, advances in network security have improved the security and operational efficiency of communication protocols in smart microgrid systems. This has enabled faster and more precise device interactions, as well as improved malfunction monitoring and troubleshooting.

Secure connection solutions are developed to meet certain requirements and objectives in smart microgrids. These microgrids usually have a three-tier structure, with an energy management system at the highest level, local controllers in the middle, and IoT devices such as smart meters at the lowest level. Each tier has its own computational and latency needs, which are addressed by various network nodes and standards.

2.4. Microgrid Network Topology Types

Microgrid systems use HANs, NANs, IANs, and BANs. Intelligent meters, generators, energy, and residential automation equipment constitute HANs. The more comprehensive IANs and BANs have extra automation instruments and sensors for development and commercial EMS and SCADA platforms. Several microgrid connectivity techniques differ in terms of service reach and transmission bandwidth, as seen in **Figure 5** [20]. Deployment is possible, since these types of networks require minimal data transfer rates, energy usage, adaptability, and connectivity reliability. The quantity and kind of users might separate microgrids into customer-facing area networks, NANs, or FANs [20].

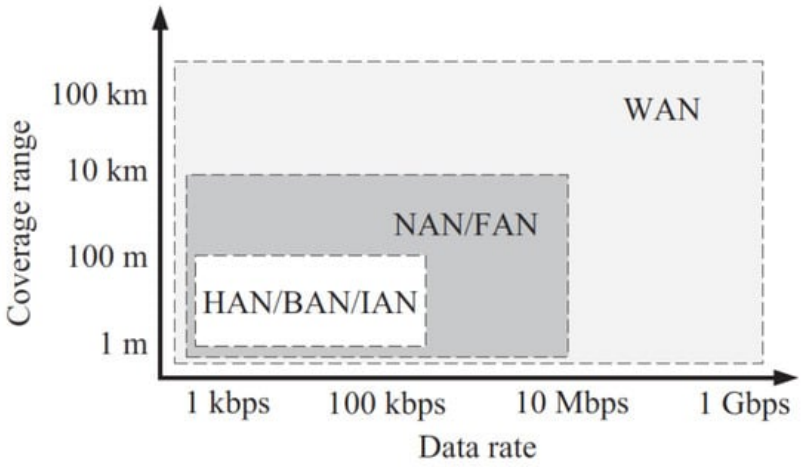

Figure 5. Subnet networks [20].

Table 1 presents a comprehensive overview of the communication technologies used in microgrid systems, along with their respective standards and applications.

Table 1. Compilation of communication modalities in microgrid systems.

Modality of Communication	Standards	Applications
Narrowband PLC [20]	IEEE P1901.2 [21], G3-PLC [22]	HAN/NAN/WAN
Wideband PLC [23]	IEEE 1901 [24], Home Plug 1.0 [25][26]	HAN/BAN/NAN
DSL [27]	ADSL [28]	NAN/FAN
VDSL [28]	VDSL [28]	NAN-FAN
HDSL [29]	HDSL [29]	NAN/FAN
Ethernet [30]	IEC 61850 [31]	HAN/BAN/NAN, SAS [32]
Optical fiber [33]	PON [33], SONET/SDH [33]	WAN
WLAN [34]	IEEE802.11 [34]	Local Networks [35]
WPAN [36]	IEEE 802.15 [36]	Bluetooth, ZigBee [37], Home Networks
Cellular [38]	Generations 2 to 5 [38]	V2G, WAN/LTE-A [39]

The illustration in **Figure 6** displays a two-level hierarchical system, referred to as a BAN, which is composed of a backbone and a control level with sensors, actuators, and controllers [20]. Internet connectivity is essential for BAN connectivity, allowing the sensors to collect data from the field at lower connection speeds. Interconnection devices (ICDs) enable the sensors to communicate with management devices at gigahertz speeds. The top tier of the BAN is made up of intelligent devices that monitor, log, document, query, and store process data values. A human–machine computing system located on the upper level produces charts and analytics reports for the management and customization of system assets. It has a user interface that can obtain data from the network and the environment. Additionally, operators can use the human–machine interface to query field equipment. Due to their location inside buildings, BANs use a low-power battery system that has little financial and environmental impact. Furthermore, BANs can communicate through ZigBee and Ethernet.

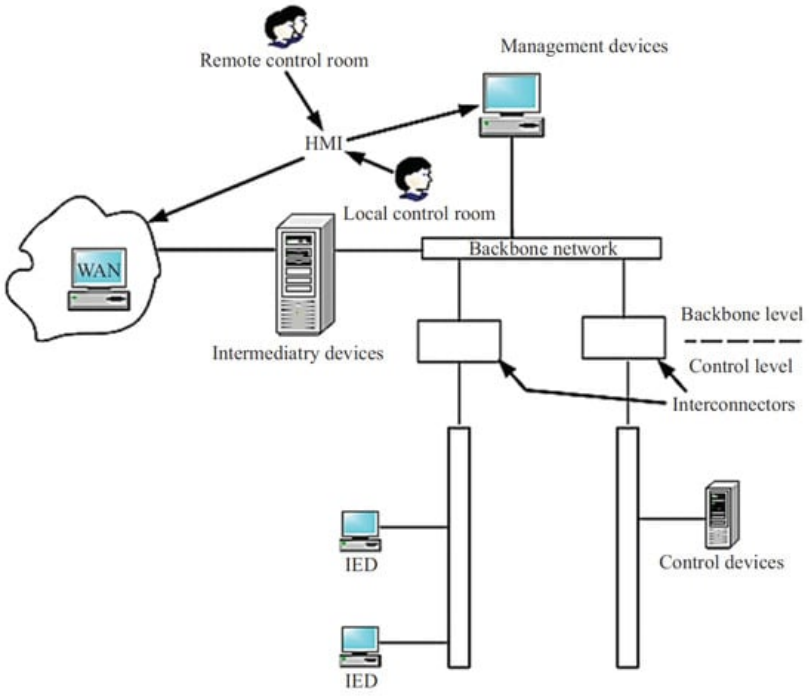

Figure 6. BAN network architecture [20].

Near area networks (NANs) enable devices to communicate with each other more quickly due to their close proximity, allowing for faster data transmission rates of 10–100 Mbps within a 10 km radius. NANs are used at the distribution level in smart microgrids [20], and can be connected to devices via wired or wireless methods. They are also used by distribution network data collectors to communicate with intelligent meters. Better than hotspots, NANs allow for devices over a broader area.

Figure 7 illustrates a FAN architecture that enables a connection between a single endpoint and several points within a decentralized control system. This architectural style is gaining popularity at an escalating rate. The system relies on the NAN and HAN network designs. The FAN technology offers a wide range of uses, including energy production, intelligent

metering, the administration of assets, or troubleshooting. As stated in reference [40], FAN is an economical solution that offers a superior degree of access to information and quality of service (QoS). Wide area networks (WANs) are telecommunications networks that cover a large geographic area. These networks provide more efficient control, protection, and monitoring over a larger area and are typically established using leased telecommunication lines. The communication speeds of WANs range from 1 Mbp to 1 Gbp [41]. WANs are the core layer of a communication system, connecting to all network nodes, including FANs and NANs, and typically have a 100 km radius. Wide area networks (WANs) can provide a reliable communication system by connecting multiple local area networks (LANs) with gateways at the end of the leased line. Two types of switching are employed in wide area networks (WANs): circuit switching and packet switching. Circuit switching creates a dedicated connection between two nodes, allowing for point-to-point communication until the call is terminated. Packet switching, on the other hand, sends data packets to each node and allows IEDs to receive them; however, this approach is more prone to errors, losses, and delays. Voice transmission is the primary application for circuit switching, while packet switching is used in networks.

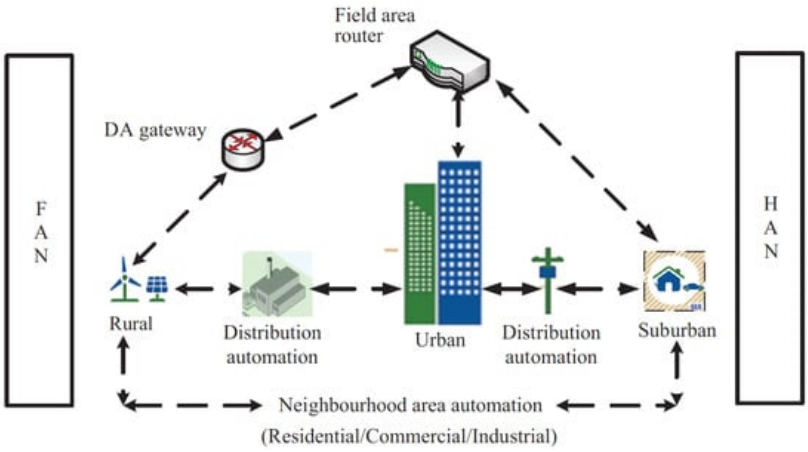

Figure 7. FAN network architecture [40].

2.5. Communication Infrastructures

The microgrid communication network can be either wired or wireless, depending on the device capabilities, the geographical region, and the available funds. Wired communication is the most straightforward option and can be achieved through power lines, twisted pair cables, and optical fibers. RF or cellular networks enable more complex wireless communication. Power line communication (PLC) technology uses power lines as signal carriers [20]. It was created in the early 1900s as a low-data-rate remote power network component control service. Since then, numerous frequency ranges and signal modulation methods have been used to reach data speeds from a few bits per second to 200 Mbps with a broad frequency range (3–20 MHz). PLC technology is susceptible to electromagnetic noise from electrical motors, radio signal interference, and power supply since power lines are not twisted and protected. Open circuits on the power line with switches and insulators can also cause disruptions of the connection. Physical grid architecture, impedance variations, and the reflection of the terminal point wave can weaken and distort signals, preventing transmission [20].

Twisted-pair wires made of copper have been widely employed in communication, from local area networks to telephone lines [33]. This cable transmits and receives electrical signals using one or multiple pairs of wires with plastic insulation. One of the wires is used to send the signal, while the other serves as a ground reference. Depending on the type of protection, twisted-pair communication cables can be unshielded, shielded, foiled, FTP, or S-FTP. The shield is composed of metal foil and braided mesh, which covers all conductor pairs or sets. This EMI shield helps to prevent noise and crosstalk from entering the communication channel. Despite its limited range and 1.54 MHz channel capacity, the twisted-pair cable is still an economical communication method.

In the 1960s, optical fiber replaced copper-wired connections in communication networks [33]. Common components of these systems include PON, WDM, SONET, and SDH, as noted in [33]. Fiber optic cables provide high data transfer rates (5, 10, 20, or 40 Gbps), immunity to RF and EMI, and the capacity to transmit data over long distances with fewer repeaters (100–1000 km) for electrical system automation. Optical fiber technology is beneficial for connecting electrical substation SG applications and communication networks. Despite its high installation cost, the technology's high bandwidth capacity allows many users to share one communication channel as a backbone, making it more attractive. This makes optical fiber communication dependable and rapid [33].

Wireless communication technologies provide several benefits for microgrid operations in high-density areas by eliminating the need for intricate wiring infrastructure. Wireless solutions simplify operational management, allow greater flexibility in system design, and facilitate installation. A range of wireless standards that are appropriate for microgrid applications are listed in **Table 1**. These include IEEE 802.11 [34] for WLAN, which offers Wi-Fi connectivity for local area networks; IEEE 802.15 [36] for WPAN, which facilitates device-to-device communication via Bluetooth and ZigBee protocols [35]; and IEEE 802.16 [37] for WiMAX, which enables wide area coverage. Microgrids can benefit from cellular technologies that offer a wide range of reliable connectivity, ranging from 2G to 4G standards. However, each technology has its own difficulties, such as radio frequency interference, the need for a direct line of sight, environmental obstructions, and susceptibility to weather conditions. These elements must be taken into consideration when constructing and executing a dependable and effective wireless communication system for microgrid settings.

References

1. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. IEEE Commun. Surv. Tutor. 2011, 14, 944–980.
2. Lasseter, R.H.; Paigi, P. Microgrid: A conceptual solution. In Proceedings of the 2004 IEEE 35th Annual Power Electronics Specialists Conference (IEEE Cat. No. 04CH37551), Aachen, Germany, 20–25 June 2004; IEEE: Piscataway, NJ, USA, 2004; Volume 6, pp. 4285–4290.
3. Hu, S.; Yuan, P.; Yue, D.; Dou, C.; Cheng, Z.; Zhang, Y. Attack-resilient event-triggered controller design of DC microgrids under DoS attacks. IEEE Trans. Circuits Syst. Regul. Pap. 2020, 67, 699–710.
4. Jamil, N.; Qassim, Q.; Bohani, F.; Mansor, M.; Ramachandaramurthy, V. Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. Appl. Sci. 2021, 11, 9812.
5. Ghiasi, M.; Dehghani, M.; Niknam, T.; Kavousi-Fard, A.; Siano, P.; Alhelou, H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. IEEE Access 2021, 9, 29429–29440.
6. Nejabatkhah, F.; Li, Y.; Liang, H.; Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. Energies 2021, 14, 27.
7. Colak, M.; Irmak, E. A State-of-the-Art Review on Electric Power Systems and Digital Transformation. Electr. Power Components Syst. 2023, 51, 1089–1112.
8. Lopes, J.A.P.; Moreira, C.L.; Madureira, A.G. Defining control strategies for MicroGrids islanded operation. IEEE Trans. Power Syst. 2006, 21, 916–924.
9. Umar, A.; Kumar, D.; Ghose, T. Peer-to-Peer Energy Trading in a Self-Sustained Microgrid System Using Blockchain Technology. In Proceedings of the 2022 IEEE International Conference on Innovative Business Technologies (ICIBT), Ranchi, India, 6–8 May 2022.
10. Hossain-McKenzie, S.; Reno, M.J.; Bent, R.; Chavez, A.R. Cybersecurity of Networked Microgrids: Challenges Potential Solutions and Future Directions; Technical Report; Sandia National Lab. (SNL-NM): Albuquerque, NM, USA, 2020.
11. Jolfaei, A.; Kant, K. Data Security in Multiparty Edge Computing Environments; Technical report; Temple University: Philadelphia, PA, USA, 2019.
12. Huq, M.Z.; Islam, S. Home area network technology assessment for demand response in smart grid environment. In Proceedings of the 2010 20th Australasian Universities Power Engineering Conference, Christchurch, New Zealand, 5–8 December 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–6.
13. Birleanu, F.G.; Bizon, N. Control and protection of the smart microgrids using Internet of Things: Technologies, architecture and applications. In Microgrid Architectures, Control and Protection Methods; Springer: Cham, Switzerland, 2020; pp. 749–770.
14. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and research trends in microgrids cybersecurity. Appl. Sci. 2021, 11, 7363.
15. Bahsi, H.; Ochieng'Dola, H.; Khalil, S.M.; Korõtko, T. A Cyber Attack Taxonomy for Microgrid Systems. In Proceedings of the 2022 17th Annual System of Systems Engineering Conference (SOSE), Rochester, NY, USA, 7–11 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 324–331.
16. IEC 62351; Power Systems Management and Associated Information Exchange—Data and Communications Security. International Electrotechnical Commission: London, UK, 2023. Available online: https://webstore.iec.ch/publication/65511 (accessed on 16 November 2023).

17. Crow, B.P.; Widjaja, I.; Kim, J.G.; Sakai, P.T. IEEE 802.11 Wireless Local Area Networks. IEEE Commun. Mag. 1997, 35, 116–126.
18. Jolfaei, A.; Kant, K. A lightweight integrity protection scheme for low latency smart grid applications. Comput. Secur. 2019, 86, 471–483.
19. Eissa, M.; Masoud, M.E.; Elanwar, M.M.M. A novel back up wide area protection technique for power transmission grids using phasor measurement unit. IEEE Trans. Power Deliv. 2009, 25, 270–278.
20. Shukla, S.; Deng, Y.; Shukla, S.; Mili, L. Construction of a microgrid communication network. In Proceedings of the ISGT 2014, Washington, DC, USA, 19–22 February 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–5.
21. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. IEEE Trans. Ind. Inform. 2011, 7, 529–539.
22. Razazian, K.; Umari, M.; Kamalizad, A.; Loginov, V.; Navid, M. G3-PLC specification for powerline communication: Overview, system simulation and field trial results. In Proceedings of the ISPLC2010, Rio de Janeiro, Brazil, 28–31 March 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 313–318.
23. Jianming, L.; Bingzhen, Z.; Liang, G.; Zhou, Y.; Yirong, W. Communication performance of broadband PLC technologies for smart grid. In Proceedings of the 2011 IEEE International Symposium on Power Line Communications and Its Applications, Udine, Italy, 3–6 April 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 491–496.
24. Goldfisher, S.; Tanabe, S. IEEE 1901 access system: An overview of its uniqueness and motivation. IEEE Commun. Mag. 2010, 48, 150–157.
25. Chung, M.Y.; Jung, M.H.; Lee, T.J.; Lee, Y. Performance analysis of HomePlug 1.0 MAC with CSMA/CA. IEEE J. Sel. Areas Commun. 2006, 24, 1411–1420.
26. Mohassel, R.R.; Fung, A.S.; Mohammadi, F.; Raahemifar, K. A survey on advanced metering infrastructure and its application in smart grids. In Proceedings of the 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), Toronto, ON, Canada, 4–7 May 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–8.
27. Cendrillon, R.; Yu, W.; Moonen, M.; Verlinden, J.; Bostoen, T. Optimal multiuser spectrum balancing for digital subscriber lines. IEEE Trans. Commun. 2006, 54, 922–933.
28. Ginis, G.; Cioffi, J.M. Vectored transmission for digital subscriber line systems. IEEE J. Sel. Areas Commun. 2002, 20, 1085–1104.
29. Ahamed, S.V.; Gruber, P.L.; Werner, J.J. Digital subscriber line(HDSL and ADSL) capacity of the outside loop plant. IEEE J. Sel. Areas Commun. 1995, 13, 1540–1549.
30. Christensen, K.; Reviriego, P.; Nordman, B.; Bennett, M.; Mostowfi, M.; Maestro, J.A. IEEE 802.3 az: The road to energy efficient ethernet. IEEE Commun. Mag. 2010, 48, 50–56.
31. Brunner, C. IEC 61850 for power system communication. In Proceedings of the 2008 IEEE/PES Transmission and Distribution Conference and Exposition, Chicago, IL, USA, 21–24 April 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 1–6.
32. Ko, M.A. Layering Serial Attached Small Computer System Interface (SAS) over Ethernet. U.S. Patent 8,140,696, 20 March 2012.
33. Stalley, K.D.; Clarke, D.E.; Rosher, P.A. Optical Fibre Communications System. U.S. Patent 5,479,286, 9 February 1995.
34. Jiang, D.; Delgrossi, L. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In Proceedings of the VTC Spring 2008-IEEE Vehicular Technology Conference, Singapore, 11–14 May 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 2036–2040.
35. Guille, C.; Gross, G. A conceptual framework for the vehicle-to-grid (V2G) implementation. Energy Policy 2009, 37, 4379–4390.
36. Rajagopal, S.; Roberts, R.D.; Lim, S.K. IEEE 802.15. 7 visible light communication: Modulation schemes and dimming support. IEEE Commun. Mag. 2012, 50, 72–82.
37. Lee, J.S.; Su, Y.W.; Shen, C.C. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In Proceedings of the IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society, Taipei, Taiwan, 5–8 November 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 46–51.
38. Mishra, A.R. Fundamentals of Cellular Network Planning and Optimisation: 2G/2.5 G/3G… Evolution to 4G; John Wiley & Sons: Hoboken, NJ, USA, 2004.
39. Ghosh, A.; Ratasuk, R.; Mondal, B.; Mangalvedhe, N.; Thomas, T. LTE-advanced: Next-generation wireless broadband technology. IEEE Wirel. Commun. 2010, 17, 10–22.

40. Xiao, X.; Ni, L.M. Internet QoS: A big picture. IEEE Netw. 1999, 13, 8–18.
41. Sundar, R.; Aravamudan, M.; Naqvi, S.A.; Iyer, P.R.; Vishwanathan, K.K.; Pai, G.U. Method, System, and Apparatus for a Mobile Station to Sense and Select a Wireless Local Area Network (WLAN) or a Wide Area Mobile Wireless Network (WWAN). U.S. Patent 7,200,112, 3 April 2007.

Retrieved from https://encyclopedia.pub/entry/history/show/126893