# Data Transmission Technologies and Networks: A Review

**Freddy Patricio Ajila Zaquinaula [a*]& Rolando Marcel Torres Castillo[a]**
[a]Escuela Superior Politécnica de Chimborazo, Sede Orellana, El Coca, 220001, Ecuador

**Abstract:**
Data transmission is the process of transmitting digital information from one device to another over a network. With the increasing demand for high-speed data transmission and the proliferation of connected devices, the development of advanced data transmission technologies and networks has become crucial. This paper reviews the most commonly used data transmission technologies and networks, including wired and wireless technologies, and highlights their advantages and limitations.
**Keywords:** ICTs; wireless networks; wired networks; data transmission; 5G networks
**DOI:** 10.24297/j.cims.2023.17

## 1. Introduction

Wireless communication has seen remarkable growth in recent years. There are several technologies that exemplify this trend, most notably cellular telephony, which has made significant advances since its formal emergence in 1972 and now has more than 1.5 billion phones in operation worldwide [1–3]. Another clear example is the wireless sensors that are now used in various applications such as fire detection, earthquake, smoke and others, forming communication networks to report such events.

Data transmission technologies and networks are the backbones of modern communication systems. They are responsible for the transfer of data between different devices and networks, enabling the seamless exchange of information [4,5]. The rapid growth of the Internet and the proliferation of mobile devices have led to an increased demand for faster and more efficient data transmission technologies and networks. In this paper, we review various data transmission technologies and networks, including wired and wireless technologies, as well as the latest developments in these areas. Another area where wireless communication is frequently used is in local area networks and its growth is extensive given its flexibility of use and the ease and speed with which a network can be implemented with this technology. (In 1996 the IEEE approved a standard for this type of network called 802.11b or Wi-Fi) [6–9].

These technologies and networks can be used to transmit data for various applications such as internet access, video streaming, online gaming, and more. The choice of technology and network will depend on the specific needs of the application and the environment in which it will be used.

Data transmission technologies and networks refer to the methods and systems used to transmit and receive digital data over a communication channel. Some examples include (see Table 1):

**Table 1. Some examples of data transmission technologies.**

| Forms of data transmission | |
|---|---|
| Ethernet | a wired technology that uses physical cables to transmit data between devices |
| Wi-Fi | a wireless technology that uses radio waves to transmit data between devices |
| Cellular networks | networks that use radio waves to transmit data between mobile devices and the internet. |
| Satellite | a network that uses satellites to transmit data over long distances. |
| Bluetooth | a wireless technology that uses short-range radio waves to transmit data between devices. |

Data transmission technologies and networks have undergone significant advancements in recent years. These advancements have enabled faster and more efficient data transfer, enabling a wide range of applications such as online streaming, telemedicine, and telecommuting. In this paper, we review various data transmission technologies and networks, including wired and wireless technologies, as well as the latest developments in these areas. We also discuss the challenges and future directions of data transmission technologies and networks [5,10–12].

## 2. Wired Technologies

The transfer of data over a network cable is known as a wired network. This was born at the beginning of the 1960s, which was the time when the first attempts to have an efficient transmission of information from one computer to another began. With the advent of the computer, the growth of network communication progressed and, in terms of cost, it became more economical to transfer information [13–15].

Wired technologies refer to the physical connection of devices through cables, such as Ethernet and USB. Ethernet is one of the most widely used wired technologies for local area networks (LANs) and is capable of transferring data at high speeds [16–18]. USB, on the other hand, is a popular wired technology used for connecting devices such as printers, keyboards, and mice to computers. However, the use of wired technologies is limited by the need for physical connections and the difficulty of installation in certain environments.

Wired technologies refer to communication and information systems that rely on physical connections, such as cables and wires, to transmit data. Examples of wired technologies include Ethernet, which is used to connect computers to networks, and telephone lines, which are used to transmit voice data. Other wired technologies include cable television and DSL internet connections. While wired technologies are generally considered to be more stable and reliable than wireless technologies, they can be less convenient due to the need for physical connections [19–22].

Wired networks are characterized by the fact that they require a physical medium to connect the computers. To set up a wired network, you should check that the PCs have a network card or board. If you need to connect only two computers, a single cable will suffice for them to share information and devices between them. But if you need to connect more than two PCs, you will need to use a device known as an active element, such as a hub [4,23–25].

### 2.1.Concentrator

A concentrator (see Figure 1) is responsible for linking all the PCs in a network. Its function is to translate the requests from each of the PCs and route them accordingly.

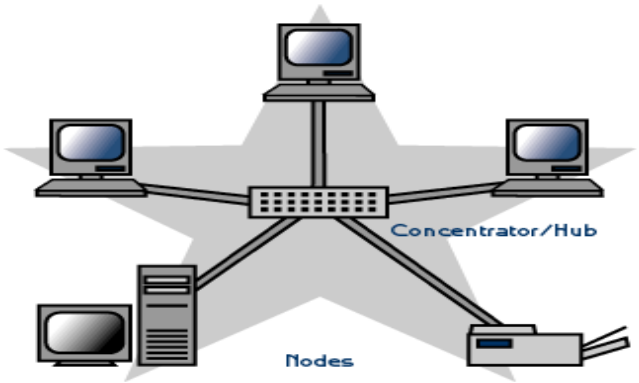


**Figure 1. Hub.**

### 2.2.Main types of networks

- LAN: Local area network of terminals.
- MAN: Wide area network, e.g., cable television.
- WAN: Networks created by private organizations; they have a wide reach.

The physical topologies of the network correspond to the strategic location of the workstations; they are based on nodes and connections to achieve communication and are determined by the configuration given to them.

The topologies are of the following types:

- Bus: All terminals are connected to a common cable segment called the backbone, the sending of information can be direct or indirect. It has the particularity that multiple terminals can be connected where if one fails the rest is not affected, although if the bus (cable) terminals are affected. It can be carried out using fiber optic cable, twisted pair, or coaxial cable.
- Star: All nodes are connected to a central node, which reduces the possibility of failure. Usually, routers, hubs or switches are used to establish this type of topology.
- Mixed: This is a combination of all the other topologies. This type is ideal in large industries where some areas need to be interconnected and others not. It is common to combine star/bus or star/ring.
- Ring: It is the interconnection of terminals in a consecutive way, where the communication is done by means of a token that is in charge of receiving and delivering the data packets.
- Double ring: It is the same concept as the previous one with the difference that being double allows the information to travel in both directions, it works in redundancy which avoids the loss of information.
- Mesh: In this topology, it is divided into full mesh where all nodes are connected to all other nodes so it does not carry a central node or partial mesh which would be when some nodes are connected to each other but there are also others that only exchange information with certain nodes. In case of an outage, it is not a failure as each server has its own connections.
- Hierarchical: Based on a central node to which all other devices are connected. It is ideal for large networks and ideal for LAN-type networks.

## 3. Wireless Technologies

Wireless technologies (see Figure 2), such as Wi-Fi, Bluetooth, and cellular networks, allow devices to communicate without the need for physical connections. Wi-Fi is a popular wireless technology used for local area networks (LANs) and is capable of transferring data at high speeds. Bluetooth is a wireless technology used for short-range communications, such as connecting wireless headphones to a smartphone. Cellular networks, such as 5G, are used for wide-area networks (WANs) and are capable of transferring data at high speeds over long distances [1,2,4,21,24].

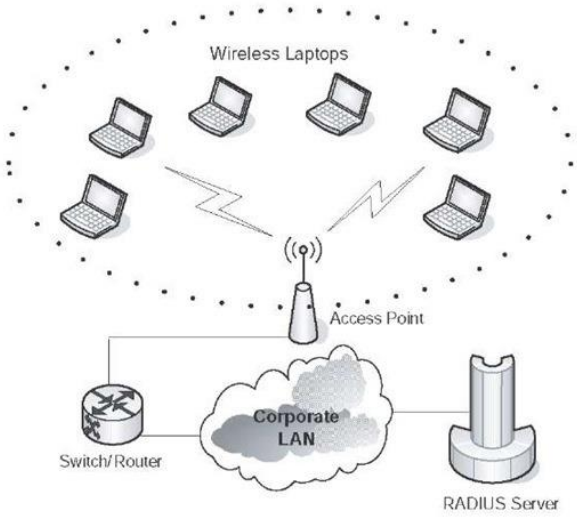


**Figure 2. Wireless network**

Wireless networks, on the other hand, are characterized by the fact that they do not require cables for interconnection. In this sense, they allow greater flexibility than wired networks, but at the same time, they depend directly on the range of the antennas and the connection speeds. There are different standards that identify the connection speed and the channel over which the connection is made. Originally, the standards were A, B and G. Networks based on the A and B standard have a speed of 11Mbps, while the G standard handles speeds of up to 54Mbps [8–11,25]. Today, the N standard is becoming widely used, allowing speeds of up to 300Mbps and longer distances between devices.

Wireless networks bring multiple benefits. However, special attention needs to be paid to the security milestone.

When using any device with a wireless board, in most cases, you will be able to see the existence of other networks and vice versa: i.e., existing networks will be able to detect you. If you do not set up any security mechanisms, then unauthorized persons will be able to enter your network without any problem. It is therefore necessary - and highly recommended - to secure networks in various ways.

Wireless networks and the subsequent mobile communication are growing by leaps and bounds in the past years and the demand for connection without cables is certainly high. Nowadays, wireless networks are quite common and can be found on university campuses, corporate offices, and in public places like hotels, airports, coffee shops, and so forth. Not only are mobile devices getting smaller and cheaper, but they are also becoming more efficient and powerful, capable of running applications and network services. This is causing the uncontrollable growth of mobile computing as we are witnessing today. Among the many applications and services that are executed by mobile devices, network and data services are in high demand. Brief descriptions of some selective wireless technologies that help mobile computing, like IEEE 802.11 networks (with infrastructure mode and ad-hoc mode), Bluetooth, HomeRF, WiMAX and cellular technologies are given below [1–7,12].

### 3.1.IEEE 802.11 Infrastructure network

Wireless local area network (WLAN) which is also known as Wi-Fi (Wireless Fidelity) networks, requires an infrastructure network that could provide the services of accessing other networks, along with forwarding functions and medium access control. The Institute of Electrical and Electronics Engineers (IEEE) in 1997 initiated the first WLAN standard and they called it 802.11. But, 802.11 only supported a maximum bandwidth of 2 Mbps, which is quite slow for most applications. The IEEE 802.11 family consists of different standards. The initial standard was approved in 1997 and it backed wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications that supported 1 Mbps and 2 Mbps data rate over the 2.4 GHz ISM band [10,26,27].

There are different wireless LAN technologies that the IEEE 802.11 standard supports in the unlicensed bands of 2.4 and 5 GHz. They share the same MAC (Medium Access Control) over two PHY layer specifications: Direct-Sequence.

Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS) technologies. Infrared technology though supported is not accepted by any manufacturer. Data rates of up to 2 Mbps were achieved initially by IEEE 802.11 systems operating at the 2.4 GHz band. Their wide acceptance initiated new versions and enhancements of the specification. The different extensions to the 802.11 standard use the radio frequency band differently. Popular 802.11 standards like 802.11a, 802.11b, and 802.11g are listed in Table 2.

**Table 2. Popular IEEE 802.11 comparisons**

| **IEEE Standard** (Legacy) | **Maximum Speed** (Mbps) | **Frequency band** (GHz) | **No. of nonoverlapping channels** | **Notes** |
|---|---|---|---|---|
| 802.11 | 1 to 2 | 2.4 | N/A | First standard (ratified in 1997). Uses FHSS and DSSS. |
| 802.11a | 54 | 5 | 8 to 14 (or more in future) | Second standard (ratified in 1999). Uses OFDM. |
| 802.11b | 11 | 2.4 | 3 (Channel 1,6 and 11) | Third and the most common standard (ratified in 1999). Uses DSSS. |
| 802.11g | 54 | 2.4 | 3 (Channel 1,6 and 11) | Popular standard (ratified in 2003). Uses OFDM. |

As a strong and robust standard, 802.11i deals with the limitations of WEP encryption that was used with 802.11b and enhances the overall wireless security. The architecture uses 802.1x for authentication (with the use of EAP and an authentication server that uses a 4-way handshake) and includes improvements in key management and the Advanced Encryption Standard (AES) for encryption. Other 802.11 extensions include 802.11c which focuses on MAC bridges, 802.11d that focuses on worldwide use of WLAN with operation at different power levels, 802.11e that focuses on Quality of Service, 802.11f that focuses on access point interoperability and 802.11h which focuses on addressing interference problems when used with other communication equipment' s. Table 1 shows the comparison of the popular 802.11 standards [28–30].

### 3.2.IEEE 802.11 AD HOC Network

A wireless ad-hoc network is a network that uses wireless links where each node is willing to forward data to the other neighbouring nodes dynamically, based on the network connectivity. Types of wireless ad-hoc networks include Mobile ad-hoc networks (MANET), Wireless Sensor Networks (WSN) and Wireless Mesh Networks (WMN). A mobile ad-hoc network can be defined

as a network of computer nodes that happens to be in proximity with each other, having no fixed infrastructure. A wireless sensor network (WSN) is a wireless network that makes use of distributed autonomous devices that uses sensors to measure or monitor environmental conditions like temperature, motion, sound, vibration, pressure and so forth, in a cooperative fashion. Wireless mesh networking (WMN) is mesh networking that is implemented on top of a wireless LAN in a decentralized (with no central server) way or centralized way (with a central server). Mesh networks are also extremely reliable with its redundant links, as each node is connected to several other nodes. If one node shuts down due to hardware errors or due to some other reason, its neighbours can easily find another route. Mesh networks can involve either fixed or mobile nodes.

Generally, in any ad-hoc network, each node can directly communicate with other nodes and so no access point or controlling station is needed. It is a self-configuring network of routers along with associated hosts connected by wireless links [6,10,11]. This union of network nodes or devices forms an arbitrary topology. This type of network provides great flexibility as it can be used for unplanned meetings and fast replacements of communication scenes far away from any infrastructure. Nodes or devices may look or rather search for target nodes that are out of vicinity by flooding the network with broadcast packets that would be forwarded by each node. Wireless connections are even possible through multiple nodes forming a multi-hop ad-hoc network. Routing protocols then provide reliable connections even if nodes are moving around.

The routers are free to move randomly and organize themselves arbitrarily, making unpredictable changes in the network’ s wireless topology. There is no need for an access point and if one station working in ad-hoc mode is connected to a wired network, stations forming an ad-hoc network have wireless access to the Internet. IEEE 802.11 technology can be used to implement single-hop ad-hoc networks where the stations need to be in the same transmission radius to be able to communicate. But in multichip ad-hoc networking, routing mechanisms can be enabled to extend the range of the ad-hoc network beyond the transmission radius of the single source station. Routing solutions for a wired network don’ t apply to ad-hoc networks, because of their dynamic topology.

Ad-hoc routing protocols are getting popular with the increase in mobile computing. Ad-hoc networks include resource-starving devices, low bandwidth, high error rates and a topology that is continuously changing. Some of the design goals with ad-hoc routing protocols are minimal

control overhead, minimal processing overhead, multihop routing capability, dynamic topology maintenance and loop prevention. The protocols should operate in a distributed manner. The nodes should operate either in proactive or reactive mode. Proactive protocols are table-based and maintain routes for the entire network within each node. The nodes must be fully aware of the changing topology. For topologies that are overtly dynamic, this approach can introduce a considerable overhead. Reactive or on-demand protocols trade off this overhead with increased delay. A route to the destination is established when it is needed based on an initial discovery between the source and the destination. Security of ad-hoc networks is a great concern with WEP (128 bits) encryption and 802.1x authentication offers some temporary solution.

## 4. Recent Developments

Recent developments in data transmission technologies and networks include the deployment of 5G networks, the use of millimeter-wave (mmWave) technology, and the development of software-defined networks (SDNs). 5G networks are expected to provide faster data transfer speeds and lower latency, enabling new applications such as virtual and augmented reality. MmWave technology is being used to increase the capacity of wireless networks, while SDNs allow for more efficient and flexible network management.

## 5. Challenges and Future Directions

Despite the significant advancements in data transmission technologies and networks, several challenges still remain. One of the major challenges is the increasing demand for bandwidth, which is putting pressure on existing networks. Another challenge is the lack of security in wireless networks, which is becoming a major concern with the proliferation of IoT devices. In the future, data transmission technologies and networks will need to address these challenges and continue to evolve to meet the growing demands of users.

## 6. Conclusions

Data transmission technologies and networks have undergone significant advancements in recent years, enabling faster and more efficient data transfer. Wired and wireless technologies are the main types of data transmission technologies, and recent developments include the deployment of 5G networks, the use of mmWave technology, and the development of SDNs. However, challenges such as the increasing demand for bandwidth and the lack of security in

wireless networks still remain. In the future, data transmission technologies and networks will need to continue to evolve to meet the growing demands of users.

Brief descriptions of popular wireless technologies were presented during the discussions. The world is increasingly becoming mobile and wireless networking is getting greater focus in the recent past, especially with hardware technology breakthroughs and price drops. As wireless networks facilitate mobile computing, the future of the above-mentioned technologies is being watched with eagerness. Mobility when combined with computing power makes a deadly combination and that' s why relentless research is going on to make wireless technologies even better. The convergence of all these wireless technologies to form one single network is the greatest challenge ahead, as they all use different networking technologies and that could take us to a world where seamless and ubiquitous computing will become a definite reality and not a future dream.

**Acknowledgments**

The lead author of this research paper thanks all the authors cited in this article for their invaluable contribution to the science of communication networks.

## References

1. K.S. Hung, W.K. Lee, V.O.K. Li, K.S. Lui, P.W.T. Pong, K.K.Y. Wong, G.H. Yang, J. Zhong, On wireless sensors communication for overhead transmission line monitoring in power delivery systems, in: 2010 First IEEE Int. Conf. Smart Grid Commun., IEEE, 2010: pp. 309–314.
2. R. Amin, J. Martin, X. Zhou, Smart grid communication using next generation heterogeneous wireless networks, in: 2012 IEEE Third Int. Conf. Smart Grid Commun., IEEE, 2012: pp. 229–234.
3. S. Galli, A. Scaglione, Z. Wang, For the grid and through the grid: The role of power line communications in the smart grid, Proc. IEEE. 99 (2011) 998–1027.
4. C.H. Hauser, D.E. Bakken, A. Bose, A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid, IEEE Power Energy Mag. 3 (2005) 47–55.

5. P.P. Parikh, M.G. Kanabar, T.S. Sidhu, Opportunities and challenges of wireless communication technologies for smart grid applications, in: IEEE PES Gen. Meet., IEEE, 2010: pp. 1–7.
6. C.-H. Lo, N. Ansari, The progressive smart grid system from both power and communications aspects, IEEE Commun. Surv. Tutorials. 14 (2011) 799–821.
7. X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—The new and improved power grid: A survey, IEEE Commun. Surv. Tutorials. 14 (2011) 944–980.
8. V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G.P. Hancke, Smart grid technologies: Communication technologies and standards, IEEE Trans. Ind. Informatics. 7 (2011) 529–539.
9. A. Zaballos, A. Vallejo, J.M. Selga, Heterogeneous communication architecture for the smart grid, IEEE Netw. 25 (2011) 30–37.
10. N. Aggarwal, D. Singh, A. Singh, A Systematic level mapping of Mushroom Cultivation using Internet of Things (IoT), Comput. Integr. Manuf. Syst. 28 (2022) 238–267.
11. A. Sisodia, A.K. Yadav, Confabulation of Different IoT Approaches with and without Data Compression, Comput. Integr. Manuf. Syst. 28 (2022) 963–981.
12. V.K. Sood, D. Fischer, J.M. Eklund, T. Brown, Developing a communication infrastructure for the smart grid, in: 2009 IEEE Electr. Power Energy Conf., IEEE, 2009: pp. 1–7.
13. S.K. Rao, R. Prasad, Impact of 5G technologies on industry 4.0, Wirel. Pers. Commun. 100 (2018) 145–159.
14. T. Rühlig, M. Björk, What to make of the Huawei debate? 5G network security and technology dependency in Europe, UI Pap. 1 (2020) 2020.
15. S.K. Rao, R. Prasad, Impact of 5G technologies on smart city implementation, Wirel. Pers. Commun. 100 (2018) 161–176.
16. M. Attaran, The impact of 5G on the evolution of intelligent automation and industry digitization, J. Ambient Intell. Humaniz. Comput. (2021) 1–17.
17. Z. Li, X. Wang, T. Zhang, 5G+: How 5G change the society, Springer Nature, 2020.
18. G.F. Huseien, K.W. Shah, Potential applications of 5G network technology for climate change control: A scoping review of singapore, Sustainability. 13 (2021) 9720.
19. Y. Liu, L.-J. Zhang, C. Xing, Review for Influence of 5G on Industry Internet, in: World Congr. Serv., Springer, 2020: pp. 93–100.
20. V. Gayatri, M.S. Kumaran, Link Failure Prediction Using Efficient Multipath Algorithm in Ad Hoc Networks, Comput. Integr. Manuf. Syst. 28 (2022) 1366–1380.

21. S. Alam, M.F. Sohail, S.A. Ghauri, I.M. Qureshi, N. Aqdas, Cognitive radio based Smart Grid Communication Network, Renew. Sustain. Energy Rev. 72 (2017) 535–548. https://doi.org/10.1016/j.rser.2017.01.086.
22. M. Kolenc, E.G. Ortega, F. Basci, J.F. Tasič, M. Zajc, Intelligent monitoring of power networks - System architecture and communication network infrastructure, Elektroteh. Vestnik/Electrotechnical Rev. 80 (2013) 245–250.
23. K. Campbell, L. Cruz, B. Flanagan, B. Morelli, B. O' neil, S. Téral, J. Watson, The 5G Economy: How 5G will contribute to the Global Economy, (2019) 1–47. https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf.
24. H. Martin-Qualcomm, Leading the world to 5g, (2016).
25. P. Orosz, P. Varga, G. Soós, C. Hegedűs, QoS Guarantees for Industrial IoT Applications over LTE-a Feasibility Study, in: 2019 IEEE Int. Conf. Ind. Cyber Phys. Syst., IEEE, 2019: pp. 667–672.
26. a.G.Watts2001, The Role of Information and Communication Technologies in, ProQuest Diss. Theses. 5 (2011) 142. http://search.proquest.com/docview/854286083?accountid=28962%5Cnhttp://sfx.metabib.ch/sfx_locater??url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&genre=dissertations+&+theses&sid=ProQ:ProQuest+Dissertations+&+Theses+A&I&atitle=&title.
27. I. Amin, A. Saeed, 5.10 Wireless Technologies in Energy Management, in: I.B.T.-C.E.S. Dincer (Ed.), Elsevier, Oxford, 2018: pp. 389–422. https://doi.org/https://doi.org/10.1016/B978-0-12-809597-3.00524-1.
28. L. Guevara, F. Auat Cheein, The role of 5G technologies: Challenges in smart cities and intelligent transportation systems, Sustainability. 12 (2020) 6469.
29. D.M. West, How 5G technology enables the health internet of things, Brookings Cent. Technol. Innov. 3 (2016) 20.
30. K. Campbell, J. Diffley, B. Flanagan, B. Morelli, B. O' Neil, F. Sideco, The 5G economy: How 5G technology will contribute to the global economy, IHS Econ. IHS Technol. 4 (2017) 16.