Science Publications

International Journal of Mathematical, Engineering, Biological and Applied Computing, 2022, 1, 22-29
www.scipublications.org/journal/index.php/ijmebac
DOI: 10.31586/ijmebac.2022.294

Review Article

Wireless Technology is Easy to Use

Sinisa Franjic*

Independent Researcher, Croatia

*Correspondence: Sinisa Franjic (sinisa_franjic@net.hr)

Abstract: Wireless networking is the connection of computers, digital communication devices, network equipment, and various other devices via radio waves. It is applied in places where the wired infrastructure cannot be installed or the price of introducing such a structure is too high. In addition, it has some features that are a great advantage over wired networking, such as customer mobility, easy expandability, and fast and low-cost temporary networking. Wireless technology allows us mobility and ease of use, but most users do not think about security. Users are insufficiently informed about the dangers of the Internet. Many of them do not pay attention to that and access important data such as bank accounts, e-mail, and any other contents that must be preserved and hidden. Today, there are more and more malicious actions, where hackers use various methods and technologies to attack users' accounts, bypassing all protections. Today, the issue of security is one of the priorities for every Internet user. Due to its characteristics, wireless communication is exposed to attacks due to the way they are sent, and there is a possibility of intercepting information.

Keywords: Wireless Technology, Smart Electronics, EMR, Security

How to cite this paper:
Franjic, S. (2022). Wireless Technology is Easy to Use. *International Journal of Mathematical, Engineering, Biological and Applied Computing*, *1*(1), 22–28. Retrieved from https://www.scipublications.com/journal/index.php/ijmebac/article/view/294

Received: May 4, 2022
Accepted: June 11, 2022
Published: June 13, 2022

1. Introduction

Communications carried by electromagnetic radio waves are used for quite 100 years currently [1]. And here we tend to ar continuously up the technological means and organization for a way to do wireless communications a lot of efficiently and quicker, each in brief and long ranges. The term wireless communication includes the use of radio and microwave frequencies, infrared and better light-weight frequencies. Acoustic waves are wireless too but aren't considered here.

One obvious advantage of wireless is that it's wireless, it permits communication while not rolling out and connecting cables, electrical conductors, or different waveguides. Microwave links cross geographical barriers like valleys and mountain ranges. Communication satellites will relay signals from one continent to a different.

While a cable has two well-defined termination locations, the radio wave channels don't. The waves will be broadcasted, reflected, and diffracted so the communication signal will reach an oversized geographic region and cover an oversized variety of receivers. Observe that the term broadcasting has become synonymous with electronic mass media.

Moreover, mobility becomes possible and could be a major feature of wireless communication. The transmitter and receiver terminals will change location and move regarding where being connected. We tend to all know the success and participate in mobile cellular phone communications with roaming terminals.

Even the core network of communication nodes doesn't have to be compelled to be tethered by cables, however, will be wireless and adapt to the location of wireless terminals. The distinction between network terminals and intermediary nodes isn't a necessity any longer, thus networks of communication nodes will type ad hoc

configurations, wherever all nodes contribute to the overall network property by forwarding data for different nodes in an exceedingly dynamic fashion. Vehicular ad hoc networks are the term used for the development of technology that gives electronic communication among vehicles and between vehicles and edge roadside and to is deployed within the close to future.

What are the distinguishing factors between wired and wireless communications once we take into account info security?

Wiretapping wants physical access to the wire, whereas wireless doesn't, therefore the geographical area for potential self-made eavesdropping becomes a lot wider. Radio signals aren't confined to physical perimeters and barriers, like within a building wall or a fence. The sender broadcasts the radio waves over a large field, which is a very important feature in several services, like TV and radio programming with many receivers geographically distributed. Some can even claim that they need rightful ownership of radio waves that enter their land and property!

Whereas observance and detection of physical intrusion to a cable are feasible, this is often hardly even a theoretical chance with passive eavesdropping of radio communication. This makes eavesdropping on wireless a lot easier than wiretapping, with no strict physical access and a small risk of detection.

Neither are active channel attackers confined to one location. Active radio transmitters are possible to find by radio-direction-finding equipment and cross-bearing methods, however, this needs active surveillance, the flexibility to distinguish between authorized and nonauthorized, and perform a response in real-time. For example, the supply of intermittent disruptions is hard to discover.

So using wireless for 2-party confidential communications is like two people attempting to possess a non-public spoken communication at far at a packed marketplace utilizing megaphones. Most can listen, and also the most interested listeners will even move on the brink of obtaining improved listening conditions as a result of it's possible to get a directional sense of the location of the communicators.

2. EMR

Wireless communication of any kind needs using electromagnetic waves to transmit the signal [2]. Our first goal is to know the spectrum, then we'll delve into the way to encode data in such transmissions. It's vital to possess a basic understanding of the basic physics of electromagnetic transmissions to know exactly how mobile devices send and receive data.

Electromagnetic waves also referred to as electromagnetic radiation (EMR) are the waves of an electromagnetic field propagating through space. Such waves include visible light, radio waves, infrared and more.

Radio transmission, still a different kind of electromagnetic radiation communication, works on the principle of manufacturing a carrier wave because of the means of communication between two wireless devices. The carrier is an associate electromagnetic wave of a specific frequency that's wont to carry data. Technically you may use any frequency to encode and transmit data. However, for rather obvious reasons gamma rays and x-rays build a poor alternative for communications. Frequency assignments are one thing you're seeming to be familiar with. Radio and TV broadcast stations are appointed specific frequencies that they have to transmit. A radio identification like 101.1 FM represents a carrier of 101.1 MHz (megahertz). The frequency of 101.1 megahertz also happens to be the frequency for the classical music station in my area.

It is vital that you simply absolutely perceive the hertz unit of measuring. A hertz is the international standard unit for frequency and is defined as one cycle per second. A cycle is moving from one peak to the next (or else from one trough to the next) in an exceedingly wave. A lot of formal definitions are the variety of oscillations per second.

Thus, we'll typically mention kilohertz (kHz), rate (MHz), gigahertz (GHz), or even terahertz (THz). Frequency isn't only used for electromagnetic radiation, but additionally for sound waves. As an example, an adult human, of traditional hearing capability, will notice sound between twenty Hz and 16,000 Hz. after you hear terms like ultrasound, that virtually means that frequencies are on the far side of traditional human hearing (ultra). The American National Standards Institute has outlined ultrasound as a touch more than that, sound frequencies larger than twenty kilohertz or 20,000 Hz.

The carrier is encoded with knowledge. This is often done through some kind of modulation. The technique of modulation is however AM radio, FM radio, and every one magnetic attraction communication works. In face, AM means AM, and FM means modulation. A straightforward broadcast consists of a transmitter, that generates the carrier and modulates info into the carrier, and a receiver, that receives the modulated wave and demodulates it. The transceiver and receiver should each be at or very close to an identical carrier frequency for communication to occur. The receiver decodes the information that was encoded within the carrier. This method is known as demodulation.

The same principle is used to transmit digital data signals. You almost certainly used such signals these days. Not only is that this, however, your mobile phone operates, but however it's also how your wireless web works. A carrier establishes the transmitter/ receiver relationship. The carrier is modulated with a wave pattern resembling the digital knowledge signal. The two waves are combined before transmission and then separated at the receiver.

3. Wireless Network

The twenty-first century is delineated because of the modern era [3]. The transformation from machinery-based production to an associate information-based economy, during which the intellectual issue plays a vital half, has resulted in the development of the data society. The efficiency of the new economy is driven by knowledge. These processes are among the continuing reduction in the prices associated with the aggregation of data and also the services associated with the most recent technology. On coming into the information age, some cultural changes are closely associated with the evolution and development of communications. A transformation has been evident from the standard mass media like TV and radio, predominant within the twentieth century, to horizontal communication networks based on the web and wireless communication. PC networks, open-source software packages (including web protocols), the fast development of digital connections, and data transmission with telecommunications networks resulted, at the start of the 1990s, in the enlargement of the web and its use for personal functions. At an identical time, a revolution started involving communications and also the dynamic development of wireless communication. The web and Internet-based technologies additionally contributed to a revolution within the understanding of ancient legal terms and establishments.

All these technological developments, and also the connected social changes, resulted within the institution of the data society and supported permanent access to info, which is crucial for each business and private life. The establishment of the new social structure was connected with and resulted from, the huge success of the web, and its growing influence, specifically its non-commercial resources. It expedited the conceptualization of real phenomena within the digital world.

Wireless networks (Wi-Fi) offer the convenience of quality for networked devices while not the inconvenience of trailing cables around to keep up connectivity [4]. Wireless networks became present considering what percentage of offices, homes, cafes and public areas use Wi-Fi networking in preference to leashing systems to network cables. Despite whether or not the network is meant for public or non-public use, the traffic from a Wi-Fi network is visible to anyone who will obtain a signal. Wherever access to a wired network is limited by physical access to network cables or devices (and the walls and doors that

separate the equipment from the outside world), visibility to a Wi-Fi network is limited only by the quality of the antenna.

The proliferation of wireless networks reintroduced several issues with clear-text protocols (communications that don't use encrypted channels). Wi-Fi networks not protected by encoding or strong access controls expose an organization's network— and its network users—to compromise by arbitrary users. Even intentionally open networks, sort of a cafe's Wi-Fi system, expose their users to threats of sniffing and spoofing attacks.

The problem of exposing traffic to anyone who will monitor a wireless signal was acknowledged when Wi-Fi was first created. The Wired Equivalent Privacy (WEP) protocol was an attempt to overcome the promiscuous nature of a wireless network. To sniff traffic on a wired network (one with CAT-5 cables, hubs, and switches), you initially should physically connect to the network. For a wireless network, you only have to be compelled to be in proximity of associate access purpose (AP). WEP is supposed to produce encoding at the physical and circuit layers of the network. In different words, it encrypts traffic despite the network protocol, like TCP/IP or IPX. If a network uses WEP, its traffic will still be sniffed, however since the information is encrypted, the associate offender shouldn't be able to understand any of the captured info. However, WEP has style flaws that considerably scale back the effectiveness of its encoding. Modern tools will extract the encoding key for WEP-protected network mistreatment with less effort than what would be needed for a brute-force guessing attack.

Another term associated with Wi-Fi networking is Service Set Identifier (SSID). The SSID identifies a network. After you connect a tool to an associate access point, you join it to the SSID served by the AP. At the packet level, the SSID is employed as a header so multiple APs and devices will separate traffic intended for their network from different wireless activities in the vicinity. The SSID will be up to 32 characters (bytes) long. By default, an AP broadcasts its SSID so devices know a wireless network is available. In practice, the broadcast could also be disabled—a questionable cloaking technique for preventing the SSID from being discovered.

4. Smart Electronics

Information and communications technologies (ICT) like the net and mobile phones have significantly influenced how people do their activities and interactions [5]. The web allows us to access an enormous amount of information and a large range of services online through a worldwide system of interconnected computer networks. With Wi-Fi technology, we can hook up with the net from any location that has a wireless local area network. Mobile phones and tablets which are equipped with increasingly powerful computing power further free us from the fixed landline phones and bulky computers, to remain connected almost anywhere and at any time. It's now feasible to search out a journal article when a library is closed, purchase an item without a physical visit to a store, and stay in touch with friends most of the time. In other words, modern technologies have removed many spatial and temporal constraints on human activities and interactions to increase our activity space. Human activities and interactions, therefore, became more flexible and spontaneous which successively can change the nature and spatiotemporal patterns of human dynamics.

The future Internet will comprise not only a lot of computing machines and software services but also billions of private and professional devices, diminutive sensors and actuators, robots, and so on, and trillions of sentient, smart, and digitized objects [6]. It's an overwhelmingly accepted indisputable fact that the fast-emerging and evolving Internet of Things (IoT) idea is certainly a strategic and highly impactful one to be decisively realized and passionately sustained with the smart adoption of the state-of-the-art information communication technology (ICT) infrastructures, a bevy of cutting-edge technologies, composite and cognitive processes, versatile and integrated platforms, several enabling tools, pioneering patterns, and futuristic architectures. Industry

professionals and academicians are constantly searching for appropriate use and business and technical cases to confidently and cogently proclaim the transformational power of the IoT concept to the larger audience of worldwide executives, end-users, entrepreneurs, evangelists, and engineers.

A growing array of open and industry standards are being formulated, framed, and polished by domain experts, industry consortiums, and standard bodies to form the IoT paradigm more visible, viable, and valuable. National governments across the world are fitting special groups to come out with pragmatic strategies, policies, practices, and procedures to require forward the groundbreaking ideas of IoT, and to understand the strategic significance of the envisioned IoT era in conceiving, concretizing, and providing a group of next-generation citizen-centric services to make sure and enhance people's comfort, choice, care, and convenience. Research students, scholars, and scientists are working collaboratively toward identifying the implementation challenges and overcoming them through different means and ways, especially through standard technological solutions.

Our living, relaxing, and working environments are envisioned to be filled up with a range of electronics including environment monitoring sensors, actuators, monitors, controllers, processors, tags, labels, stickers, dots, motes, stickers, projectors, displays, cameras, computers, communicators, appliances, robots, gateways, and high-definition IP TVs. Apart from these, all the physical and concrete items, articles, furniture, and packages will become empowered with computation and communication-enabled components by attaching specially made electronics onto them. Whenever we walk into such forms of empowered and augmented environments lightened up with a legion of digitized objects, the devices we carry and even our e-clothes will enter into a calm yet logical collaboration mode and form wireless ad hoc networks with the inhabitants in this environment. As an example, if someone wants to print a document on his or her smartphone or tablet, and if he or she enters an area where a printer is situated, the smartphone will begin a conversation with the printer automatically and send the document to be printed.

Thus, in that era, our everyday spots are made informative, interactive, intuitive, and invigorated by embedding and imbedding intelligence into their constituents (audio or video systems, cameras, information and web appliances, consumer and household electronics, and other electronic gadgets besides digitally augmented walls, floors, windows, doors, ceilings, and the other physical objects and artifacts). The disappearing computers, communicators, sensors, and robots are instructing, instigating, alerting, and facilitating deciding in a very smart way, apart from accomplishing all types of everyday needs proactively for human beings. Humanized robots are extensively used to fulfill our daily physical chores. That is, computers of different sizes, looks, capabilities, interfaces, and prizes are fitted, glued, implanted, and inserted everywhere to be coordinative, calculative, and coherent, yet invisible to discerning human minds. In summary, the IoT technologies in sync up with cloud infrastructures are to lead to people-centric smarter environments. Context-awareness is the key motivator for business and IT (Information Technology) systems to be distinct in their operations, offerings, and outputs. The times of ambient intelligence (AmI) aren't far away because of the speed and sagacity with which scores of implementation technologies are being unearthed and nourished by product vendors and system integrators.

The IoT encompasses scores of computer-based devices that transmit data over the net autonomously [7]. These include smart home devices and automation products like smart thermostats, smart bulbs, smart TVs, and wearable sensors like heart rate and respiratory rate monitors. Thanks to technological advances, cheap data storage, and fast internet connections, the Internet of Things (IoT) is everywhere.

5G is the next generation of mobile broadband which will ultimately replace current 4G LTE connections. 5G has been developed with three major improvements: superior

speed, lesser latency (the time it takes for data to go back and forth, and therefore the ability to connect more IoT devices directly. The growing number of devices will create large cyber attacks, and we must remember that each device connected to the net is usually under threat of assault.

IoT devices make our lives better, softer, and healthier, utilizing real-time monitoring, medical assistance, tracking, and alerts. Consequently, cybercriminals will have access to more and more personal and medical information. Many IoT devices have been manufactured using unsecured communications protocols and open-source codes, allowing anyone to use or modify a code or a program. Additionally, manufacturers often use and share code from one source across devices and multiple brands. As a result, many IoT devices have hard-coded backdoor passwords built into them, meaning that anyone can type within the default password and gain access. In some cases, the password will be found on the web (YouTube) or in hacking forums.

Cybercriminals perform these attacks remotely and anonymously. Thus, the ability to impose ransomware thousands of miles away on owners of countless IoT devices is possible. Cybercriminals are constantly searching for ways to achieve control of them via password cracking and exploiting additional vulnerabilities.

5. Security

Wireless networks and communication links became pervasive for both personal and organizational communications [8]. A large kind of technologies and network types are adopted, including Wi-Fi, Bluetooth, WiMAX, ZigBee, and cellular technologies. Although the protection threats and countermeasures discussed throughout this book apply to wireless networks and communications links, there are some unique aspects to the wireless environment.

Wireless networks, and therefore the wireless devices that use them, introduce several security problems over and above those found in wired networks. Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include the following:

- Channel: Wireless networking typically involves broadcast communications, which are much more vulnerable to eavesdropping and jamming than wired networks. Wireless networks are more prone to active attacks that exploit vulnerabilities in communications protocols.
- Mobility: Wireless devices are, in principle and frequently in practice, way more portable and mobile than wired devices. This mobility ends up in a variety of risks, described subsequently.
- Resources: Some wireless devices, like smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware.
- Accessibility: Some wireless devices, like sensors and robots, could also be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks.

In simple terms, the wireless environment consists of three components that provide a point of attack. The wireless client is often a cellular phone, a Wi-Fi-enabled laptop or tablet, a wireless sensor, a Bluetooth device, and so on. The wireless access point provides a connection to the network or service. Examples of access points are cell towers, Wi-Fi hot spots, and wireless access points to wired local or wide-area networks. The transmission medium, which carries the radio waves for data transfer, is also a source of vulnerability.

6. Conclusions

Wireless networks can be quickly and easily established in temporary locations during certain events such as scientific meetings, sporting events, unwanted emergencies, and various other gatherings and events. Since such events impose the need for a network of very fast realization and limited duration, installing a classic wired infrastructure would be too slow and too expensive. An access point is a base station that connects the wireless clients assigned to it to a wireless network. It manages the allocation of radio channels and mediates the transmission of data between clients. The access point can connect to a wired network via an Ethernet connection. This connection allows data to be exchanged between wireless clients and servers or workstations that make up a wired network. Accordingly, the access point in addition to the wireless network card must also contain a classic Ethernet card intended for communication in the wired network. This role of the access point is its basic mode of operation. If required, the access point can be configured to operate in a special mode such as repeater mode, bridge mode, and ordinary wireless client mode. The wireless technology is vastly applied in solving channel allocation and graph coloring applications using different soft computing strategies [9-17].

References

[1] Mjølsnes, S. F.; Eian, M. (2012.): „Wireless Network Access" in Mjølsnes, S. F. (ed): „A Multidisciplinary Introduction to Information Security", CRC Press, Taylor & Francis Group, Boca Raton, USA, pp. 132. - 133.

[2] Easttom, C. (2022.): „ An In-Depth Guide to Mobile Device Forensics", CRC Press, Taylor & Francis Group, LLC, Boca Raton, USA, pp. 3. - 5.

[3] Kurek, J. (2022.): „Operational Activities in the Field of Cybersecurity" in Chałubińska-Jentkiewicz, K.; Radoniewicz, F.; Zieliński, T. (eds): „Cybersecurity In Poland - Legal Aspects", Springer Nature Switzerland AG, Cham, Switzerland, pp. 455. - 456.

[4] Shema, M. (2014.): „Anti-Hacker Tool Kit, Fourth Edition", McGraw-Hill Education, New York, USA, pp. 356.

[5] Shaw, S. L. (2021.): „ Urban Human Dynamics" in Shi, W.; Goodchild, M. F.; Batty, M.; Kwan, M. P.; Zhang, A. (eds): „Urban Informatics", Springer Nature Singapore Pte Ltd., Singapore, Singapore, pp. 48.

[6] Raj, P.; Raman, A. C. (2017.): „Abusing the Internet of Things - Enabling Technologies, Platforms, and Use Cases", CRC Press, Taylor & Francis Group, Boca Raton, USA, pp. 1. - 3.

[7] Alexandrou, A. (2022.): „Cybercrime and Information Technology - The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices", CRC Press, Taylor & Francis Group, LLC, Boca Raton, USA, pp. 78. - 79.

[8] Stallings, W.; Brown, L. (2015.): „Computer Security - Principles and Practice, Third Edition", Pearson Education, Inc., Boston, USA, pp. 734-735.

[9] R. Marappan and G. Sethumadhavan, "Solving channel allocation problem using new genetic algorithm with clique partitioning method," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2016, pp. 1-4, doi: 10.1109/ICCIC.2016.7919671.

[10] R. Marappan and G. Sethumadhavan, "Divide and conquer based genetic method for solving channel allocation," 2016 International Conference on Information Communication and Embedded Systems (ICICES), 2016, pp. 1-5, doi: 10.1109/ICICES.2016.7518914.

[11] Raja Marappan, Gopalakrishnan Sethumadhavan. Solving Fixed Channel Allocation using Hybrid Evolutionary Method MATEC Web of Conferences 57 02015 (2016) DOI: 10.1051/matecconf/20165702015

[12] Raja Marappan, Gopalakrishnan Sethumadhavan, U. Harimoorthy, Solving channel allocation problem using new genetic operators – An experimental approach, Perspectives in Science, Volume 8, 2016, Pages 409-411, ISSN 2213-0209, https://doi.org/10.1016/j.pisc.2016.04.091.

[13] S. Balakrishnan, Tamilarasi Suresh, Raja Marappan. (2021) A New Multi-Objective Evolutionary Approach to Graph Coloring and Channel Allocation Problems. Journal of Applied Mathematics and Computation, 5(4), 252-263. DOI: http://dx.doi.org/10.26855/jamc.2021.12.003

[14] Raja Marappan: A New Multi-Objective Optimization in Solving Graph Coloring and Wireless Networks Channels Allocation Problems. Int. J. Advanced Networking and Applications Volume: 13 Issue: 02 Pages: 4891-4895 (2021)

[15] Marappan, R.; Sethumadhavan, G. Complexity Analysis and Stochastic Convergence of Some Well-known Evolutionary Operators for Solving Graph Coloring Problem. Mathematics 2020, 8, 303. https://doi.org/10.3390/math8030303

[16] Marappan, R., Sethumadhavan, G. Solving Graph Coloring Problem Using Divide and Conquer-Based Turbulent Particle Swarm Optimization. Arab J Sci Eng (2021). https://doi.org/10.1007/s13369-021-06323-x

[17] Marappan, R., Sethumadhavan, G. Solution to Graph Coloring Using Genetic and Tabu Search Procedures. Arab J Sci Eng 43, 525–542 (2018). https://doi.org/10.1007/s13369-017-2686-9