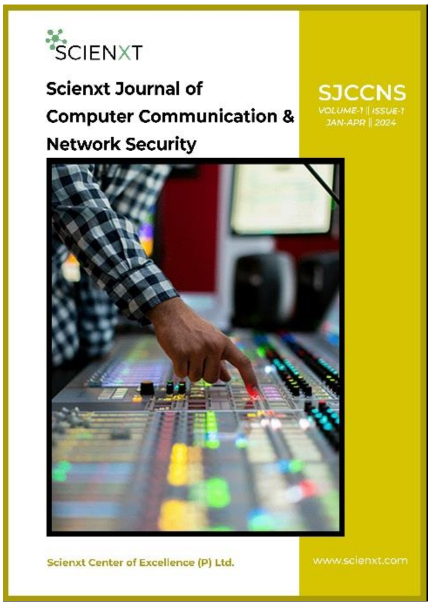

Scienxt Journal of Computer Communication & Network Security
Volume-1 || Issue-1 || Jan-Apr || Year-2024 || pp. 29-36

Analysis of wireless local area networks

Elilmani Jacob*[1]

[1]Prathyusha Engineering College, Department of Electronics & Communications,
Chennai, Tamil Nadu, India

Shanmugam Panneerselvam[2]

[2]Assistant Professor, Department of Electronics & Communications,
Prathyusha Engineering College, Chennai, Tamil Nadu, India

Corresponding Author*: ***Elilmani Jacob*
Email: ***elilmajacob21@rediffmail.com***

Abstract:

The planning of a wireless LAN is the subject of this study (WLAN). This research aims to measure the network and find solutions to reduce power losses by measuring and analyzing parameters such as data transmission, free space loss, power output, and reception quality. There is a lot of misunderstanding about how point-to-point, as well as point-to-multipoint systems, should be implemented in a Wireless Local Network's design. The researchers have used a technique that strategically places the transmitting antenna to maximize the effectiveness of the high-frequency radio transmission. The information received just at receiving end confirms that the calculated as well as simulated values are same, proving that a set of devices such as computers were linked together by a wireless link, as shown by the results produced from this design.

Keywords:

Computers, Direct Sequence Spread Spectrum (DSSS) Design, Wireless LAN, Radio frequency signal transmitting antenna.

1. Introduction:

Traditionally, protecting sensitive information has involved putting up physical barriers, such as locked cabinets and security personnel. This concept went through a transition when personal computers first became widely available. Digital files, in contrast to traditional documents, each possess their own set of distinctive qualities. They are susceptible to being changed or reproduced without leaving any traces behind, such as fingerprints, DNA, or other forms of evidence in the case (Souppaya and Scarfone, 2020). They need to utilize security services in order to have the same characteristics as physical papers and, thus, the same level of protection (Souppaya and Scarfone, 2020). This field that information security has also been significantly influenced by network security in a big way. It is imperative that the data transit be secure. The creation of more robust and trustworthy wired networks has now been sped up by the advent of the Internet. It was not until recently that wireless networks were made accessible to the general population. Because of the features of radio transmission, professionals in the field of cyber security have an increased level of complexity in their work.

1.1. Background:

Wireless local area networks become ubiquitous due to the growing need for wireless Internet access and the widespread adoption of Wi-Fi technology in homes, businesses, schools, and public spaces (Chao Yang and Guofei Gu, 2021). A wireless local area network is a network joining two or more devices by employing wireless distribution methods (often spread-spectrum and orthogonal frequency-division multiplexing radios), as well as usually giving a link through an access point to the wider Internet.

1.2. Research aim:

This study's purpose is to examine the security mechanisms of wireless local area networks in depth.

1.3. Research objective:

1) To talk about the many different parts of a wireless LAN,
2) The goal is to talk about the different wireless LAN security protocols.
3) Finally, point out how weak current wireless protocols are.

1.4. Research question:

1) What proportion of infrastructure-mode WLANs have WEP encryption turned on?
2) How much use have you made of the available and relevant security tools?

2. Literature review:

In this part of the Research, we will briefly discuss the most useful resources that were consulted. The several subsections of this chapter cover every significant aspect of the study.

2.1. Wireless local area networks (WLANs):

Similar to a conventional local area network (LAN), a Wireless Local Area Network (WLAN) uses radio waves for transmission rather than physical wires (Networks, 2018). Consequently, users can roam about a specific area while being online. As a result, WLANs enable mobile LANs by combining data access with user mobility and requiring less effort in terms of deployment (Networks, 2018). WLANs, on the other hand, offer the same capabilities as wireless Local area networks, but without the limitations imposed by the wires themselves.

A wireless local area network (in Infrastructure mode) typically has one main hub for connections, known as an "Access Point" (AP). It functions similarly to a hub or switches in wired LANs based on the classic star architecture (Networks, 2018). Typically, the sole connection between a wireless LAN and a wired LAN is through the access point, which transports data between the various nodes on the network (Networks, 2018). Within a 300-foot radius of a typical access point, it may support a large number of users. Clients, or wireless nodes, in a wireless local area network, are the individual devices that make up the network. Fig. 1 below depicts a wireless LAN.

2.2. Types of wireless networks:

The three main categories of wireless networks are wide area networks (WAN), local area networks (LAN), and personal area networks (PAN).

2.2.1. Wireless wide area networks (WWAN):

The signals used to build WWANs are typically supplied and maintained by individual mobile phone companies (Amit Agarwal, 2022). Wireless wide area networks (WWANs) can let you stay online even when you aren't close to a traditional network connection.

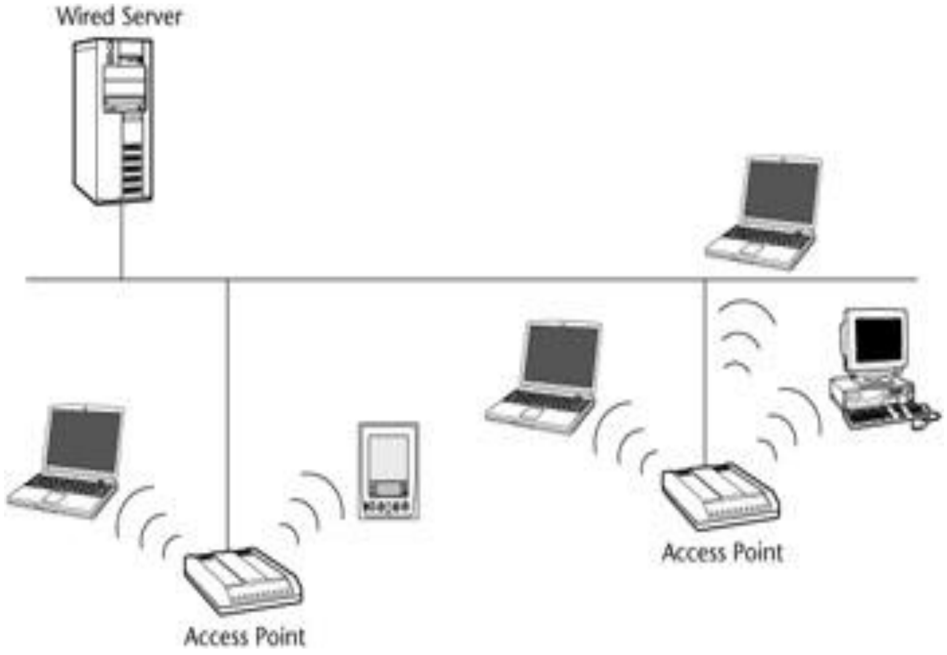

Figure. 1: wireless local area network

2.2.2. Wireless local area network (WLAN):

Local Area Networks (WLAN) are radio-based wireless data networks. Typically, cables are used for the backbone of a network, while wireless users connect to a wired network by one or more access points (Amit Agarwal, 2022). WLANs' coverage areas might be as little as one room or as large as an entire university.

2.2.3. Wireless personal area network (WPAN):

Wireless personal area networks (WPANs) are Bluetooth-based, short-range networks. They are frequently used to link together a group of devices in close proximity to a central hub, like a workstation. Commonly, the range of a WPAN is just approximately 30 inches (Amit Agarwal, 2022).

2.3. Wireless networking standards:

The importance of wireless networking in today's enterprises, both big and small, continues to grow. Learn how wireless LAN protocols stack up with this handy diagram (St. Petersburg, 2021). Managing, maintaining, and improving the quality of the network over the entire campus is a priority, and this includes the wireless component. Therefore, we anticipate that individuals and departments will not set up their own wireless infrastructure on campus, just as we anticipate that they would not establish their own hard-wired network equipment on campus (St. Petersburg, 2021). The term "wireless technology" encompasses not only routers, but also wireless printers, portable hotspots, and wireless speakers. Wireless networking presents more potential conflict zones with campus services than conventional networking does. Critical campus services may be jeopardized by channel allocations, device placement, and network name (SSID) setup. Wireless technology, in contrast to wired networks based on copper or fiber optic cables, necessitates a more complex, three-dimensional layout. Cisco Species are commonly Wireless Access Points, which support IEEE 802.11n and 802.11ac, and are the gold standard for wireless LAN hardware (St. Petersburg, 2021). Remember that wireless technology has always been developing, and that Campus Computing is always working to ensure that our network architecture meets the standards of the mobile sector.

3. Methodology:

3.1. Data collection:

Data that has usually come from secondary sources such as newspapers and the web. The security for wireless local area networks was analyzed using Direct Sequence Spread Spectrum (DSSS) methods.

3.2. Data analysis:

Direct Sequence Spread Spectrum (DSSS) is a technique that analyses data based on the transformation in which each bit of the original signal is transformed into a variable quantity of bits in the spread signal. This transformation is based on the original signal. The chipping code consists of a series or bits with a little higher bit rate than the data bits, and these bits can be multiplied with the data bits using the XOR operation to accomplish the desired result. This stream that is produced does, in fact, have a rate that is equivalent to the chip code, and it is then sent into a modulator, which converts it to an analog structure so that it may be broadcast. Spreading factors used in commercial systems range from 10 to 100, with 10 representing the lowest possible ratio for chip rate and 100 representing the highest possible ratio.

4. Findings and discussion:

Because of the growing need for bandwidth and the imperative to address latency issues, new possibilities have emerged in the realm of wireless communication. To enhance wireless transmission quality, defend better use of limited resources, offer additional stronger signal transmission quality, support multipath exclusion, and the double capacity without continuing to increase spectrum as well as antennas, businesses, and consumers are looking to nextgeneration networking systems like deep learning. However, there are significant limitations to developing traditional systems' architecture and processes. The wireless industry's goal is to provide better services at lower prices, analyze client wants, and also be better committed to assist needs, which motivates the industry to provide new and improved technology. Researchers and businesses agree that one of the wireless communication's primary goals is the simplified administration of complexities.

5. Conclusion:

In this research, we analyze wireless LAN safety and offer a solution that, if implemented, would allow organizations and individuals to provide their end users with a wirelessly secured channel. We've demonstrated in our work that a particular wireless LAN has insufficient security measures, or that those currently in place can be bypassed by skilled cybercriminals.

6. Reference:

(1) Amit agarwal, 2022. Types of wireless networks - digital inspiration. [Online] digital inspiration. Available at: <https://www.labnol.org/tech/types-of-wireless-networks/13667/> [accessed 23 July 2022]

(2) Chao yang and guofei gu, 2021. [Online] cic.ipn.mx. Available at: <http://www.cic.ipn.mx/~pescamilla/ms/papers_2014/yangandgu2013.pdf> [accessed 23 july 2022].

(3) Mobile wireless, 2021. Wireless local area networks (WLANs): chapter 3: wireless networks: part one: introduction to the mobile and wireless landscape: mobile and wireless design essentials: mobile devices: etutorials.org. [Online] etutorials.org. Available at: <http://etutorials.org/mobile+devices/mobile+wireless+design/part+one+introduction+to+the+mobile+and+wireless+landscape/chapter+3+wireless+networks/wireless+local+area+networks+wlans/> [accessed 23 July 2022].

(4) Networks, 2018. Wireless local area network security analysis: a case study of a wireless local area network – easy project materials. [Online] easyprojectmaterials.com.ng. Available at: <https://easyprojectmaterials.com.ng/project/wireless-local-area-network-

security-analysis-a-case-study-of-abu-wireless-local-area-network/> [accessed 23 july 2022].

(5) Souppaya, m. and scarfone, k., 2020. Guidelines for securing wireless local area networks (WLANs).

(6) Stpetersburg, 2021. [Online] stpetersburg.usf.edu. Available at: <https://www.stpetersburg.usf.edu/resources/computing/documents/wireless-network-standard.pdf> [accessed 23 july 2022].