EMERGING DIGITAL TECHNOLOGIES AND INTELLIGENT INFRASTRUCTURES

THE EVOLUTION OF WI-FI NETWORKS

CZU: 621.396(091)
DOI: https://doi.org/10.53486/tids2026.23

VICTOR ANDRONATIEV
Academy of Economic Studies of Moldova (ASEM)
e-mail: andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

AURELIU ZGUREANU
Academy of Economic Studies of Moldova (ASEM)
e-mail: zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

Abstract: In today's world, computer networks are utilized in almost every aspect of our lives (work, home, travelling). We use the Internet and its resources almost constantly. The Internet began by connecting computers with wired connections, but now in most cases, we use wireless connections. Since 2014, wireless traffic exceeded wired traffic, since 2015 on average 90% of the content accessed by users is video that means millions of minutes of video transmitted each second, and in 2020, due to the Internet of Things technologies, there were about 50 billion devices connected to the Internet.

As addressed by these facts, we see an importance placed on wireless networks and especially Wi-Fi networks, which are a part of local networks. In addition to Wi-Fi networks, we use many other wireless networks: satellite networks, mobile phone networks, metropolitan wireless networks. Wi-Fi networks hold the largest share, for the simple reason that they represent a high speed of access at a reasonable price. The first Wi-Fi standard 802.11 operated at a speed of 2 Mbps, today; the 802.11be (Wi-Fi 7) standard can reach speeds of approximately 40 Gbps.

That wireless networks are used in almost every aspect of our lives also brings with it certain demands: the need for higher and higher working speeds, use in new environments, security needs, etc. Furthermore, the fact that we are using wi-fi networks in various environments potentially brings different demands for the network. In most cases, users want high speed Internet access but on the other hand, in Internet of Things networks, where data volume is not so high, and only small equipment powered by a small battery are used, battery economy is a very important premise. Enterprise networks need increased security with the latest protocols of new equipment, a Radius server, etc. which raise latency in data traffic, whereas small networks or personal networks can run without a Radius server, etc. and therefore see a lower latency. The most secure protocols and operating systems run on new equipment but as we have seen when we attempt to connect old equipment incapable of operating in the new networks, the administrator must determine whether to continue using old equipment, or to attempt to keep using new equipment, resulting in additional costs. Taken together, these premise delineate both the relevance and importance of the topic on hand.

Keywords: Wi-Fi network, 802.11 network, Wi-Fi topology, BSS, IBSS, mesh BSS

JEL Classification: D85, L86

INTRODUCTION

The prevalence of Wi-Fi technology is so common that users continuously interact with it, without always being conscious of the complex nature and importance of Wi-Fi behind the scenes. Its continuous evolution, the exponential growth of connected devices, and the scale of its current growth, all speak to our collective reliance on Wi-Fi. Wi-Fi is the most common type of network for exchanging data without cables, supporting every activity imaginable, including surfing the Internet, social interaction, and critical business activities, as well as controlling smart homes. Everywhere Wi-Fi exists, it can typically be regarded as significant arteries for the flow of information, making Wi-Fi network security a primary concern.

MAIN CONTENT

1. Modern Wi-Fi digital infrastructure

1.1. The pressing need for Cybersecurity in the Wi-Fi Ecosystem

Although Wi-Fi offers users conveniences and productivity, an open network transmitting through the air creates particular security concerns (Bheevgade et al., 2023; Young, 2025). The properties of radio signal propagation, the mechanics of communication, and standardized schemes of transmission, make the characteristics of wireless of communication networks exceedingly vulnerable to eavesdropping and spoofing attacks. Eavesdropping and spoofing are further opportunistic by the fact that anything that travels over the air can be captured by anyone within range of the signal.

Wi-Fi technology progresses quickly, moving to increases in speed, capacity, and "fun" wireless technologies. New generations of Wi-Fi standards offer increased speed and an increased number of devices. Along with these improvements in performance and other qualities, Cybersecurity must adapt and respond with new protection strategies for the new vulnerabilities and threats introduced by the next generation. Thus, in order to create successful defenses, a good knowledge of the Wi-Fi architecture, security protocols and attacks is highly important.

1.2. Presentation of the structure and the aims of the article

The structure of this article is to provide a thorough and balanced study of Wi-Fi networks. It will begin by describing the technological principles of Wi-Fi networks, stemming from the development of the IEEE 802.11 standards and architecture. The article will then discuss security protocols, from old to new. The article will then propose best practices and risk management for users or organizations. The article intends, in totality, to support a well-informed and well-researched academic article contributing to the understanding and implementation of wi-fi networks.

2. Technological fundamentals of Wi-Fi networks

2.1. Evolution of IEEE 802.11 standards: from origins to Wi-Fi 7

IEEE 802.11 standards were created in 1997 with the intention to provide wireless connections of local area networks (WLAN), and for standardizing access to various frequency bands (Young, 2025). IEEE 802.11 can use several frequencies depending on the country and region in which it is being operated, but the frequencies that are most commonly used are: 2.4 GHz, 5 GHz, 6 GHz and 60 GHz. For security purposes, Wi-Fi networks used the WEP protocol from the beginning. Currently, WPA3 is the most recommended protocol. This standardization is significant in IT and cyber security because it provides explicit expectations, safety of measures, and helps ensure the

qualifications for products, and practices. standards encourages the utilization of new technologies, lowers the time and cost of development, and minimizes market risks. The historical progression of these standards has produced accelerated improvement of speed, range, and reliability of wireless networks.

802.11 (1997): The first standard, with a maximum bandwidth of 2 Mbps, operated in the 2.4GHz frequency band (Bolun, I., Andronatiev, V., 2014). However, it quickly became outmoded, as it was succeeded by 802.11b.

802.11a (1999) / Wi-Fi 2: Released in the same year as 802.11b, the 802.11a standard offered higher speeds of 54 Mbps and operated in the 5 GHz band. Although it operates at a faster speed, the 802.11a standard's higher signal frequency reduced the range and ability to penetrate physical barriers, thereby limiting its usage to business applications.

802.11b (1999) / Wi-Fi 1: The 802.11b standard had a maximum operating speed of 11 Mbps and operated in the 2.4 GHz band. Although it was slower than 802.11a, its overall lower costs extended its popularity and usage for the public. The 802.11b standard operated at a bandwidth of 20 MHz, was limited to a maximum of 11 Mbps, and was subject to interference from various 2.4 GHz devices like microwave ovens and cordless phones.

802.11g (2003) / Wi-Fi 3: This standard leveraged both the 802.11a and 802.11b standards that enabled speeds as high as 54 Mbps in the 2.4 GHz band. It used the same OFDM (Orthogonal Frequency-Division Multiplexing) based transmission scheme as 802.11a but, while it became widely accepted, it still experienced the interference problems caused by collisions typical of 802.11b in the crowded 2.4 GHz band.

802.11n (2009) / Wi-Fi 4: 803.11n was a giant leap in technology with MIMO (Multiple-Input Multiple-Output) technology, which utilizes multiple antennas to significantly increase speed and distance. 802.11n could utilize both the 2.4 GHz and 5 GHz bands, allowing for hardware that had capacity needs up to 600Mbps (Dell, 2024; CBT Nuggets, 2024). 802.11n also offered 20 and 40 MHz bandwidths. 802.11n is starting to become noticeable obsolete, but is likely "good enough" for some existing networks, if also older.

802.11ac (2013) / Wi-Fi 5: Widely used almost exclusively on the 5 GHz band, with speed above 1 Gbps. It has larger bandwidth options up to 160 MHz and introduced Multi-User MIMO (MU-MIMO) allowing access point to be able to send and receive information from multiple devices at once. 802.11ac began to standardize beamforming - a method to better focus the wireless signal for better optimized performance. While used often in denser environments, it is still in the majority of devices today, and is often the quickest and cheapest option today.

802.11ax (2019) / Wi-Fi 6 & Wi-Fi 6E: Optimized for high-density device environments, 802.11ax uses both the 2.4 GHz and 5 GHz bands. 802.11ax boasts speeds up to 9.6 Gbps and is optimized to allow multiple devices connecting at once while also providing better efficiency in terms of power played to all devices. Wi-Fi 6E takes advantage by providing another band with 6 GHz. The promise is less congestion and interference and faster speeds - future-proofing. Wi-Fi 6E devices must employ WPA3 encryption, the latest version of Wi-Fi encryption.

802.11be (2024) / Wi-Fi 7: Finally, the newest protocol is expected to promise theoretical peak speeds of greater than 40,000 Mbps (40 Gbps) operating on the 2.4/5/6 Ghz bands, (CBT Nuggets, 2024). Some devices are in testing with this protocol. Mass consumer use is still a few years away but, represents amazing speeds and predictability compared to wired networks.

The past history of the development of the Wi-Fi standard is a constant attempt of improved performance measures, speed, bandwidth, and capacity to manage devices. This constant throttling of longer throughput is a direct result of the demand for data and the increasing number of devices connected.

It should be noted that, both fast and slow frequencies and changes to primary working frequency bands have been made, with the frequency band challenge primarily moving in around the area of RF 2.4 GHz, and moving to RF 5 GHz, eventually to RF 6 GHz; the fast focus search was driven by data rate movement on new wireless protocols and devices (Bolun, I., Andronatiev, V., 2014). The frequency challenges that are found in RF 2.4, a common frequency for wireless devices, has in some ways been left neglected for those devices that are simply obsolete, causing congested conditions leading to breakdown as other RF devices in the home for example such as microwaves and Bluetooth devices degrade signal fidelity and reliability. While it is not perfect, migrating to less cluttered bands (5 GHz; 6 GHz) would by definition eliminate the "noise"... This reduction in interference is a performance benefit, but there are ancillary security benefits as well. A cleaner spectrum makes it more difficult for attackers to perform certain types of signal manipulation, eavesdropping, or jamming attacks, as their malicious signals would be more obvious or have less existing noise to blend into.

2.2. Basic Wi-Fi Network Model: MAC and PHY

The architecture model of Wi-Fi Networks are referenced based on the IEEE 802.11 standards. The 802.11 standards define a basic architecture model with two basic sublayers: the Media Access Control (MAC) sublayer and the Physical (PHY) sublayer. The standard outlines rooms for the MAC layer to design the optimal wireless communications network while meeting acceptable performance for the PHY layer provided everything is functioning.

Media Access Control (MAC) sublayer: Sometimes referred to as the "brain" of the network, the MAC layer coordinates and maintains all communications between the 802.11 stations (radio network cards and access points). The MAC layer allocates and hands-off the communications over a shared radio channel and will use protocols that are developed for assuring the reliability of communications in a wireless network. This is a subset of the hierarchy of basic functions that determine the overall performance. The MAC layer is responsible for (Wi-Fi Planet, 2024):

- Medium Access (DCF and PCF): The standard describes two forms of medium access in the standard: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is mandatory and is based on CSMA/CA protocol (carrier sense multiple access with collision avoidance). The model is very simple every 802.11 stations will compete for access, and will simply transmit frames when there are no other stations transmitting. If another station transmits a frame, stations will wait until the channel is clear. One of the important features of DCF is the random "back-off" timer a station employs if it finds the medium busy. This is to help prevent stations that want to send data at the same time from colliding with one another. PCF is an optional feature in which the access point polls a station, granting them access to the medium during the contention-free period, making it more useful for time-sensitive applications (like video). Most of today's wireless devices do not support PCF.
- Scanning: The MAC sublayer specifies both passive and active scanning, which is how a wireless network card can find accessible access points.

- Authentication: The process of proving identity, with two specified methods: open system authentication, and shared key authentication.
- Association: After authentication, a radio initiates association by sending an association request frame to the access point. The access point responds with an association response frame including an association ID and other details about the access point.
- 802.11 frame format: 802.11 frames are categorized into three primary types, management frames, control frames, and data frames, with each frame type having several subtypes (dot11AP, 2024).
    - Management frames: These are used by wireless stations for associating relating to a basic service set (BSS) and de-associating with a BSS. Management frames are the most common frame type in WLANs and include association request and response, probe request and response, beacons, authentication and de-authentication. Beacons are the "heartbeat" of the wireless network. Access points transmit beacons approximately 10 times per second. A beacon contains important information for client stations to know about the BSS parameters before trying to associate.
    - Control frames: These frames help deliver data frames and are transmitted at one of the basic rates. Control frames are used to release the channel, acquire the channel, and to send a unicast frame acknowledgement. Examples include Request to Send (RTS), Clear to Send (CTS), and Acknowledgement (ACK).
    - Data frames: These frames actually carry the data sent by higher-level protocols. Higher-layer data at layers 3-7 are conveyed as a MAC Service Data Unit (MSDU) payload, which is generally encrypted for data confidentiality.

PHY (Physical Layer): is responsible for carrier detection, transmission, and reception of 802.11 frames. The PHY is broken into three sub-layers (Tektronix, 2024):

- Physical Layer Convergence Procedure (PLCP): The PLCP is the adaptation layer, provides Clear Channel Assessment (CCA), forms packets for different physical layer technologies.
- Physical Medium Dependent (PMD): The PMD layer provides modulation and coding.
- PHY Management Layer: The PHY Management Layer is responsible for managing items like channel tuning.

The 802.11 standard originally defined three alternative physical layer technologies: diffuse infrared, frequency hopping spread spectrum and direct sequence spread spectrum, which all have data rates of 1 or 2 Mbps. Then 802.11b changed the game by increasing the data rates to 11 Mbps, using the same medium access method. Additionally, 802.11a introduced OFDM at 54 Mbps, and 802.11g combined the 2.4 GHz band along with the OFDM features from 802.11a to also achieve 54 Mbps. Since then, 802.11n added MIMO and higher bandwidths to the PHY so that much higher data rates can be achieved to fulfill future demand. There are many more standards that have followed and continue to evolve to continue to advance data rates.

2.3. Wi-Fi Network Topologies

Wi-Fi networks can be deployed in a number of different topologies, based upon the connectivity and scaling needs of the provider. These topologies are defined by the relationship between the access points (APs) and client stations and how they communicate and disperse their signal (dot11AP, 2024).

Infrastructure Mode (Basic Service Set - BSS): The most common topology involves all wireless devices (client stations) connecting to a central access point (AP). The AP operates as the hub, facilitating communication between the connected stations, and usually entitles the wireless network to connect with an existing wired connection (Internet). A BSS is identified by an SSID (Service Set Identifier). The SSID is the name of the Wi-Fi network. An Extended Service Set (ESS) is a collection of BSSs that are connected via distributed networks. ESS allows the client to seamlessly roam between APs.

Ad-Hoc Mode (Independent Basic Service Set - IBSS): In this topology, wireless devices have the potential to connect directly to one another in what is considered a construct less environment and with no central access point. Essentially, it is a peer-to-peer, or "one drop" network, that is often used for a quick form of file sharing between two or more devices in close proximity. While physically ad-hoc is simple to set-up, these networks tend to be insecure and cannot provide access to a wired network or the internet unless one of the devices has the capability to act as a gateway. Unlike a BSS, client stations can only transmit beacons when participating in an IBSS communication.

Mesh Networks: A mesh network consists of more than one access point or mesh nodes. Mesh networks can be thought of a dynamic self-organizing topology, where the access points communicate with each other to increase Wi-Fi coverage, provide expansive seamless connectivity in larger areas where typically, only multiple BSS's would be the solution. A mesh network is one of the types of wireless topologies that differs from a traditional topology in that instead of using a single router, it uses multiple access points in combination to provide the benefits of a single, extended-range network. This type of network is useful in larger homes or office space where a single router cannot adequately serve an entire area. Depending on the implementation, each mesh node has the capacity to be both a router and/or a repeater by directing data traffic toward the best destination, which can enhance performance and reliability.

Mixed Topologies: In practice, when Wi-Fi networks are deployed, they usually are of a mixed topology type which is equal parts infrastructure and mesh. For instance, the enterprise model is distinctly rigid with only managed APs able to determine which network to connect to, while adopting mesh (Wi-Fi later) may also be done to cover difficult to reach areas or provide temporary backhaul with different APs. This flexibility allows different combinations of performance and coverage to meet an individual's needs.

3. Security of Wi-Fi Networks

Unfortunately, security enhancements have often been reactive, as previous protocols have therefore lingered around as work-arounds or forms of upgrades to fix basic problems. A major challenge is "backward compatibility," or discarding the desperately floundering previous protocol, leaving oneself with legacy devices, as well as potential physical devices (or logic, if on some mixed HW configuration), which can and often do create security risks; a "network is as secure as its weakest link." Security has always been a second concern to speed; consequently, the Wi-Fi ecosystem is in a never ending state of which there is little use. The legacy burden of older devices and standards makes ownership of network security problematic, be it at home or enterprise level. When your network is based on a latest-standards Wi-Fi 6E supported by a Wi-Fi WPA3, the possible devices connecting to your network can again produce a headache; if devices connecting: WPA2, or worse, the infamous WEP? Future proofing and transitioning protocols that encourage but do not encourage 100% transitioning modes (WPA2/WPA3 Transitional; Apple, 2025) is important; ultimately, luck is an important security consideration too. Active management, log files and segmented networks are

and should be seen as part of the action, as old protocol and devices can never be completely eliminated.

The ubiquitous use of Wi-Fi networks in all areas of life, means users place higher expectations on them in terms of security. There are security methods in all current computer networks, however they are stronger with Wi-Fi networks. Due to the nature of a wired network, an unauthorized user must connect on that wired network, that is must connect to something in building, or in the network building. Wi-Fi presents a different challenge in that the unauthorized user can stand outside the building and see the packets being sent over the air. As a result, in the case of a WI-FI network must take additional measures of security, along with the existing ones or add an additional one in an attempt to provide a high level of security. Generally speaking, WEP was the original encryption standard for 802.11 networks, and it was used when wireless networks were first created in 1999. WEP was the first choice to be enabled in wireless networks based on its list of security features in all router configuration tools. WEP utilizes a 40-bit or 104-bit encryption key (password), manually entered at the wireless access point, static in nature, and never changes.

The WEP standard was replaced by WPA (Wi-Fi Protected Access) in 2003. WPA may also be added to existing wireless network cards designed for WEP with some adjustments to the firmware, a capability that is not provided with the IEEE 802.11i - Encryption Protect. The WPA protocol implements a subset of functions outlined in the IEEE 802.11i standard. In particular, WPA provides an implementation of TKIP (Temporal Key Integrity Protocol), which provides message integrity.

The next protocol developed is WPA2 (aka RSN - Robust Security Network), which implements the mandatory functions of the IEEE 802.11i standard voted into place in 2004. The main feature of WPA2 is the inclusion of CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). CCMP is AES (Advanced Encryption Standard) in a new mode of encryption with a good secure standard. CCMP and WPA2 uses 128-bit keys while using 128-bit data blocks, which provides increased security over TKIP. Specifically, breaking CCMP with 128-bit keys requires 2^{64} operations.

Launched in 2018, WPA3 is the latest and most secure Wi-Fi security protocol to date, intended to correct the flaws in WPA2 and offer more protection. The process of adopting WPA3 is yet to deliver, Although WPA3 is mandatory after our original cutoff date of July 2020 on devices displaying the "Wi-Fi CERTIFIED™" logo.

There are two alternatives for implementing WPA protocols (Bolun, I., Andronatiev, V., 2014):

- Enterprise, which must use a specific IEEE 802.1x authentication server (RADIUS server) and is typically used for relatively large networks seeking advanced security;
- Personal, which is also known as PSK (Pre-Shared Key) and does not require any specific authentication server, and is typically used for office or home networks that do not seek advanced security.

However, implementation of new most secure protocols is not enough. Subsequently the following general recommendations can be laid out to secure Wi-Fi networks (Apple, 2025; Andronatiev, 2018):

- Changing default passwords
- Restricting access
- Encrypting data on the network
- Installing a firewall
- Maintaining antivirus software

- Using file sharing with caution
- Regularly updating the access point firmware
- Disabling Wi-Fi when not in use

4. The Future of Wi-Fi Networks

As we have seen, the latest Wi-Fi 7 standard allows us to reach speeds of about 46 Gbps and for security the use of the WPA3 protocol is mandatory. The future consists of even greater increases in speeds, decreasing data transmission latency, and increasing security. It would seem that speeds of 46 Gbps are enough, but with the connection of new users, new equipment, and the wider integration of the Internet of Things (IoT), ever higher speeds are needed. This is easier to achieve with the integration of Artificial Intelligence (AI).

Machine learning algorithms allow networks to predict congestion and dynamically adjust channel settings to minimize interference (Zhang et al., 2022). Future networks will use the intelligence of IoT devices to map the radio environment, optimizing coverage, while the network, in turn, will provide an isolated and secure environment (micro-segmentation) for each class of devices (Patel, 2025). This segmentation is vital. In a smart home or factory, where the security system must communicate on the same channel as media entertainment devices. By using advanced spectrum management technologies, Wi-Fi will be able to create virtual "slices" of the network, dedicated to each specific need, guaranteeing both performance and critical isolation.

With the advent of quantum computers, existing security measures will not be able to cope. Nguyen and Smith (2023) argue that the implementation of quantum-resistant cryptography is necessary to protect data privacy in the long term. Here, again, AI comes to the rescue, where security can no longer be based on static rules. Implementing AI in security management enables real-time anomaly detection. An AI system that monitors Wi-Fi traffic can identify unusual behavior from an IoT device - for example, a temperature sensor trying to access unknown external servers - and automatically isolate it before a breach occurs (Zhang *et al.*, 2022). This "Zero Trust" approach is becoming the gold standard in enterprise networks.

CONCLUSION

In modern society, and further afield, as widely utilized internet it is used in a multiplicity of fields of activity with different specifications. The type of connection we are used to is wi-fi networks, and as it's convenient, and a reasonable price, and provides enough speed etc. Which means that the Wi-Fi networks must allow for connections of different types based on the field. Therefore, this article is about wi-fi networks: generations of wi-fi networks, bands used, description of layer 2 of the OSI model for wi-fi networks, network topologies, security of wi-fi networks.

As an example usually the user is looking for the highest possible speed, therefore requires the latest generations of wi-fi networks. In the specific case when the user finds a weak connection, meaning they are too far away from the access point, repeaters or 2.4 GHz bands can be implemented. If the client (enterprise) wants better security, the enterprise version can be implemented, but requires an authentication server, and higher costs etc. For the Internet of Things we do not require high speed, battery saving is more important. In this way, based on wi-fi networks, we can choose the necessary topology for our fields.

REFERENCES

Andronatiev, V., 2018. *Securitatea în rețele informatice***.** În: Conferința științifică internațională: „Competitivitatea şi inovarea în economia cunoașterii.” 22 – 23 septembrie 2017, ASEM, Chişinău, p. 129-134, 0,82 c.a., E-ISBN 978-9975-75-891-8.

Apple, 2025. *Recommended settings for Wi-Fi routers and access points*. Available at: https://support.apple.com/en-us/102766 (Accessed: 22 August 2025).

Bheevgade, P. et al., 2023. ‘The Rise of Public Wi-Fi and Threats’, *Lecture Notes in Electrical Engineering*. Available at: https://www.researchgate.net/publication/375230379_The_Rise_of_Public_Wi-Fi_and_Threats (Accessed: 22 August 2025).

Bolun, I., Andronatiev, V., 2014. *Internet şi Intranet.* Chişinău, ASEM, pp 275-329.

CBT Nuggets, 2024. *When to Use 802.11 a/b/g/b/n/ac Wi-Fi Standards*. Available at: https://www.cbtnuggets.com/blog/technology/networking/when-to-use-802-11-a-b-g-b-nc-wifi-standards (Accessed: 22 August 2025).

Dell, 2024. *Wi-Fi Network Standards Overview*. Available at: https://www.dell.com/support/contents/en-ke/article/product-support/self-support-knowledgebase/networking-wifi-and-bluetooth/wi-fi-network-standards-overview (Accessed: 22 August 2025).

dot11AP (2024) *802.11 Frame Format and Types*. Available at: https://dot11ap.wordpress.com/802-11-frame-format-and-types/ (Accessed: 22 August 2025).

Nguyen, T. and Smith, D. (2023). Post-Quantum Cryptography for Wireless Security. Cambridge: University Press.

Patel, J. (2025). IoT Connectivity and the Role of Wi-Fi 7. San Francisco: TechInsight Books.

Tektronix (2024) *Wi-Fi Overview: 802.11 Physical Layer and Transmitter Measurements*. Available at: https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements (Accessed: 22 August 2025).

Wi-Fi Planet (2024) *802.11 MAC Layer Defined*. Available at: https://wi-fiplanet.com/802-11-mac-layer-defined/ (Accessed: 22 August 2025).

Young, A. (2025). Detecting Wireless Security Threats Through IEEE 802.11 Frame Field Anomalies. *Honors Research Projects*. Available at:

https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=3686&context=honors_research_projects (Accessed: 22 August 2025).

Zhang, Z., Liu, Q. and Wang, F. (2022). Autonomous optimization of Wi-Fi networks using reinforcement learning. IEEE Access, 10, pp. 88400-88415.