Journal of Technology Research (JTR)
Volume 4, Special Issue, (2026), pp 810-824, ISSN 3005-639X
The 7th Conference of Engineering Sciences and Technology
(CEST-2025)

A Systematic Approach to Selecting the Proper WLAN Solution

Ahmed Jaha[*1], Anwar Alhenshiri[1]

[1] Department of Computer Science, Faculty of Information Technology, Misratah University, Misratah, Libya,
*Corresponding author email: goha_99@yahoo.com.

Received: 24-09-2025 | Accepted: 30-11-2025 | Available online: 03-01-2026| DOI:10.26629/jtr.2026.**

ABSTRACT

A Wireless Local Area Network (WLAN) utilizes radio frequency technology to enable communication within limited environments such as homes, enterprises, universities, and public spaces. Unlike wired networks, WLANs provide greater mobility, lower deployment costs, and enhanced flexibility and scalability. However, selecting the most proper WLAN solution remains a big challenge due to the varied and progressing users' requirements. By categorizing WLAN technologies based on their standards, architectural designs, and security features, this work offers a methodical framework to aid in the WLAN selection decision-making process. It also pinpoints important client needs and creates an organized mapping between these needs and matching WLAN setups. The study presents an improved logical model that assists users and businesses in choosing the most suitable WLAN solution, guaranteeing coherence between technical capabilities and organizational requirements.

Keywords: WLAN, 802.11, WiFi, AC, Fat AP, Fit AP, Cloud

طريقة منهجية لاختيار شبكة محلية لاسلكية مناسبة

أحمد جحا[1]، أنور الهنشيري[1]

[1]قسم علوم الحاسوب ، كلية تقنية المعلومات ، جامعة مصراتة ، مصراتة، ليبيا

ملخـــــص البحـــــث

تعتمد الشبكات المحلية اللاسلكية (WLAN) على الترددات الراديوية لتمكين الاتصال ضمن نطاقات محددة مثل المنازل، الجامعات، المؤسسات، والمناطق العامة. وتتميز هذه الشبكات عن نظيراتها السلكية بقدرتها العالية على توفير حرية الحركة للمستخدمين، وسهولة التركيب، وانخفاض تكاليف التنفيذ، مع قابلية أكبر للتوسع والتطوير. ومع ذلك، يمثل اختيار الحل المناسب للشبكات اللاسلكية تحديا كبيرا نظرا لتنوع متطلبات المستخدمين وتطورها المتمر. تتناول هذه الدراسة وضع إطار منهجي منظم يساعد في عملية اختيار الحلول المناسبة، حيث يقوم بتصنيف الشبكات المحلية اللاسلكية وفقًا لمعاييرها القياسية، وهياكلها المعمارية، وآليات الأمان التي تعتمدها. كما تستعرض الدراسة أبرز المتطلبات الفنية للمستخدمين، وتربطها مع الحلول المقترحة بشكل منهجي. أخيرا، تقدم الورقة نموذجًا منطقيًا مطوّرًا يساعد الأفراد والمؤسسات على اختيار الحل الأمثل للشبكة اللاسلكية المحلية بما يحقق التوازن بين الإمكانات التقنية والاحتياجات.

الكلمات الدالة: شبكة محلية لاسلكية، 802.11، WiFi، متحكم وصول (AC)، نقطة وصول ثخينة (Fat AC)، نقطة وصول أنيقة (Fit AC)، السحابة.

1. INTRODUCTION

In the past, wired networks faced a number of challenges, including high installation costs, limited scalability and flexibility, deployment difficulties, and inadequate mobility support. WLAN technologies have made significant advancements to overcome these challenges. WLANs, as opposed to wired networks, provide mobility and low deployment costs by using unlicensed radio frequencies [1]. This paper focuses on the classification of different WLAN solutions and the requirements that must be considered for selecting a proper WLAN solution. The detailed technical aspects of each WLAN solution are not discussed.

The paper presents a systematic approach that provides a broad overview of various classifications and requirements, supported by relevant tables and formulas. A WLAN matrix has been generated to map customer requirements to appropriate WLAN solutions. In addition, an enhanced logic formula has been proposed to help customers select an appropriate WLAN solution.

1.1 WLAN Standards

In July 1990, the IEEE 802.11 Working Group was established, which defined the standards related to the first and second layers of the TCP/IP model [2]. Wi-Fi can be considered as an implementation of WLAN technology. It works on 2.4 GHz, 5 GHz, and 6 GHz frequency bands, providing data rates ranging from 2 Mbps to 46 Gbps [3]. The latest released standards, IEEE 802.11n/ac/ax/be, improved WLAN features and performance [3][4].

WLAN technology based on IEEE 802.11n standard, Known as Wi-Fi 4, was announced in 2009, and introduced some new enhancements such as, multiple-input multiple-output (MIMO) technology, orthogonal frequency division multiplexing (OFDM) modulation, channel bonding, frame aggregation, and spatial multiplexing [4]. Wi-Fi 4 operates in both 2.4 GHz and 5 GHz bands, offering data rates of up to 600 Mbps [5].

In 2013, WLAN technology built on IEEE 802.11ac standard, also known Wi-Fi 5, was introduced, and presented numerous improvements. These improvements featured increased channel bandwidth (up to 160 MHz), more advanced modulation (up to 256-QAM), and multi-user MIMO (MU-MIMO) technology [2]. Wi-Fi 5 works only on the 5 GHz band and offers data rates of up to 6.9 Gbps [5].

WLAN technology based on IEEE 802.11ax standard, or Wi-Fi 6, was released in 2019, and brought several new advancements. These advancements comprised orthogonal frequency division multiple access (OFDMA), uplink MU-MIMO, target wake time (TWT), spatial reuse, and 1024-QAM modulation [4]. Wi-Fi 6 used both of the 2.4 GHz and 5 GHz frequency bands, delivering data rates of up to 9.6 Gbps [5].

In July 2025, WLAN technology advancements continue with the development of IEEE 802.11be, marketed as Wi-Fi 7, which focuses on Extremely High Throughput. Wi-Fi 7 has introduced revolutionary features, notably the use of 320 MHz channel bandwidths in the 6 GHz band, 4096-QAM modulation, and Multi-Link Operation (MLO), which allows devices to transmit and receive data simultaneously across multiple frequency bands (2.4, 5, and 6 GHz). This significantly reduces latency and increases overall throughput. Wi-Fi 7 is designed to support the next generation of applications, such as augmented reality (AR), virtual reality (VR), and 8K streaming, theoretically delivering data rates up to 46 Gbps [3].

Table 1 shows the most widely used WLAN technologies based on the IEEE 802.11 standards

Table 1. WLAN Technologies.

Standard		Physical Layer Technologies	Frequency Band	Max Data Rate
-	802.11	FHSS, SSS/DQPSK	2.4 GHz	2 Mbps
-	802.11b	DSSS/CCK	2.4 GHz	11 Mbps
-	802.11a	OFDM/64-QAM	5 GHz	54 Mbps
-	802.11g	OFDM/64-QAM	2.4 GHz	54 Mbps
Wi-Fi 4	802.11n	OFDM/64-QAM	2.4/5 GHz	600 Mbps
Wi-Fi 5	802.11ac	OFDM/256-QAM, DL MU-MIMO	5 GHz	6.9 Gbps
Wi-Fi 6	802.11ax	OFDMA/1024-QAM, DL/UL MU-MIMO	2.4/5 GHz	9.6 Gbps
Wi-Fi 7	802.11be	OFDMA/4096-QAM, MLO	2.4/5/6 GHz	46 Gbps

1.2 Related Work

Over the past 20 years, research on WLAN technology has been increasingly important in terms of both theory and application. A wide range of WLAN performance, security, and deployment options have been the subject of investigation. In the work of [6], the author examined several Wi-Fi network management topics, including the architecture and standards of IEEE 802.11 WLAN networks, planning and constructing WLAN networks, and controller-based wireless architecture. In the extensive survey described in [5], a detailed comparative investigation of the IEEE 802.11 family of protocols was conducted. The study covered the years 1999 to 2020. While focusing on important factors including range, channel bandwidth, RF band, data rate, and modulation type, the study looked at different versions of the IEEE protocol. The design and setup of a Wi-Fi 6 network to replace the wired network in an enterprise setting [7] was examined. The study included security issues, best placement procedures for access points, and a detailed research of Wi-Fi 6.

In the research described in [8], the researchers examined the development, encryption techniques, and known weaknesses of the Wi-Fi Protected Access 3 (WPA3). The study reviewed 36 publications from 2018 to 2023 and highlighted the improvements made in WPA3 over earlier protocols such as WEP, WPA, and WPA2. A profound review of WLAN technology was given in [9]. The research tested various WLAN topologies, including the Fat AP and AC+Fit AP architectures. Fat APs independently managed functions like wireless user access, encryption, and data forwarding. The AC+Fit AP architecture applied a centralized control through an access controller (AC) that manages access control, configuration, roaming, and security of the Fit APs.

Previous researches offered a strong foundation for understanding various facets of WLAN technology, architecture, and security measures. This work expands previous efforts by providing a well-defined classification of WLAN solutions and attempting to identify the essential customer needs when setting up a WLAN.

On the other hand, research [10] presented a comprehensive study on virtual private networks (VPNs), provided a systematic categorization of VPN solutions, identified the main requirements of VPN customers, and proposed a VPN matrix and a logical formula to assist in the process of selecting an appropriate VPN solution. However, it was limited to

specifying only two values for each need (low or high).

This work presents a WLAN matrix to match customer requirements (where more than two values can be assigned to each requirement) with a proper WLAN solution. In addition, a novel WLAN logic formula has been generated to help with the WLAN selection process.

1.3 Research Methodology

A mixed methodology was used by integrating qualitative criteria with quantitative modeling. This approach consists of the following steps:

- A detailed literature review on WLAN technologies, standards, and selection factors was conducted. This step includes books, academic papers, industrial white papers, and technical standards.
- Constructing a classification system for WLAN solutions, and taking into account factors like standards, architectures, and security rules.
- The main requirements for implementing a WLAN were defined and analyzed, such as coverage area, user density, scalability, security, cost, and flexibility support.
- Leveraging the data gathered in the previous steps, a WLAN matrix has been created to connect the desired requirements with a proper solution.
- Proposing a logical formula that can be used to guide the process of choosing an appropriate WLAN solution.
- A hypothetical scenario has been used to validate the usability of the proposed model in real-world scenarios.

This methodology, which integrates theoretical concepts and practical factors, provides a systematic approach to help the procedure of choosing a proper WLAN solution.

2. WLAN CLASSIFICATION

There are various types of WLANs available. This section provides a brief overview of some WLANs mentioned in the literature. It is important to note that WLAN categorization can be challenging due to potential overlaps. WLANs can be classified in multiple ways, some of which are described in Table 2

Table 2. Classification of WLANs.

<table>
<tr><th>Infrastructureless WLANs</th><th colspan="4">Infrastructure WLANs</th></tr>
<tr><td rowspan="2">Ad Hoc</td><td>Autonomous architecture</td><td colspan="3">Controlled Architecture</td></tr>
<tr><td rowspan="2">Fat AP</td><td rowspan="2">Leader AP</td><td colspan="2">AC+Fit AP</td><td rowspan="2">Cloud managed</td></tr>
<tr><td>Layer 2 networking</td><td>Layer 3 networking</td></tr>
</table>

WLANs can be classified as infrastructure WLANs or infrastructure-less WLANs. In infrastructure WLANs, a central access point (AP) serves as a bridge that connects wireless clients to the wired network infrastructure. This topology is highly scalable, allows central network management, offers a large coverage area, and is commonly used in public Wi-Fi networks, enterprise networks, and home networks [11].

In infrastructure-less WLANs, also known as Ad Hoc WLANs, the wireless devices can communicate directly with each other without the need for an infrastructure network. They can form a temporary network. This topology is peer-to-peer communication and it does not

enable central network management. It is less scalable than infrastructure WLANs, has a limited coverage area, and is commonly used in temporary networks, emergencies, and remote areas [11].

According to the architecture categorization, WLAN solutions can be divided into Autonomous and Controlled WLANs. In the autonomous architecture, Fat AP is an access point that operates independently without any reliance on another centralized control device. Fat AP can implement functions such as wireless user access, service data encryption, and service data packet forwarding. If the WLAN coverage area and the number of users are increased, more Fat APs are required and cannot be easily managed or maintained. Therefore, autonomous architecture is suitable for small-office home-office (SOHO) WLANs [9]. Controlled architecture WLANs require a centralized mechanism to manage and configure the connected APs [9]. It can be classified into AC+Fit AP, Cloud management, and Leader AP.

In AC+Fit AP architecture, the AC communicates with Fit APs through control and provisioning wireless access points (CAPWAP). An access control (AC) is responsible for WLAN access control, data forwarding, AP configuration and monitoring, roaming management, and security control. This architecture is characterized by ease of configuration and deployment, high security, and simplicity of update and expansion. Therefore, it is appropriate for large and medium-sized WLANs [9]. Cloud management platform manages and configures WLAN entities in a central unified manner. Plug-and-play and automatic deployment are used to reduce network deployment costs. This architecture is proper for widely distributed WLANs due to its flexible deployment and low operation and maintenance costs [6].

Leader AP architecture involves APs only. One AP is configured as a leader AP. It controls the connection of other APs to the network in the Fit AP mode. The leader AP provides unified access, management, configuration, and continuous roaming experience. This architecture is not expensive and it is suitable for small-sized WLANs where a few APs are required due to the small number of STAs and the small wireless coverage area [12].

AC + Fit AP WLANs can be divided into layer 2 and layer 3 networking WLANs. In Layer 2 networking, the AC and Fit APs are placed in the same broadcast domain. The Fit APs can discover the AC through local broadcast. The configuration, and management of this networking are simple. Therefore, it is applicable for medium-scale networks. In Layer 3 networking, the AC and Fit APs are located in different network segments. The intermediate network must ensure that the Fit APs and AC are reachable to each other. Additional configurations are required to enable the Fit APs to discover the AC. Layer 3 networking is suitable for large-scale networks [9].

3. WLAN SECURITY

WLAN technology uses radio signals to transmit service data, which means that service data can easily be captured or altered by attackers when sent over open wireless channels. WLAN security mechanisms ensure the security of the user's data of sent via a wireless network. WLAN security policies have a series of security mechanisms, including authenticity to confirm the validity of user access on the wireless network, confidentiality to protect transmitted data from being captured by unauthorized users, and integrity to protect data from being altered by attackers.

WLAN available security policies include Open security, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3 [13]. Open security policy requires no authenticity, no confidentiality, and no integrity mechanisms. WEP security policy supports open and shared key authentication. It uses Rivest Cipher 4 (RC4) algorithm to encrypt data includes Cyclic Redundancy Code (CRC-32) to

validate data integrity. WEP uses a static key. All STAs associated with the same SSID use the same key to join a WLAN [8], [14].

WPA security policy defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm, supports Pre-Shared Key (PSK) authentication protocol, and uses Message Integrity Code (MIC) to protect transmitted data from being captured or changed [8], [14]. WPA2 security policy uses Cipher Block Chaining Message Authentication Code (CBC-MAC) to validate data integrity, defines Advanced Encryption Standard (AES) in Counter Mode with CBC-MAC Protocol (CCMP) to ensure confidentiality, and supports PSK authentication protocol for WPA2 personal and 802.1x for WPA2 enterprise [8], [14]. WPA3 security policy replaces PSK with Simultaneous Authentication of Equals (SAE) protocol for authenticity, uses AES in Galois/Counter Mode (GCM) for encryption, and defines Secure Hash Algorithm (SHA) for data integrity [8], [14]. Table 3 listed the following available security policies.

Table 3. WLAN Security Policies

WLAN Security Policy	Authentication	Encryption	Data Integrity	Security level
Open	No	No	No	Very weak
WEP	Open/Shared key	RC4	CRC-32	Weak
WPA	PSK	TKIP	MIC	Moderate
WPA2	PSK/802.1x	AES-CCMP	CBC-MAC	High
WPA3	SAE/802.1x	AES-GCM	SHA	Very High

4. WLAN REQUIREMENTS

In order to decide what WLAN solutions to choose, the selected solution should be the one that best meets the requirements of the customer. Some of the key requirements that must be considered are discussed in the following sections.

4.1 Coverage Area

Determining the required coverage area for customers and ensuring that the WLAN solution can provide adequate and consistent signal strength throughout the entire area are essential considerations [15]. Fat AP WLAN solution is well suited for SOHO networks, as increasing the coverage area needs increasing the number of Fat APs required, which can't be easily managed or maintained [9]. Ad- Hoc WLAN solutions are suitable for very small temporary networks with limited coverage area. In addition, the infrastructure should either be unavailable or unnecessary such as unarranged meetings or emergency scenarios [11]. A Leader AP WLAN solution is a good choice for small scale networks where a few APs are required due to the small number of STAs and the small wireless coverage area [12]. Layer 2 AC+Fit APs WLAN solutions are inapplicable for complex networks because the AC and Fit APs are in the same broadcast domain [9]. Layer 3 AC+Fit APs WLAN solutions are more suited for medium- to large- scale networks where the AC and Fit APs are in different network segments [9]. Cloud managed WLAN solutions are appropriate for networks that are distributed over widely separated areas [6].

4.2 User Density

User density is the evaluation of the maximum number of concurrent users who will connect to the WLAN simultaneously. Moreover, it includes the density of users in specific areas [7]. WLAN solutions based on older standards like 802.11a/b/g may struggle in high-density environments due to their lower data rates and

lack of advanced features [4]. WLAN solutions based on 802.11n standard (Wi-Fi 4) introduced technologies like MIMO and channel bonding, which improved capacity and throughput, making it better suited for moderate-density environments [5]. However, for high-density scenarios, the more recent 802.11ac standard (Wi-Fi 5), 802.11ax standard (Wi-Fi 6), and 802.11be standard (Wi-Fi 7) are preferred. Those standards offer advanced features like MU-MIMO, OFDMA, and higher-order modulation. As a result, efficient handling of a large number of simultaneous connections is enabled while maintaining optimal performance [3][5].

4.3 Scalability

Scalability is selecting a solution that can easily be expanded to accommodate future growth. In other words, it means the ability to expand the network as the number of users and devices grow [16]. Ad Hoc and Fat AP WLAN solutions offer minimal scalability where they make it challenging to manage a growing network beyond a few devices [17]. Leader AP solutions provide better scalability for small networks but may struggle as the network expands beyond a certain point [2]. AC+Fit AP solutions offer high scalability due to the centralized management and easy addition of new access points to expand coverage or capacity [18]. Cloud-managed WLAN solutions guarantee the highest degree of scalability, allow organizations to easily add new sites or expand existing networks without significant infrastructure changes. This kind of solutions provides the ability to upgrade to newer standards or technologies as they become available. Moreover, it ensures long-term scalability and future-proofing of the network infrastructure [18].

4.4 Security

Security ensures the WLAN solution supports policies to protect the network and its users. WLAN solutions established with open security policy suffer from very weak security levels due to absence of authentication, encryption, data integrity, and key management mechanisms [13]. WLAN solutions based on WEP security policy provide weak security levels because they use low authentication, encryption, data integrity, and key management procedures such as shared key, RC4, CRC-32, and static algorithms [19]. WLAN solutions created with WAP security policy offer a moderate security level as they add PSK authentication, TKIP encryption, MIC data integrity, and pre-shared key management techniques [19]. WLAN solutions based on WAP2 provide high security levels due to the use of strong authentication, encryption, data integrity, and key management methods like PSK/802.1x, AES-CCMP, CBC-MAC, and 802.1x/EAP algorithms [19]. WLAN solutions based on WAP3 offer very high security levels since they incorporate SAE/802.1x authentication, AES-GCM encryption, SHA data integrity, and 802.1x/EAP key management mechanisms [19].

4.5 Cost

That is evaluating the total cost of ownership (TCO) of the WLAN solution including initial hardware and software costs, installation expenses, licensing fees, and ongoing maintenance costs [20]. Ad Hoc WLAN solutions typically have the lowest cost as they require no additional infrastructure beyond the hardware used. Fat AP and Leader AP WLAN solutions often have lower costs due to the absence of expensive AC devices. AC+Fit APs solutions typically have higher costs because they incorporate expensive AC devices to centrally manage and maintain the network. Cloud-managed WLAN solutions often use a subscription-based model, which can reduce upfront costs and provide more predictable ongoing expenses. Nonetheless, the long-term costs of cloud solutions should be carefully evaluated against on-premises alternatives.

4.6 Flexibility Support

That is evaluating the ability to quickly establish networks in unpredictable environments such as emergency services, military operations, or temporary event setups [21]. Ad Hoc WLAN solutions excel in scenarios requiring immediate network establishment without a pre-existing infrastructure due to self-organizing, dynamic topology, location change support, and disaster recovery characteristics. Other WLAN solutions generally require more setup time and fixed infrastructure which limits the flexibility support [11].

5. CHOOSING A PROPER WLAN SOLUTION

Creating a WLAN is not simple due to the fact that there are many different WLAN solutions available. Nonetheless, deciding which one to choose can be difficult since they each of which has its own advantages and disadvantages.

Based on the collected information in the previous sections, WLAN matrix has been generated to show how different customer requirements can be systematically mapped to an appropriate WLAN solution. Then, a WLAN logic formula has been derived to guide the process of choosing proper WLAN solution.

5.1 WLAN Matrix

Table 4 shows the proposed WLAN matrix that is going to organize the collected information, map requirements to appropriate solutions, and help customers to select a proper WLAN solution. It is clearly shown that AC+Fit AP Layer2 WLAN solution is a suitable WLAN solution for the customers with medium coverage area requirement.

Table 4. WLAN Matrix

WLAN requirements	Value	Proper solution
Coverage Area	SOHO	Fat AP WLAN solution
	Small	Ad Hoc WLAN solution
		Leader AP WLAN solution
	Medium	AC+Fit AP Layer2 WLAN solution
	Large	AC+Fit AP Layer3 WLAN solution
	Widely	Cloud managed WLAN solution
Users Density	Low	WLAN solution based on 802.11a/b/g standards
	Medium	WLAN solution based on 802.11n standard (Wi-Fi 4)
	High	WLAN solution based on 802.11ac/ax standard (Wi-Fi
	Very High	WLAN solution based on 802.11be standard (Wi-Fi 7)
Scalability	Low	Ad Hoc WLAN solution
		Fat AP WLAN solution
	Medium	Leader AP WLAN solution
	High	AC+Fit AP Layer2 WLAN solution
		AC+Fit AP Layer3 WLAN solution
	Very High	Cloud managed WLAN solution
Security	Very Low	WLAN solution with Open security policy
	Low	WLAN solution with WEP security policy
	Medium	WLAN solution with WAP security policy

	High	WLAN solution with WAP2 security policy
	Very High	WLAN solution with WAP3 security policy
Cost	Low	Ad Hoc WLAN solution
		Fat AP WLAN solution
	Medium	Leader AP WLAN solution
	High	Cloud managed WLAN solution
	Very High	AC+Fit AP Layer2 WLAN solution
		AC+Fit AP Layer3 WLAN solution
Flexibility Support	High	Ad Hoc WLAN solution
	Low	Other WLAN solutions

5.2 WLAN Formula

In this section, a logical formula has been developed to simplify the WLAN solution choosing process. Tables 5 and 6 show symbols used in this formula to represent WLAN solutions and WLAN customer requirements respectively.

Each WLAN requirement can take more than two values (high, low). For example, symbols CA_1, CA_2, CA_3, CA_4, and CA_5 are assigned to SOHO, small, medium, large, and wide distributed WLAN coverage area requirements respectively.

Table 5. WLAN Solutions Symbols

WLAN Solution	Symbol
Ad Hoc WLAN solution	S_1
Fat AP WLAN solution	S_2
Leader AP WLAN solution	S_3
AC+Fit AP Layer2 WLAN solution	S_4
AC+Fit AP Layer3 WLAN solution	S_5
Cloud managed WLAN solution	S_6
WLAN solution based on 802.11a/b/g standards (Wi-Fi 1-3)	$W_{1\text{-}3}$
WLAN solution based on 802.11n standard (Wi-Fi 4)	W_4
WLAN solution based on 802.11ac/ax standard (Wi-Fi 5/6)	$W_{5/6}$
WLAN solution based on 802.11be standard (Wi-Fi 7)	W_7
WLAN solution with Open security policy	P_1
WLAN solution with WEP security policy	P_2
WLAN solution with WAP security policy	P_3
WLAN solution with WAP2 security policy	P_4
WLAN solution with WAP3 security policy	P_5

Table 6. WLAN Requirements Symbols

WLAN requirements	Symbol		Value
Coverage Area	CA	CA_1	SOHO area (CA_1 =1) and ($CA_{2,3,4,5}$ = 0)
		CA_2	Small area (CA_2 =1) and ($CA_{1,3,4,5}$ = 0)
		CA_3	Medium area (CA_3 =1) and ($CA_{1,2,4,5}$ = 0)

		CA_4	Large area (CA_4 =1) and ($CA_{1,2,3,5}$ = 0)
		CA_5	Wide distributed area (CA_5=1) and ($CA_{1,2,3,4}$ =
Users Density	*UD*	UD_1	Low density (UD_1 =1) and ($UD_{2,3.4}$ = 0)
		UD_2	Medium density (UD_2 =1) and ($UD_{1,3,4}$ = 0)
		UD_3	High density (UD_3 =1) and ($UD_{1,2,4}$ = 0)
		UD_4	Very high density (UD_4 =1) and ($UD_{1,2,3}$ = 0)
Scalability	*SC*	SC_1	Low scalability (SC_1 =1) and ($SC_{2,3,4}$ = 0)
		SC_2	Medium scalability (SC_2 =1) and ($SC_{1,3,4}$ = 0)
		SC_3	High scalability (SC_3 =1) and ($SC_{1,2,4}$ = 0)
		SC_4	Very high scalability (SC_4 =1) and ($SC_{1,2,3}$ = 0)
Security	*SE*	SE_1	Very low level (SE_1 =1) and ($SE_{2,3,4,5}$ = 0)
		SE_2	Low level (SE_2 =1) and ($SE_{1,3,4,5}$ = 0)
		SE_3	Medium level (SE_3 =1) and ($SE_{1,2,4,5}$ = 0)
		SE_4	High level (SE_4 =1) and ($SE_{1,2,3,5}$ = 0)
		SE_5	Very high level (SE_5 =1) and ($SE_{1,2,3,4}$ = 0)
Cost	*CO*	CO_1	Low cost (CO_1 =1) and ($CO_{2,3,4}$ = 0)
		CO_2	Medium cost (CO_2 =1) and ($CO_{1,3,4}$ = 0)
		CO_3	High cost (CO_3 =1) and ($CO_{1,2,4}$ = 0)
		CO_4	Very high cost (CO_4 =1) and ($CO_{1,2,3}$ = 0)
Flexibility Support	*FS*	FS_1	Low support (FS_1 =1) and (FS_2 = 0)
		FS_2	High support (FS_2 =1) and (FS_1 = 0)

Tables 4, 5, and 6 are used to develop a logic formula for each WLAN requirement. For example, WLAN coverage area requirement logic formula can be derived from the first six proper solution rows in the WLAN matrix shown in table 4:

$$WLAN_{CA} = CA_1 . (S_2) + CA_2 . (S_1 + S_3) + CA_3 . (S_4) + CA_4 . (S_5) + CA_5 . (S_6) \quad (1)$$

where:

$CA_1 . (S_2)$ illustrates that Fat AP WLAN solution is the suitable WLAN solution for SOHO coverage area.

$CA_2 . (S_1 + S_3)$ demonstrates that Ad Hoc WLAN solution or Leader AP WLAN solution are the right WLAN solutions for small coverage area.

$CA_3 . (S_4)$ depicts that AC+Fit AP Layer2 WLAN solution is the best WLAN solution for medium coverage area.

$CA_4 . (S_5)$ shows that AC+Fit AP Layer3 WLAN solution is the proper WLAN solution for large coverage area.

$CA_5 . (S_6)$ indicates that Cloud managed WLAN solution is the appropriate WLAN solution for widely distributed coverage area.

The same criteria can be used to derive the other WLAN customer requirements logic formulas.

$$WLAN_{SC} = SC_1 . (S_1 + S_2) + SC_2 . (S_3) + SC_3 . (S_4 + S_5) + SC_4 . (S_6) \quad (2)$$

$$WLAN_{CO} = CO_1 . (S_1 + S_2) + CO_2 . (S_3) + CO_3 . (S_6) + CO_4 . (S_4 + S_5) \quad (3)$$

$$WLAN_{FS} = FS_1 . (S_2 + S_3 + S_4 + S_5 + S_6) + FS_2 . (S_1) \quad (4)$$

$$WLAN_{UD} = UD_1 . (W_{1\text{-}3}) + UD_2 . (W_4) + UD_3 . (W_{5/6}) + UD_4 . (W_7) \quad (5)$$

$$WLAN_{SE} = SE_1 . (P_1) + SE_2 . (P_2) + SE_3 . (P_3) + SE_4 . (P_4) + SE_5 . (P_5) \quad (6)$$

where:

$WLAN_{CA}$ is the WLAN coverage area requirement logic equation.

$WLAN_{SC}$ is the WLAN scalability requirement logic equation.

$WLAN_{CO}$ is the WLAN cost requirement logic equation.

$WLAN_{FS}$ is the WLAN flexibility support requirement logic equation.
$WLAN_{UD}$ is the WLAN user density requirement logic equation.
$WLAN_{SE}$ is the WLAN security requirement logic equation.

By taking the common terms using intersection operation from (1) and (2), the formula that indicates the requirements of coverage area and scalability is obtained:

$$\begin{aligned} WLAN_{CA+SC} = {} & CA_1 \,.\, SC_1 \,.\, (S_2) \\ & + CA_2 \,.\, SC_1 \,.\, (S_1) \\ & + CA_2 \,.\, SC_2 \,.\, (S_3) \\ & + CA_3 \,.\, SC_3 \,.\, (S_4) \\ & + CA_4 \,.\, SC_3 \,.\, (S_5) \\ & + CA_5 \,.\, SC_4 \,.\, (S_6) \end{aligned} \quad (7)$$

By taking the common terms using intersection operation from (7) and (3), the formula that denotes the requirements for each of coverage area, scalability, and cost is formed:

$$\begin{aligned} WLAN_{CA+SC+CO} = {} & CA_1 \,.\, SC_1 \,.\, CO_1 \,.\, (S_2) \\ & + CA_2 \,.\, SC_1 \,.\, CO_1 \,.\, (S_1) \\ & + CA_2 \,.\, SC_2 \,.\, CO_2 \,.\, (S_3) \\ & + CA_3 \,.\, SC_3 \,.\, CO_4 \,.\, (S_4) \\ & + CA_4 \,.\, SC_3 \,.\, CO_4 \,.\, (S_5) \\ & + CA_5 \,.\, SC_4 \,.\, CO_3 \,.\, (S_6) \end{aligned} \quad (8)$$

By taking the common terms using intersection operation from (8) and (4), the formula that represents the requirements for each of coverage area, scalability, cost, and flexibility support is produced:

$$\begin{aligned} WLAN_{CA+SC+CO+FS} = {} & CA_1.\, SC_1.\, CO_1.\, FS_1.\, (S_2) \\ & + CA_2.\, SC_1.\, CO_1.\, FS_2.\, (S_1) \\ & + CA_2.\, SC_2.\, CO_2.\, FS_1.\, (S_3) \\ & + CA_3.\, SC_3.\, CO_4.\, FS_1.\, (S_4) \\ & + CA_4.\, SC_3.\, CO_4.\, FS_1.\, (S_5) \\ & + CA_5.\, SC_4.\, CO_3.\, FS_1.\, (S_6) \end{aligned} \quad (9)$$

By simplifying (9), the logic formula will be:

$$\begin{aligned} WLAN_{CA+SC+CO+FS} = {} & FS_2 \,.\, CA_2 \,.\, SC_1 \,.\, CO_1 \,.\, (S_1) \\ & + FS_1 \,.\, [CA_1 \,.\, SC_1 \,.\, CO_1 \,.\, (S_2) \\ & + CA_2 \,.\, SC_2 \,.\, CO_2 \,.\, (S_3) \\ & + CA_3 \,.\, SC_3 \,.\, CO_4 \,.\, (S_4) \\ & + CA_4 \,.\, SC_3 \,.\, CO_4 \,.\, (S_5) \\ & + CA_5 \,.\, SC_4 \,.\, CO_3 \,.\, (S_6)] \end{aligned} \quad (10)$$

By rearranging (10), the logic formula will be:

$$\begin{aligned} WLAN_{CA+SC+CO+FS} = {} & FS_2 \,.\, CA_2 \,.\, SC_1 \,.\, CO_1 \,.\, (S_1) \\ & + FS_1 \,.\, [CA_1 \,.\, SC_1 \,.\, CO_1 \,.\, (S_2) \\ & + CA_2 \,.\, SC_2 \,.\, CO_2 \,.\, (S_3) \\ & + SC_3 \,.\, CO_4 \,.\, (CA_3 \,.\, (S_4) \\ & + CA_4 \,.\, (S_5)) \\ & + CA_5.\, SC_4.\, CO_3.\, (S_6)] \end{aligned} \quad (11)$$

By merging logic formulas indicated in (11), (5), and (6), the following proper WLAN solution logic equation is generated:

$WLAN_{ProperSolution} = WLAN_{CA+SC+CO+FS}$ based on $WLAN_{UD}$ standard and using $WLAN_{SE}$ security policy (12)

5.3 WLAN Logic Formula Validation

The usability and effectiveness of the above logic formula can be evaluated using a scenario-based validation method to demonstrate how the proposed logic formula can be applied to real-world situations. For example, an Information Technology College (ITC) at Misratah University asked the IT department to implement a WLAN solution that ensures seamless connectivity and meets the following requirements:

- **Coverage area**: WLAN solution services must be available to multiple departments that occupy medium coverage area (CA_3=1).
- **User density**: As the number of students and employee are increased exponentially, the WLAN solution has to be capable to handle high concurrent connections (UD_3=1).
- **Scalability**: The WLAN solution needs to have the ability to support future growth without major changes (SC_3=1).
- **Security**: Since the college deals with sensitive data, the WLAN solution has to guarantee very high security level (SE_5 =1).
- **Cost**: The above mentioned high standards require very high cost requirement (CO_4 =1).

- **Flexibility support**: WLAN solution will concentrate on permanent installation rather than unpredictable environment (FS_1 =1).

By substituting the WLAN requirements symbols by the above values in (11), (5), (6), and (12), the proper WLAN solution can be obtained:

$$WLAN_{CA+SC+CO+FS} = 0 \,.\, 0 \,.\, 0 \,.\, 0 \,.\, (S_1) + 1 \,.\, [0 \,.\, 0 \,.\, 0 \,.\, (S_2) + 0 \,.\, 0 \,.\, 0 \,.\, (S_3) + 1 \,.\, 1 \,.\, (1. (S_4) + 0 \,.\, (S_5)) + 0 \,.\, 0 \,.\, 0 \,.\, (S_6)]$$

$$WLAN_{CA+SC+CO+FS} =. S_4$$

$$WLAN_{UD} = 0. (W_{1\text{-}3}) + 0. (W_4) + 1. (W_{5/6}) + 0. (W_7)$$

$$WLAN_{UD} = W_{5/6}$$

$$WLAN_{SE} = 0. (P_1) + 0. (P_2) + 0. (P_3) + 0. (P_4) + 1. (P_5)$$

$$WLAN_{SE} = P_5$$

$WLAN_{ProperSolution}$ = $WLAN_{CA+SC+CO+FS}$ based on $WLAN_{UD}$ standard and using $WLAN_{SE}$ security policy

$WLAN_{ProperSolution}$ = S_4 based on $W_{5/6}$ standard and using P_5 security policy

which means that, the proper WLAN solution is an AC+Fit AP Layer2 WLAN solution based on 802.11ac/ax standard (Wi-Fi 5/6) and using WAP3 security policy.

6. DISCUSSION RESULTS

The WLAN matrix and logical formula developed in this study present multiple advantages to the WLAN selection process by providing a systematic and data-driven framework for evaluating different WLAN architectures. This approach helps decision-makers match technical capabilities with user requirements more effectively and ensures consistency, accuracy, and transparency in the selection process. The aforementioned advantages are described as follows.

- **Comprehensiveness**: The method addresses multiple factors, such as the most recent WLAN technology standard (Wi-Fi 7) and modern architectures like cloud-managed solutions. This ensures that the selection process remains relevant in the rapidly evolving context of WLANs.
- **Flexibility**: The logical formula permits for easy adaptation to specific customer needs by modifying the values of various requirements.
- **Objectivity**: The subjectivity in the decision-making process is reduced by converting qualitative requirements into a quantitative model.
- **Scalability**: The proposed model can be easily modified to adapt new requirements.
- Experiments through different real-world scenarios enhances its effectiveness.

7. CONCLUSION

The work presented here introduced a systematic approach to selecting appropriate WLAN solutions, and addressing the complexity of modern wireless networking requirements. It has provided an up-to-date overview of WLAN standards and architectures, developed a classification system for WLAN technologies, identified key selection criteria, and proposed both a WLAN matrix and a logical formula to help in the decision-making process.

While the suggested method shows the ability to simplify WLAN selection process, further work is needed to confirm its efficiency in different real-world scenarios. Also, proposed model can be used to develop User-friendly applications to conduct an extensive evaluation. As WLAN technologies continue to evolve, the importance of selection methods will be increased. This research provides a basis for future studies in the area of network infrastructure planning.

REFERENCES

[1] Faraj K. Security technologies for wireless access to local area networks [Master's dissertation]. Algarve: Universidad do Algarve; 2019. Available from: https://sapientia.ualg.pt/bitstream/10400.1/15018/1/thesis.pdf

[2] Hiertz G, Denteneer D, Zang Y, Costa X. The IEEE 802.11 Universe. IEEE Commun Mag. 2010;48(1). doi:10.1109/MCOM.2010.5394032

[3] Rosen E, Rekhter Y. The evolution of WiFi technology and standards. IEEE Standards Association; 2023. Available from: https://web.archive.org/web/20230516173837/https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/

[4] Alin M, Hossain M. Wireless evolution: IEEE 802.11n, 802.11ac, and 802.11ax performance comparison. Int J AdHoc Netw Syst. 2024;14(1).

[5] Felemban E. A comparative study of IEEE 802.11 family protocols. Int J Comput Sci Netw Secur. 2020;20(7).

[6] Pekevski B. Control and management of WiFi networks [Master's thesis]. Ljubljana: University of Ljubljana; 2016. Available from: https://openwisp.io/docs/24.11/_downloads/d6b0bc2085f3fc5537fb47233afafcb8/control-and-management-of-wifi-networks.pdf

[7] Piva M. Planning and realization of a WiFi 6 network to replace wired connections in an enterprise environment [Master's thesis]. Padova: University of Padova; 2022. Available from: https://thesis.unipd.it/retrieve/add80634-c372-439f-a2b2-7eff006f82c1/Piva_Matteo.pdf

[8] Halbouni A, Ong L, Leow M. Wireless security protocols WPA3: A systematic literature review. IEEE Access. 2023;11:112438-50. doi:10.1109/ACCESS.2023.3322931

[9] Huawei Technologies Co., Ltd. Data communications and network technologies. Singapore: Springer; 2023. doi:10.1007/978-981-19-3029-4

[10] Jaha AA, Shatwan FB, Ashibani M. Proper Virtual Private Network (VPN) solution. In: 2008 Second International Conference on Next Generation Mobile Applications, Services and Technologies; 2008; Cardiff, UK. p. 309-14. doi:10.1109/NGMAST.2008.18

[11] Sawai F. Mobile Ad-Hoc Network: Issues and challenges. Int J Adv Res Sci Commun Technol. 2023;3(1).

[12] Gollakota S, Perli S, Katabi D. Interference alignment and cancellation. In: SIGCOMM'09; 2009 Aug 17–21; Barcelona, Spain. ACM; 2009.

[13] Huawei Technologies Co., Ltd. Configuring a WLAN security policy. Available from: https://support.huawei.com/enterprise/en/doc/EDOC1100064365/8096b3dc/configuring-a-wlan-security-policy

[14] Reddy B, Srikanth V. Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). Int J Sci Res Comput Sci Eng Inf Technol. 2019;5(4). doi:10.32628/CSEIT1953127

[15] Ogunjemilua K, Davies J, Picking R, Grout V. An investigation into signal strength of 802.11n WLAN. In: Fifth Collaborative Research Symposium on Security, E-Learning, Internet and Networking (SEIN); 2009 Nov 26–27; Darmstadt, Germany. p. 191–204.

[16] Sallam K, Mohamed A, Mohamed M. Internet of Things (IoT) in supply chain management: challenges, opportunities, and best practices. Sustain Mach Intell J. 2023;2(3):1–32. doi:10.61185/SMIJ.2023.22103

[17] Huawei Technologies Co., Ltd. Huawei AP4030DN and AP4130DN access points datasheet. 2015. Available from: https://studylib.net/doc/8813520/huawei-ap4030dn-and-ap4130dn-access-points-datasheet

[18] Youssef A, McDonald D II, Linton J, Zemke B, Earle A. WiFi enabled healthcare. CRC Press; 2014. Available from: https://library.oapen.org/handle/20.500.12657/41272

[19] Al-Mejibli I, Alharbe N. Analyzing and evaluating the security standards in

wireless network: a review study. Iraqi J Comput Inform. 2020;46(1). doi:10.25195/ijci.v46i1.248

[20] Panjaitan D, Bahagia S, Raja A, Abduh M. Total cost of ownership factors in procurement and technology economic assessment: a systematic literature review. E3S Web Conf. 2024;484. doi:10.1051/e3sconf/202448401022

[21]