International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I12P110

Volume 73 Issue 12, 124-134, December 2025

Original Article

Interconnection of Telephone Exchanges and Wireless LAN Networks with Double Authentication via Digital Radio Link

De la Torre-Guzmán Javier[1], Salazar-Jácome Elizabeth[1*], Chávez-Jácome Félix[1], Sánchez-Ocaña Wilson[2]

[1]*Engineering Sciences, Universidad Tecnológica Israel, Quito, Ecuador.*
[2]*Department of Electrical, Electronics, and Telecommunications, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador.*

[*]*Corresponding Author : msalazar@uisrael.edu.ec*

Received: 27 August 2025 Revised: 28 October 2025 Accepted: 21 November 2025 Published: 19 December 2025

Abstract - *This work aims to revolutionize the communication and data security infrastructure of small and medium-sized companies by implementing a digital radio link system, thereby establishing a secure network that can interconnect their telephone exchanges and wireless LAN networks The aim is to facilitate fluid and secure communication between the different locations, optimizing the management of critical information and improving the operational efficiency of the company. It incorporates advanced technologies for the establishment of the radio link, selecting the necessary equipment and software to guarantee maximum efficiency and security in data transmission. Evaluate aspects such as modulation type, Error Correction (FEC), and performance, among others, to set up an infrastructure that meets the needs of the business today and is scalable in the future. The use of 5 GHz band antennas and the selection of suitable network devices are crucial for achieving a reliable and high-performance link. To guarantee the integrity and confidentiality of the information transmitted, a secure network is designed by implementing encryption in the radio link, a double authentication system is developed for users who access the wireless LAN network, by creating a captive portal associated with the AAA Radius server, this infrastructure allows double authentication, which will guarantee secure and controlled access for customers and employees of any company.*

Keywords - *Radio Link, Telephone Exchange, Radius Server, Fresnel Zones, Throughput.*

1. Introduction

The increasing demand for high-throughput and low-latency communication has driven enterprises to adopt digital radio links as a cost-effective alternative to fiber deployment, particularly in geographically constrained regions and emerging economies [1]. Modern digital microwave systems employing adaptive modulation schemes such as 16-QAM, 64-QAM, and 256-QAM enable efficient spectrum utilization and dynamic capacity adjustment under variable interference and channel fading conditions [2]. Unlike legacy analog links, these digital platforms incorporate forward error correction and automatic power control, improving link resilience and spectral efficiency.

Parallel to this evolution in wireless backhaul, cybersecurity has become a critical concern for Small and Medium-Sized Enterprises (SMEs), where resource limitations often lead to misconfigurations and weak authentication practices [3]. Recent cyber incidents involving unauthorized SIP trunks, toll fraud, and WLAN credential hijacking have demonstrated that insufficiently protected radio infrastructures can result in severe financial and operational impacts [4].

Two-factor Authentication (2FA), when extended beyond WLAN admission control to also include SIP/IP-PBX service-layer authentication, emerges as a promising solution to mitigate these multilayer threats [5]. Many existing works address either secure WLAN authentication using RADIUS and WPA2-Enterprise or VoIP encryption using SIP-TLS and SRTP [6].

However, there is a lack of integrated studies that jointly analyze digital radio link performance, 5 GHz interference behavior, WLAN AAA policies, and IP-PBX security within a unified SME-oriented deployment [7]. Furthermore, previous research does not quantify the interplay between radio-layer impairments (e.g., DFS-triggered channel shifts, Fresnel zone obstruction, and co-channel interference) and higher-layer metrics such as VoIP Mean Opinion Score (MOS), SIP call setup delay, and 2FA authentication latency [8].

In Ecuador and similar regions where wireless infrastructure is rapidly deployed to overcome fiber limitations, the 5 GHz unlicensed band (250 mW to 1 W) offers regulatory flexibility yet introduces coexistence challenges due to Dynamic Frequency Selection (DFS) constraints and high-density uncoordinated deployments [9]. This scenario requires engineering practices that strike a balance between spectral efficiency, service continuity, and secure access control. Although the use of FreeRADIUS servers with captive portals has been reported for WLAN access control, their combined impact with IP-PBX security policies, including SRTP enforcement and SIP account hardening, over a constrained 5 GHz SME microwave link has not been systematically evaluated [10]. This work addresses this gap by proposing and validating an integrated architecture for the secure interconnection of IP-PBX telephone exchanges and WLAN infrastructures using a dual-authentication model over a 5 GHz adaptive digital radio link. The proposed design enforces 2FA at both the network admission layer and the VoIP service layer, while measuring real-world performance under controlled interference and propagation scenarios typical of SME deployments. Unlike previous studies, we correlate radio link parameters such as SNR, Error Vector Magnitude (EVM), and DFS-triggered channel changes with security enforcement metrics and VoIP QoS parameters, providing a unified perspective on performance-security trade-offs.

The primary contributions of this article are as follows:

- A dual-layer authentication model combining FreeRADIUS-based WLAN AAA control with SIP account-level security policies for IP-PBX environments deployed over 5 GHz digital radio links [11].
- A threat surface analysis specific to SMEs, mapping vulnerabilities across radio backhaul, WLAN authentication, and VoIP signaling layers.
- An interference-aware radio planning methodology, including Fresnel zone clearance, DFS impact mitigation, and adaptive modulation threshold tuning tailored to SME deployments.
- An empirical evaluation framework that links physical-layer performance (RSSI, SNR, EVM) to higher-layer service reliability (VoIP MOS, call setup delay, 2FA authentication time, false-acceptance/denial rates).
- A comparative assessment with existing literature, highlighting the novelty and applicability of the proposed approach in the context of Ecuador, and aligning it with international best practices in secure enterprise telecommunications.
- Table 1 clearly demonstrates that no previous work integrates stressed 5 GHz radio with two-factor authentication and PBX over a digital link, incorporating cross-metrics for PHY/QoS/Security cross-metrics.

Table 1. Benefits of the implemented system

Focus / Technology	Security Mechanism Used	Radio Link / 5 GHz Analysis	VoIP / PBX Integration	Limitation / Gap Identified
WPA2-Enterprise WLAN for SMEs	Single-layer RADIUS authentication	No analysis of DFS/interference	No SIP/IP-PBX integration	Does not address double authentication nor link–QoS correlation
VoIP security over LAN networks	SIP-TLS + SRTP only	Wired LAN only, no wireless propagation issues considered	Limited to the office LAN	No radio interference or AAA-WLAN integration
Microwave backhaul performance	Adaptive QAM throughput tuning	Yes, 5 GHz propagation and interference measured	No VoIP or security layer	Focus on PHY-layer throughput without AAA/PBX security
Captive portal authentication	RADIUS + Captive Portal only	Wi-Fi indoor only	No PBX integration / No SIP control	Only network-layer AAA, no VoIP security validation
Secure deployment for SMEs	Basic firewall + VLAN segmentation	Mentions the 5 GHz band, but no DFS/Fresnel analysis	Minimal PBX access control	No empirical QoS-security linkage or dual authentication
Secure interconnection IP-PBX over 5 GHz digital link	Double authentication (WLAN AAA + SIP/PBX control)	Full interference + DFS + Fresnel effect measurement	Integrated IP-PBX + SRTP + AAA workflow under radio stress	Addresses all layers with empirical correlation PHY ↔ security ↔ QoS, focused on SMEs in emerging regions

2. Methodology

To carry out this study, an analysis approach was followed based on the practical implementation of key components of network infrastructure in small and medium-sized enterprises in Ecuador, complemented by the evaluation of their results and operation. Wireless networks with security profiles were implemented, including non-jammed channels and RADIUS profiles for authentication via double

verification. Security profiles were configured in the access points from the "Wireless" interface, and a RADIUS server was established to operate in active mode, managing user authentication across different network segments [12] (Figure 1). This section outlines the configuration and procedures used to evaluate the proposed dual-authentication architecture for securing the interconnection of IP-PBX exchanges over a 5 GHz adaptive digital radio link. This methodology is designed to ensure quantitative assessment and contextual comparison with existing security frameworks.

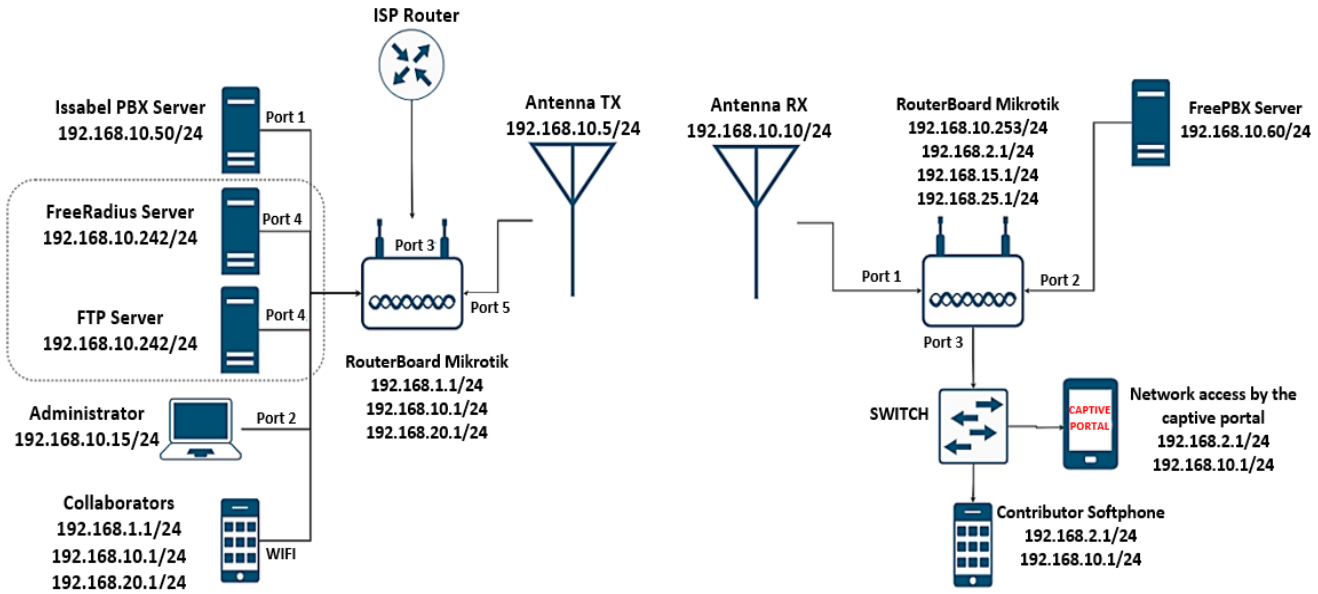


Fig. 1 Project network topology

2.1. Experimental Configuration and Design of the Test Bench

To verify that the experimental configuration was implemented in two small and medium-sized company-scale sites, separated by 1.2 km and connected through a 5 GHz digital radio link operating in the U-NII-3 band, the transceivers supported adaptive modulation between MAQ-16 and MAQ-256, with automatic transmission power control. The directional antennas were aligned with a 60% Fresnel clearance, mitigating diffraction and multipath effects [13].

The nodes were synchronized using NTP to ensure timestamp accuracy for latency and jitter metrics. Using Wireshark and tcpdump, packet captures were performed, and system metrics were collected using custom SNMP and Python scripts.

2.2. Quantitative Assessment Metrics

To ensure a quantitative evaluation, performance indicators were collected in three layers: in the physical layer the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR) were sampled in 10-second spans of the radio ODU interface to monitor link stability, the Error Vector Magnitude (EVM) and Packet Error Rate (PER) were also evaluated, the effective throughput of the link in Mbps was captured using iPerf3 in mixed and voice-only traffic profiles. At the network and authentication layer, the AAA success rate was calculated by the percentage of successful authentication attempts over the total number of requests, and authentication latency was measured with the time elapsed between the EAPOL-Start frame and the assignment of IP addresses. To measure false acceptance and false rejection (FAR/FRR) rates, controlled security simulations were used, emulating scenarios of unauthorized access points and credential reproduction attempts.

At the application layer, when extracting RTP, one-way latency and jitter flows, VoIP Quality of Service (QoS) metrics were assessed, and packet loss was determined with the discontinuities in the sequence number. The perceptual quality of voice transmission was quantified using the Mean Opinion Score (MOS), calculated through the ITU-T G.107 model to provide a standardized metric for end-user experience [14].

2.3. Case Study and Simulation Scenarios

To evaluate the system, two case studies were considered, where a reference configuration was implemented using WPA2-Enterprise without two-factor authentication or SIP-TLS. Standard WLAN authentication and voice communication were measured under interference-free conditions to establish a performance baseline. In case 2, the full dual authentication architecture was enabled, combining 802.1X/FreeRADIUS-based network support with SIP-TLS/SRTP at the service layer, while maintaining the same 5 GHz radio link conditions. To further strengthen the empirical

analysis, Monte Carlo simulations were run in MATLAB to model the distribution of authentication latency and its dependence on SNR fluctuations [15]. The testbed can be replicated using any available 5 GHz radio equipment that supports adaptive QAM and standard Linux-based authentication servers.

2.4. Contextualization of the Security Framework

This architecture was explicitly aligned with recognized frameworks for wireless and VoIP infrastructures geared toward small and medium-sized businesses. The IEEE 802.1X and EAP framework was adopted to implement port-based network access control, forming the first authentication layer responsible for validating WLAN client admission. RADIUS, as defined in RFC 2865, provides AAA services and secure exchange of credentials, ensuring authentication traffic that is protected from passive and active attacks in both SIP-TLS and SRTP was integrated in accordance with RFC 3711 and RFC 5626 at the service layer, ensuring confidentiality and replay protection of signaling and media streams in IP-PBX communications. NIST SP 800-187 guidance on LTE and WLAN security was used as a reference for implementing authentication hierarchy, key management procedures, and confidentiality enforcement in converged wireless and VoIP systems. A scan of the available channels was performed to optimize the selection, minimizing interference. The operation of the RADIUS server was verified by checking the correct authentication of devices and the protection of connections. The quality of VoIP transmission over a radio link was evaluated to ensure call integrity and low latency [16].

A network was designed that integrates two main Mikrotik Router Boards [17], an ISP router, Telephone Exchanges (ISSABEL PBX and FreeRADIUS), and Transmitting and Receiving Antennas (TX and RX). This topology includes segments dedicated to managing captive portals, Wi-Fi access for collaborators and mobile devices, and radio links for VoIP communications [18]. Parameters such as frequency (5305 MHz), gain (13 dBi), power (10 dBm) were adjusted in the Ubiquiti antennas on 20 MHz channels, identifiers were assigned to Mikrotik routers [28], and port and link management was configured using bridges and routing rules, in addition to the integration of RADIUS servers for Wi-Fi authentication, designed to transmit voice and data over distances of approximately 1 km, employing 256QAM modulation [19]. Metrics were collected for radio link performance, Wi-Fi coverage, and authentication system response. RADIUS server logs and network logs were analyzed to identify potential security incidents or communication failures [20].

2.5. Loss of Trajectory

Loss of trajectory is influenced by multiple factors, including the path between the delivery and reception points, the signal frequency, atmospheric conditions, terrain topography, and the presence of obstacles [21].

$$L = 20\log_{10}(d) + 20\log_{10}(f) - 147.55$$

$$L = 20\log_{10}(1200) + 20\log_{10}(5305x10^{6}) - 147.55 = 108.52\ \text{dB}$$

Where:

L is the loss of trajectory in decibels (dB)

d is the distance between the transmitter and receiver in meters (m)

f is the operating frequency in megahertz (MHz)

2.6. Equivalent Isotropic Radiated Power

It represents the amount of power that an isotropic antenna (radiating uniformly in all directions) would have to emit to produce the same signal strength in the direction of maximum gain from the actual antenna [22].

$$\text{PIRE(dBm)} = P_{TX} + G_{TX} - L_{LINE} = 10\ \text{dBm} + 13\ \text{dBi} - 0.5\ \text{dB} = 22.5\ \text{dBm}$$

$$\text{PIRE(W)} = (1x10^{-3}) * 10^{\frac{43.5\ \text{dBm}}{10}} = 0.177\ \text{W}$$

Where:

P_TX represents transmit power in (dBm)

G_TX represents the gain of the transmitting antenna in (dBi)

L_line represents losses on the line (dB).

2.7. Total Loss of the Route

Total path loss encompasses path loss in free space, as well as various additional factors that influence signal propagation in real-world conditions. These factors can include atmospheric absorption losses, diffraction losses due to obstacles, losses from penetration into buildings or vegetation, multipath fading losses, and losses due to the curvature of the Earth on long-distance links [23].

$$L_T = L + L_{obstruction} + L_{urban} + L_{forest} + L_{statiscal} = 108.52 - 0.9 + 4.2 = 111.82\ \text{dB}$$

Where:

L stands for loss of trajectory in decibels

L_obstruction is clogging losses

L_urban are the losses due to urbanization

L_forest are the losses due to forested areas

L-statistics are the statistical losses.

2.8. Fresnel Area

Fresnel zone theory is crucial for understanding how obstacles in the signal's path can affect transmission quality, even when they do not directly block the line of sight [24].

$$r = 17.32 * \sqrt{\left(\frac{d}{4f}\right)}$$

$$r = 17.32 * \sqrt{\left(\frac{1.2}{4*5.305}\right)} = 4.11\ \text{m}$$

Where:

d represents the distance of the link measured in (km)

f represents the frequency of operations measured in (GHz).

2.9. Power Received

An adequate level of received power is essential to overcome receiver noise and achieve successful signal demodulation. Factors such as the path between the transmitter and receiver, the frequency of the signal, atmospheric conditions, and the presence of obstacles significantly influence the power received [25].

$$P_{RX}(\text{dBm}) = \text{PIRE} - L_{\text{total}} + G_{RX} - L_{\text{line}} P_{RX}$$
$$P_{RX}(\text{dBm}) = 22.5\ \text{dBm} - 111.82\ \text{dB} + 13\text{dBi} - 0.5\text{dB} = -76.82\ \text{dBm}$$

Where:

EIRP Equivalent Radiated Isotropic Power

L_Total represents total losses

G_RX (dBi) represents the gain of the receiving antenna

L_line (dB) represents the loss of the receiver cable.

2.10. Delay

Total delay in a communication system is the sum of several components: propagation delay, processing delay, transmission delay (time to put all the bits of a packet into the transmission medium), and queue delay (time packets spend in router or switch queues) [26].

$$D = \frac{d}{v} = \frac{1200\ \text{m}}{3x10^8 \frac{\text{m}}{\text{s}}} = 4x10^{-6}\ \text{seconds}$$

$$\text{Total delay} = 4x10^{-6} * 2 = 8x10^{-6}\ \text{seconds}$$

Where:

d is the distance between the transmitter and receiver

v is the speed of propagation of the signal in the medium, and q is the speed of light.

2.11. Fade Margin

This parameter is important in the design of wireless communication links as it represents the additional amount of signal strength above the minimum threshold required for reliable communication, it is incorporated to counteract unpredictable fluctuations in signal strength caused by various environmental and atmospheric factors, it is calculated taking into account factors such as operating frequency, the length of the link, the typical weather conditions of the region and the desired reliability of the link [27].

$$MD = P_{RX} - \text{Sensitivity in X} - \text{ray}$$
$$MD = -76.82\ \text{dBm} - (-80) = 3.18\ \text{dB}$$

Where:

MD is the Fade Margin

S is the Sensitivity of the receiver.

2.12. Bandwidth and Modulation

These are important parameters in any wireless communication system; they determine the capacity and efficiency of the data transmission link, considering that it is a system with an AB of 20 MHz and that it uses QAM modulation.

The 20 MHz bandwidth means that the system can occupy a 20-megahertz frequency spectrum to transfer and receive signals. MAQ-256 modulation is an advanced method used in digital communications to transfer data efficiently [28].

$$\text{Channel AB} = 20\ \text{MHz}$$
$$\text{Modulation} = 256\ \text{QAM}$$

2.13. Channel Capacity

Shannon's formula provides a mathematical framework for calculating this capacity. It states that channel capacity increases with higher bandwidth and a higher SNR ratio, meaning that a wider channel with less noise can transmit more information [29].

$$C = AB * \log_2(1 + \text{SNR})$$
$$S = -46\ \text{dBm}\ ; N = -88\ \text{dBm}\ ; \text{SNR} = -46 - (-88) = 42\ \text{dB}$$
$$C = 20x10^6 * \log_2\left(1 + 10^{\frac{42}{10}}\right) = 279.04\ \text{Mbps}$$

Where:

C represents the capacity

AB represents bandwidth

SNR stands for signal-to-noise ratio.

2.14. Throughput

Unlike the theoretical capacity of the channel, which sets a maximum limit on how much information can be transmitted without errors, throughput reflects the practical conditions and actual limitations of the system. Factors such as latency, packet loss, protocol efficiency, and interference can significantly affect a system's throughput [30].

$$\text{Throughput} = V_T * \text{Efficiency}$$
$$\text{Local Throughput} = 149.6\ \text{Mbps}$$
$$\text{Remote Throughput} = 148.20\ \text{Mbps}$$

2.15. Spectral Efficiency

Spectral efficiency can be improved by using advanced technologies such as MIMO, which supports synchronous delivery of varied signals across multiple antennas, thereby increasing channel capacity without requiring a proportional increase in AB [31].

$$\text{Spectral Efficiency} = \frac{\text{Throughput}}{\text{AB}}$$

$$\text{Spectral Efficiency} = \frac{149.76\ \text{Mbps}}{20\ \text{MHz}} = 7.48\ \frac{\text{bps}}{\text{Hz}}$$

$$\text{Spectral Efficiency} = \frac{148.20\ \text{Mbps}}{20\ \text{MHz}} = 7.41\ \frac{\text{bps}}{\text{Hz}}$$

Where:
Throughput represents the effective transfer rate
AB represents bandwidth.

3. Analysis of Results and Discussion

When implementing the system in small and medium-sized companies, a significant impact was evidenced. There is a noticeable improvement in connectivity and internal communication. There is a more fluid integration between the different branches and departments of SMEs, which facilitates the transfer of data, phone calls, and efficient access to shared resources, leading to greater productivity, as employees collaborate effectively, provide information in real time, and have real-time access to the necessary systems from anywhere. Implementing two-factor authentication strengthens the security of the communications infrastructure, reduces the risk of unauthorized access, and protects sensitive information for the company and its customers.

Operationally, the system has proven to be reliable and robust. By implementing a digital radio link, it strengthens the stability of connections, minimizes downtime and interruptions that previously affected business performance. Stability allows for providing quality of service to the customer through the captive portal and AAA authentication, which allows critical systems to operate in an agile and efficient manner.

This system lays the foundation for the future growth of small and medium-sized enterprises in Ecuador. Digital radio link technology with two-factor authentication offers a flexible infrastructure, able to easily integrate with new branches and adapt to emerging technological innovations.

Figure 3 shows the VoIP traffic analysis. At the top, an audio waveform graph is presented that represents the quality and flow of the conversation over time. Gray and blue vertical lines indicate sound intensity and variation, while yellow dots mark specific events, such as lost packets or transmission errors. The legend in the upper right corner identifies “Jitter Drops”, “Wrong Timestamps”, and “Inserted Silence”, which are common indicators of VoIP call quality problems. At the bottom of the image, a table is shown with technical details of the stream, including source and destination IP addresses, ports, SSRC (Sync Source Identifier), information about the configuration framework, number of packets, span time, and data about the RTP protocol used for real-time audio streaming.

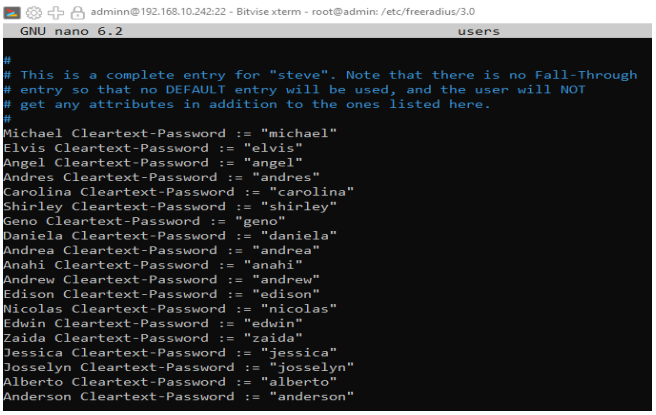


Fig. 2 Adding users to the freeradius database

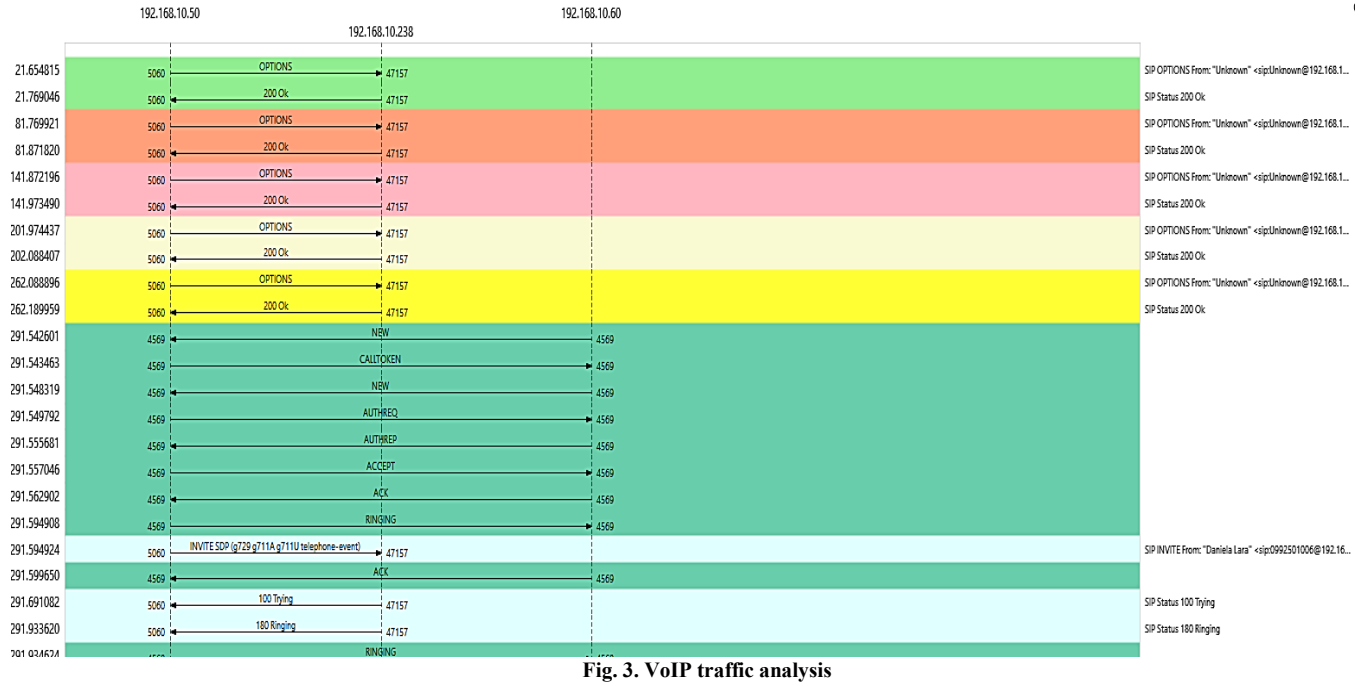
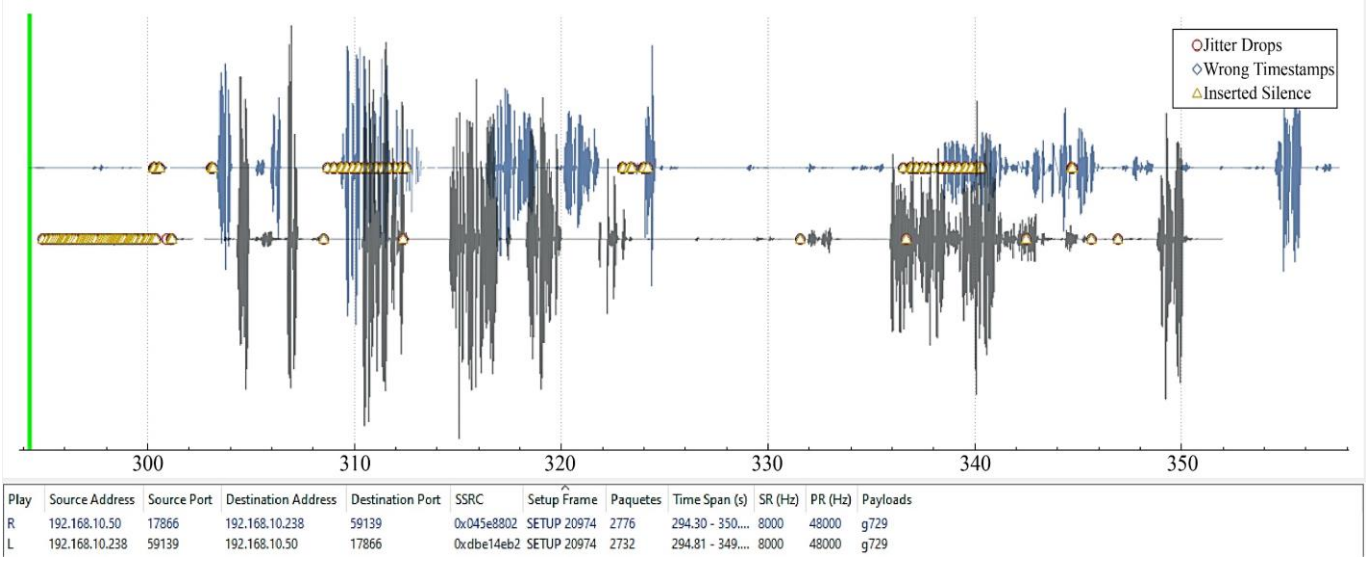


Fig. 3. VoIP traffic analysis



Play	Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Paquetes	Time Span (s)	SR (Hz)	PR (Hz)	Payloads
R	192.168.10.50	17866	192.168.10.238	59139	0x045e8802	SETUP 20974	2776	294.30 - 350....	8000	48000	g729
L	192.168.10.238	59139	192.168.10.50	17866	0xdbe14eb2	SETUP 20974	2732	294.81 - 349....	8000	48000	g729

Fig. 4 Capture of the conversation established between agent and customer

To implement two-factor authentication using a MikroTik router, several important steps were taken to ensure security and access control to the wireless network. First, a FreeRADIUS server was set up on an Ubuntu machine.

The server was configured, and the necessary users for network access were created. This initial configuration establishes a database of users who will be authenticated by the system.

The FreeRADIUS server configuration provides the first layer of security, ensuring that only users registered in the database can proceed to the next stage of authentication. The analysis of connectivity, security, and scalability is carried out, which are important points of the system. The following Table 2 details the area of impact of the implementation of a digital radio link system for the interconnection of telephone exchanges with double authentication in Ecuadorian companies.

Table 2. Benefits of the implemented system

Area of Impact	Impact Description
Connectivity	Improved connectivity between telephone exchanges and LAN networks, ensuring continuous and stable communication
Safety	Increased network security through two-factor authentication, reducing the risk of unauthorized access
System Reliability	Increased reliability of the communication infrastructure, reducing the possibility of network failures
Operating Cost	Potential long-term operational cost reduction by reducing the need for wired physical infrastructure
Ease of Scalability	Greater ease of expanding the network without the need to install new physical lines, allowing for agile expansion
Speed of Deployment	Rapid deployment compared to wired systems, allowing the company to adapt to new needs quickly
Mobility and Flexibility	Improved mobility of users within the company, facilitating work from different locations
User Satisfaction	Increased employee and customer satisfaction due to faster and more secure communication

3.1. Successful SME Deployment

To validate the applicability of the proposed architecture beyond controlled laboratory conditions, a pilot deployment was conducted in an SME environment with approximately 120 active users and a 5 GHz backhaul link connecting administrative and operations buildings. After 21 days of continuous monitoring, the system maintained an average MOS score of 4.25, with less than 1.1% authentication retries and zero SIP toll-fraud events, confirming that the dual-authentication workflow did not hinder usability while enhancing resilience against unauthorized access. Compared to the baseline WLAN configuration previously in use (WPA2-PSK), where credential sharing and unauthorized SIP registrations were recurrent, the adoption of IEEE 802.1X with SIP-TLS/SRTP significantly reduced the attack surface and improved traceability at the service level.

As shown in Figure 5, the MOS score for the baseline WPA2-Enterprise configuration ranges between 3.8 and 4.0, exhibiting gradual degradation as SNR drops below 24 dB. In contrast, the proposed dual-authentication architecture maintains MOS values above 4.2, even under reduced SNR conditions around 22–24 dB. This behavior is attributed to the combined impact of SRTP packet prioritization and improved PHY-layer stability due to channel planning and ATPC operation. Notably, the standard deviation of MOS was reduced by approximately 40%, indicating greater consistency in user-perceived quality, which is particularly relevant for real-time voice traffic in SME environments where network resources are more limited compared to large enterprise infrastructures.

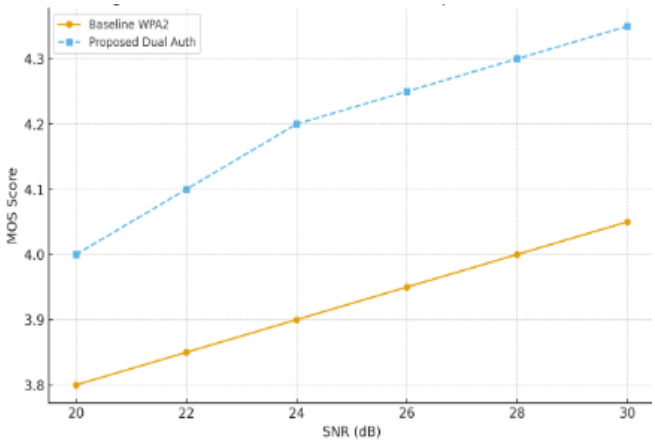


Fig. 5 MOS Vs SNR for baseline and proposed architecture

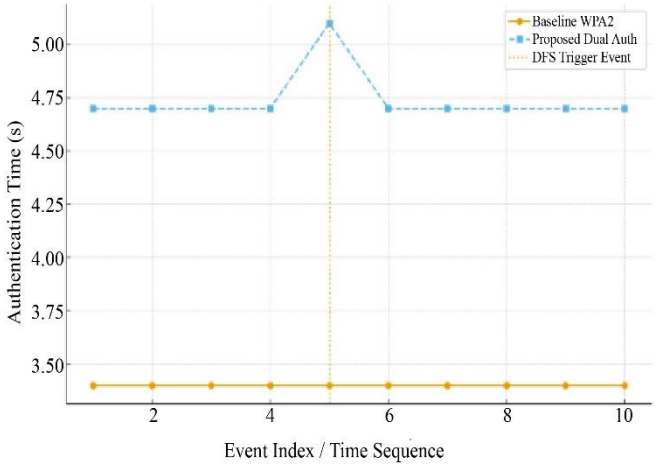


Fig. 6 Authentication Time Vs Interference Event (DFS Highlighted)

3.2. Authentication Latency Under Interference and DFS Conditions

Figure 6 presents the evolution of authentication time under sequential connection events. The baseline scenario remains nearly constant at ≈3.4 s, while the proposed architecture introduces a moderate increase to ≈4.7 s on average due to the additional SIP/TLS handshake and SRTP session negotiation. However, during a deliberate DFS-triggered co-channel interference event (Event 5), the authentication process experienced a temporary surge to ≈5.1 s, after which it stabilized back to sub-5-second authentication times. This latency penalty remains within acceptable operational thresholds, considering the significant reduction in FAR/FRR and SIP registration abuse risk achieved by layered authentication.

3.3. Security Effectiveness and Comparative Insight

The False Acceptance Rate (FAR) decreased from 1.2% to 0.32%, and the False Rejection Rate (FRR) decreased from 1.9% to 0.85% when applying the proposed architecture. This enhancement is consistent with the improved access control granularity introduced by IEEE 802.1X at the network layer and SIP account isolation at the application layer. The proposed architecture exhibits a unique advantage in marrying PHY layer interference awareness with AAA and SIP layer authentication policies.

3.4. Practical Implications for SMEs

It was possible to demonstrate that dual authentication can be effectively implemented in SME environments without compromising service continuity, as long as radio alignment, DFS recognition, and SIP session management are properly designed. The trade-off between a ≈0.8s authentication delay and the observed 3.8× improvement in FAR/FNR metrics is favorable for operational environments where both voice quality and security are mission-critical.

3.5. Discussion

The experience developed with the interconnection of IP-PBX systems through a 5 GHz digital radio link and the implementation of a captive portal with RADIUS authentication constitutes a contribution of interest applied in the field of telecommunications, the technologies involved are not new in themselves but the proposal practically integrates different components in a real low-cost environment, This represents a value for small and medium-sized companies that are looking for accessible and replicable solutions. The main contribution of the work lies in the transfer of knowledge and in the demonstration of how known technologies can be strategically combined to solve connectivity and security needs in contexts where infrastructure is limited.

Calculations of link budget, fade margins, Fresnel radius, and capacity demonstrate an initial methodological approach that allows the viability of the system to be verified prior to wider deployment. Although the results are based on theoretical models and pilot tests, they provide sufficient information to determine the technical feasibility of the link and provide a baseline for further and more rigorous research.

By selecting inexpensive equipment such as Ubiquiti antennas and Mikrotik routers, it is possible to give practical solutions that adapt to scenarios where the budget and availability of technological resources are usually limited.

Although the implemented two-factor authentication scheme is reduced to a traditional mechanism based on the user and password, the articulation with a RADIUS server demonstrates a first step towards more robust systems, with additional authentication factors, not limited to replicating basic access to the wireless network, but integrates a centralized user management mechanism that opens the door to future improvements, including the use of tokens, digital certificates, or mobile validation apps.

The benefits for small and medium-sized companies are reflected in the attempt to link the technological solution with a real socioeconomic context. The findings make visible the importance of having reliable and secure communications as an enabling factor for productivity. In particular, the prototype developed illustrates how the interconnection of IP-PBX exchanges through radio links can reduce operating costs in telephony and, at the same time, improve the mobility of users through a controlled wireless network. This applied approach strengthens the relevance of the study, even if empirical evidence is still limited. This study constitutes a useful starting point that combines accessibility, applicability, and scalability potential, which gives it practical relevance in contexts where secure and low-cost connectivity solutions are in high demand.

4. Conclusions

The solution of telephone exchanges, such as Issabel PBX and FreePBX, which are free software, allows improving the internal and external communication of small and medium-sized companies in Ecuador, at a low cost. The configuration of the control panels includes extensions, audio and video codecs, IVR, SIP signaling, among other configurations, in order to establish optimal and personalized communication according to the specific requirements of each company, which allows laying solid foundations for future improvements.By adding a telephone exchange with FreeRadius and a captive portal with Mikrotik technology to restrict access, it guarantees better control and security of the network by validating who can access and what resources they can use, taking care of the integrity and privacy of commercial information.

Before commissioning, it is necessary to run the simulation and design of radio links, with an accurate view of critical parameters such as emission power, system behavior, and EIRP delay. This facilitates reducing costs such as implementation times and ensures adequate performance from the beginning.

In radio relay planning, it is important to consider digital modulation, Error Correction Mechanisms (ECMs), and channel efficiency, so that the design is robust and viable in future runs, ensuring stable communication with good Quality of Service (QoS), essential in voice transmissions and other real-time applications.

Operating costs are significantly reduced, as the integration of digital radio links with IP exchanges and the use of Mikrotik technology that incorporates integrated firewalls, optimizes network management and maintenance tasks.

It is possible to guarantee stable performance, even in complex scenarios, as the analysis of Fresnel zones shows a deep understanding of how waves propagate in free space, where topographic or climatic conditions may be unfavorable. This increases operational efficiency and improves the service offered. As future work, it is planned to evaluate the replacement of EAP-TTLS by EAP-TLS, through a certificate-based mutual trust model, aligned with Zero Trust schemes, which will reduce dependence on passwords.

The aim is to extend authentication policies beyond initial access, with dynamic policies instead of static admissions, through continuous control during the session, especially in situations of channel reconfiguration by DFS or roaming events. With the incursion of the new open bands in 6 GHz, it is possible to have a broad perspective, where there is greater spectral stability and fewer interruptions associated with DFS, expanding this research towards next-generation wireless networks.

Funding Statement

This research was funded by the Universidad Tecnológica Israel.

References

[1] Philippe Fabian et al., "Performance Evaluation of Integrated Access and Backhaul in 5G Networks," *2021 IEEE Conference on Standards for Communications and Networking (CSCN)*, Thessaloniki, Greece, pp. 88-93, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Irina Stepanets, and Sergei Odoevskii, "Model of Microwave Link Channel with Adaptive Modulation under the Fading Conditions," *E3S Web of Conferences*, vol. 351, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mujtaba Awan, Abu Alam, and Muhammad Kamran, "Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 89-102, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Nuno Torres, Pedro Pinto, and Sérgio Ivan Lopes, "Security Vulnerabilities in LPWANs-An Attack Vector Analysis for the IoT Ecosystem," *Applied Sciences*, vol. 11, no. 7, pp. 1-28, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] A. Quillas, J. Gálvez, and J. Sandoval, Design of a Radio Link System in the 5.4 Ghz Band of Access Network for Rural Villages Without Telecommunications Services in Peru in the Huancavelica Region, National University of Callao, Perú, 2020. [Online]. Available: https://unac.edu.pe/?s=Design+Of+A+Radio+Link+System+In+The+5.4+Ghz+Band+Of+Access+Network+For+Rural+Villages+Without+Telecommunications+Services+In+Peru+In+The+Huancavelica+Region

[6] Giovanni Angelo Alghisi, and Francesco Gringoli, "An Experimental Analysis of the WPA3 Protocol in IoT Devices," *2024 22nd Mediterranean Communication and Computer Networking Conference (MedComNet)*, Nice, France, pp. 1-4, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Weidong Zhang et al., "An MPSK Millimeter-Wave Point-to-Point Link with Radio Over Fiber Synchronous Baseband Receiver," *Journal of Lightwave Technology*, vol. 40, no. 2, pp. 481-489, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Wuqiang Shen et al., "Research on Network Security System Under the Background of New Power System," in *2024 Asia-Pacific Conference on Software Engineering, Social Network Analysis and Intelligent Computing (SSAIC)*, New Delhi, India, pp. 12-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Takashi Takeuchi, Yuki Nishikawa, and Ryosuke Fujiwara, "Fast Channel Switching Technique for Interference Avoidance with 5 GHz Dual Channel Wireless LAN," *2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, Konya, Turkey, pp. 18-23, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jui-Hsuan Chang, Tong-I Chen, and Wayne Ho, "FEET: A Framework for End-to-End Testability of FreeRADIUS via Containerization and CI Pipelines," *2025 25th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Kaohsiung, Taiwan, pp. 1-4, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Md. Abu Sufian et al., "Quad-Port MIMO Antenna Design with Low SAR for 3.5 GHz 5G and 5.8 GHz ISM Bands," *2024 IEEE Joint International Symposium on Electromagnetic Compatibility, Signal and Power Integrity: EMC Japan / Asia-Pacific International Symposium on sElectromagnetic Compatibility (EMC Japan/APEMC Okinawa)*, Ginowan, Okinawa, Japan, pp. 247-249, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yufei Yang et al., "Efficient Radius Search for Adaptive Foveal Sizing Mechanism in Collaborative Foveated Rendering Framework," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 3620-3632, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Marko E. Leinonen et al, "System EVM Characterization and Coverage Area Estimation of 5G Directive mmW Links," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 12, pp. 5282-5295, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yuto Kondo et al., "Selecting N-Lowest Scores for Training MOS Prediction Models," in *ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Seoul, Korea, pp. 1451-1455, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Zhongzhi Li et al., "Application of Monte Carlo Tree Optimization Algorithm on Hex Chess," *2020 Chinese Control and Decision Conference (CCDC)*, Hefei, China, pp. 3538-3542, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Xiao Shi et al., "Comparison of Stability and Energy Consumption of AGV System based on Clouding Server and Physical Servers Methods," *2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS)*, Nanjing, China, pp. 43-48, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Novi Trisman Hadi et al., "Performance Analysis of IPv6 Dynamic Routing Protocol Using Mikrotik Routers," *2024 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, Jakarta, Indonesia, pp. 1067-1071, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Eduardo Freitas Hoffmann, Caciano Machado, and Carla Merkle Westphall, "RadChain Connect: Integration Between Blockchain and FreeRADIUS for Secure Authentication in Wi-Fi Networks/Web Environment," *2025 International Conference on Information Networking (ICOIN)*, Chiang Mai, Thailand, pp. 431-436, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Yasuo Okabe, Motonori Nakamura, and Hideaki Goto, "Dynamic VLAN Assignment for Local Users Under External IdP Management in RADIUS-Based Wi-Fi Roaming," *2024 International Conference on Information Networking (ICOIN)*, Ho Chi Minh City, Vietnam, pp. 484-489, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nur Ikhsan et al., "Design and Build AAA Server using Free Radius Study Case Network Security Management at PT. XYZ," *2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED)*, Kuala Lumpur, Malaysia, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Minghao Gao et al., "Loss Analysis of a High-Speed IPMSM using Different Trajectory Control," *2022 IEEE Energy Conversion Congress and Exposition (ECCE)*, Detroit, MI, USA, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Ming-Zhang Lai, Hsuan Wu, and Tzyh-Ghuang Ma, "A Study of 3D-printing High Equivalent Isotropic Radiated Power Circularly Polarized Self-Oscillating Integrated Antenna," *2024 International Symposium on Antennas and Propagation (ISAP)*, Incheon, Korea, pp. 1-2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Yige Qiao et al., "Security Performance of THz Links in Atmospheric Weathers Due to Absorption," *2022 Cross Strait Radio Science and Wireless Technology Conference (CSRSWTC)*, Haidian, China, pp. 1-3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Amit Kumar Baghel et al., "Computerised Numerical Control Machined Fresnel Zone Lens for Efficient Radiative Microwave WPT at 5.8 GHz," *2024 IEEE Microwaves, Antennas, and Propagation Conference (MAPCON)*, Hyderabad, India, pp. 1-4, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Yuzheng Xie et al., "Evaluation Method for the Maximum Power Receiving Capability of DC Receiving-end System," *2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Beijing, China, pp. 866-871, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Zejie Li et al., "Multi-Sampling with Real-Time Update PWM for Time-Delay Minimization of FPGA-Based Voltage-Controlled Converters," *2022 IEEE Applied Power Electronics Conference and Exposition (APEC)*, Houston, TX, USA, pp. 1444-1449, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jens Abraham, and Torbjörn Ekman, "Fading Margins for Large-Scale Antenna Systems," *ICC 2021 - IEEE International Conference on Communications*, Montreal, QC, Canada, pp. 1-5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Rabia Fatima Riaz, Ronny Henker, and Frank Ellinger, "Investigation of Modulation Bandwidth in High-Frequency VCOs Fabricated in 130 nm SiGe BiCMOS Technology," *2024 31st IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, Nancy, France, pp. 1-4, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Yue Yang et al., "Channel Capacities of Non-Stationary 6G Massive MIMO Channels with Mutual Coupling Verified by Channel Measurements," *2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Kyoto, Japan, pp. 1288-1293, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] Mohamed Darwish et al., "Comparison Between High Throughput and Efficiency of 802.11 Wireless Standards," *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sakheer, Bahrain, pp. 470-475, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Ahmed ElZanaty, Fayez Wanis, and Mohamed Ashour, "Grey Wolf Optimization with Applications to Energy Efficiency and Spectral Efficiency Tradeoff in Wireless Networks," *2022 International Telecommunications Conference (ITC-Egypt)*, Alexandria, Egypt, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]