DESIGN OF EXTERNAL ANTENNA FOR WI-FI ANTI-THEFT USING TV WHITE SPACE SPECTRUM

[1]KHOLA AZHAR, [2]M.OMAR, [3]M. USMAN, [4]H. ATIQ, [5]S. S. KHAN, [6]S.LARKIN

[1,2,3,4]Technosense21, Private Limited, Islamabad, Pakistan
[5]National Transmission and Dispatch Company Limited, Islamabad, 44000, Pakistan
[6]Africa New Energies Limited, Private Limited, London, 533416, United Kingdom
E-mail: khola.azhar25@gmail.com

Abstract - This study investigates the usage of the TVWS spectrum in an antenna-based Wi-Fi anti-theft design. Stealing Wi-Fi signals for illegal activities is frequently observed and an anti-theft antenna system is proposed. The antenna operates at Wi-Fi frequency (2.4GHz),but due to the short-range line-of-sight approach of Wi-Fi, the antenna transmission over a longer range is impractical. Therefore, a second TVWS antenna i.e., a dipole antenna operating at 654 MHz is used for long-range transmission to the user end. The purpose of this paper is to design the antennas in High-Frequency System Simulator (HFSS). The electric field, 3D radiation pattern, and polar plots are discussed. Fabrication of proposed antennas using flame retardant (FR4), and the acrylic substrate is shown. Advanced Design Simulator (ADS)is used to improve the antenna design by making suitable modifications. Finally, the external antenna-based design is efficient for Wi-Fi anti-theft applications.

Keywords - Anti-theft, External Antenna, Rectangular Patch, TVWS.

I. INTRODUCTION

Wireless Local Area Network (WLAN) or Wi-Fi is the primary internet connection for individuals and organizations. WLAN will reach more than 3.47 trillion in 2023 and is expected to increase even more by 2030[1]–[3]. Despite its popularity, it is unsafe because Wi-Fi transmits radio signals for clients to receive. Every day many consumers throw out Wi-Fi signals from their windows that cannot be seen, heard, or felt and can be easily stolen. Wi-Fi signals from a home Wi-Fi router or access point can transmit 46 meters approximately. Even at home or at the workplace, one of the crucial concerns for end users is the risks or vulnerabilities involved in Wi-Fi usage. The unauthorized use of Wi-Fi for illegal activities can lead to serious threats for the owner[4].When the investigation for internet crimes is carried out, the investigators search for the Internet Protocol (IP) as the first evidence. The activities performed by the unauthorized person over an internet connection could include sharing copyrighted content or executing a denial-of-service attack that is linked to the owner. There is a growing demand for Wi-Fi anti-theft systems to accurately protect and detect the loss or stealing of Wi-Fi signals which is required for a reliable internet network. Internet security and surveillance are important issues[5].Moreover, the conventional detection and recognition method becomes very difficult when the intruder is far away from the theft location, as in the case of Wi-Fi theft. Legacy systems cannot provide real-time theft notification, and the availability of the owner is required[6].Managing the router's default settings (name and login credentials) can make the Wi-Fi network less of a target for potential thefts. However, it is still vulnerable as attackers can steal Wi-Fi signals using tricks and techniques. The commonly known anti-theft devices such as CCTV or other surveillance systems cannot work for wi-fi anti-theft. Therefore, an external antenna-based system is proposed.

A. TVWS and Wi-Fi:

The proposed design is based on two patch antennas, operated at Wi-Fi and TV White Space (TVWS)frequency range (470-790 MHz). TVWS is an unused band that is being utilized here for wireless access to transmit signals using Ultra-High Frequency(UHF) and Very-High Frequency(VHF) bands. The analysis shown in *Fig. 1* estimates that TVWS is expected to reach USD 346.5 million market by 2028 [7].

The lower frequency range of TVWS is considered favorable. Using TVWS, for the same power budget a wider coverage area and better propagation through obstacles are made possible [8], [9]. The comparison of TVWS and Wi-Fi is given in Table I. From the table the range of TVWS is up to 100km.

Wi-Fi 2.4/ 2.5 GHz	TVWS (470-790 MHz)
Short range: Router range 100m (45-90m for 2.4 GHz). For long-range: Antenna alignment is challenging.	Long range: 20km, 40km, 60km, and some solutions up to 100km.
Works only for line-of-sight (LOS) scenarios.	Works best for non-line-of-sight (NLOS) scenarios.
High data rate: 300Mbps and reach up to 450 Mbps	Low data rate: 186 Mbps.

Table I: TVWS vs Wi-Fi.

Section II presents the proposed solution along with a comparison of feeding techniques and the dimensions of the antenna. The antenna simulation results, and fabrication are discussed in section III. In Section IV, a comparison between measured and simulated results has been shown. Finally, the conclusion and future work are discussed.

II. PROPOSED SOLUTION

This paper aims to provide a solution for Wi-Fi antitheft, based on the external antenna. An external antenna can be easily set up or mounted in remote locations. It has the best aerial gain, extended range, and significantly improved performance. As Wi-Fi short-range issue is discussed, another TVWS antenna (operated at TVWS frequency 654MHz) is used for long-range NLOS data transmission at the user end. Two micro strip patch antennas (rectangular and dipole)have been fabricated to adequately cover the 2.4-2.5 GHz frequency band for Wi-Fi, and 470-790 MHz for TVWS respectively. The frequency down converter is used to convert the Wi-Fi frequency into TVWS frequency. The simulation and fabrication of the antennas are discussed in this paper. The micro strip antennas (Rectangular patch and Dipole) are the main components of the proposed anti-theft system. The micro strip patch antennas are light weight, low profile, and easy to feed.

A. Feeding Techniques:

The simplest and most efficient design of the antenna depends on the feeding technique. The return loss of the antenna is controlled by proper impedance matching which is influenced by the selection of the appropriate feeding method. Microstrip line feeding is one of the popular techniques for perfect matching and improved impedance used in the proposed antenna. It is easily integrated; the conducting line can be engraved on the same substrate and the edge of the patch is directly connected to the conducting strip. For better performance, antenna parameters can be controlled by estimating the proper feeding location using a suitable feeding technique [10]. The advantages and disadvantages of various antenna feeding techniques are tabulated in Table II.

B. Mathematical Model:

The mathematical model for rectangular patch and dipole antenna is discussed:

Dipole Antenna: The antenna length is 200.3mm.

Rectangular Patch Antenna: The dimensions of the rectangular patch antenna operated at Wi-Fi frequency are described with the help of equations.

Patch Width: Equation (1) is used to calculate W which is equal to **38.7609mm.**

$$W = \frac{v_0}{2f_r}\sqrt{\frac{2}{\varepsilon_r + 1}} \qquad (1)$$

Patch Length: Equation (2) is used to calculate L which is equal to **29.7319 mm.**

$$L = \frac{v_0}{2f_r\sqrt{\varepsilon_{reff}}} - 2\Delta L \qquad (2)$$

where;

$$\varepsilon_{reff} = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2\sqrt{1 + \frac{12h}{W}}}$$

$$\Delta L = 0.412h\frac{(\varepsilon_{reff} + 0.3)\left(\frac{W}{h} + 0.264\right)}{(\varepsilon_{reff} - 0.258)\left(\frac{W}{h} + 0.8\right)}$$

v_0 : speed of light in free space, f_r: resonance frequency, ε_r: relative permittivity, ε_{reff} : effective dielectric constant, h: substrate height.

Feeding Techniques	Advantages	Disadvantages
Microstrip Line	This technique is simple and easy to obtain input match.	In the case of deep notches, the pattern may show some distortions.
Proximity Coupled Feed	The technique allows for planar feeding, and less line radiation is observed.	It Requires multilayer fabrication, and the alignment is important for input match.
Aperture Coupled Feed	In this technique feed radiation is isolated from patch radiation.	Generally, multilayer fabrication is required, and alignment is very tricky for a perfect input match.
Coaxial Probe Feed	The feed can be placed anywhere inside the patch to match the input impedance.	For thicker substrates, it is challenging to match the input due to probe inductance.

Table II: Antenna Feeding Techniques [11], [12]

III. SIMULATION AND RESULTS

The external antenna-based anti-theft system comprised of a rectangular patch antenna operated at Wi-Fi frequency 2.4GHz and a dipole antenna operated at TVWS frequency i.e., 654MHz.The proposed antennas are designed on FR4 and acrylic substrate and simulated using the HFSS. The dimensions of the antenna were estimated by using the equations described above. The antenna dimensions are shown. Both the antennas have been simulated using the HFSS by inset feed method and the schematics are shown in Fig. 2 (a) & 2(b) respectively.

A. Resonance Frequency:

The return loss [S11] parameter for rectangular patch and dipole antenna is shown in Fig. 2 (c) & 2 (d)

respectively. In rectangular patch antenna the -24dB gain is obtained at resonance frequency 2.4 GHz, and -20.4254dB gain for dipole antenna at resonance frequency 654 MHz.

The rectangular patch antenna has a center frequency of 2380 MHz, with a lower cut-off frequency of 2366 MHz to a higher cut-off frequency of 2390 MHz which lies in the ISM band ranges. The dipole antenna covers a bandwidth that lies within the UHF band from a lower cut-off frequency of 648.8 MHz to a higher cut-off frequency of 660.6 MHz.

B. Radiation Pattern:

The radiation pattern describes how the antenna radiates energy into space. The maximum radiation is presented by the red-colored region. The radiation pattern of the rectangular patch antenna shown in Fig.3 (a), radiates only in the z-axis. The radiation pattern of the dipole antenna in Fig.3 (b) shows that it radiates along sideways. Therefore, the dipole antenna operating at TVWS frequency is capable of transmission to the user end over a longer range.

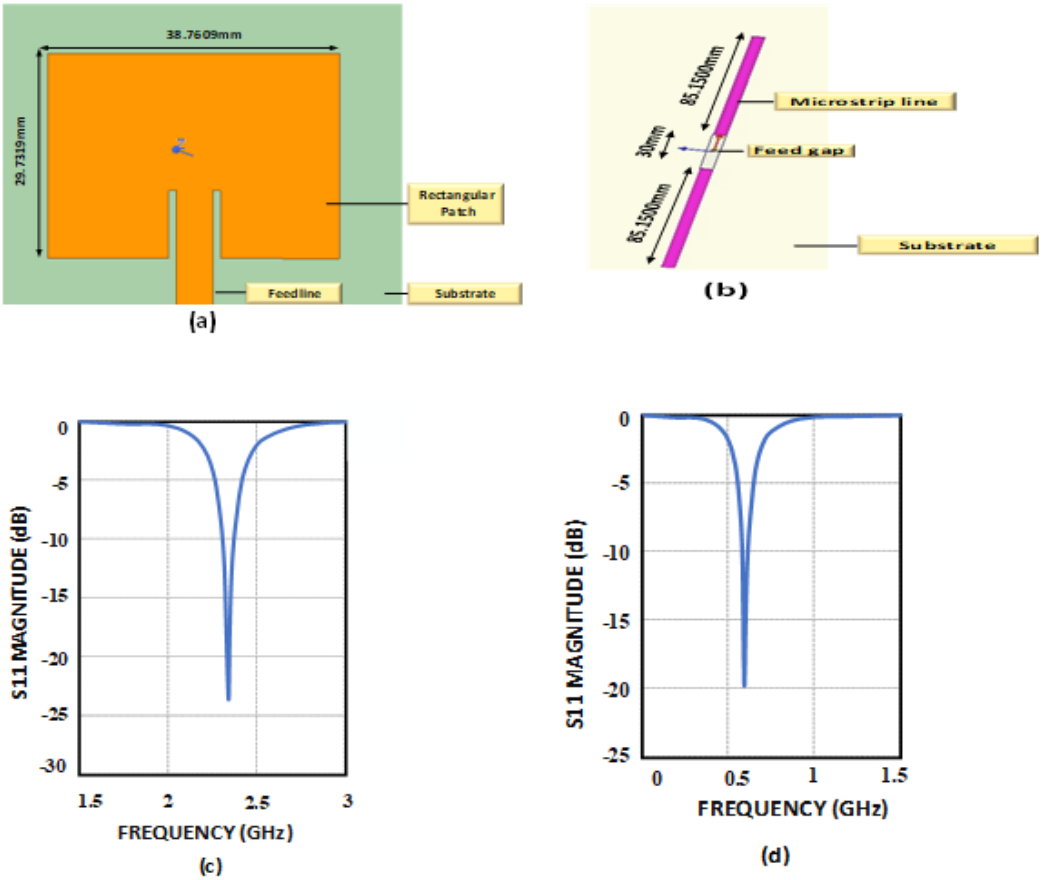


Fig. 1: Antenna simulation in HFSS (a) Rectangular Patch (b) Microstrip Dipole (c) Resonance Frequency Rectangular Patch (d) Resonance Frequency Microstrip Dipole.

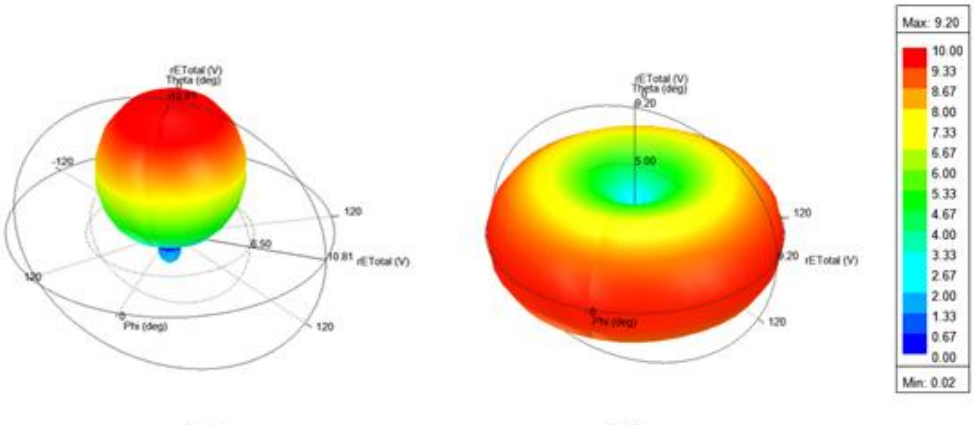


Fig.3:Radiation Pattern (a) Rectangular Patch (b) Microstrip Dipole.

C. Electric Field Pattern:

The electric field pattern is the two-dimensional view ofthe 3D radiation pattern shown above. For Wi-Fi rectangular antenna the antenna radiates in one direction as depicted by the curve. The maximum radiation is shown in the upper lobe similar to the 3D pattern as shown in Fig.4 (a).The radiation pattern displayed in Fig.4 (b)indicates that the designed TVWS dipole antenna radiates along sideways. Both the lobes (right and left) present the antenna radiating regions.

D. Antennas Fabrication:

The fabricated rectangular patch antenna and dipole antenna are shown in Fig. 5 (a) &5(b) respectively. The rectangular antenna is fabricated using an FR4 substrate with a dielectric thickness of 2.54mm and the relative permittivity is 4.2. The dipole antenna has a feed in the center and is fabricated using an acrylic substrate with two copper sheets. The feed of the antennas is connected with an SMA connector. The connector has two terminals, one is ground and the other is a wave port. These two antennas are the main components used in the anti-theft system.

E. Antenna Parameters:

Table III summarizes the designed antenna parameters. The directivity, gain, efficiency, decay factor, and power are tabulated at a rated frequency 2.4GHz and 654MHz for the rectangular patch and dipole antenna respectively.

Quantity	Rectangular Patch Antenna	Dipole Antenna
Max U (W/sr)	0.154267	0.154267
Peak Directivity	4.020165	4.265102
Peak Gain	1.957686	1.998765
Peak Realized Gain	1.938628	1.945789
Radiated Power (W)	0.482226	0.520876
Accepted Power (W)	0.990265	0.999824
Incident Power (W)	1.000000	1.000000
Radiation Efficiency	0.486967	0.698722
Front-to-Back Ratio	25.577802	20.698771
Decay Ratio	-0.000000	-0.000001

Table III: Antenna parameters.

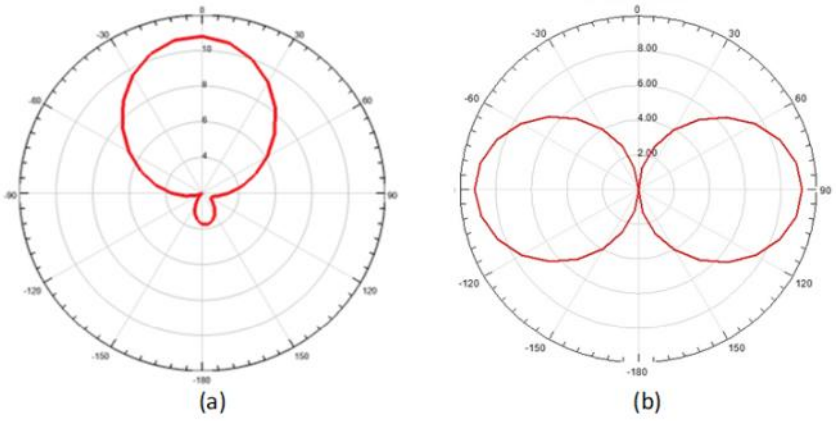


Fig.4: E-Field Pattern (a) Rectangular Patch (b) Microstrip Dipole.

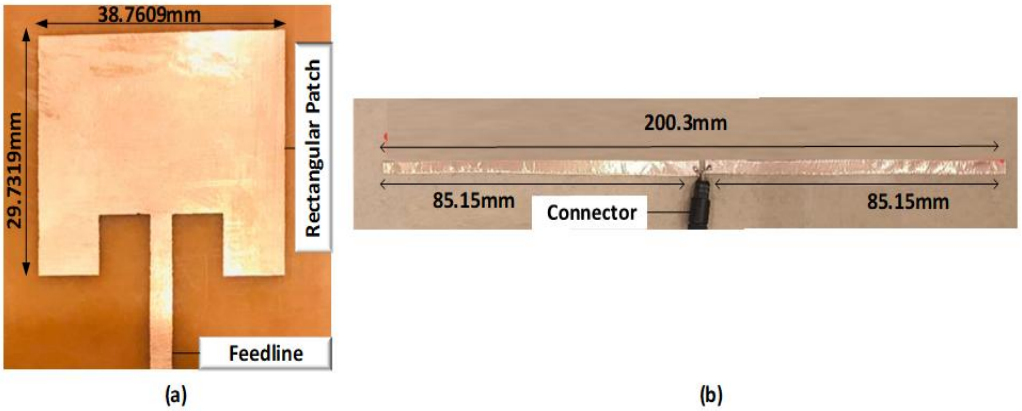


Fig. 5: Antenna Fabrication (a) Rectangular Patch (b) Microstrip Dipole.

F. System Design:

Fig. 6 is a visualization of the proposed anti-theft design with the fabricated antennas. A rectangular patch connected with Wi-Fi as an external antenna, with an operating frequency of 2.4 GHz. The 2.4 GHz frequency is down converted to the TVWS frequency (654 MHz) for the dipole antenna. The lower frequency of TVWS is then used for the dipole antenna which transmits the signal to the user end. The transmission takes place within the low-frequency TVWS spectrum. Therefore, long-range transmission takes place from the antenna to the user end.

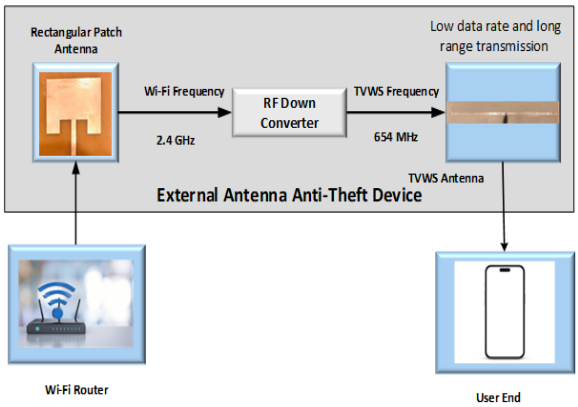


Fig. 6:Anti-Theft system based on patch antennas.

VI. COMPARISON OF RESULTS

The simulated and fabricated results for both antennas are compared, as shown in *Fig. 7*. The difference between the two graphs is due to the measured values taken on the antenna fabricated by chemical etching. Therefore, some deviation is seen between simulated and measured results. The deviation between simulated and measured results has been improved by making modifications and phase analysis in the design using Advanced Design Simulation (ADS). The modified simulation results are achieved because ADS is mostly focused on planar geometries. However, HFSS is a sophisticated tool. Therefore, in ADS simulations the gain is further improved to -27dB as shown *Fig. 8.*

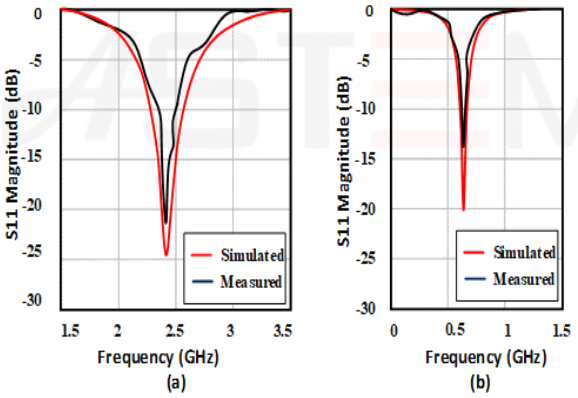


Fig. 7: Comparison of Simulated and Measured Results (a) Rectangular Patch (b) Microstrip Dipole.

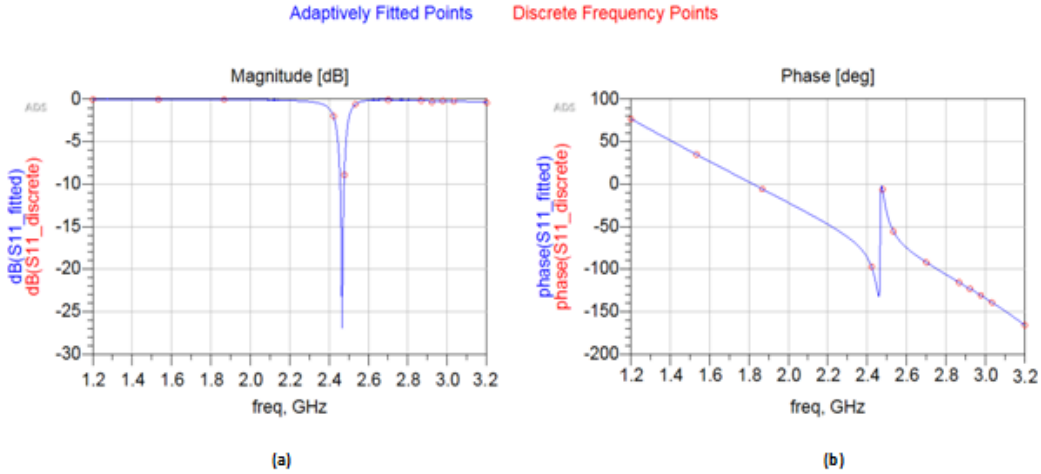


Fig. 8: Improved results in ADS (a) Return Loss [S11] (b) Phase

V. CONCLUSION

The antenna used inside the anti-theft device has been simulated and fabricated. The proposed rectangular antenna operates at a frequency of 2.4 GHz -24 dB, within a range of 2380 MHz which is useful for Wi-Fi. TVWS supports long-range data transmission therefore, the dipole antenna is fabricated operating at a frequency of 654 MHz -20 dB, with bandwidth within a range of 470-790 MHz, which is useful for TVWS. The performance parameters such as return loss and radiation pattern are obtained using HFSS. The parameters such as peak gain, peak directivity, accepted power, and antenna efficiency are tabulated for the design. Hence, both the antennas intended to be used in the anti-theft device are simulated and fabricated.In general, WLANs are vulnerable to both passive and active attacks. Intruders not only steal band width but can also steal personal data. Therefore, it is expected that the research problem will be further resolved in the future. Integration of the anti-theft system consisting of proposed antennas can be tested in real-time and RF front-end development could be possible by a suitable selection

of amplifiers and oscillators for the system. Theft protection and detection will be done using the proposed antennas.

ACKNOWLEDGMENT

The project CMG016 is funded by Africa New Energies Ltd, UK.

REFERENCES

[1] V. O. Etta, A. Sari, A. L. Imoize, P. K. Shukla, and M. Alhassan, "Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique," Mobile Information Systems, vol. 2022, 2022.

[2] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," Computer Networks, vol. 197, p. 108359, 2021.

[3] L. Galeazzi, C. Barría, and J. Hurtado, "Conceptual Model of Security Variables in Wi-Fi Wireless Networks," in ITNG 2021 18th International Conference on Information Technology-New Generations, 2021, pp. 59–67.

[4] C. Meshram, A. L. Imoize, S. S. Jamal, A. Aljaedi, and A. R. Alharbi, "SBOOSP for Massive Devices in 5G WSNs Using Conformable Chaotic Maps," CMC-COMPUTERS MATERIALS & CONTINUA, vol. 71, no. 3, pp. 4591–4608, 2022.

[5] H. S. Choi, D. Carpenter, and M. S. Ko, "Risk taking behaviors using public Wi-fiTM," Information Systems Frontiers, vol. 24, no. 3, pp. 965–982, 2022.

[6] S. Yang, P. Luo, C. C. Loy, and X. Tang, "Faceness-net: Face detection through deep facial part responses," IEEE Trans Pattern Anal Mach Intell, vol. 40, no. 8, pp. 1845–1859, 2017.

[7] R. Mines, "Global Tv White Space Spectrum Market Growth 2022-2028," Jan. 2022.

[8] D. Johnson et al., "Head to head battle of TV White Space and WiFi for connecting developing regions," in International Conference on e-Infrastructure and e-Services for Developing Countries, 2016, pp. 186–195.

[9] L. Simić, M. Petrova, and P. Mähönen, "Wi-Fi, but not on steroids: Performance analysis of a Wi-Fi-like network operating in TVWS under realistic conditions," in 2012 IEEE International Conference on Communications (ICC), 2012, pp. 1533–1538.

[10] H. K. Varshney, M. Kumar, A. K. Jaiswal, R. Saxena, and K. Jaiswal, "A survey on different feeding techniques of rectangular microstrip patch antenna," International Journal of Current Engineering and Technology, vol. 4, no. 3, pp. 418–423, 2014.

[11] K. P. Kumar, K. S. Rao, T. Sumanth, N. M. Rao, R. A. Kumar, and Y. Harish, "Effect of feeding techniques on the radiation characteristics of patch antenna: design and analysis," International Journal of Advanced Research in computer and communication Engineering, vol. 2, no. 2, pp. 1–8, 2013.

[12] L. S. Aji, G. Wibisono, and D. Gunawan, "The adoption of TV white space technology as a rural telecommunication solution in Indonesia," in 2017 15th International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering, 2017, pp. 479–484.

★★★