Signals and Communication Technology

Mohammed El Ghzaoui
Sudipta Das
Varakumari Samudrala
Nageswara Rao Medikondu *Editors*

Next Generation Wireless Communication

Advances in Optical, mm-Wave, and THz Technologies

Springer

Signals and Communication Technology

This series is devoted to fundamentals and applications of modern methods of signal processing and cutting-edge communication technologies. The main topics are information and signal theory, acoustical signal processing, image processing and multimedia systems, mobile and wireless communications, and computer and communication networks. Volumes in the series address researchers in academia and industrial R&D departments. The series is application-oriented. The level of presentation of each individual volume, however, depends on the subject and can range from practical to scientific.

Indexing: All books in "Signals and Communication Technology" are indexed by Scopus and zbMATH

For general information about this book series, comments or suggestions, please contact Mary James at mary.james@springer.com or Ramesh Nath Premnath at ramesh.premnath@springer.com.

Mohammed El Ghzaoui · Sudipta Das ·
Varakumari Samudrala ·
Nageswara Rao Medikondu
Editors

Next Generation Wireless Communication

Advances in Optical, mm-Wave, and THz Technologies

Springer

Editors
Mohammed El Ghzaoui
Faculty of Sciences Dhar El Mahraz
Sidi Mohamed Ben Abdellah University
Fez, Morocco

Varakumari Samudrala
Department of Electronics
and Communication Engineering
NRI Institute of Technology
Vijayawada, Andhra Pradesh, India

Sudipta Das
Department of Electronics
and Communication Engineering
IMPS College of Engineering
and Technology
Malda, West Bengal, India

Nageswara Rao Medikondu
School of Mechanical and Civil Sciences
KLEF Deemed to be University
Guntur, Andhra Pradesh, India

ISSN 1860-4862 ISSN 1860-4870 (electronic)
Signals and Communication Technology
ISBN 978-3-031-56143-6 ISBN 978-3-031-56144-3 (eBook)
https://doi.org/10.1007/978-3-031-56144-3

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024, corrected publication 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

Preface

The primary focus of this book proposal is to highlight advancements in the design of sophisticated components and systems catering to optical, mm-wave, and THz technologies. The exploration of these domains commenced over a century ago, even before these terms were coined. During that era, scientist began delving into the unexplored region of the electromagnetic spectrum situated between infrared and microwave frequencies. Today, these fields of research have gained substantial popularity, witnessing the development of numerous wireless components and experiencing continued expansion. This comprehensive book encompasses the entire scope of the emerging and interdisciplinary field of the electromagnetic spectrum in a concise format. This book could eventually work as a textbook for engineering and communication technology students or science master's programs and for researchers as well. The content includes a thorough exploration of the physical phenomena and cutting-edge wireless components and technologies.

This book explores recent and upcoming technological breakthroughs within the optical, millimeter-wave (mm-wave), and terahertz (THz) frequency ranges. Encompassing a substantial portion of the electromagnetic spectrum, the scope extends up to the conclusion of the near-IR spectrum (i.e., 450 THz). Notably, this frequency span captures a crucial transition zone in technology, marking the shift from electronics to photonics. The focus of the book is on recent advancements and various research challenges pertaining to materials, antennas, detectors, passive circuits, as well as advanced signal processing algorithms tailored for optical, mm-wave, and THz frequency bands. Catering to a broad readership, the book addresses individuals ranging from those with a foundational understanding of basic science to technological experts and research scholars. This comprehensive resource serves as a valuable guide to the diverse aspects of technological evolution in the specified frequency spectrums, making it relevant for a wide audience, including both novices and seasoned professionals.

This book compiles scientific and technological innovations from the academic, industry, and research sectors. Catering to a diverse readership, including undergraduate and master's degree students, research scholars, microwave engineers, biomedical engineers, and professionals in electronics and electrical engineering, the book is poised to serve as an indispensable reference highlighting advanced ideas and concepts in mm-wave, THz, and optical communication technology. It is envisioned as an ideal choice for those seeking to explore fundamental and pivotal advancements in the domain of advanced communication technology, particularly relevant to microwave, electrical, and communication engineers engaged in shaping the next generation of technology.

Fez, Morocco	Mohammed El Ghzaoui
Malda, West Bengal, India	Sudipta Das
Vijayawada, Andhra Pradesh, India	Varakumari Samudrala
Vijayawada, Andhra Pradesh, India	Nageswara Rao Medikondu

Contents

Part I Millimeter Wave (mm-Wave) Technology and Its Applications

Part II Terahertz Technology and Its Applications

Part III Advances in Materials for Optical Spectrum Applications

Part IV Recent Developments in Optical Wireless Communication Technology

Part I
Millimeter Wave (mm-Wave) Technology and Its Applications

Chapter 1
Compact MIMO Antenna Design with Enhanced Isolation for mm-Wave Applications

Navneet Kaur, Aarti Bansal, Surbhi Sharma, and Jaswinder Kaur

1.1 Introduction

The millimeter (mm)-wave-based technology for wireless communication has rapidly gained significant importance owing to its high data rate, high channel capacity to accommodate video streaming, 5G cellular, and mobile communication applications [1, 2]. Millimeter-wave (mm-wave) technology is authorized to be used free of license and highly resistant to atmospheric attenuation with compatibility toward recent 5G technology [3]. Some of the challenges in its implementation are atmospheric attenuation, reflection, and diffraction of electromagnetic waves (EM) leading to multipath fading and low transmission quality in the dense medium [4, 5]. Also, wearable antenna design demands a flexible substrate having the advantage of bending easily on a curved surface [6]. Recently designed conformal antennas have employed [7, 8] conductive textiles, liquid material, and polydimethylsiloxane (PDMS) as their substrates. These materials offer the advantage of being portable supporting the mobility of a person. However, these materials still pose challenges such as integration into application boards or soldering different components. Further, the proposed antenna's performance is severely deteriorated when bending over the surface due to significant multipath reflections and scattering [9, 10]. This further leads to a reduced data rate. Therefore, to overcome these challenges there is a need to increase frequency spectrum and power resources which are restricted. Hence, mm-wave band MIMO antenna has been proposed to increase diversity and spatial multiplexing. However, the MIMO antenna must employ a suitable mutual coupling reduction technique to increase isolation.

N. Kaur · S. Sharma · J. Kaur
Thapar Institute of Engineering and Technology, Patiala, India

A. Bansal (✉)
Chitkara University, Institute of Engineering and Technology, Chitkara University, Patiala, Punjab, India
e-mail: aarti.bansal@chitkara.edu.in

M. El Ghzaoui et al. (eds.), *Next Generation Wireless Communication*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-56144-3_1

Several isolation techniques were introduced to minimize the coupling in MIMO antennas [11–17]. But, still, these are not suitable to be employed in compact wearable antennas. Moreover, optimal placement of antenna elements is required to achieve miniaturization [18]. MIMO antenna design discussed in [19] to achieve resonance in the ISM band. The designed antenna covers a bandwidth of 20% and utilizes a ground plane at its back serving as its radiating element. Further, a wearable antenna designed in [20] uses jeans as its substrate covering a 2.7–12.33 GHz frequency range. To add further, the MIMO antenna designed in [21] exhibits linear polarization in the range from 2.4 to 2.49 GHz. Circularly polarized (CP) MIMO antenna designs enhance communication performance and reduce interference due to multipath propagation while the wearer device is on the move [22]. To summarize, there is a need to design antenna structures with novel isolation techniques and better diversity performance to attain extreme data rates and radiation characteristics. To further enhance performance, MIMO technology is employed, achieving up to a thousand-fold increase in data rates through spatial diversity and multiplexing techniques. The biggest task in the MIMO antenna is to minimize coupling to obtain the acceptable value of isolation within antenna elements.

Here, a compact flexible wearable MIMO antenna with dual-element exhibiting good isolation is designed for 5G mm-wave operating band applications. The suggested design for the proposed antenna utilizes a circular-shaped patch antenna with sectored slots etched around its periphery exciting the specific resonating mode. The slot size and its position are chosen for optimizing its resonance frequency. Also, multiple slots with similar dimensions lead to attaining wide bandwidth resonance. Further, we have optimized distance between antenna elements to minimize the coupling between its individual elements. Also, elements are strategically placed to significantly enhance isolation between them, resulting in optimal diversity. Furthermore, an in-depth evaluation of the suggested MIMO antenna has been done, encompassing analysis of S-parameters and MIMO performance parameters like ECC, diversity gain, etc. From the results, the designed MIMO antenna is justified to be considered as a compelling contender for seamless integration into 5G mm-wave applications such as radar, military, and radio astronomy. The chapter is organized into different sections as detailed here: MIMO antenna design in Sect. 1.2, Sect. 1.3 presents the various significant result parameters such as reflection coefficient, transmission coefficient, ECC, and DG for the proposed antenna design. At last, Sect. 1.4 presents the conclusion of the presented work.

1.2 MIMO Antenna Design

A dual-element MIMO antenna for wideband millimeter-wave operation is constructed with two circular radiating patches positioned on a top plane of the middle substrate layer, as depicted in Fig. 1.1. Individual unit of antenna elements incorporates four sectored slots and excited with a 50-Ω microstrip-fed. Further, dimensions of suggested antenna have been determined through fundamental equations. The final design of antenna has been fabricated on a RT/duroid 5880 a semi-flexible characterized by a ε_r of 2.2, tan δ of 0.0004, and a thickness (h) of 0.508 mm. In Fig. 1.1a, the perspective plane of designed MIMO antenna is presented. On the bottom side, a partial ground plane is integrated for wider bandwidth as portrayed in Fig. 1.1b. The size of the suggested MIMO antenna is 22.5 × 36.0 × 0.508 mm^3, and the optimized value of different dimensions parameters has been tabulated in Table 1.1.

Evolution of Suggested MIMO Antenna

The MIMO antenna design evolution is depicted in Fig. 1.2. The simulation of proposed design has been carried out using CST microwave EM software which involves different design steps as Design-1 (Fig. 1.2a), Design-2 (Fig. 1.2b), and Design-3 (Fig. 1.2c).

This design comprises dual circular-shaped radiating patches fed by simple microstrip feed lines while maintaining the same ground plane as substrate which is shown in Fig. 1.2a. After that design-1 ground plane has been modified to partial

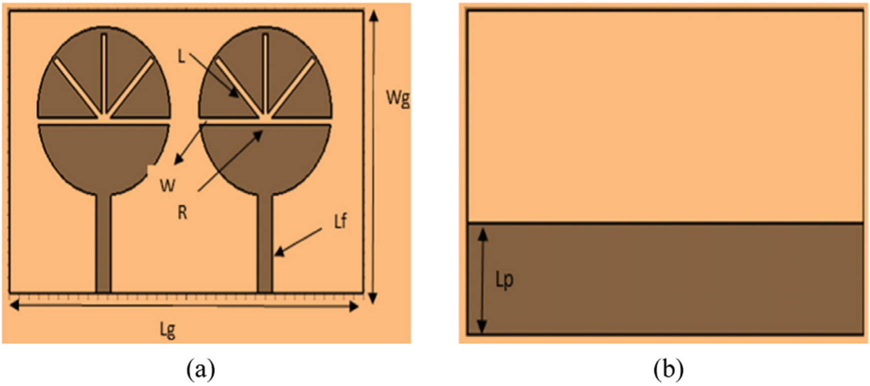

Fig. 1.1 MIMO antenna design: **a** perspective plane, **b** back plane

Table 1.1 Optimized parametric value of suggested MIMO antenna

Parameters	Value (mm)
L	7
W	0.5
R	6.73
Lf	7.7
Lg	22.5
Wg	36
Lp	7.5

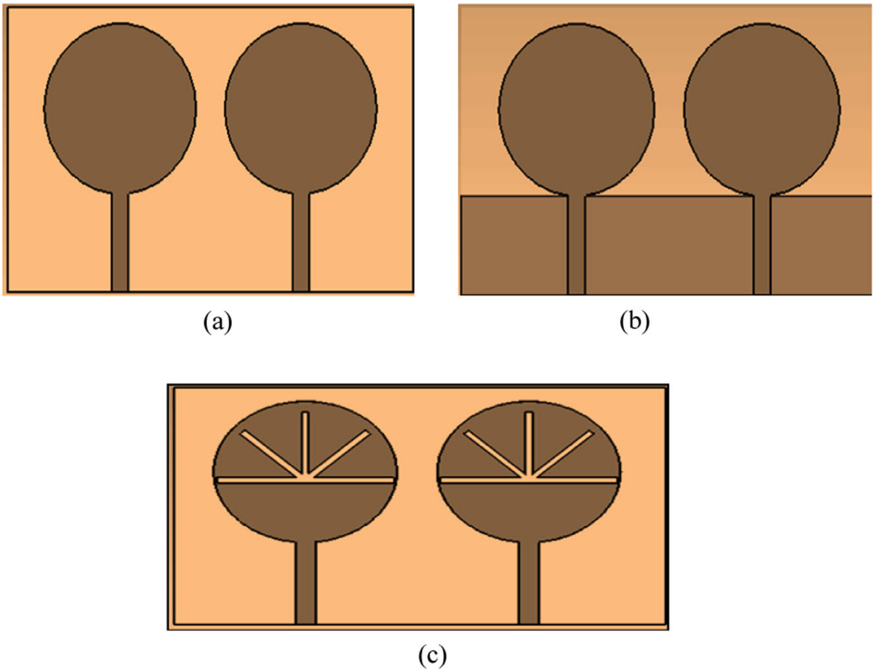

Fig. 1.2 Evolution of suggested MIMO antenna **a** Design step-1, **b** Design step-2, **c** Design step-3

plane as depicted in Fig. 1.2b, thereby enhancing the bandwidth as reported in [23, 24]. In the last step, multiple slots have been etched out from the radiating element of antenna for desired band of 19.7–29.02 GHz as shown in Fig. 1.2c. The resonating frequency (fr) has been determined using equations, thereby radiating patch is acting as a circular waveguide [25–27].

Parametric Studies

The geometry of suggested MIMO antenna has been optimized with parametric sweep of software. Therefore, parametric studies of some important parameters have been discussed in this section.

- **Length of Partial Ground Plane (Lp)**

In the designed part of antenna, partial ground plane plays a crucial role to attain the wider bandwidth of 2 GHz. Thus, a parametric sweep in the CST window has been performed with step size of 0.5 mm from 6.5 to 7.5 mm. As depicted in Fig. 1.3, optimized results have been obtained at Lp equal to 7.5 mm.

- **Length of Slots (*L*)**

Slots have been etched out from the proposed MIMO antenna. These slots are helping in alteration of surface current, and designed antenna is resonating in the desired band.

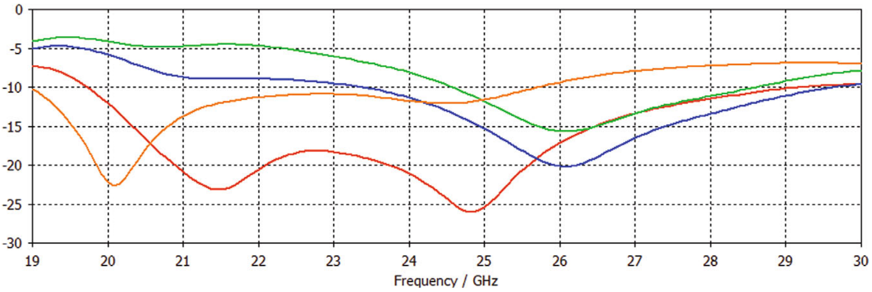

Fig. 1.3 Parametric of partial ground plane

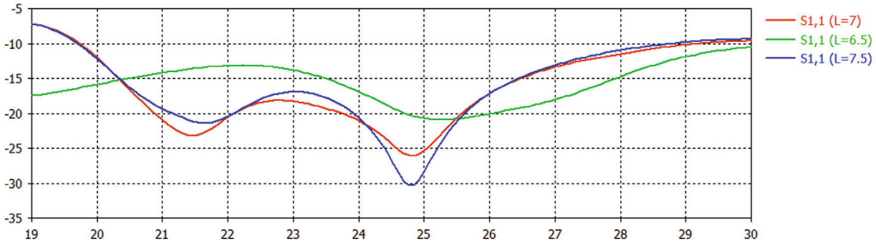

Fig. 1.4 Parametric on length of slots

Thus, a parametric analysis is depicted in Fig. 1.4 with a step size of 0.5 mm. The desired results of proposed antenna are achieving at *L* equal to 7 mm.

1.3 Results and Discussions

The suggested two element MIMO antenna is simulated, and the performance has been analyzed for reflection coefficient, transmission coefficient, ECC, and diversity gain. It is observed from the reflection coefficient results in Fig. 1.5 that the designed antenna resonates in the millimeter range and exhibits bandwidth of around 10 GHz from 19.7 to 29 GHz. Further, the transmission coefficient is displayed in Fig. 1.6 to observe the isolation between adjacent elements of proposed MIMO antenna design. It is revealing that the S_{12} parameter lies below − 10 dB in the complete resonance band between − 19 and − 29 GHz frequency range. This validated that the proposed elements are isolated with each other.

Transmission Coefficient (S_{12})

Envelope Correlation Coefficient (ECC)

The relationship between the individual elements of antenna has been described with envelope correlation coefficient (ECC). It is computed by either *S*-parameters given

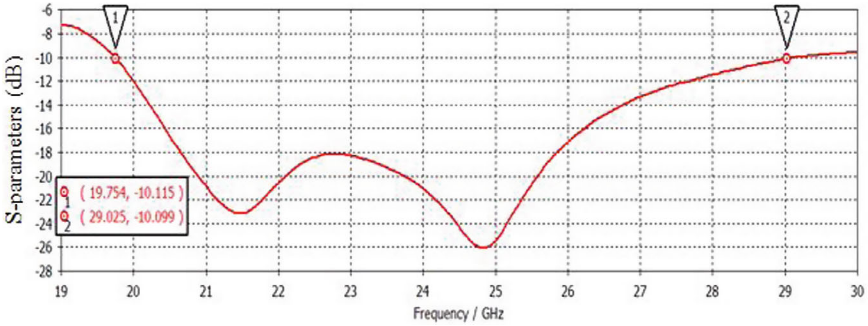

Fig. 1.5 Reflection coefficient of suggested MIMO antenna

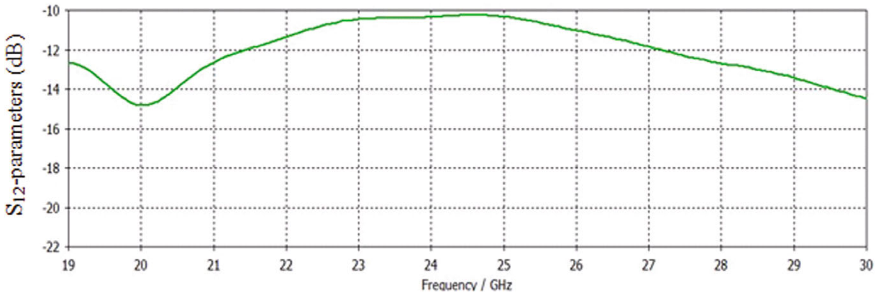

Fig. 1.6 Transmission coefficient of suggested MIMO antenna

in (1.1) or field pattern equation in [2] (Fig. 1.7).

$$\mathrm{ECC_S}(\rho_\mathrm{s}) = \frac{|S_{11}^* S_{12} + S_{21}^* S_{22}|^2}{\left(1 - |S_{11}|^2 - |S_{21}|^2\right)\left(1 - |S_{22}|^2 - |S_{12}|^2\right)} \tag{1.1}$$

$$\mathrm{ECC_F}(\rho_\mathrm{F}) = \frac{|\iint [F_i(\theta,\phi) \cdot F_j(\theta,\phi)]\mathrm{d}\Omega|^2}{\iint |F_i(\theta,\phi)|^2 \mathrm{d}\Omega \iint |F_j(\theta,\phi)|^2 \mathrm{d}\Omega} \tag{1.2}$$

Here, ECCs stands for the envelope correlation coefficient obtained through *S*-parameters, while $\mathrm{ECC_F}$ represents the envelope correlation coefficient determined using far-field methods. Furthermore, the symbol ρ denotes the correlation coefficient specifically associated with MIMO antennas. In case of an ideal MIMO system, this is recommended to keep the ECC value less than 0.5 for optimal performance.

Diversity Gain

Diversity gain (DG) refers to the enhancement in signal-to-noise ratio for the multiple antenna system with respect to the individual antenna. General equations for the calculation of diversity gain are given below [20]:

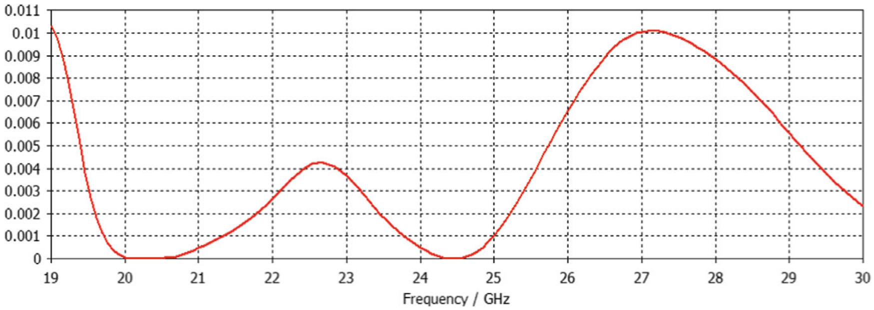

Fig. 1.7 ECC characteristics of MIMO antenna

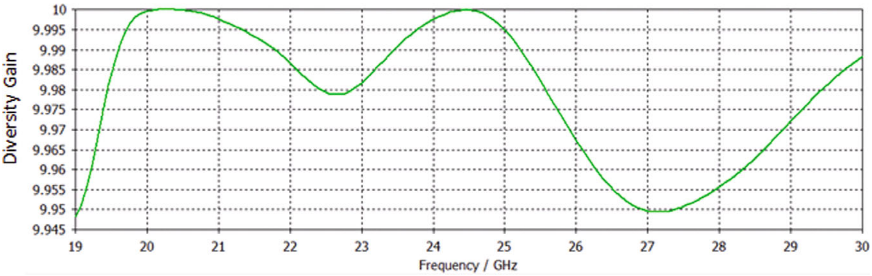

Fig. 1.8 Diversity gain characteristic of MIMO antenna design

$$DG_S = 10\sqrt{1 - (ECC_S)^2} \tag{1.3}$$

$$DG_F = 10\sqrt{1 - (ECC_F)^2} \tag{1.4}$$

Here, DG_s and DG_F are referred for diversity gain using reflection coefficient (*S*-parameters) and far-field methods, respectively. For an ideal MIMO antenna, the value of diversity gain should be equal to 10 (Fig. 1.8).

1.4 Conclusion

MIMO antennas are designed to overcome the challenges of deterioration in data rate, and multipath reflections in conformal antenna design. However, these antennas demand reduced mutual coupling resulting in enhanced isolation amid its individual antenna components. This work discusses and explores various techniques for addressing the issue of mutual coupling. The proposed antenna has been meticulously engineered to deliver exceptional features, including compact size, high isolation, and better diversity performance achieved through precise alignment of radiating elements of the MIMO antenna. This antenna system has demonstrated impressive performance metrics, featuring minimal coupling below − 10 dB, lower ECC (< 0.005), and an ideal diversity gain of 10 dBi. Furthermore, its compact and cost-effective design characteristics make it particularly well-suited for mm-wave 5G applications, facilitating seamless integration into various applications of mm-wave. Additionally, the recommended MIMO design being portable and high performing is a suitable choice for consideration in 5G mm-wave broad spectrum-oriented applications.

References

1. Rappaport, T.S., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., Wong, G.N., Schulz, J.K., Samimi, M., Gutierrez, F.: MillimeterWave mobile communications for 5G cellular: it will work! IEEE Access **1**, 335–349 (2013)
2. Hasan, M., Faruque, M.R.I., Islam, M.T.: Dual band metamaterial antenna for LTE/Bluetooth/WiMAX system. Sci. Rep. **8**, 1240 (2018)
3. Ur-Rehman, M., Malik, N.A., Yang, X., Abbasi, Q.H., Zhang, Z., Zhao, N.: A low profile antenna for millimeter-wave body-centric applications. IEEE Trans. Antennas Propag. **65**(12), 6329–6337 (2017). https://doi.org/10.1109/TAP.2017.2700897
4. Abbas, M.A., Allam, A., Gaafar, A., Elhennawy, H.M., Sree, M.F.: Compact UWB MIMO antenna for 5G millimeter-wave applications. Sensors **23**(5), 2702 (2023)
5. Nadeem, I., Choi, D.-Y.: Study on mutual coupling reduction technique for MIMO antennas. IEEE Access **7**, 563–586 (2018)
6. Pi, Z., Khan, F.: An introduction to millimeter-wave mobile broadband systems. IEEE Commun. Mag. **49**, 101–107 (2011)
7. Katalinic, A., Nagy, R., Zentner, R.: Benefits of MIMO systems in practice: increased capacity, reliability and spectrum efficiency. In: Proceedings of the Proceedings ELMAR 2006, Zadar, Croatia, 7–10 June 2006, pp. 263–266 (2006). ess2020, 8, 100337–100345 [CrossRef]
8. Kumar, S., Dixit, A.S., Malekar, R.R., Raut, H.D., Shevada, L.K.: Fifth generation antennas: a comprehensive review of design and performance enhancement techniques. IEEE Access **8**, 163568–163593 (2020)
9. Molisch, A., Win, M.: MIMO systems with antenna selection. IEEE Microw. Mag. **5**, 46–56 (2004)
10. Paulraj, A., Gore, D., Nabar, R., Bolcskei, H.: An overview of MIMO communications—a key to gigabit wireless. Proc. IEEE **92**, 198–218 (2004)
11. Roshna, T.K., Deepak, U., Sajitha, V.R., Vasudevan, K., Mohanan, P.: A compact UWB MIMO antenna with reflector to enhance isolation. IEEE Trans. Antennas Propag. **63**(4), 1873–1877 (2015). https://doi.org/10.1109/TAP.2015.2398455
12. Deng, J.Y., Li, J., Zhao, L., Guo, L.: A dual-band inverted-F MIMO antenna with enhanced isolation for WLAN applications. IEEE Antennas Wirel. Propag. Lett. **16**, 2270–2273 (2017). https://doi.org/10.1109/LAWP.2017.2713986
13. Wang, L., et al.: Compact UWB MIMO antenna with high isolation using fence-type decoupling structure. IEEE Antennas Wirel. Propag. Lett. **18**(8), 1641–1645 (2019). https://doi.org/10.1109/LAWP.2019.2925857
14. Xu Mao, C., Zhou, Y., Wu, Y., Soewardiman, H., Werner, D.H., Jur, J.S.: Low-profile strip-loaded textile antenna with enhanced bandwidth and isolation for full-duplex wearable applications. IEEE Trans. Antennas Propag. **68**(9), 6527–6537 (2020). https://doi.org/10.1109/TAP.2020.2989862
15. Mirmozafari, M., Zhang, G., Fulton, C., Doviak, R.J.: Dualpolarization antennas with high isolation and polarization purity: a review and comparison of cross-coupling mechanisms.

IEEE Antennas Propag. Mag. **61**(1), 50–63 (2019). https://doi.org/10.1109/MAP.2018.2883032. Tiwari, R.N., Singh, P., Kanaujia, B.K., Kumar, P.: Compact circularly polarized MIMO printed antenna with novel ground structure for wideband applications. Int. J. RF Microw. Comput.-Aided Eng. **31**(8) (2021). https://doi.org/10.1002/mmce.22737

16. Ren, Z., Zhao, A., Wu, S.: MIMO antenna with compact decoupled antenna pairs for 5G mobile terminals. IEEE Antennas Wirel. Propag. Lett. **18**(7), 1367–1371 (2019). https://doi.org/10.1109/LAWP.2019.2916738
17. Iqbal, A., Smida, A., Alazemi, A.J., Waly, M.I., Mallat, N.K., Kim, S.: Wideband circularly polarized MIMO antenna for high data wearable biotelemetric devices. IEEE Access **8**, 17935–17944 (2020). https://doi.org/10.1109/ACCESS.2020.2967397
18. Li, H., Sun, S., Wang, B., Wu, F.: Design of compact singlelayer textile MIMO antenna for wearable applications. IEEE Trans. Antennas Propag. **66**(6), 3136–3141 (2018). https://doi.org/10.1109/TAP.2018.2811844
19. Biswas, A.K., Chakraborty, U.: Compact wearable MIMO antenna with improved port isolation for ultra-wideband applications. IET Microw. Antennas Propag. **13**(4), 498–504 (2019). https://doi.org/10.1049/iet-map.2018.5599
20. Jilani, S.F., Munoz, M.O., Abbasi, Q.H., Alomainy, A.: Millimeterwave liquid crystal polymer based conformal antenna array for 5G applications. IEEE Antennas Wirel. Propag. Lett. **18**(1), 84–88 (2019). https://doi.org/10.1109/LAWP.2018.2881303
21. Wen, D., Hao, Y., Munoz, M.O., Wang, H., Zhou, H.: A compact and low-profile MIMO antenna using a miniature circular highimpedance surface for wearable applications. IEEE Trans. Antennas Propag. **66**(1), 96–104 (2018). https://doi.org/10.1109/TAP.2017.2773465
22. Qu, L., Piao, H., Qu, Y., Kim, H.-H., Kim, H.: Circularly polarised MIMO ground radiation antennas for wearable devices. Electron. Lett. **54**(4), 189–190 (2018). https://doi.org/10.1049/el.2017.4348
23. Ullah, U., Al-Hasan, M., Koziel, S., Mabrouk, I.B.: A series inclined slot-fed circularly polarized antenna for 5G 28 GHz applications. IEEE Antennas Wirel. Propag. Lett. **20**(3), 351–355 (2021). https://doi.org/10.1109/LAWP.2021.3049901
24. Xia, Z., et al.: A wideband circularly polarized implantable patch antenna for ISM band biomedical applications. IEEE Trans. Antennas Propag. **68**(3), 2399–2404 (2020). https://doi.org/10.1109/TAP.2019.2944538
25. Sharma, M.: Design and analysis of MIMO antenna with high isolation and dual notched band characteristics for wireless applications. Wirel. Pers. Commun. **112**, 1587–1599 (2020). https://doi.org/10.1007/s11277-020-07117-4
26. Garg, R., Bhartia, P., Bahl, I., Ittipiboon, A.: Microstrip Antenna Design Handbook. Artech House, London, UK (2001)
27. Tayyab, U., Kumar, A., Petry, H.P., Asghar, M.E., Hein, M.A.: Dual-band nested circularly polarized antenna array for 5G automotive satellite communications. Appl. Sci. **13**(21), 11915 (2023)

Chapter 2
Security Threats and Privacy Challenges in Millimeter-Wave Communications

A. Amsaveni and M. Bharathi

2.1 Introduction

This chapter aims to provide an extensive overview of the security threats and privacy challenges faced in the realm of Millimeter-wave communications, addressing both current concerns and potential future issues. It explores various vulnerabilities, and potential exploits, and, importantly, offers a range of mitigation strategies to safeguard networks and protect individual privacy in the rapidly advancing landscape of wireless communication technologies.

2.1.1 Evolution of mmWave Communications

Millimeter-wave (mmWave) communications represent a revolutionary leap in wireless technology. Traditionally confined to lower frequency bands, the integration of mmWave has unleashed a new era of high-speed data transmission, enabling applications in 5G networks, point-to-point communication, and various other wireless technologies. These extremely high frequencies, ranging from 30 to 300 GHz, have unlocked the potential for faster data rates and low-latency connectivity, contributing significantly to digital transformation across various industries. Initial research in this field aimed to explore the feasibility of mmWave frequencies for wireless communications, emphasizing their ability to carry large amounts of data due to their high bandwidth.

A. Amsaveni (✉) · M. Bharathi
Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, Tamilnadu 641049, India
e-mail: amsaveni.a.ece@kct.ac.in

M. Bharathi
e-mail: bharathi.m.ece@kct.ac.in

M. El Ghzaoui et al. (eds.), *Next Generation Wireless Communication*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-56144-3_2

Advancements in antenna design, semiconductor technologies, and signal processing have played a crucial role in shaping the evolution of mmWave communications. Breakthroughs in phased array antennas and beamforming techniques have enabled the efficient focusing and directing of signals, compensating for the propagation limitations associated with mmWave frequencies [1].

The advent of 5G technology marked a pivotal point in integrating mmWave frequencies into commercial networks. 5G networks incorporated mmWave bands, leveraging their potential for ultra-fast, high-bandwidth applications. Initial commercial deployments, primarily in dense urban areas, aimed to exploit the high data rates offered by mmWave frequencies [2].

2.1.2 Scope and Significance of Security Threats

The implementation of mmWave communications has expanded the scope of connectivity and introduced a new frontier of security threats. With its unique characteristics, such as shorter transmission ranges and higher susceptibility to signal attenuation, mmWave technology faces a spectrum of security challenges. Threats such as eavesdropping, interception, man-in-the-middle attacks, and vulnerability at the physical layer pose significant risks to the confidentiality, integrity, and availability of data transmitted over mmWave networks. Understanding and mitigating these threats are imperative to ensure the reliability and security of these networks in our increasingly interconnected world [3].

2.1.3 Privacy Challenges in mmWave Networks

In tandem with security threats, mmWave technology confronts substantial privacy challenges. The high data transfer speeds and the ability to support numerous connected devices intensify concerns regarding user privacy. Issues like location tracking, identity theft, and unauthorized surveillance raise significant concerns about individual privacy rights. The seamless and pervasive nature of mmWave networks heightens the risk of personal information exposure, demanding effective measures to protect users' sensitive data while maintaining a balance between innovation and privacy.

As the utilization of mmWave communications becomes more prevalent, an in-depth understanding of the security threats and privacy challenges is essential. This chapter aims to explore these critical issues, providing insights into the vulnerabilities, potential exploits, and strategies to safeguard the integrity and privacy of mmWave networks in this rapidly evolving technological landscape [4].

2.2 Security Threats in mmWave Communications

2.2.1 Eavesdropping and Interception

Eavesdropping and interception represent critical threats in millimeter-wave (mmWave) communications due to the vulnerability of these high-frequency signals to interception, potentially compromising the confidentiality of transmitted data [5]. MmWave signals are more prone to line-of-sight transmission, making interception relatively easier. Malicious actors can exploit this vulnerability to passively intercept data transmitted between devices, compromising the confidentiality of information. The directional nature of mmWave transmission, often used in point-to-point and point-to-multipoint communications, can be advantageous for high-speed data transfer. Still, it also increases the susceptibility of intercepted signals [6].

Encryption plays a crucial role in mitigating eavesdropping threats. Implementing robust encryption algorithms, such as Advanced Encryption Standard (AES) or Elliptic Curve Cryptography (ECC), ensures that data is protected during transmission, preventing unauthorized access and interception of sensitive information [7].

Additionally, advancements in beamforming technology have introduced adaptive beamforming techniques, enabling better signal control and directionality. Secure beamforming strategies play a role in reducing the vulnerability to eavesdropping by limiting the accessibility of signals to intended recipients and reducing the exposure to potential eavesdroppers [8].

However, ensuring the security of mmWave communications against eavesdropping (as in Fig. 2.1) requires a holistic approach, incorporating encryption, secure beamforming, and continual advancements in cryptographic protocols to counter potential threats to the integrity and confidentiality of data transmitted over mmWave networks.

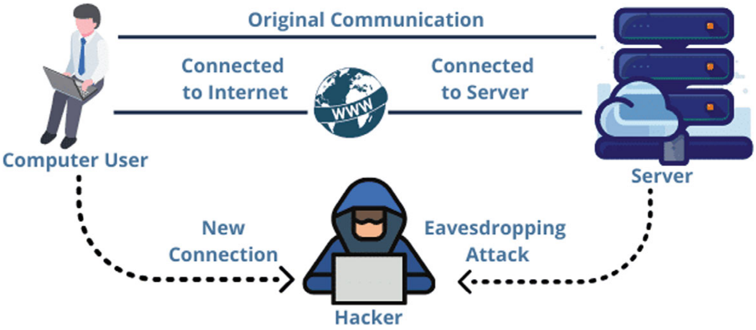

Fig. 2.1 Illustration of eavesdropping attack

2.2.2 *Man-in-the-Middle Attacks*

Man-in-the-middle (MitM) attacks pose a serious threat in millimeter-wave (mmWave) communications, exploiting the characteristics of these high-frequency transmissions. As shown in Fig. 2.2, MitM attacks occur when an attacker intercepts communication between two parties and may either passively eavesdrop on the transmission or actively modify the data being exchanged [9]. The directional nature of mmWave transmission, typically employed in point-to-point and point-to-multipoint communication, presents a particular vulnerability to such attacks due to the focused transmission patterns.

Secure beamforming, a fundamental technology in mmWave networks, is integral in reducing the susceptibility to MitM attacks. Properly implemented beamforming enables precise control over the direction of the transmitted signal, limiting its accessibility to intended recipients and reducing the chance of interception by unauthorized entities [10].

The integration of robust authentication protocols is critical in preventing MitM attacks. Utilizing strong authentication mechanisms, such as mutual authentication and digital signatures, ensures the integrity and authenticity of communication channels. Implementing secure key exchange protocols, such as the Diffie–Hellman key exchange or Public Key Infrastructure (PKI), fortifies the communication channel against potential manipulation or eavesdropping by unauthorized entities [11].

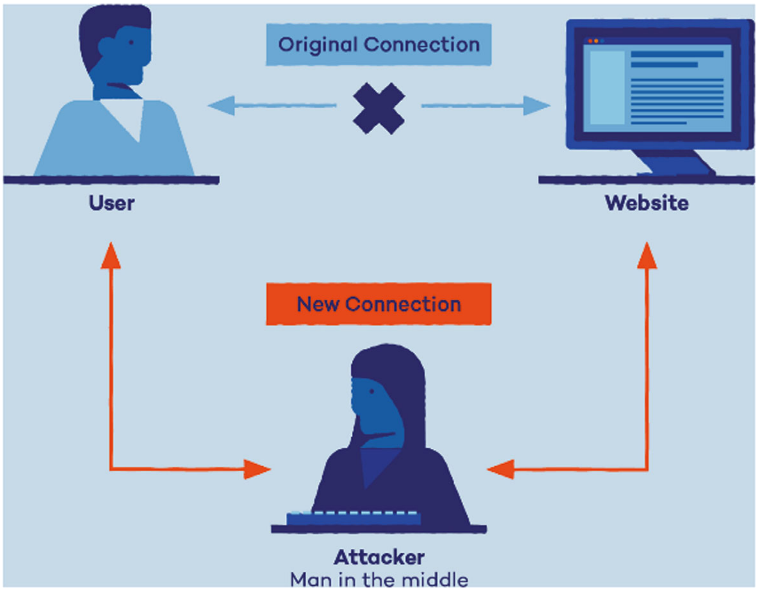

Fig. 2.2 Illustration of meet-in-the middle attack

Moreover, continuous monitoring using intrusion detection systems in mmWave networks is vital. These systems can identify anomalous behaviors and potential threats, providing a layer of defense against MitM attacks by detecting any deviations in the normal transmission patterns [12].

While these measures contribute to mitigating the risks associated with MitM attacks in mmWave communications, a comprehensive security approach is necessary, combining secure beamforming, robust authentication, secure key exchange, and active monitoring to protect against these sophisticated attack vectors.

2.2.3 Denial-of-Service (DoS) Attacks

Denial-of-Service (DoS) attacks pose a significant threat to millimeter-wave (mmWave) communications, potentially disrupting the availability and reliability of these networks. These attacks aim to overwhelm a network's resources, rendering it inaccessible to legitimate users as depicted in Fig. 2.3 [13].

The vulnerability of mmWave signals to atmospheric conditions and physical obstacles can be exploited in DoS attacks. Adversaries can manipulate these vulnerabilities to create signal obstructions or introduce interference, leading to disruptions in the transmission of mmWave signals [14].

Implementing traffic filtering mechanisms and rate limiting is crucial in mitigating DoS attacks. These mechanisms help in identifying abnormal traffic patterns and restricting excessive incoming traffic that may overwhelm the network infrastructure [15].

Advanced anomaly detection systems, particularly Intrusion Detection and Prevention Systems (IDPSs), play a pivotal role in identifying and mitigating DoS attacks. These systems monitor network behavior and patterns, identify unusual

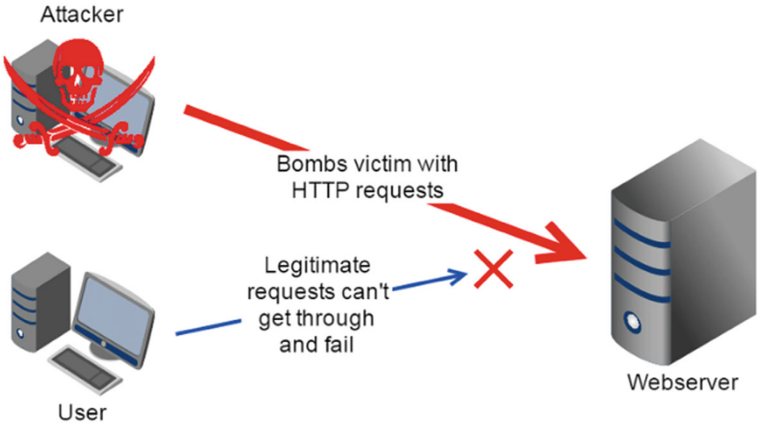

Fig. 2.3 Illustration of Denial-of-Service attack

traffic and behavior that could indicate a potential DoS attack, and then take preventive measures to mitigate the impact of such attacks.

Moreover, dynamic spectrum access techniques can be employed to mitigate the impact of DoS attacks. Dynamic frequency allocation and spectrum management allow for efficient utilization of available frequency bands, enabling the network to switch to less congested or interference-free frequency channels when an attack is detected [16].

The combined application of these strategies—traffic filtering, anomaly detection systems, and dynamic spectrum access—can effectively mitigate the impact of DoS attacks, ensuring the availability and reliability of mmWave networks.

2.2.4 Physical Layer Attacks

Physical layer attacks in millimeter-wave (mmWave) communications exploit vulnerabilities in the underlying transmission medium, potentially compromising the integrity and reliability of the communication. The susceptibility of mmWave signals to environmental conditions, such as rain, humidity, and atmospheric absorption, can be manipulated to launch physical layer attacks. Adversaries might utilize signal obstructions or interference to disrupt the transmission of mmWave signals, causing signal degradation, packet loss, or complete communication failure [17].

Radio Frequency (RF) interference is a significant threat to the physical layer. Adversaries might deploy unauthorized transmitters or intentionally generate interference that disrupts the mmWave signal, causing communication degradation or Denial of Service [18].

To mitigate these threats, implementing secure physical layer transmission techniques is essential. Beamforming technology, when used securely, can direct signals precisely, mitigating interference and ensuring more reliable communication paths.

Employing advanced modulation and coding schemes can also enhance resilience against physical layer attacks. Using error-correcting codes and robust modulation schemes increases the system's ability to tolerate interference and maintain communication integrity even in the presence of noise or interference.

Furthermore, adaptive and cognitive radio techniques offer a way to dynamically adjust to changing environmental conditions and counteract physical layer attacks by allowing devices to dynamically change their transmission parameters to optimize communication in the presence of interference [19].

By integrating secure transmission techniques, advanced modulation schemes, and adaptive radio techniques, mmWave systems can improve their resilience against physical layer attacks, ensuring reliable and robust communication.

2.2.5 Authentication and Authorization Vulnerabilities

Authentication and authorization vulnerabilities in millimeter-wave (mmWave) communications can potentially compromise the security and integrity of these networks. Weaknesses in these mechanisms can lead to unauthorized access, data breaches, and various security threats.

Weak Authentication Protocols: Flaws in authentication protocols can open gateways for attackers to gain unauthorized access to the network as shown in Fig. 2.4. Inadequate authentication mechanisms or weak password policies can allow adversaries to infiltrate the system [20].

Lack of Mutual Authentication: One-way authentication in mmWave communications might leave the network susceptible to impersonation attacks. Lack of mutual authentication mechanisms could enable attackers to impersonate legitimate users or devices, gaining access to the network and compromising its security [21].

Inadequate Authorization Controls: Authorization mechanisms might not be sufficiently robust, allowing unauthorized users or devices to access sensitive data or network resources. Lack of stringent access control can lead to unauthorized usage or manipulation of network resources.

Implementing robust authentication and authorization measures is crucial to reinforce mmWave networks against these vulnerabilities. Utilizing strong encryption, two-way authentication protocols, and stringent access control policies can help mitigate the risks associated with these vulnerabilities, safeguarding the integrity and confidentiality of communication in mmWave systems.

These vulnerabilities necessitate a comprehensive approach to strengthen authentication and authorization protocols, ensuring the resilience of mmWave networks against potential security breaches.

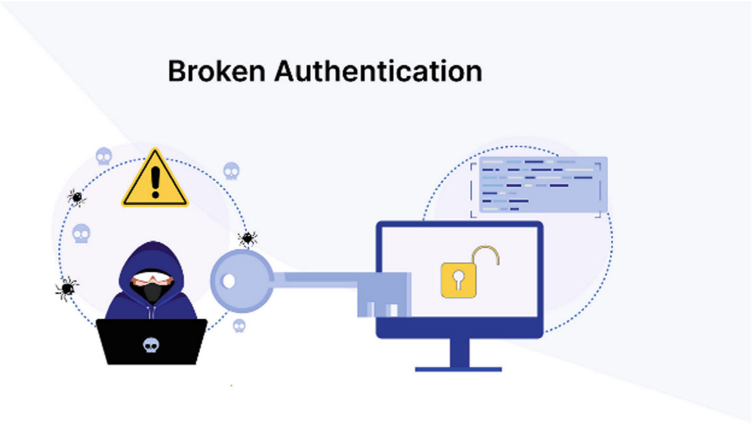

Fig. 2.4 Broken authentication

2.3 Privacy Concerns in mmWave Networks

2.3.1 Location Tracking and Profiling

One of the foremost privacy concerns in mmWave networks revolves around location tracking and user profiling. The directional and focused nature of mmWave signals, integral to achieving high data rates, also brings about the potential for precise location tracking. The use of phased array antennas and beamforming techniques for signal transmission and reception enables more accurate localization of devices within the network. This precision could lead to detailed and specific tracking of device locations.

While precise location tracking can offer various benefits, it also raises significant privacy concerns. The ability to accurately track and trace the movements of devices within the coverage area poses potential threats to individual privacy. Adversaries could potentially exploit this characteristic to track user movements, creating detailed profiles of an individual's activities, routines, and habits. This information could be misused for targeted advertising, invasion of personal space, or even physical security threats.

The detailed information gathered through location tracking might facilitate the creation of user profiles and behavioral patterns. Profiling users based on their movement, habits, and frequent locations could result in the potential misuse of this data for targeted advertising, surveillance, or even invasive tracking without user consent. The sample of this is shown in the Fig. 2.5.

2.3.2 Data Breaches and Information Leakage

The high-speed, high-bandwidth capabilities of mmWave networks also expose users to increased risks of data breaches and information leakage. The transfer of large volumes of data through these networks heightens the potential impact of a breach. Weaknesses in encryption methods, inadequate security measures, or vulnerabilities in the protocols used for data transfer can lead to unauthorized access and exposure of sensitive information, resulting in data breaches that compromise user privacy. Figure 2.6 compares data breaches and data leaks.

2.3.3 Identity Theft and Impersonation

MmWave networks, if compromised, can become a breeding ground for identity theft and impersonation. Attackers, by exploiting vulnerabilities in the network, could gain access to user identities or impersonate legitimate users. Such breaches not only compromise the individual's personal information but could also lead to