International Journal in IT & Engineering (IJITE)
Volume 13 Issue 02, February 2026 ISSN: 2321-1776 Impact Factor: 8.256
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

AN INVESTIGATION OF THE ATTITUDES, BEHAVIOURS, AND CONCERNS OF USERS WITH REGARD TO THE SECURITY OF MILLIMETRE-WAVE COMMUNICATION SYSTEMS

Sachin Kataria[1], Dr. Sandeep Kumar Kulhari[2], Dr. Gireesh Kumar Dixit[3]
[1]Research Scholar, [2]Professor, [3]Associate Professor
[1,2,3]Department of Engineering and Technology
Shyam University, Dausa, Rajasthan

ABSTRACT

Millimetre wave encompasses the electromagnetic spectrum ranging from 30 GHz to 300 GHz, corresponding to wavelengths between 10 mm and 1 mm. Millimeter wave technology is applicable for high-speed wireless broadband communications. Millimeter wave technology is an advanced wireless technology capable of delivering multi-Gbps communication across small distances between electronic devices. This research investigates the attitudes, behaviours, and concerns of users with regard to the security of millimetre-wave communication systems**.** Throughout this methodology, a quantitative approach is employed, utilizing a close-ended questionnaire based on a Likert scale. The questionnaire is distributed to respondents, and data is collected from them using a random sampling method. Additionally, secondary data is gathered from various sources, including published journals, online libraries, and academic papers. This research concludes that mmWave communication systems are secure for communication in terms of data transmission due to improvements made in wireless communication technology. The role that security features play is vital for users' perceptions of these communication systems, hence motivating them to use high-frequency communication technology for their communication needs. The need for security and the significance of receiving security updates for these communication systems encourage users to access mmWave communication technology. Users are very careful with their information; hence, a good security system is a motivating factor for client trust with mmWave technology. Surveillance, jamming, and breaches are some of the factors indicating the need to educate users about mmWave technology's benefits and dangers.

Keywords:- Mmwave Communication Systems, Users, Technology, Attitude, Behaviour

1. INTRODUCTION

Millimetre wave encompasses the electromagnetic spectrum ranging from 30 GHz to 300 GHz, corresponding to wavelengths between 10 mm and 1 mm. Millimeter wave technology is applicable for high-speed wireless broadband communications. Millimeter wave technology is an advanced wireless technology capable of delivering multi-Gbps communication across small distances between electronic devices. The anticipated transmission rate is projected to be 40–100 times faster than current wireless LAN technologies, capable of transmitting a complete DVD's data in approximately 15 seconds. This will provide advanced wireline access without concerns over cable connections. The chipsets, inclusive of antennas, will become compact and economical. It enables the wireless transmission of signals utilizing a 60 GHz band carrier frequency. This frequency range is over 1,000 times greater than that utilized for FM radio. Moreover, dependable digital data transfer at multi-Gbps rates needs advanced coding algorithms. Consequently, the digital data must be encoded and decoded accurately at multi-Gbps data speeds to ensure efficient and reliable transmission [1-2]. The swift proliferation of mobile data and smartphone usage is presenting unparalleled problems for wireless service providers in addressing a global bandwidth deficit.

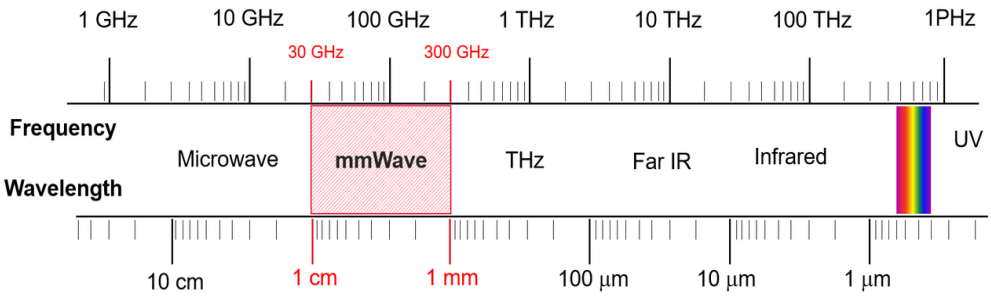

Fig 1: Millimeter wave [3]

Figure 1 illustrates communication within millimeter wave frequency ranges. Millimeter wave is an underutilized frequency band that can be employed in a wide array of products and services, including high-speed networks and point-to-point communications. For many decades, military applications have predominantly utilized millimeter wave technology's systems. Due to advancements in process technologies and cost-effective integration solutions, millimeter wave technology has begun to get significant attention from academics, industry,

and standardization organizations. The development of Complementary Metal Oxide Semiconductor technology, which is cheap and uses little power, has made it easier to use the millimeter wave spectrum for wireless communications, including applications that require high Quality of Service (QoS) [4].

Millimeter wave communications in the 60 GHz band are regarded as a pivotal technology for facilitating multigigabit wireless transmission. The large bandwidth of 60 GHz provides numerous advantages regarding capacity and flexibility. The 5G cellular network enhances system rates by 1000 times compared to current systems within a decade, owing to mobile traffic demands. Numerous research studies examine the incorporation of millimeter wave access into existing cellular networks as a multiband heterogeneous network that leverages the ultra-wideband characteristics of millimeter wave communication. The proliferation of mobile data and the utilization of improved mobile phone technology present a challenge for wireless service providers to address a bandwidth scarcity issue. Consequently, the use of millimeter wave frequencies has increased. It is necessary to provide higher information rates, broadened breadth, reduced limitations, and diminished latency to address the continuously growing demand and facilitate new applications [5].

1.2. CURRENT SECURITY TECHNOLOGY FOR MM-WAVE WIRELESS COMMUNICATION SYSTEM

The rapid advancement of wireless communication networks, particularly with the emergence of 6G technology and the Internet of Everything (IoE), has resulted in increased complexity and sophistication. This environment facilitates the integration of artificial intelligence (AI) technologies, such as machine learning (ML), into various interconnected networks, users, and devices [6]. However, this complexity also heightens the risk of advanced cyberattacks, as malicious actors can exploit vulnerabilities using AI methods, complicating the development of effective security protocols. To tackle these challenges, a novel intrusion detection system (IDS) has been proposed, which employs feature selection (FS) and AI techniques like ensemble learning (EL) to improve accuracy and minimize false positive rates (FAR) [7]. The model incorporates various machine learning algorithms for precise identification of threats. The chi-square method is applied for processing four unbalanced datasets—NSL_KDD, UNSW_NB15, CIC_IDS17, and SCE_CIC_IDS18—

thus enhancing the training and testing phases, reducing processing time, and improving accuracy [8].

This also presents a meta-model intended to integrate the previously mentioned datasets with various machine learning techniques, including random forest (RF), gradient boosting, AdaBoosting, LightGBM, XGBoosting, and CatBoosting. The objective is to develop a method that effectively identifies and combines the results of different classifiers during the testing phase.As the demand for modern wireless communication networks rises, the widespread adoption of 5G technologies is expected between 2027 and 2030. Networks employing microwave technology highlight the critical role of small-cell networking for better encryption and modulation techniques. However, existing security measures are predominantly based on traditional cryptographic techniques, which fail to adequately address the distinct challenges posed by wireless networks. Additionally, the convergence of blockchain technology, AI, and ML presents significant potential for improving the security of data technologies used in healthcare environments, notably by protecting sensitive information through a distributed architecture. This approach mitigates risks associated with insider threats and enhances the security of data handling across the network, which is crucial in addressing national security concerns related to modern wireless communication network design and implementation [9-10].

1.3. ATTITUDES, BEHAVIOURS, AND CONCERNS OF USERS

User perception of security in millimeter-wave (mmWave) communication systems is nuanced, highlighting both security advantages and vulnerabilities. The high directivity of mmWave provides inherent security benefits, making wide-angle interception challenging; however, this same characteristic enables new threats. Attackers can exploit these narrow beams for eavesdropping, service disruption, and data interception through AI techniques. Key issues include the vulnerability to eavesdropping from sophisticated radars that can monitor private communications despite the theoretical security. Additionally, mmWave's sensitivity to environmental blockages poses risks related to connection loss and denial-of-service (DoS) attacks. The need for enhanced security solutions, particularly Physical-Layer Security (PLS), is emphasized due to the limitations of traditional cryptographic methods in high-speed, low-latency scenarios. Moreover, continuous beam alignment in mmWave is a

critical vulnerability that attackers can exploit. To mitigate these risks, researchers are focusing on advanced techniques such as injecting artificial noise to confuse eavesdroppers, utilizing machine learning for secure key generation and beam prediction, and employing reconfigurable intelligent surfaces to strengthen legitimate signals while disrupting attacks. This multifaceted approach aims to improve the security landscape for mmWave communication systems.

1.3 EFFECTIVE SECURITY FRAMEWORKS AND TECHNIQUES

The transition from 4G to 5G networks starts with the deployment of standalone (NSA) 5G solutions, emphasizing new radio components while still relying on 4G protocols for user equipment control. Consequently, current 5G implementations inherit several security vulnerabilities from 4G systems. This document analyzes both standalone and non-standalone 5G networks, focusing on potential risks through a risk matrix that evaluates 12 possible threat scenarios affecting core and radio access networks [11-14]. Five primary security challenges associated with 5G technology are identified:

1. Mitigating DDoS attacks due to vulnerabilities in IoT devices.
2. Managing the reliability of Radio Access Networks (RAN) and small cells in diverse wireless environments.
3. Enhancing visibility for security monitoring in a decentralized mobile network.
4. Addressing issues related to third-party applications, API reliability, and internal mobile communication connections due to Multi-Access Edge Computing (MEC).
5. Implementing dynamic security management by integrating physical hardware with virtualization platforms and network slicing [15-18].

To confront these security obstacles, 5G standards have introduced enhancements, particularly focusing on the signaling control plane, while user plane security features require further development. The SBI interface poses additional vulnerabilities due to traditional HTTP weaknesses. As modern telecommunications continue to evolve, 5G offers significant advantages over previous generations, including adaptability, reduced latency, compatibility with various systems, and improved data transfer rates. However, the rapid growth of 5G infrastructure introduces new security challenges, particularly with wireless backhaul processes, which are more susceptible to attacks compared to wired connections. It also

discusses the development of a multirate feed forward controller to enhance tracking performance in MIMO LTI systems, utilizing HNOMA for improved spectrum efficiency in uplink scenarios. The system addresses the challenges of multiple access in real-world conditions and enhances reliability while reducing latency, particularly when precise channel state information (CSI) is unavailable [19-24]. The 5G network must effectively accommodate numerous users across its different service categories, focusing on energy efficiency in Call Admission Control (CAC) to support the growing number of networked devices and applications, thereby facilitating the expansion of the Internet of Things [25-27].

2. LITERATURE REVIEW

M. Faisal, G., et al. (2022) incorporated security and privacy in millimeter-wave communications. Millimeter-wave communication mechanisms engage three major components of secure communication operations. The suggested approach for mmWave communication enables the identification of the principal signal at the physical (PHY) layer to ascertain the spectrum throughput for the primary user (PU) and secondary user (SU). The maximum throughput for the primary user (PU) in SC is 0.7934, but the maximum throughput for the secondary user (SU) is 0.7679. We will develop a millimeter-wave communication system to address this issue. The probability of detection (PD) is forecasted at a specified range of 690 km with an estimated accuracy of 83.56%, whilst the probability of false alarm (PFA) is anticipated at a defined range of 230 km with an estimated accuracy of 81.39%. This contradictory yet interconnected issue is examined in three phases to resolve it using a cross-layer model encompassing MAC and PHY levels for a secure communication network (SCN), simultaneously mitigating the collision effect by 92.76% for both layers. MATLAB 2019b will be utilized, as the rising requirement for enhancing bandwidth in secure communications has driven technological advancement.

Saini, M., and Grewal, S.K., (2024) discovered that millimeter wave MIMO wireless communication techniques are utilized in 5G and subsequent generation networks. The literature has demonstrated the efficacy of deep learning models in enhancing the performance of these systems. However, many deep learning models are vulnerable to security issues, such as adversarial attacks. Consequently, it is imperative to ensure that these systems are resilient to such threats in order to facilitate high-quality, secure communication. Adversarial training

is a method whereby deep learning models are preemptively trained to withstand adversarial attacks. This work implements adversarial training for three types of adversarial attacks: Fast Gradient Sign Method, Iterative Fast Gradient Sign Method, and Momentum Iterative Fast Gradient Sign Method. The simulation findings illustrate a reduction in error at the receiving end following adversarial training, even in the presence of an adversarial attack.

Rajendran, S., et al. (2018) discovered that millimeter wave MIMO wireless communication techniques are utilized in 5G and subsequent generation networks. Literature has demonstrated the efficacy of deep learning models in enhancing the performance of these systems. Nonetheless, numerous deep learning models are susceptible to security concerns, including adversarial attacks. Consequently, it is imperative to ensure that these systems are resilient to such threats in order to facilitate high-quality, secure communication. Adversarial training is a method whereby deep learning models are preemptively trained to withstand adversarial attacks. This work implements adversarial training for three types of adversarial attacks: Fast Gradient Sign Method, Iterative Fast Gradient Sign Method, and Momentum Iterative Fast Gradient Sign Method. The simulation results indicate a reduction in error at the receiving end following adversarial training, even in the presence of an adversarial attack.

Ye, H., et al. (2017) demonstrated our preliminary findings on deep learning for signal recognition and channel estimation in orthogonal frequency-division multiplexing (OFDM) systems. In this paper, they use deep learning to manage wireless OFDM channels from beginning to end. The suggested deep learning-based method estimates channel state information (CSI) implicitly and recovers the sent symbols directly, in contrast to current OFDM receivers that first estimate CSI explicitly and then use the estimated CSI to detect or recover the transmitted symbols. A deep learning model is initially trained offline using simulated data based on channel characteristics to mitigate channel distortion. The online transmitted data is then immediately recovered using the deep learning model. According to the simulation results, the deep learning-based method performs similarly to the minimal mean square error (MMSE) estimator in terms of detecting transmitted signals and addressing channel distortion. Additionally, when nonlinear clipping noise is present, the cyclic prefix (CP) is removed, and fewer training pilots are employed, the deep learning-based method outperforms traditional techniques. In conclusion, deep learning shows promise as a technique

for signal recognition and channel estimation in wireless communications with complex interference and channel distortion.

Renda, A., et al. (2021) discovered that the design stage of next-generation cellular networks is anticipated to be a critical time for understandable artificial intelligence (XAI). It is becoming more and more obvious that AI will be necessary to handle the network's ever-increasing complexity as 5G is being deployed and 6G is only being conceptualized. However, AI models will need to have high levels of explanation in addition to great performance. In this study, we demonstrate how fuzzy models could be a good fit for this problem. Using a Random Forest (RF) classifier on a Quality of Experience classification dataset, we contrast fuzzy and classical decision tree models. According to the study, fuzzy decision trees outperform classical ones in detecting stall occurrences in a video streaming application and are simpler to understand in our context. There is a notable increase in explainability that offsets the accuracy loss compared to the RF classifier, which is regarded as a black-box ensemble model.

Amsaveni, A., & Bharathi, M. (2024) identified that millimeter-wave (mmWave) communication, functioning within the high-frequency band of 30 to 300 GHz, is set to transform wireless connectivity. mmWave communications offers high-speed (up to 10 Gbps), low-latency wireless connectivity in the 5G era and beyond. It can facilitate high-speed internet connectivity for residences and enterprises, in addition to supporting emerging applications like virtual reality and augmented reality. Nonetheless, the implementation of mmWave technology presents numerous security vulnerabilities and privacy concerns that require meticulous attention. This chapter examines the diverse array of security concerns and privacy issues associated with mmWave communication. This chapter examines the distinctive attributes of mmWave technology, including its directional properties and vulnerability to signal obstruction, which present new security risks. The many security and privacy vulnerabilities of mmWave networks are further examined. The chapter details the numerous security and privacy measures that can protect mmWave networks effectively. The chapter underscores the necessity for robust security techniques to safeguard against emerging threats in mmWave networks. The chapter finishes with an examination of the unresolved research difficulties in security and privacy pertaining to mmWave communications.

3. METHODOLOGY

In the previous section we assessed the review of literature to identify the gaps and provide this research in new direction. For that in this section we are mention the material and methods for gathering the data and interpret the results. This study investigates the attitudes, behaviours, and concerns of users with regard to the security of millimetre-wave communication systems**.** Throughout this methodology presents quantitative method. Where we prepared close ended questionnaire in a likert scale form and distributing the questionnaire to respondents and gather the data from them. The data has been gathered from selected respondents through random sampling mode. The selected sampling size is 100. In secondary data we gather the data from published journals, online libraries and published papers etc. The data has been analysed through excel 2010. The data collected for this research includes two modes: 1) The Primary mode of data, and 2) The Secondary mode of data.

Primary data: - The primary source of data has been gathered from respondents through survey mode. We selected 100 respondents through random sampling mode. With this we prepare a close ended survey in likert scale form and distributing the survey to respondents. In the questionnaire part we prepare a question regarding demographic variables, attitude and user behaviour and advantages and security concerns challenges. The collected data from respondents are analysed in excel 2010.

Secondary data: - The secondary sources of data are collected from published journal, online libraries and govt. published papers etc.

4. RESULTS

In the previous section, we discussed about the research methodology that shows the methods used in this research to get data and do the analysis. The current section reflects the in-depth analysis and the interpretation of the data gathered about the attitudes, behaviours, and concerns of users with regard to the security of millimetre-wave communication systems.

4.1.Demographic Variables

Demographic Variables	Frequency	Percentage
Gender		
Male	61	61%
Female	49	49%
Age of the Respondents		
16-25	37	37%
26-40	45	45%
40+	18	18%
Education Background of the respondents		
12^{th}	10	10%
UG	17	17%
PG	10	10%
IT	34	34%
NON-IT	29	29%
Location		
Urban	49	49%
Rural	27	27%
Semi-Urban	24	24%
Marital Status		
Unmarried	27	27%
Married	45	45%
Separated/Divorced	10	10%
Widowed	18	18%
Income Status		
25,000-50,000	50	50%
51,000-1,00,000	27	27%
1,00,001 above	23	23%
Stake holder group		
Industry Experts	19	19%
Researchers	24	24%
Legislators	16	16%
End Users	41	41%

The above table indicates the demographic variables of this research. We selected 61 male and 49 female respondents for this research. The age category for this research is divided into three groups: 37 respondents lie about being age 16-25, 45 respondents lie about being age 26-40, and 18 respondents lie about being age above 40. The educational qualifications of the respondents are divided into four categories. 1) High school 2) Graduation 3) Post graduation and 4) Professional degree (IT background) and 5) Professional degree (Non- IT background). Among these respondents, 12 respondents did high school, 17 respondents did graduation, 10

respondents did post-graduation, and 34 respondents did a professional degree (IT Background) and 29 respondents did a professional degree (Non- IT background). The locations of the respondents come from different backgrounds. 1) Rural, 2) Semi-urban, and 3) Urban. Among these respondents, 49 respondents come from urban backgrounds, 24 respondents come from semi-urban backgrounds, and 27 respondents come from rural backgrounds. The selected respondents come from different Marital status. Among these respondents, 27 participants are unmarried, 45 respondents are married, 10 respondents are separate/divorced, and 18 respondents come widows. The income scales of the respondents are categorized in 3 parts due to the respondents' income status. 1) 25,000-50,000 2) 51,000-1,00,000 3) 1,00,001 above. Among these respondents, 50 have incomes earn between 25,000-50,000, 27 have incomes between 51,000 and 1,00,000 23 primarily earn above 1,00,001. The respondents' are from different stakeholder groups. Among these respondents, there are 19 respondents that are industry experts along with 24 respondents are researchers and 16 respondents are legislators and lastly 41 respondents are end users.

4.2. Attitudes and user behaviour regarding Security of Mm-wave communication systems

Attitudes and user behaviour regarding Security of Mm-wave communication systems	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Millimetre wave communication systems appear to be secure for data transmission in daily life.	17	35	16	12	20
Advanced wireless technology is believed to offer protection for critical personal information.	23	31	17	9	19
Security features play a significant role in forming an opinion about mmWave communication systems.	25	28	15	16	16
Higher confidence in the security of mmWave networks motivates users to use high-frequency wireless services.	39	31	17	8	5

Good security measures contribute to increased trust in mmWave-based networks.	24	41	5	17	13
The security aspects affect the choice of devices that facilitate mmWave communication.	31	28	15	16	6
The use of mmWave-based services depends on knowledge of potential security threats.	39	38	10	8	5
Security settings are also considered essential in using high-speed wireless networks.	17	35	16	12	20
Upgrades/patches are considered useful in the maintenance of security, particularly in advanced communication systems.	29	35	16	10	10
Caution is observed while sharing personal information via the mmWave network.	34	37	4	10	15

The above table presents *Attitudes and user behaviour regarding Security of Mm-wave communication systems*. With the statement that *Millimetre wave communication systems appear to be secure for data transmission in daily life* shows that majorly respondents are agreeing. Out of the total respondents, 17 respondents strongly agree, 35 respondents agree, 16 are neutral, 12 respondents are disagree and 20 respondents are strongly disagree. With the statement that *Advanced wireless technology is believed to offer protection for critical personal information* shows that majority of respondents are agreeing. Out of the total respondents there are 23 respondents are strongly agree along with 31 respondents are agreeing, 17 are neutral and 9 respondents are disagree and lastly 19 respondents are disagree. With the statement that *Security features play a significant role in forming an opinion about mmWave communication systems* shows that majority of respondents are agreeing. Out of the total respondents there are 25 respondents are strongly agree along with 28 respondents are agreeing, 15 are neutral and 16 respondents are disagree and lastly 16 are strongly disagree. With the statement that *Higher confidence in the security of mmWave networks motivates users to use high-frequency wireless services* shows that majority of respondents are agreeing. Out of the total respondents, there are 39 respondents are strongly agree along with 31 respondents are agreeing and 17 respondents are neutral and 8 respondents are disagree and lastly 5 are strongly disagree. With the statement that *Good security measures contribute to increased trust in MmWave-based*

networks shows that majority of respondents are agreeing. Out of the total respondents, there are 24 respondents are strongly agree along with 41 respondents are agreeing and 5 respondents are neutral and 17 respondents are disagree and lastly 13 respondents are strongly disagree. With the statement that *the security aspects affect the choice of devices that facilitate mmWave communication* shows that majority of respondents are strongly agree. Out of the total respondents 39 respondents are strongly agree along with 28 respondents are agreeing and 15 respondents are neutral and 16 respondents are disagree and lastly 6 respondents are strongly. With the statement that *the use of mmWave-based services depends on knowledge of potential security threats* shows that majority of respondents are strongly agree. Out of the total respondents there are 39 respondents are strongly agree along with 38 respondents are agreeing and 10 are neutral and 8 respondents are disagree and lastly 5 respondents are strongly disagree. With the statement that *Security settings are also considered essential in using high-speed wireless networks* shows that majority of respondents are agreeing. Out of the total respondents, there are 17 respondents that are strongly agreed along with 35 respondents are agreeing, 16 respondents are neutral and 12 respondents are disagreeing and lastly 20 respondents are strongly disagreeing.With the statement that *Upgrades/patches are considered useful in the maintenance of security, particularly in advanced communication systems* shows that majority of respondents are agreeing. Out of the total respondents, there are 29 respondents that are strongly agreed along with 35 respondents are agreeing, 16 respondents are neutral and 10 respondents are disagreeing and lastly 10 respondents are strongly disagreeing. With the statement that *Caution is observed while sharing personal information via the MmWave network* shows that majority of respondents are agreeing. Out of the total respondents, there are 34 respondents that are strongly agreed along with 37 respondents are agreeing, 4 respondents are neutral and 10 respondents are disagreeing and 15 respondents are strongly disagreeing.

4.3. Advantages Of Security Of Millimetre-Wave Communication Systems

Advantages Of Security Of Millimetre-Wave Communication Systems	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Security protocol increases confidence in mmWave communication.	34	22	14	12	18
Transparent security information helps alleviate concerns about mmWave technology.	29	27	22	8	14
The trust in service providers also influences perceptions of mmWave network security.	31	42	15	5	7
Better security standards are anticipated for future mmWave communication systems.	41	34	5	12	8
Overall Security Assurance and Its Influence on the Long-Term Acceptance of mmWave Communication Technology	71	21	1	3	4

The above table presents *Advantages of Security of Millimetre-Wave Communication Systems*. With the statement that *Security protocol increases confidence in mmWave communication* shows that majorly respondents are strongly agree. Out of the total respondents, 34 respondents strongly agree, 22 respondents agree, 14 are neutral, 12 respondents are disagree and 18 respondents are strongly disagree. With the statement that *Transparent security information helps alleviate concerns about mmWave technology* shows that majority of respondents are strongly agree. Out of the total respondents there are 29 respondents are strongly agree along with 27 respondents are agreeing, 22 are neutral and 8 respondents are disagree and lastly 14 respondents are disagree. With the statement that *The trust in service providers also influences perceptions of mmWave network security* shows that majority of respondents are agreeing. Out of the total respondents there are 31 respondents are strongly agree along with 42 respondents are agreeing, 15 are neutral and 5 respondents are disagree and lastly 7 are strongly disagree. With the statement that *Better security standards are anticipated for future mmWave communication systems* shows that majority of respondents are strongly agree. Out of the total respondents, there are 41 respondents are strongly agree along with 34 respondents are agreeing

and 5 respondents are neutral and 12 respondents are disagree and lastly 8 are strongly disagree. With the statement that *Overall Security Assurance and Its Influence on the Long-Term Acceptance of mmWave Communication Technology* shows that majority of respondents are strongly agree. Out of the total respondents, there are 71 respondents are strongly agree along with 21 respondents are agreeing and 1 respondents are neutral and 3 respondents are disagree and lastly 4 respondents are strongly disagree.

4.4. Disadvantages Of Security Of Millimetre-Wave Communication Systems

Disadvantages Of Security Of Millimetre-Wave Communication Systems	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Eavesdropping	22	56	1	9	12
Jamming	31	39	6	10	14
Interference	29	45	7	12	7
Data breach	23	53	9	6	9
Lack of awareness	26	58	4	6	6
Limited range	28	48	6	9	9
Unauthorised access	17	53	8	7	15

The above table presents *Disadvantages of Security of Millimetre-Wave Communication Systems.* In the terms of *Eavesdropping* shows that majorly respondents are agreeing. Out of the total respondents, 22 respondents strongly agree, 56 respondents agree, 1 are neutral, 9 respondents are disagree and 12 respondents are strongly disagree. In the terms of *Jamming* shows that majorly respondents are agreeing. Out of the total respondents, 31 respondents

strongly agree, 39 respondents agree, 6 are neutral, 10 respondents are disagreeing and 14 respondents are strongly disagreeing. In the terms of *Interference* shows that majorly respondents are agreeing. Out of the total respondents, 29 respondents strongly agree, 45 respondents agree, 7 are neutral, 12 respondents are disagreeing and 7 respondents are strongly disagreeing. In the terms of *Data breach* shows that majorly respondents are agreeing. Out of the total respondents, 23 respondents strongly agree, 53 respondents agree, 9 are neutral, 6 respondents are disagreeing and 9 respondents are strongly disagreeing. In the terms of *Lack of awareness* shows that majorly respondents are agreeing. Out of the total respondents, 26 respondents strongly agree, 58 respondents agree, 4 are neutral, 6 respondents are disagree and 6 respondents are strongly disagree. In the terms of *Limited range* shows that majorly respondents are agreeing. Out of the total respondents, 28 respondents strongly agree, 48 respondents agree, 6 are neutral, 9 respondents are disagree and 9 respondents are strongly disagree. In the terms of *Unauthorised access* shows that majorly respondents are agreeing. Out of the total respondents, 17 respondents strongly agree, 53 respondents agree, 8 are neutral, 7 respondents are disagree and 15 respondents are strongly disagree.

5. CONCLUSION

In conclusion, it can be understood that the research in this study has shown that mmWave communication systems are considered to be secure for the transmission of data in general due to the rapid developments in wireless technology that ensure the security of critical personal information. The presence of security features is important because it shapes users' perceptions of mmWave communication systems. This encourages trust in the security measures taken in the communication systems, and therefore, the users are encouraged to connect to high-frequency wireless networks since they are convinced that the security features are effective in that aspect. Security needs are critical factors to consider when choosing communication devices for mmWave communication systems. Additionally, the likelihood that users are willing to connect to mmWave communication depends on their level of awareness about security concerns. It is considered that updates are critical in enhancing security integrity, especially in sophisticated communication systems. Users are aware that security settings are critical in accessing high-speed wireless networks. Users cautiously share personal information through mmWave networks. The advantages associated with the security of mmWave communication include the establishment of security protocols to ensure that the clients have

confidence in the security measures and the provision of security information that is transparent to alleviate concerns about the security of mmWave communication. The anticipation for the improvement of security standards for future mmWave communication systems is affected by the trust that the clients have in the service providers. As far as the security of the mmWave communication systems is concerned, it also comes with certain drawbacks such as surveillance activities, jamming, interference, data breaches, lack of awareness amongst users regarding the system, the range of the system, as well as a chance of unauthorized access. Moreover, these issues make a case for the significance of educating users about the benefits of the mmWave communication technology.

REFERENCES

1. Pi, Z., & Khan, F. (2011). An introduction to millimeter-wave mobile broadband systems. *IEEE Communications Magazine. IEEE Communications Society*, *49*(6), 101–107. doi:10.1109/mcom.2011.5783993
2. Yong, S. K. (2005). Multi gigabit wireless through millimeter wavein 60 GHz band. In *Proceedings of Wireless Conference Asia*. Singapore.
3. Rappaport, T. S., Murdock, J. N., & Gutierrez, F. (2011). State of the art in 60 GHz integrated circuits & systems for wireless communication. *Proc. IEEE*, *99*, 1390–1436.
4. What is mmWave (millimeter wave). (n.d.). Retrieved February 10, 2026, from Dfrobot.com website: https://wiki.dfrobot.com/What_is_mmWave_Millimeter_Wave
5. Pi, Z., & Khan, F. (2011). An introduction to millimeter wave mobile broadband system. *IEEE Communication. Mag*, *49*(6), 101–107.
6. Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *24*(2), 767–809. https://doi.org/10.1109/comst.2022.3159185
7. Oleiwi, H. W., Mhawi, D. N., & Al-Raweshidy, H. (2023). A meta-model to predict and detect malicious activities in 6G-structured wireless communication networks. *Electronics*, *12*(3), 643. https://doi.org/10.3390/electronics12030643
8. Chandan, R. R., Balobaid, A., Cherukupalli, N. L. S., Gururaj, Flammini, F., & Natarajan, R. (2023). Secure modern wireless communication network based on

blockchain technology. *Electronics*, *12*(5), 1095. https://doi.org/10.3390/electronics12051095

9. Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y.-J. A. (2019). The roadmap to 6G: AI empowered wireless networks. *IEEE Communications Magazine*, *57*(8), 84–90. https://doi.org/10.1109/mcom.2019.1900271
10. Duan, Z., Song, P., Yang, C., Deng, L., Jiang, Y., Deng, F., Jiang, X., Chen, Y., Yang, G., Ma, Y., & Deng, W. (2022). The impact of hyperglycaemic crisis episodes on long-term outcomes for inpatients presenting with acute organ injury: A prospective, multicentre follow-up study. *Frontiers in Endocrinology*, *13*. https://doi.org/10.3389/fendo.2022.1057089
11. Lin, Z., An, K., Niu, H., Hu, Y., Chatzinotas, S., Zheng, G., & Wang, J. (2022). SLNR-based secure energy efficient beamforming in multibeam satellite systems. *IEEE Transactions on Aerospace and Electronic Systems*, 1–4. https://doi.org/10.1109/taes.2022.3190238
12. Mokhtari, S., Abbaspour, A., Yen, K. K., & Sargolzaei, A. (2021). A machine learning approach for anomaly detection in industrial control systems based on measurement data. *Electronics*, *10*(4), 407. https://doi.org/10.3390/electronics10040407
13. Sommestad, T., Holm, H., & Steinvall, D. (2022). Variables influencing the effectiveness of signature-based network intrusion detection systems. *Information Security Journal A Global Perspective*, *31*(6), 711–728. https://doi.org/10.1080/19393555.2021.1975853
14. Laxman, M. M., & Prof. Sapike N. S. (2024). Securing the next wave: A comprehensive review of 5G system security. *International Journal of Advanced Research in Science, Communication and Technology*, 146–157. https://doi.org/10.48175/ijarsct-17427
15. Arip Winanto, E., Yazid Idris, M., Stiawan, D., & Sulkhan Nurfatih, M. (2021). Designing consensus algorithm for collaborative signature-based intrusion detection system. *Indonesian Journal of Electrical Engineering and Computer Science*, *22*(1), 485. https://doi.org/10.11591/ijeecs.v22.i1.pp485-496
16. Creech, G., & Hu, J. (2014). A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. *IEEE Transactions on Computers. Institute of Electrical and Electronics Engineers*, *63*(4), 807–819. https://doi.org/10.1109/tc.2013.13

17. Mhawi, D. N., & Hashem, P. S. H. (2021). Proposed Hybrid CorrelationFeatureSelectionForestPanalizedAttribute Approach to advance IDSs. *Karbala International Journal of Modern Science*, *7*(4). https://doi.org/10.33640/2405-609x.3166
18. Oleiwi, H. W., Saeed, N., Al-Taie, H. L., & Mhawi, D. N. (2022). Evaluation of differentiated services policies in multihomed networks based on an interface-selection mechanism. *Sustainability*, *14*(20), 13235. https://doi.org/10.3390/su142013235
19. Rajagopal, S., Kundapur, P. P., & Hareesha, K. S. (2020). A stacking ensemble for network intrusion detection using heterogeneous datasets. *Security and Communication Networks*, *2020*, 1–9. https://doi.org/10.1155/2020/4586875
20. Gui, G., Liu, M., Tang, F., Kato, N., & Adachi, F. (2020). 6G: Opening New Horizons for integration of comfort, security, and intelligence. *IEEE Wireless Communications*, *27*(5), 126–132. https://doi.org/10.1109/mwc.001.1900516
21. Zhang, J., Su, Q., Tang, B., Wang, C., & Li, Y. (2023). DPSNet: Multitask learning using geometry reasoning for scene depth and semantics. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(6), 2710–2721. https://doi.org/10.1109/tnnls.2021.3107362
22. Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open Journal of the Communications Society*, *1*, 957–975. https://doi.org/10.1109/ojcoms.2020.3010270
23. Chowdhury, M. Z., Shahjalal, M., Hasan, M. K., & Jang, Y. M. (2019). The role of optical wireless communication technologies in 5G/6G and IoT solutions: Prospects, directions, and challenges. *Applied Sciences (Basel, Switzerland)*, *9*(20), 4367. https://doi.org/10.3390/app9204367
24. Hu, X., Jin, L., Lou, Y., Zhong, Z., & Sun, X. (2021). *Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions*. https://doi.org/10.36227/techrxiv.14125346
25. Parvathy, & Rajalakshmi, S. (2021). A review on network layer attacks in wireless sensor networks. *International Journal of Computer Sciences and Engineering*, *9*(3), 45–48. https://doi.org/10.26438/ijcse/v9i3.4548

26. Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. *Electronics*, *10*(12), 1437. https://doi.org/10.3390/electronics10121437
27. Jasim, Ögren, Minovski, & Andersson. (2020). Packet probing study to assess sustainability in available bandwidth measurements: Case of high-speed cellular networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *11*(2), 106–125. https://doi.org/10.22667/JOWUA.2020.06.30.106
28. M. Faisal, G., Abed Alshadoodee, H. A., Hadi Abbas, H., Muwafaq Gheni, H., & Al-Barazanchi, I. (2022). Integrating security and privacy in mmWave communications. *Bulletin of Electrical Engineering and Informatics*, *11*(5), 2856–2865. doi:10.11591/eei.v11i5.4314
29. Saini, M., and Grewal, S.K., (2024) "Security Enhancement of mmWave MIMO Wireless Communication System Using Adversarial Training." *IEEJ Transactions on Electrical and Electronic Engineering*, vol. 19, no. 6, pp. 967–974, doi:10.1002/tee.24025.
30. Rajendran, S., Meert, W., Giustiniano, D., Lenders, V., & Pollin, S. (2018). Deep learning models for wireless signal classification with distributed low-cost spectrum sensors. *IEEE Transactions on Cognitive Communications and Networking*, *4*(3), 433–445. doi:10.1109/tccn.2018.2835460
31. Ye, H., Li, G. Y., & Juang, B.-H. F. (2017). Power of deep learning for channel estimation and signal detection in OFDM systems. Retrieved from http://arxiv.org/abs/1708.08514
32. Renda, A., Ducange, P., Gallo, G., & Marcelloni, F. (2021). XAI models for quality of experience prediction in wireless networks. *2021 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE.
33. Amsaveni, A., & Bharathi, M. (2024). Security threats and privacy challenges in millimeter-wave communications. In *Signals and Communication Technology* (pp. 13–33). Cham: Springer Nature Switzerland.