RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Protecting 5G Wireless Networks through Physical Layer Security

Rosaria Arokia raj[1], C.Sivasamy[2], Dr.M.Vadivel[3]

Assistant Professor, Information Technology, Excel Engineering College, Namakkal[1,2]
Associate Professor, Information Technology, Excel Engineering College, Namakkal[3]

Abstract

Meeting the ever-increasing needs for future wireless *applications—such as ultra-high data rates, ultra-wide radio coverage, ultra-large device counts, and ultra-low latency—will be made possible in large part by the fifth generation (5G) network. In the context of the 5G network, where wireless signals are intrinsically susceptible to security breaches, security is a crucial topic that this article addresses. In particular, we concentrate on physical layer security, which uses the disruptive technologies to 5G to its advantage while protecting data confidentiality by taking use of the inherent randomness of the communications medium. Three of the most promising technologies are discussed: millimetre wave, huge multiple-input multiple-output, and heterogeneous networks. Based on the fundamental ideas behind each technology, we pinpoint the vast opportunities and enduring difficulties that security designers need to overcome. It is anticipated that this identification will significantly increase our understanding of physical layer security in the future.*

Keywords: 5G wireless, Physical Layer Security, Hetrogeneous Network,Spatial Modeling.

Introduction

Due to its appealing properties, such as ease and mobility, wireless communication is the most popular data transfer technology and is widely used in modern life. As a result, it has several uses in the areas of banking, entertainment, communication, defence, and finance, among others. The sent data in the majority of these applications may contain confidential information to which unauthorised access is prohibited. When unauthorised users obtain access and alter the confidential information of authorised users, security is compromised. However, in wired networks, where the signal goes over wires and data is therefore difficult for unauthorised users to access, the threat posed by malevolent attackers is less serious. Since signals from wireless networks travel through the atmosphere as electromagnetic waves, the communication system is more open to attack. Although wireless networks provide users with greater mobility and flexibility, they also present far greater security challenges than wired networks.

A trustworthy communication system is essential for the safe and secure transfer of sensitive data. Information security is necessary for all communication systems, but because wireless networks have open access and are more vulnerable, it becomes even more important and difficult. Despite this, information security is still a difficult problem. Cryptographic techniques are used in conservative security measures, and they are applied at higher communication layers. The computational complexity of the cryptographic algorithms determines the secrecy strength of the cryptosystem. However, modern wireless systems such as Body Area Networks (BAN), Internet of Things (IoT), Radio Frequency Identification (RFID) systems, Visible Light Communication (VLC), and Power Line Communication (PLC) have limited resources in terms of computational capacity, processing, and power, so such highly sophisticated, computationally complex cryptographic techniques cannot be fully adapted to them.

The main concept behind Physical Layer Security (PLS) is to create secure information transfer to intended users in the presence of adversaries by taking advantage of the limitations and features of wireless transmission media. (Aghdam et al, 2019) PLS seeks to create gearbox that is less complicated and more

energy-efficient. strategies based on the wireless physical layer to improve security performance. Additionally, it can support the augmentation of current cryptographic techniques with extra layer of protection.

PLS is built on Shannon's (1949) groundbreaking work on the mathematical theory of communication, which established the information theory of secrecy. (Güvenkaya et al, 2017) This article presents a theoretical characterization of PHY's capacity to enable secure communication. This, however, concentrated on symmetric key encryption, which has problems with key generation, handling, and sharing. (Hamamreh et al, 2019) Furthermore, the entropy of the information and the secret key must almost equal each other. Afterwards, the wiretap channel used by the eavesdropper is louder than the channel used by the legal user, private communication between authorised users can occur even when there are eavesdroppers present.

Because wireless networks are by their very nature open access and broadcasting, they are susceptible to a wide range of attacks. (Ji et al, 2018) There are two main categories for the attacks: passive attacks and aggressive attacks. During active attacks, adversaries attempt to disrupt communication, change or modify the information being communicated, or use techniques like denial of service, masquerading, message manipulation, and so forth. (Liu et al, 2017) Passive attacks, such as eavesdropping and traffic analysis, limit the adversary's ability to get information without interfering with communication.

It is insufficient to address all information security concerns in wireless networks by depending solely on higher layer security techniques, particularly those involving traffic analysis and eavesdropping assaults. (Poor et al, 2017) This thesis proposes PLS strategies that may withstand these two kinds of security threats at the physical layer of wireless networks, together with masquerading, by accomplishing security qualities including secrecy, authentication, and privacy.

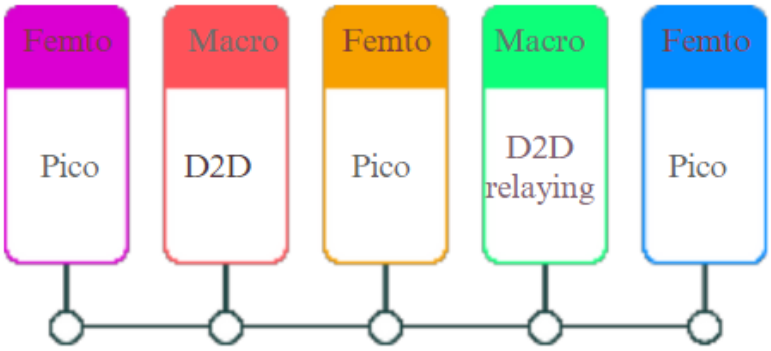

Figure 1. Heterogeneous network.

PHYSICAL LAYER SECURITY IN HETEROGENEOUS NETWORKS

In the 5G era, the HetNet is a promising network densification design. The HetNet's goal is to offer an energy- and spectrum-efficient solution that meets the dramatically increasing data requirements of future wire-less applications. (Sánchez et al, 2021) The multi-tier hierarchical design of the HetNet is formed by the deployment of nodes with varying transmit powers, coverage areas, and radio access protocols, as seen in Figure 1. (Sanenga et al, 2020) Large radio coverage regions are assigned to high-power nodes (HPNs) in macro cell tiers, whereas tiny radio coverage areas are assigned to low-power nodes (LPNs) in small cell tiers. Small cells, like pico and femto cells, are placed under macro cell canopies to increase coverage outdoors in densely populated urban, suburban, or rural locations as well as indoors in heavily occupied buildings, multi-tenant housing units, and businesses. (Tange tla, 2019) Different radio access technologies, including WLAN, LTE, WiMAX, and WCDMA, are used to offer a range of communication services across multiple tiers.

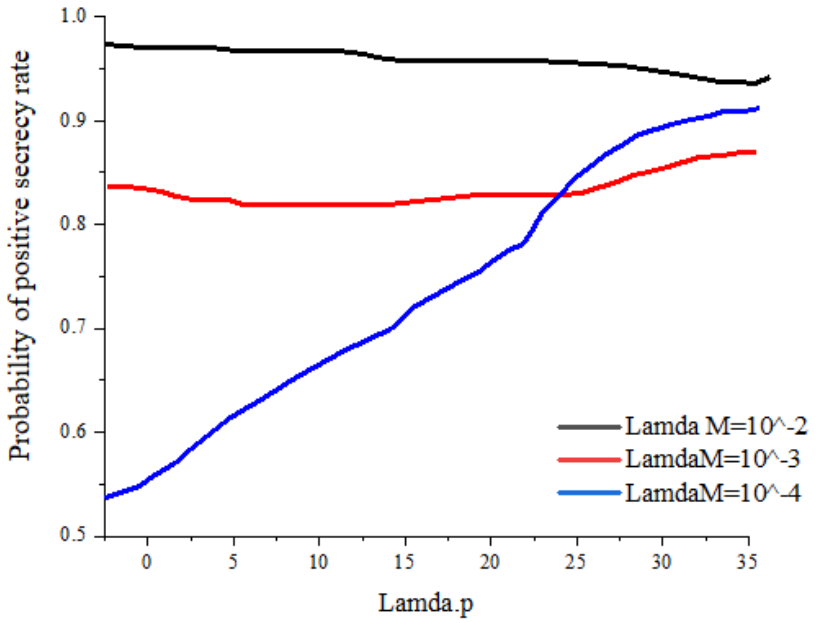

Figure 2: Probability of positive secrecy

The likelihood of a two-layer network with a macro cell tier superimposed on top of a pico cell tier having a positive secrecy rate. It is expected that the frequency band used by the marco and pico cells is shared.

Spatial modeling

The question of "How does the spatial modelling of nodes' locations affect and guide the physical layer security design" naturally arises in the HetNet due to the disparate spatial modelling of HPN and LPN locations. (Vaigandla et la, 2020) The reasoning behind this question is that, whilst the position of an LPN may be modelled as a uni-form distribution, namely a Poisson point process in the two-dimensional plane, the location of an HPN is currently modelled as a point at the centre of a hexagonal grid. (Wang et al, 2019) It appears that the Poisson model for LPN sites corresponds to total unpredictability, while the deterministic model for HPN locations appears to provide no randomness at all. (Wang et al, 2019) This means that in order to incorporate the characteristics and nature of the two models into the physical layer design, several mathematical techniques must be used.

Graph theory and stochastic geometry knowledge can be used to investigate how the positions of HPNs and LPNs affect physical layer security. (Wu et la, 2018) Furthermore, if a suitable degree of practical correlation is added to the placement of HPNs and LPNs, new solutions to the SINR distributions are needed. These solutions will necessitate a significant improvement above the present research that rely on the assumption of HPNs and LPNs being placed independently.

Figure 2 uses simulations to assess how the densities of HPNs and LPNs affect secrecy performance. (Yerrapragada etal, 2021) The probabilities of a positive secrecy rate in a two-tier network with a macro cell tier superimposed on top of a pico cell tier are displayed in this picture. It is clear that as pico cell LPN density rises, so does the likelihood of positive secrecy rate1. (Zeng et al, 2018) Furthermore, it has been noted that a higher density of macro cell HPNs has no additional effect on secrecy performance if the density of pico cell LPNs grows above a certain threshold. Consequently, network security designers can use Fig. 2 as a guide to determine the optimal density for implementing HPNs and LPNs in the HetNet. Naturally, as we have already covered, the creation of useful mathematical instruments will allow us to carry out the assessment shown in this figure in a way that is computationally efficient.

Mobile Association

One difficult but intriguing question that arises from associating mobile users with HPNs and LPNs is, "What is the optimal strategy for users to select HPNs/LPNs under security constraints?" Signal-to-interference-plus-noise ratios (SINRs) and the associated quality of service (QoS) characteristics have long been used. However, the quantity of interference increases rapidly when small cells are added on. As a result, simulation complexity rises significantly, increasing the complexity and time required for performance evaluation and optimisation. In order to assess the level of randomness, the locations of the HPNs have been lately been modelled as a PPP. In light of this, network security designers must create efficient macro-cell-only cellular networks. As a result, this supposition informs the design of the physical layer security mechanisms seen in the open literature. Therefore, when designing physical layer security, the uneven load should be taken into consideration.

Prioritising the optimisation of secrecy performance, such as the secrecy rate and the secrecy outage probability, is important when constructing these strategies. This prioritisation allows for the development of intelligent mobile association policies, which assign mobile users to HPNs or LPNs judiciously based on achievable secrecy performance, instantaneous load, and other variables like transmit power, coverage area, and density of HPNs/LPNs. Some basic yet suboptimal mobile association policies are necessary since such sophisticated and ideal policies would impose a large computational burden. These suboptimal strategies help to ensure near-optimal secrecy performance at a reduced computational cost. Furthermore, collaboration between HPNs and LPNs provides a workable solution to improve secrecy performance. In order to investigate this possibility, network security designers should create new cooperative techniques that let nearby HPNs and LPNs share secure user data, their own instantaneous load, and other network parameters in order to achieve near-maximum secrecy performance.

Device Connection

The advent of device-to-device (D2D) communication raises an important security question: "How can data confidentiality between connected devices be protected against data leakage?" Since all nearby devices may be able to overhear the data being transferred between connected devices, data security must unquestionably be maintained in D2D conversations.

It should be noted that because authentication is not present in either the macro cell or micro cell levels, closed access may not always be enforced. In this instance, known as "open access," nearby HPNs and LPNs may potentially operate as eavesdroppers for the connected devices in addition to surrounding devices. This means that they stand to gain financially from listening to transmitted data and seriously jeopardise data security. Network designers must create new secure data exchange strategies that completely account for the physical traits of hostile HPNs/LPNs and uninvited devices, such as ambiguous location, uncertain mobility, and unknown configuration, in order to address security challenges in open access. Furthermore, it is imperative to do a thorough analysis and integration of malicious HPNs/LPNs and unintentional devices to mitigate potential assaults and threats.

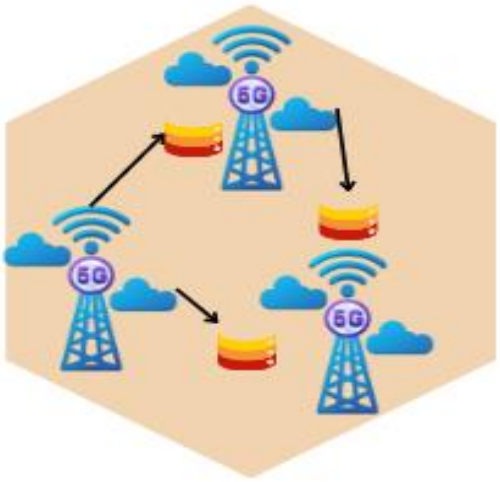

Figure 3. Cellular network with the deployment of massive MIMO.

A fascinating paradigm in D2D communications outside of direct D2D connections is D2D relaying, in which a device with superior geometry to the transmitter device can serve as a relay for the receiver device. Even with the existing relay-assisted physical layer security methods, this kind of design creates additional security issues that need to be resolved. For instance, it is necessary to ascertain the best way to choose candidate relays and look at ways to guard against unreliable relays. Moreover, the effect of multi-hop coordination on the secrecy performance must be investigated if more than one device is needed to relay data between the linked devices.

PHYSICAL LAYER SECURITY IN MASSIVE MIMO SYSTEMS

Scientists and industry alike are showing a great deal of interest in the emerging topic of massive MIMO systems research. Large antenna arrays (usually tens or even hundreds) at the transmitter and/or receiver are required to realise the benefits of the massive MIMO technology. Future massive MIMO cellular networks, like the one shown in Fig. 3, will include many more antenna arrays at the base stations (BSs)—up to ten times more than the number of data streams available to every user in a cell. When compared to the existing counterpart, huge MIMO systems take advantage of low-complexity transmission designs' big array gain to achieve excellent power and spectrum efficiencies.

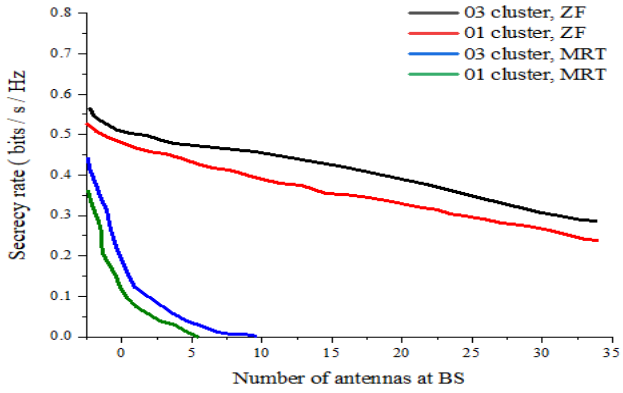

Figure 4: Massive MIMO system

The downlink secrecy outage probability at the BS using MRT and ZF precoding algorithms. Three hexagonal compartments with a radius of 350 metres each are taken into consideration, devoid of

sectorization. One eavesdropper and seven evenly distributed single-antenna consumers are present in each cell. The graphic indicates that the frequency reuse pattern in the "01 cluster" is 1, and in the "03 cluster," it is 3.

the design of physical layer security based on the enormous potential of massive MIMO systems, since massive MIMO will be a key enabling technology for the 5G wireless network. It goes without saying that a design like this offers up a brand-new, promising study direction, expanding the scope of present research in traditional MIMO systems.

Low power consumption

Reducing power consumption in giant MIMO systems can markedly improve the secrecy performance. There are two main reasons for the improvement. First, there is a significant reduction in the receive signal-to-noise ratios (SNRs) at the eavesdropping sites due to the broadcast power level being lowered. The eavesdroppers' channel capacity are severely reduced as a result.

Time division duplex operation

Utilising channel reciprocity, the training burden in the TDD mode is unaffected by the quantity of BS antennas. Eavesdroppers may encounter unique challenges when wiretapping in TDD massive MIMO systems since the TDD mode does not require downlink pilot signals from the BS to the consumers. In particular, uplink pilot signals from users are used by the BS with huge antenna arrays to get the uplink channel status information (CSI). Next, using the reciprocity between the uplink and downlink, it obtains the downlink CSI. Moreover, if the pilot signals used in various cells are not orthogonal, pilot contamination happens in the TDD mode. Therefore, the impact of a contaminated pilot's erroneous channel estimation on the secrecy performance. Reciprocity calibration is also necessary for the TDD operation. The hardware chains at the base station (BS) and users could not be reciprocal between the uplink and the downlink in real-world systems. This encourages the investigation of how incorrect calibration affects secrecy performance.

Artificial noise

The secrecy outage probability in the downlink of a three-hexagonal-cell network is displayed in Fig. 4 at a rate threshold of 2 bits/s/Hz. We take into consideration two popular precodpers and weaken the signals they receive. For AN-based gearbox, new issues arise in massive MIMO systems. Transmitting AN signals in a spatial null space, for instance, might not be feasible due to the null space's computational complexity. Furthermore, because there are a lot of antennas available, random and independent AN averages out. Thus, it is necessary to design new AN-based transmission methods. Thus, it is necessary to determine the best way to divide up the power between information signals and AN signals and to assess the achievable secrecy performance.

Antenna Correlation

A practical issue that underpins the implementation of huge MIMO systems is antenna correlation. In particular, a lack of dispersion or the antenna array's restricted aperture may result in a sizable degree of correlation between large antenna arrays. Because of the non-isotropic antennas' decreased separation, the BS experiences antenna correlation in several diversity branches during uplink transmission, for instance.

Confidential Broadcasting

Every base station (BS) in a vast MIMO system connects with many consumers at once. Achieving secret broadcasting in the downlink is one of the challenges facing multiuser security. Specifically, every message must be kept private from all users save the intended recipient; in other words, every user can be considered an eavesdropper on all messages except their own. A precoder must be associated with each data stream in order to protect secrecy. This will help to minimise information leakage as well as interference from other

users. Creating the ideal precoder frequently requires solving numerically-only optimisation problems. Thus, more practical and almost-optimal precoders are needed. To ensure private broadcasting in large MIMO systems, it is crucial to quantify the best possible secrecy performance and provide design guidance for linear pre-coders.

Hardware Impairements

The low-cost hardware components utilised in huge MIMO systems may result in hardware impairments, in contrast to conventional MIMO systems with perfect hardware. Large-scale array deployment asymptotically eliminates the impact of hardware impairments, even as they deteriorate the channels used by authorised receivers. We see that the eavesdroppers' channels worsen in the face of hardware defects, which is advantageous for enhancing security. Therefore, in large MIMO systems with less-than-ideal hardware, it is worthwhile to look into physical layer security.

PHYSICAL LAYER SECURITY IN MILLIMETER WAVE COMMUNICATION

Nowadays, practically all mobile communication systems limit their use to the 300 MHz–3GHz frequency band. Regretfully, this spectral band is currently almost completely occupied. mmWave communication solutions, which operate in the 30-300 GHz frequency range, have been acknowledged as a promising way to get around the restriction and satisfy a 1,000-fold capacity increase in the 5G network. To provide dependable and quick data transmissions, mmWave BSs can be placed alongside microwave BSs, as shown in Fig. 5.

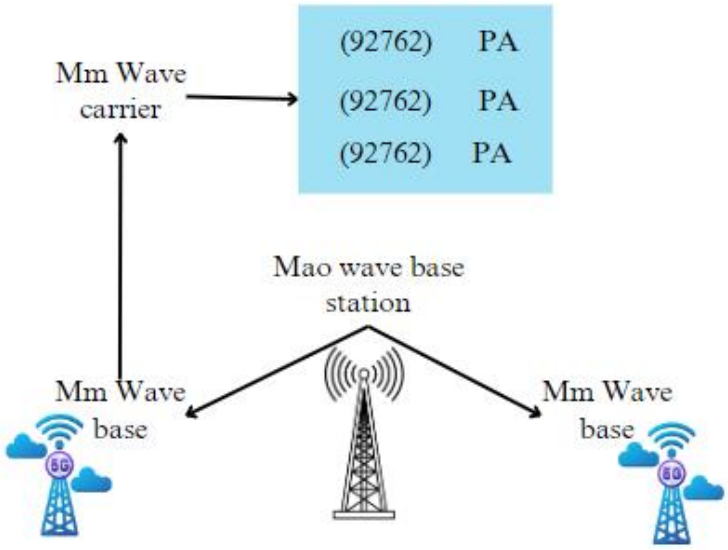

Figure 5. Deployment of mmWave BSs.

A number of research initiatives have been launched to investigate the possibilities of millimeter-wave communication technologies, even if some work needs to be done to make the GHz frequency bands usable on mobile cellular networks. Needless to say, while implementing mmWave communication systems, security and privacy concerns must be taken into consideration. For the following reasons, we think that studying physical layer security in mmWave communication systems is an extremely fascinating and promising field.

Large Bandwidth: Using carrier aggregation, the current maximum aggregated bandwidth in 4G LTE is 20+20 MHz. GHz band-widths are offered by mmWave communication systems, however. Therefore, if the transmitter specifies a lower transmission secrecy rate in mmWave communications, the risk of a secrecy outage in the passive eavesdropping scenario is significantly reduced. Large mmWave bandwidths can also yield great secrecy throughput.

Short-Range Transmission: The higher frequencies of mmWave transmissions result in several orders of magnitude increase in free-space route loss as compared to the existing microwave communication systems. As a result, users who are geographically distant are unable to intercept the data transmission, while eavesdroppers who are nearby can only hear the signals.

Safe downlink mmWave transmission using AN A N-antenna When a single-antenna eavesdropper is present, mmWave BS forwards the private communications to the user. Analogue beamforming using AN is used by the BS.

Directionality: To reduce neighbour interference in millimeter-wave systems, highly directed communication using narrow beams is used. As a result, the eavesdroppers' receive signal-to-noise ratios (SNRs) can be so low that they are unable to retrieve information signals from the messages they have overheard.

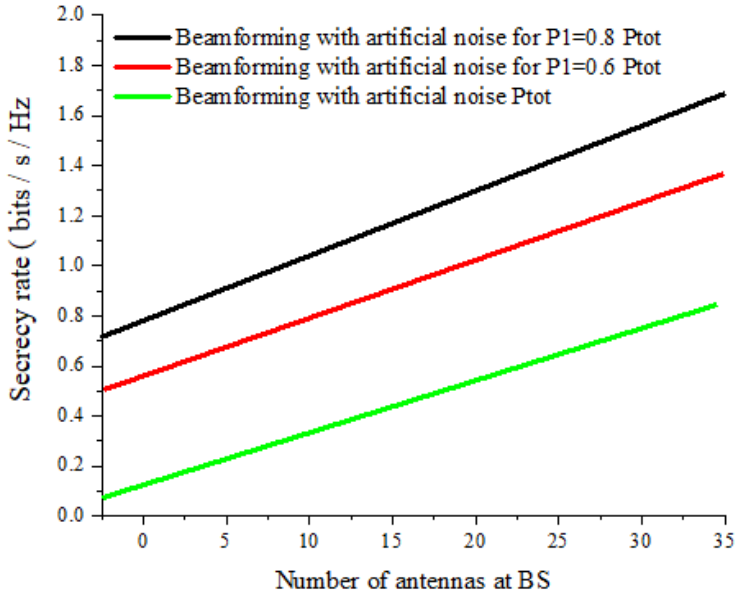

Figure 6. Millimetre wave communication

Big Antenna Arrays: To reduce propagation attenuation and preserve transmit power, large antenna arrays offer excellent beamforming gains. The shorter wavelengths at the mmWave frequencies allow the mmWave base stations to accommodate more antennas for a fixed array aperture. Large antenna array mmWave systems, therefore, present a multitude of opportunities for mmWave communication security at the physical layer. In light of this, the transmission of AN signals in mmWave communication networks appears promising. The beam pattern of AN signals can be easily restricted to the orthogonal direction of the beam pattern of information signals with the use of analogue beamforming with phase shifters. Integrating AN signals into secure communication significantly increases the secrecy rate, as shown in Fig. 6.

Conclusion

As a result of the introduction of D2D connections and small cell deployments, the utilisation of a vast array of antennas, and the investigation of the unused mmWave frequency spectrum, we think the 5G network is poised to fulfil the escalating demand for data-centric applications in the upcoming ten years. The design of physical layer security will be significantly impacted by the nearly irreversible transition to 5G. This article outlines the scientific prospects and technical obstacles related to massive MIMO, mmWave communication, and HetNet. Our innovative solutions have the potential to revolutionise data secrecy and usher in a new security paradigm deserving of the 5G name.

Abbreviation

5G	- fifth generation
BAN	- Body Area Networks
IoT	- Internet of Things
RFID	- Radio Frequency Identification
VLC	- Visible Light Communication
PLC	- Power Line Communication

Competing interests

The authors declare that they have no competing interests.

Consent for publication

Not applicable

Ethics approval and consent to participate

Not applicable

Funding

This research study is sponsored by the institution name. Thank you to this college for supporting this article!

Availability of data and materials

Not applicable

Authors' contribution

Author A supports to find materials and results part in this manuscript. Author B helps to develop literature part.

Acknowledgement

I offer up our fervent prayers to the omnipotent God. I want to express my sincere gratitude to my co-workers for supporting me through all of our challenges and victories to get this task done. I want to express my gratitude for our family's love and support, as well as for their encouragement. Finally, I would like to extend our sincere gratitude to everyone who has assisted us in writing this article.

References

Aghdam, Sina Rezaei, Alireza Nooraiepour, and Tolga M. Duman. Secondquarter (2019). "An Overview of Physical Layer Security With Finite-Alphabet Signaling." *IEEE Communications Surveys & Tutorials* 21 (2): 1829–50.

Güvenkaya, Ertuğrul, Jehad M. Hamamreh, and Hüseyin Arslan. (2017). "On Physical-Layer Concepts and Metrics in Secure Signal Transmission." *Physical Communication* 25 (December): 14–25.

Hamamreh, Jehad M., Haji M. Furqan, and Huseyin Arslan. Secondquarter (2019). "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials* 21 (2): 1773–1828.

Ji, Xinsheng, Kaizhi Huang, Liang Jin, Hongbo Tang, Caixia Liu, Zhou Zhong, Wei You, et al. (2018). "Overview of 5G Security Technology." *Science China. Information Sciences* 61 (8): 081301.

Jiao, Long, Ning Wang, Pu Wang, Amir Alipour-Fanid, Jie Tang, and Kai Zeng. (2019). "Physical Layer Key Generation in 5G Wireless Networks." *IEEE Wireless Communications* 26 (5): 48–54.

Liu, Yiliang, Hsiao-Hwa Chen, and Liangmin Wang. Firstquarter (2017). "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges." *IEEE Communications Surveys & Tutorials* 19 (1): 347–76.

Poor, H. Vincent, and Rafael F. Schaefer. (2017). "Wireless Physical Layer Security." *Proceedings of the National Academy of Sciences of the United States of America* 114 (1): 19–26.

Sánchez, José David Vega, Luis Urquiza-Aguiar, Martha Cecilia Paredes Paredes, and Diana Pamela Moya Osorio. (2021). "Survey on Physical Layer Security for 5G Wireless Networks." *Annals of Telecommunications* 76 (3): 155–74.

Sanenga, Abraham, Galefang Allycan Mapunda, Tshepiso Merapelo Ludo Jacob, Leatile Marata, Bokamoso Basutli, and Joseph Monamati Chuma. (2020). "An Overview of Key Technologies in Physical Layer Security." *Entropy* 22 (11). https://doi.org/10.3390/e22111261.

Tang, Jie, Hong Wen, Kai Zeng, Run-Fa Liao, Fei Pan, and Lin Hu. Sep-Oct (2019). "Light-Weight Physical Layer Enhanced Security Schemes for 5G Wireless Networks." *IEEE Network* 33 (5): 126–33.

Vaigandla, Karthik Kumar, and Dr N. Venu. (2021). "A Survey on Future Generation Wireless Communications-5G: Multiple Access Techniques, Physical Layer Security, Beamforming Approach." *Journal of Information and Computational Science* 11 (9): 449–74.

Wang, Dong, Bo Bai, Wenbo Zhao, and Zhu Han. Secondquarter (2019). "A Survey of Optimization Approaches for Wireless Physical Layer Security." *IEEE Communications Surveys & Tutorials* 21 (2): 1878–1911.

Wang, Ning, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng. (2019). "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities." *IEEE Internet of Things Journal* 6 (5): 8169–81.

Wu, Yongpeng, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong, and Xiqi Gao. (2018). "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead." *IEEE Journal on Selected Areas in Communications* 36 (4): 679–95.

Yerrapragada, Anil Kumar, Taylor Eisman, and Brian Kelley. (2021). "Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications." *IEEE Open Journal of the Communications Society* 2: 2232–42.

Zeng, Wen, Jiayi Zhang, Shuaifei Chen, Kostas P. Peppas, and Bo Ai. (2018). "Physical Layer Security Over Fluctuating Two-Ray Fading Channels." *IEEE Transactions on Vehicular Technology* 67 (9): 8949–53.