Physical Layer Security Attacks of Massive MIMO Relying on Passive Eavesdropper Cases

Samarth Gupta
B.Tech. Computer Science Engineering
Shiv Nadar University
Noida, India
sg384@snu.edu.in
1910110338

***Abstract*—Physical layer security techniques utilize the characteristics of the propagation medium to provide a secure mode of communication [1]. The fifth generation (5G) network is predicted to satisfy the continuously increasing demands for future wireless applications. It is expected that great volume of sensitive data will be transmitted via 5G channels, necessitating a greater prevention against security attacks. The present article reviews typically used physical layer security techniques over massive multiple-input multiple-output (MIMO), an enabling 5G technology. For the MIMO technology, both passive and active eavesdroppers can be considered. The focus of the present work is on the passive eavesdroppers as eavesdroppers are typically passive to conceal their existence [1]. Starting from [1] as the base paper, the review charts a progress path till date and also mentions future scope in the focus area.**

***Index Terms*—5G, massive MIMO, physical layer security, artificial noise, Beam domain, channel state information (CSI), power allocation, secrecy capacity**

I. Introduction

The fifth generation of wireless networks (5G) is predicted to steadily advance in addressing the increasing demands for wireless applications. Past decade has seen the number of connected users increase exponentially, necessitating greater challenges in the areas of reliability, security, and efficiency. Confidentiality of wireless communication is a core problem to be considered in 5G. Physical layer security (PLS) uses the inherent randomness and the imperfections of the communications medium. 5G network designers have used this idea to deteriorate the quality of signal reception at eavesdroppers. The entire focus of PLS is to ensure that illegal receivers/devices are not able to acquire confidential information. The traditional method is of using cryptographics techniques to protect data. As compared to them, PLS does not depend on computational complexity and have a high scalability. Therefore, the security level achieved will not be affected even if the eavesdropper has unlimited computing capabilities [2]. Encryption-based approaches rely on the eavesdropper's reduced computational capabilities to solve difficult mathematical problems in limited periods. A 5G network allows devices to be connected to nodes varying computational capacities and the devices can ve added or removed at random intervals of time. The 5G network has a decentralized nature resulting in an inefficient and tough distribution and management of cryptographic keys. This can be countered by PLS providing either a direct secure data communication or facilitating the distribution of cryptographic keys in the 5G network [1].

A popular measure in PLS evaluation for wireless mediums is the *secrecy capacity*, defined as the maximum data rate that can be safely transmitted without being decoded by an eavesdropper [2]. In practice, due to the intrinsic randomness of the medium, the *signal-to-noise ratio (SNR)* of the eavesdropper can be close to that of the actual channel. This is more so in cases when the eavesdropper is nearer to the source than the actual receiver [2]. Given the potential of physical layer security for the 5G era, the goal of the present review is to outline the work done in the context of PLS for the disruptive technologies enabling 5G. Among the various technologies, the present review focusses on Massive Multiple-Input Multiple-Output (Massive MIMO). By deploying a very large number (hundreds) of antennas at base stations to serve many tens of users simultaneously, massive MIMO reaps all the benefits offered by conventional MIMO, but on a much larger scale [1]. Massive MIMO is a multi-user topology in which the base station (BS) has a large number of antennas (Figure 1). Massive MIMO systems provide high degree of freedom, better channel capacity, and improved communication capacity in 5G networks and give a focussed beam guides to the location of the actual user. So, the information leakage is reduced to undesired locations, that is eavesdroppers, significantly [2]. Unlike the traditional MIMO, the challenges presented by massive MIMO include difficulty in channel state information (CSI) estimation process and that the channels models are not independent as the distances of antennas are shorter than a half of the wavelength. Many researchers continue to work in the area of Massive MIMO systems. The present article also surveys the current literature addressing the issues of channel security for massive MIMO relying on passive eavesdropper cases (Table I).

The remainder of this paper is organized as follows. Section II presents covers the key research objective and contributions of the base paper [1] with respect to PLS in Massive MIMO

Systems. Section III outlines the important results and findings of the base paper [1]. The section also talks about the open research questions, limitations, and future work presented in the base paper [1]. Section IV presents a discussion on how [3]–[7] improve upon the base paper [1] and answer the open research questions/limitations raised in Section III. Section IV concludes the report.

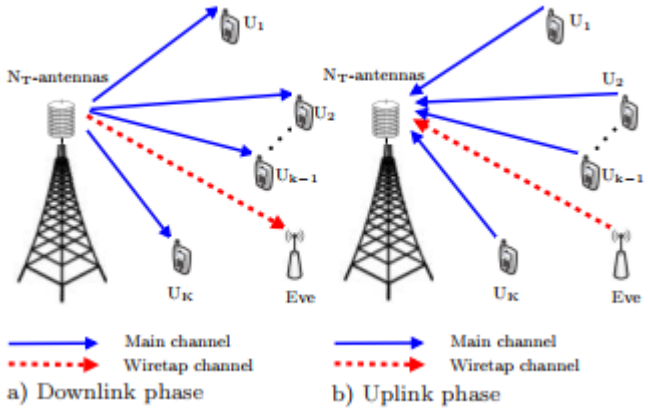

Fig. 1. Massive MIMO downlink with K legitimate user nodes, U_i for i = 1, . . ., K, and an eavesdropper [2].

II. Physical Layer Security in Massive MIMO Systems

Past few years have seen interest from researchers in Massive MIMO systems. Massive MIMO technique uses tens or even hundreds of antenna arrays at the transmitter and/or the receiver (Figure 2). The number of antenna arrays at the base stations is much larger than the number of data streams served to all users in a cell. Massive MIMO systems provide greater power and spectrum efficiencies as they utilize the large arrays gain offered by low-complexity transmission designs. Random impairments in the channel such as small-scale fading and noise can be averaged out when a large number of antennas are deployed at the base station. The interference, channel estimation errors, and hardware impairments vanish when the number of antennas grows large, leaving only pilot contamination as the performance limit [1]. According to the authors of [1], to exploit the advantages of massive MIMO in physical layer security, challenges related to pilot contamination, power management, channel reciprocity, and eavesdropper-targeted signal processing needed to be resolved during the design process. The authors of [1] identified the scientific opportunities and discussed the technical challenges driven by the various disruptive technologies to 5G including massive MIMO.

III. Base Paper [1]

The section covers the important results and findings in the base paper [1]. Open research questions, limitations of the work done, and future directions for the considered base paper are also discussed and are presented in bold.

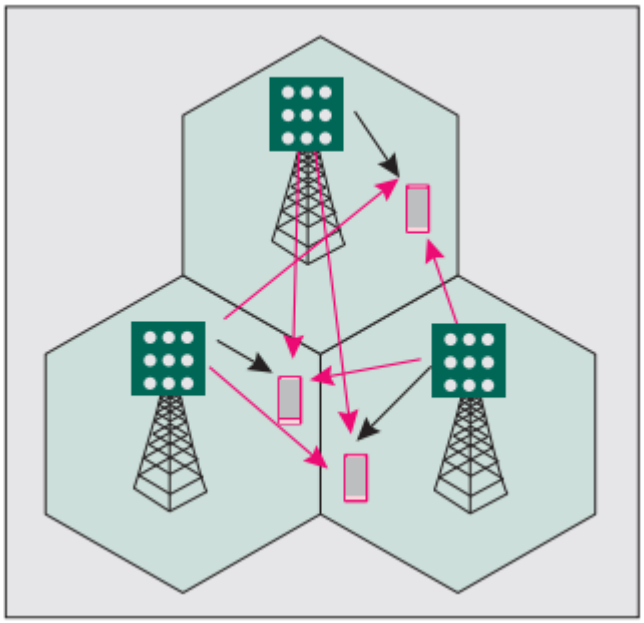

Fig. 2. Cellular network with the deployment of massive MIMO [1]

A. Low Power Consumption in Massive MIMO Systems

The authors of [1] reasoned that reduced power consumption enhances the secrecy performance in massive MIMO systems since 1) when the transmit power level is cut, the receive signal-to-noise ratios (SNRs) at the eavesdroppers are reduced leading to a significant decrease in the eavesdroppers channel capacities. 2) The transmit power and the expected secrecy rate at the transmitter are given. The expected , the secrecy outage can be very small as an unbounded growth is observed in the number of antennas [1]. The authors of [1] consider two commonly-used precoding methods, namely, maximal ratio transmission (MRT) and zero-forcing (ZF). The authors have surmised that ZF performs better than MRT because it neutralizes the the intra-cell interference. They also observed that the secrecy outage probability declined when the number of antennas at the base station grew large [1]. **Thus, the authors surmised that the minimum power consumption achieving the target secrecy performance level needs to be determined and commented on the need to develop mathematical tools to eliminate the burden of performance evaluation incurred by time-consuming simulations [1].**

B. Time Division Duplex Operation in Massive MIMO Systems

Whereas conventional MIMO systems generally operate in a frequency division duplex (FDD) mode, Massive MIMO systems are recommended to operate in a time division duplex mode as the channel training overhead in the FDD mode scales linearly with the number of transmit antennas and imposes a severe limit on the number of antennas. TDD mode works independent of the number of base station antennas and utilizes the channel reciprocity. TDD massive MIMO systems have been seen to make it difficult for the eavesdroppers since they

do not requires as the downlink pilot signals from the base station to the users. Specifically, the base station with massive antenna arrays obtains the uplink channel state information (CSI) via uplink pilot signals from the users and gets the downlink CSI. The authors use the fact that the uplink and downlink are reciprocal to each other. As such, it becomes difficult for eavesdroppers to know the CSI between themselves and the base station, as well as the CSI from other users to the base station. Therefore, the method to design secure transmission under the assumption of imperfect CSI at the eavesdroppers has tremendous application in massive MIMO systems. TDD mode can suffer from pilot contamination if the pilot signals employed in different cells are not orthogonal and also necessitates reciprocity calibration. In practical systems, the hardware chains at the base station and users may not be reciprocal between the uplink and the downlink [1]. **This motivated the observation from the authors that the impact of improper calibration on the secrecy performance should be examined [1].**

C. Artificial Noise in Massive MIMO Systems

Traditionally, MIMO systems use the artificial noise (AN)-based transmission to create interference to the eavesdroppers and degrade their received signals. However, in massive MIMO systems, transmitting artificial noise signals in a spatial null space may not be practical since the computation complexity of the null space is extremely high for the large-dimensional channel matrix. Moreover, random and independent artificial noise (AN) is averaged out given the availability of a large number of antennas [1]. **The authors of [1] proposed that new AN-based transmission schemes need to be developed. The authors also pointed out the need for determining the optimal power allocation between information signals and artificial noise signals and the achievable secrecy performance [1].**

D. Antenna Correlation in Massive MIMO Systems

The authors of [1] identified antenna correlation as a practical challenge underlying the deployment of massive MIMO systems. The authors reasoned that a significant amount of correlation may exist between large antenna arrays, due to either the limited aperture of the antenna array or a lack of scattering [1]. **The authors observed that, in the literature, very little work existed to analyse the effect of antenna correlation on the secrecy performance of massive MIMO systems and emphasized the the value of research in this area [1].**

E. Confidential Broadcasting in Massive MIMO Systems

The authors of [1] identified the challenges to multi-user security in confidential broadcasting in the downlink. The authors explained that every user in the system could be potentially treated as as an eavesdropper for all messages other than its own. In order to preserve this confidentiality, the authors proposed that a pre-coder be associated with each data stream. This will allow both a way to control the interference at other users and also to minimize the leakage of data [1]. **The authors identified that designing optimal pre-coder involved optimization problems that can only be solved numerically and therefore suggested that more practical and near-optimal pre-coders were required. The authors also siggested that a numerical estimation of the optimal achievable secrecy performance of linear pre-coders be done to guarantee confidential broadcasting in massive MIMO systems [1].**

F. Hardware Impairments in Massive MIMO Systems

Since the hardware components for massive MIMO systems tend to be inexpensive, as compared to traditional MIMO systems, hardware impairments can arise and lead to a reduced quality for actual users/receivers. However, the this impact reduces asymptotically as the greater antenna arrays are deployed. The authors [1] noted that the presence of hardware impairments also deteriorates the eavesdroppers channels, which appears to be beneficial for security enhancement. **The authors proposed that physical layer security in massive MIMO systems be investigated with non-ideal hardware [1].**

IV. Recent Developments in PLS for Massive MIMO Systems

Since the work by the authors of [1], many researchers have worked in the related areas. The present work considers the work presented in [3]–[7] and reviews how they address the open research questions/limitations raised by the authors of [1].

A. Paper1 [3]

The authors of [3] proposed a massive MIMO approach with passive eavesdroppers that includes the effect of hardware deficiencies on the PLS performance of massive downlink MIMO in the existence of eavesdropper with multiple antennas (Section III-F). The considered system model comprised an N-antenna BS, K single-antenna mobile terminals, and an N_E-antenna eavesdropper. The eavesdropper is passive in order to hide its existence from the BS and the mobile terminals. The authors [3] observed that the hardware costs of future communications systems can be kept manageable by using low-cost hardware components, especially for massive multiple-input multiple-output (MIMO) systems which equip base stations with a large number of antenna elements. Using of cheaper hardware designs will only increase the problem of hardware impairments that the current systems already suffer from. The authors [3] went on to study the significance of hardware impairments in the PLS for downlink massive MIMO systems. The authors focussed on the case of a passive multiple-antenna eavesdropper. For the BS and the legitimate users, the joint effects of multiplicative phase noise, additive distortion noise, and amplified receiver noise were taken into account. On the other hand, the eavesdropper was assumed to employ ideal hardware. The authors [3] proved a lower bound for the ergodic secrecy rate of a given user when matched

TABLE I
ARTICLES CONSIDERED IN THE REVIEW

Paper	Reference	Year	Publisher	Problem Addressed (Section)	Title
Base Paper	[1]	2015	IEEE Communications Magazine	-	Safeguarding 5g wireless communication networks using physical layer security
Paper1	[3]	2017	IEEE Transactions on Wireless Communications	III-F	Analysis and design of secure massive mimo systems in the presence of hardware impairments
Paper2	[4]	2018	IEEE Transactions on Vehicular Technology	III-A	Beam domain secure transmission for massive mimo communications
Paper3	[5]	2018	IEEE Access	III-D	Secure performance analysis for multipair af relaying massive mimo systems in ricean channels
Paper4	[6]	2018	IEEE Journal on Selected Areas in Communications	III-C	Secure massive mimo with the artificial noise-aided downlink training
Paper5	[7]	2018	IEEE International conference on communications	III-E	Performance analysis of secure communication in massive mimo with imperfect channel state information

filter data precoding and artificial noise (AN) transmission are employed at the BS. Further, the paper stuidies the effect of parameters on the secrecy rate. The pilot sets used for uplink training and the artificial noise (AN) precoding were optimized. The authors found that the additive distortion noise at the BS may be beneficial for the secrecy performance, especially if the power assigned for artificial noise emission is not sufficient. It was also deduced that all other hardware impairments had a negative impact on the secrecy performance. The authors also concluded that the proposed generalized null-space artificial noise precoding method efficiently mitigated the negative effects of phase noise [3].

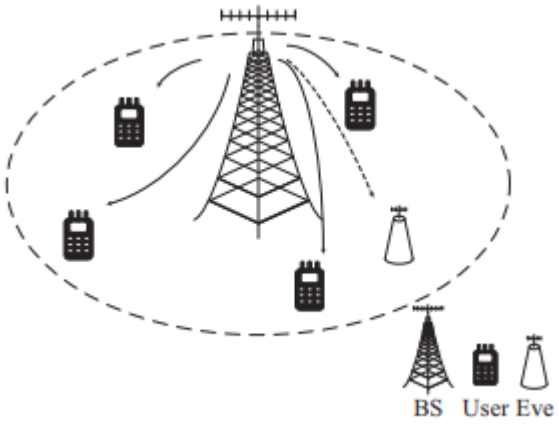

Fig. 3. System Model [4]

B. Paper2 [4]

The authors of [4] investigated the optimality and power allocation algorithm (Section III-A) of beam domain transmission for single-cell massive multiple-input multiple-output (MIMO) systems with a multi-antenna passive eavesdropper, where only statistical CSI of legitimate users and the eavesdropper is available at the BS. The authors considered secure downlink transmission in a system model (Figure 3) consisting of a base station with M antennas, allowing K actual users. Each user has N_r antennas. A passive eavesdropper with N_e antennas is also a part of the system. The BS transmits private and independent messages to each legitimate user. All messages are required to be confidential to the eavesdropper. Neither the BS nor the users are assumed to know which user is eavesdropped and that any user may be potentially targeted by the eavesdropper. The passive eavesdropper shows nil impact on the beam of transmission at the base station. Also, very small impact is visible on the secrecy capacity [2]. As the number of BS antennas goes to infinity, the eigenmatrices of the channel transmit covariance matrices turn to be identical and independent of mobile terminals. The authors [4] analysed that the eigenmatrix of the optimal input covariance matrices. For the case of single-antenna legitimate users, the authors [4] revealed that it is optimal to allocate no power to the beams, especially in the case when eavesdropper's beam gains are stronger than those of the actual users. Additionally, the authors [4] developed an algorithm to optimize power allocation of beam transmission for the given system. The paper shows that with respect to the secrecy capacity, beam transmission can attain optimal performance.

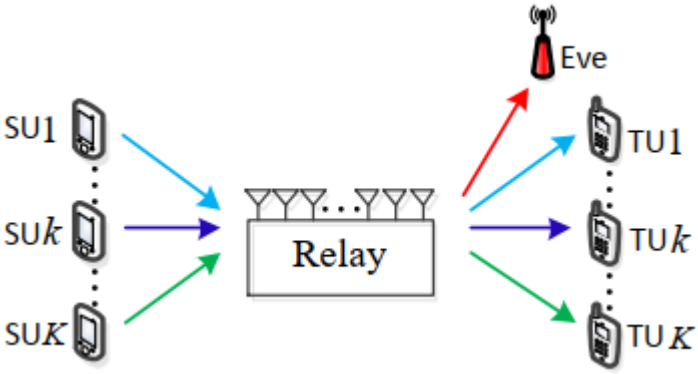

Fig. 4. Secure Multi-pair Massive MIMO Relaying System [5]

C. Paper3 [5]

Authors in [5] investigated secure transmissions of multi-pair massive MIMO amplify-and-forward (AF) relaying systems by considering Ricean fading. In this work, the attainable

sum secrecy rate is maximized by using a power control topology (Section III-D). The considered system model (Figure 4) has K single-antenna source users (SU1, SU2, ..., SUK) who transmit information to their corresponding single-antenna terminal users (TU1, TU2, ..., TUK) in pairs through a M-antenna relay. A single-antenna eavesdropper (Eve) is concealed on the receiving side and tries to intercept the transmitting information from the relay's forward signals. The authors [5] consider the scenario where the relay operates in half-duplex time-division duplex (TDD) mode and assume that there are no direct communication links between the source users and terminal users (eavesdropper) due to the far distance [5]. Based on the estimated channel state information, AF relay exploits MRC/MRT beam forming for signal forwarding. Using random matrix theory, the authors first deduce asymptotic equivalents of the end-to-end SINRs at the target user and Eve with infinite antennas. Then they obtain asymptotic results are obtained at infinite Ricean K-factor, unbounded transmit power or relay power conditions. According to the authors, these results illustrate that the achievable ergodic information rates of legitimate users and Eve all converge to some fixed values in these extreme cases. Also the authors considered the power scaling laws for transmit and relay power of the considered massive MIMO relaying system. According to the authors, theoretical analyses showed that the power can be scaled down in inverse proportion to the number of relay antennas in Ricean channels. Additionally, the authors derive a simple power control scheme to maximize the achievable sum secrecy rate by using successive approximations, geometric programming and iterative computation. The authors also present numerical results are presented to demonstrate the performance and effectiveness of this secure massive MIMO AF relaying system [5].

D. Paper4 [6]

The authors of [6] analysed the use of AN-aiding schemes to degrade the eavesdropping channel to improve the security in massive MIMO (Section III-C). The authors [6] considered a massive MIMO network which includes one M-antenna BS, K single-antenna end users and one N-antenna eavesdropper (Figure 3). As is expected, a passive eavesdropper attemps to listen to the secret communication in the down-link transmission. The authors [6] proposed two artificial noise(AN)-aiding schemes to secure the confidential information. In the first scheme, artificial noise is injected into the downlink training signals. In the second scheme, artificial noise is deployed in both downlink training phase and payload data transmission phase to further degrade the eavesdropping channel. Analytical expressions and tight approximations of the achievable secrecy rate of the considered systems are derived with taking imperfect channel estimation and two types of precoding, that is, maximum ratio-transmission and zero-forcing, into consideration. The authors [6] proposed optimization algorithms for power allocation to enhance the secrecy performance of the proposed AN-aiding schemes. The results reveal that deploying artificial noise in the downlink training phase of massive MIMO networks does not affect the downlink channel estimation process at users. On the other side, it allows the system to suppress the downlink channel estimation process at eavesdropper. That is, the proposed schemes show a significant boost to the system performance. Furthermore, implementing artificial noise in both phases allows the considered system having a flexible solution to maximize its secrecy performance at the price of higher complexity.

E. Paper5 [7]

The authors of [7] studied the performance analysis of wireless communications in a multi-user massive MIMO by using imperfect CSI (Section III-E). The considered system comprised of a base station with N_t antennas intends to transmit signals to K legitimate users. The eavesdropper is equipped with N_e antennas, and intends to wiretap the channels between the BS and the legitimate users with only 1 antenna available to each user. The passive eavesdropper only overhears the channels between the BS and the users, but does not launch the pilot contamination attack. The authors [7] derived a tight asymptotic lower bound of the ergodic system secrecy capacity under imperfect CSI, and then analysed how imperfect CSI affects the system secrecy performance. Simulation results revealed the negative impact of the imperfect CSI on the secrecy performance of massive MIMO systems and the accuracy of their theoretical derivations and analysis.

V. Conclusion

The present review focusses on physical layer security of massive MIMO systems relying on passive eavesdroppers. PLS safeguards data confidentiality by exploiting the intrinsic randomness of the communications medium and reaping the benefits offered by the disruptive technologies, like Massive MIMO, to 5G. The base paper [1] chosen for this review talks about the basis of the key principles of three disruptive technologies to 5G, including Massive MIMO technology and identifies the opportunities and the outstanding challenges that security designers must tackle. The motivation of the authors of [1] is to advance the understanding of future physical layer security. The various issues raised by the authors in [1] and other directions have been explored by many researchers, of which, in the present work, [3]–[7] are considered.

Physical layer security has continued to be a topic of interest to the researchers in the context of allowing a secure mode of communication, especially in next generation wireless/mobile systems. The authors of [3] investigated the impact of hardware impairments such as multiplicative phase noise, additive distortion noise, and amplified receiver noise on the secrecy performance of massive MIMO systems employing matched filter precoding for downlink data transmission. The authors of [4] worked in the area iof downlink single-cell massive MIMO transmission. They concentrated on a passive eavesdropper who has multi-antennas. The base station has the statistical CSI of actual users and of the eavesdropper. They developed an algorithm for solving the power allocation

problem [4]. The authors of [5] studied the secure transmission of multi-pair massive MIMO AF relaying system over Ricean fading channels where a passive eavesdropper intends to eavesdrop the transmitted confidential information. They [5] proposed a power control scheme to maximize the achievable sum secrecy rate and demonstrated the effectiveness of the proposed secure multi-pair massive MIMO relaying system. A passive eavesdropper tries to overhear the confidential information being communicated by a user in the down-link transmission. The authors of [6] worked on improving the secrecy performance of a massive MIMO network. They considered a system with multiple-antenna eavesdropper and suggested an AN-based scheme [6]. It is expected in theory that massive MIMO can allow considerable improvement of the system secrecy performance. This can be attributed to its potential in shaping the transmitted signals to eliminate the impact of the eavesdropper. However, in practical systems, the channel state information is often imperfect due to the outdated channel effect and the channel estimation error. The authors of [7] investigated the physical layer security problem in a multi-user massive MIMO system under imperfect CSI.

As future research scope for their work, the authors of [3] proposed a study of the impact of hardware impairments on the physical layer security of multi-cell massive MIMO systems, pilot sequence design under an average power constraint, and optimal artificial noise (AN) pre-coder design for secrecy rate maximization under hardware impairments. The authors of [7] identified designing an effective channel prediction method to alleviate the harmful impact of the imperfect CSI as their future work.

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[2] J. D. V. Sánchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5g wireless networks," *Annals of Telecommunications*, vol. 76, no. 3, pp. 155–174, 2021.

[3] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive mimo systems in the presence of hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2001–2016, 2017.

[4] W. Wu, X. Gao, Y. Wu, and C. Xiao, "Beam domain secure transmission for massive mimo communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7113–7127, 2018.

[5] X. Zhang, D. Guo, and K. Guo, "Secure performance analysis for multi-pair af relaying massive mimo systems in ricean channels," *IEEE Access*, vol. 6, pp. 57 708–57 720, 2018.

[6] N.-P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and K. Tourki, "Secure massive mimo with the artificial noise-aided downlink training," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 802–816, 2018.

[7] T. Yang, R. Zhang, X. Cheng, and L. Yang, "Performance analysis of secure communication in massive mimo with imperfect channel state information," in *2018 IEEE International conference on communications (ICC)*. IEEE, 2018, pp. 1–6.