Securing 5G NR Networks: Innovative Artificial Noise Methods for Protecting Cell-Free Massive MIMO

Mostafa Rahmani*, Junbo Zhao*, Manijeh Bashar†, Kanapathippillai Cumanan*, Alister Burr*, Rahim Tafazolli‡
*University of York, UK
† Senior DevOps Engineer, British Telecom, UK
‡ ICS, 5/6GIC at The University of Surrey, UK

Abstract—**This paper explores the vulnerability of downlink cell-free massive MIMO systems to passive and active eavesdropping, focusing on a 5G New Radio framework. To enhance the security of downlink transmissions over the Physical Downlink Shared Channel (PDSCH) against eavesdropping threats, we propose two novel methods based on cooperative artificial noise (AN). The first approach, called cooperative artificial noise (CAN), involves all access points (APs) broadcasting AN in the null space of the users' channel matrix to confuse potential eavesdroppers. The second approach, named partial artificial noise (PAN), divides the APs into two groups: one group cooperatively transmits AN, while the other group serves the legitimate users. Additionally, we implement three different precoding schemes for legitimate users: maximum ratio transmission, zero-forcing, and minimum mean square error. We conduct link-level simulations of wiretap channels under various frequency-selective fading scenarios and noise conditions, using tapped delay line channel models as defined by the 3GPP TR 38.901 standard. The system's security performance is evaluated by analyzing the block error rate of legitimate users and the block success rate of eavesdroppers. Despite the limitation of having only one antenna per access point, our findings demonstrate that AN can be strategically designed through the cooperation of APs. By designing appropriate groups of APs specifically for generating AN, our second approach, PAN, significantly reduces the block successive rate of eavesdroppers, lowering it from 0.2 without AN to 0.1 with CAN and further down to 0.025 with PAN.**

Index Terms—**Physical layer security, fading channels, 5G New Radio, cell-free massive MIMO, artificial noise.**

I. Introduction

A. Security aspect of cell-free massive MIMO

Cell-free massive MIMO (CF-mMIMO) is a promising architecture for beyond 5G networks, offering consistently high quality of service across wide coverage areas. Unlike traditional co-located massive MIMO systems, where many antennas are concentrated at a single base station, CF-mMIMO distributes massive number of access points (APs) throughout the service area. Each AP, equipped with a small number of antennas, collectively provides extensive coverage and service to all users, enhancing spatial diversity and array gain through cooperative beamforming [1]. The key advantage of CF-mMIMO lies in its collaborative service model, where all APs jointly serve all users, regardless of location. This approach not only combats fading and shadowing effects but also boosts signal strength and reduces interference through coordinated transmission. Such features make CF-mMIMO an ideal solution for meeting the stringent performance demands of future wireless networks [2], [3]. Despite these benefits, CF-mMIMO systems are vulnerable to eavesdropping due to the broadcast nature of wireless channels. This risk is exacerbated by two types of threats: passive eavesdroppers, who discreetly intercept transmissions, and active eavesdroppers, who interfere by mimicking legitimate nodes or generating interference [4].

To address these challenges, physical layer security (PLS) leverages the dynamic characteristics of the wireless medium to secure data transmissions against eavesdropping. As illustrated in Fig. 1, a CF-mMIMO network uses multiple APs to serve User Equipments (UEs) while protecting against potential eavesdroppers (Eves). To achieve this, APs transmit artificial noise (AN) along with the signals intended to the legitimate users [5]. The AN is strategically placed in the null space of the intended users' channel matrix, effectively confusing eavesdroppers without disrupting legitimate communications. By carefully controlling the direction and power of both legitimate signals and AN, the system minimizes information leakage (shown as dashed lines) to unintended receivers. This approach enhances security at the physical layer, complementing traditional cryptographic methods, and is particularly effective in dynamic, densely populated wireless environments typical in next-generation wireless networks.

B. Related works

The first study to investigate PLS in CF-mMIMO systems was presented in [6], focusing on the security of these networks under pilot spoofing attacks. This study illuminates the challenges of maintaining secure communications in scenarios where eavesdroppers attempt to intercept transmissions by mimicking legitimate users during the pilot transmission phase. In [7] the authors delve into securing downlink communications in CF-mMIMO systems against sophisticated eavesdropping threats. By assuming APs equipped with low-resolution digital-to-analog converters and operating over Rician fading channels, the research derives closed-form expressions for achievable secrecy rates. The study's

The work presented in this paper was funded by UK Department for Science, Innovation and Technology under project YO-RAN.

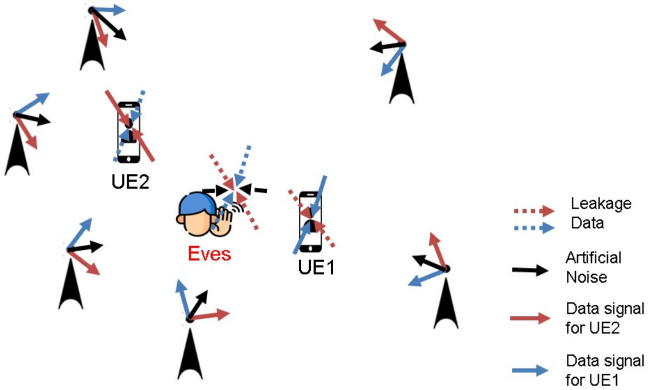


Fig. 1: CF-mMIMO system using physical layer security technique where the Eves intercepts the signals intended for legitimate users.

comprehensive analysis and simulations not only underline the practical challenges posed by active eavesdroppers but also offer robust strategies to mitigate such threats, marking a significant advancement in the physical layer security of future wireless networks.

In [8], Ma et al. conducted a pioneering analysis of downlink secure transmissions in scalable CF-mMIMO systems. The study used a stochastic geometry framework to model the locations of APs, UEs, and Eves as independent homogeneous Poisson point processes. The authors integrated maximum ratio transmission (MRT) and null-space artificial noise to enhance secrecy, analyzing the system's performance using outage-based secrecy transmission rates and ergodic secrecy rates across different fading scenarios. In [9] addressed securing user-centric CF-mMIMO systems against collaborative eavesdroppers by optimizing downlink precoding. The study utilized shared channel state information (CSI) among APs and a central processing unit (CPU) to enhance secrecy rates, considering user minimum rate requirements and AP power constraints.

The work in [10] explored optimizing secrecy in CF-mMIMO systems with network-assisted full duplexing to counter both colluding and non-colluding eavesdroppers. The study proposed a joint optimization of duplex mode selection and secrecy transceivers to maximize secrecy spectral efficiency, incorporating artificial noise to disrupt eavesdroppers. Chen et al. in [11] investigated pilot assignment and power control to improve security in UAV-enabled CF-mMIMO networks. Addressing pilot spoofing by eavesdroppers, the study combined a weighted graphic framework with genetic algorithms for pilot assignment to reduce contamination and enhance fairness. The research derived closed-form expressions for achievable secrecy rates, analyzing the impact of various parameters such as power levels, antenna configurations, and UAV altitude on security.

In [12], the authors investigate secure communications in CF-mMIMO systems using multi-antenna APs and protective partial zero-forcing (PPZF) precoding to defend against active eavesdropping attacks. They formulate an optimization problem to maximize the signal-to-noise ratio (SINR) for legitimate users while limiting the SINR for eavesdroppers, considering power constraints at each AP and SINR requirements for other users. A path-following algorithm and a large-scale greedy AP selection scheme are proposed to enhance secrecy spectral efficiency (SSE). The findings show PPZF provides around a two-fold SSE improvement over conventional MRT. In [13], the authors examine the impact of hardware impairments (HWIs) on the security performance of CF-mMIMO systems using AN as a PLS technique. By deriving the Signal-to-Noise Ratio (SNR) for both legitimate users and eavesdroppers, they show that, unlike previous studies, AN can degrade security performance in the presence of HWIs. The results highlight that fluctuations in hardware quality of users, eavesdroppers, and APs directly affect the system's ability to mitigate AN, emphasizing the need to account for HWIs when deploying AN-based PLS techniques.

C. Contributions

The main contributions of this paper are as follows:

1) Innovative system architecture for PLS in 5G New Radio (NR): We propose a novel system architecture that embeds PLS techniques directly into 5G NR downlink transmissions. This design leverages the physical layer's unique properties to enhance data security against eavesdropping attacks, providing a robust defense that functions independently of conventional cryptographic methods.
2) Comprehensive analysis of secrecy performance through link-level simulations: We conduct a thorough analysis of the secrecy performance of downlink transmissions by performing link-level simulations through 5G NR framework. These simulations extract key metrics, such as block error rate (BLER) and block successive rate (BLSR), under diverse frequency-selective fading scenarios and noise conditions, using tapped delay line (TDL) channel models as defined by the 3GPP TR 38.901 standard. This detailed evaluation provides essential insights into the effectiveness and reliability of our security strategies in realistic wireless environments.
3) Development of novel cooperative AN methods: We introduce two new methods to bolster security using cooperative AN. The first method, cooperative artificial noise (CAN), has all APs broadcast AN in the null space of the users' channel matrix, effectively confusing eavesdroppers without requiring extra antennas. The second method, partial artificial noise (PAN), strategically divides the APs into two groups: one group transmits AN cooperatively, while the other serves legitimate users, optimizing both security and user service.
4) Evaluation of advanced precoding schemes for enhanced security: To further strengthen downlink transmission security, we implement and evaluate three advanced precoding schemes for legitimate users: MRT, Zero-Forcing (ZF), and Minimum Mean Square Error (MMSE). These

schemes are assessed for their effectiveness in maximizing signal strength for legitimate users while minimizing eavesdropping risks, providing a thorough evaluation of their performance in secure communication scenarios.

The key advantage of our proposed approaches over existing methods is that they can be implemented just by using single-antenna APs, eliminating the need for complex beamforming towards eavesdroppers. Additionally, our methods are designed with practical system implementation in mind, taking into account all necessary details to ensure seamless integration into real-world scenarios.

II. System Model

We consider a CF-mMIMO system with M APs, K UEs and a Eves, all equipped single antenna, as shown in Fig.1. We assume Eves works individually and listen the signals transmission from the APs without any collaboration on the downlink. The APs and UEs do not know where the Eves are located and which targeted user will be eavesdropped upon. The 5G NR PDSCH link and the TDL channel model are applied. We assume the frequency-selective channel coefficients between the k^{th} UE and the m^{th} AP are represented by $\mathbf{g}_{km} = [g_{km,1}, \dots, g_{km,N}]^T$ with N sub-channels and the system is time-invariant within one transmission slot. This leads to the constant value for all OFDM symbols on the same sub-channel [14, Sec. 7.7.2].

In this paper, we also assume perfect channel estimates can be obtained and the sub-channels are uncorrelated with each other. Then, the transmitted data from the m^{th} AP on the n^{th} sub-channel is expressed by

$$x_{m,n} = \sum_{k=1}^{K} w_{mk,n} s_{k,n} \tag{1}$$

where $w_{mk,n}$ denotes the weight decided by different combining techniques and $s_{k,n}$ is the modulated symbol with $\sigma_s^2 = 1$ which should be sent to the k^{th} UE via the n^{th} sub-channel. The received data at the k^{th} UE on the n^{th} sub-channel is

$$\begin{aligned} r_{k,n} &= \sum_{m=1}^{M} g_{km,n} x_{m,n} + z_{k,n} \\ &= \sum_{m=1}^{M} g_{km,n} \sum_{k'=1}^{K} w_{mk',n} s_{k',n} + z_{k,n} \end{aligned} \tag{2}$$

where $z_{k,n}$ is the frequency response of the additive white Gaussian noise. We consider MRT, ZF and MMSE precoding, in which weights are given by [15]

$$w_{mk,n} = \begin{cases} [\mathbf{G}_n^H]_{mk} & \text{MRC} \\ [\mathbf{G}_n^H(\mathbf{G}_n\mathbf{G}_n^H)^{-1}]_{mk} & \text{ZF} \\ [\mathbf{G}_n^H(\mathbf{G}_n\mathbf{G}_n^H + \sigma_z^2\mathbf{I})^{-1}]_{mk} & \text{MMSE} \end{cases} \tag{3}$$

where $\mathbf{G}_n \in \mathbb{C}^{K\times M}$ is formed by $g_{km,n}$ for all n^{th} sub-channels between M APs and K UEs, $\mathbf{I}$ represents the identity matrix with size K, σ_z^2 is the variance of the noise z, and $[\cdot]_{mk}$ denotes the m^{th} row and k^{th} column element of the matrix.

III. Physical Layer Security System

This section explores the strategy of broadcasting AN in the null space of users' channel matrices through the cooperation of APs. We present the design of an AN matrix tailored for two proposed approaches to enhance the security of downlink transmissions. Both methods leverage the cooperative capabilities of APs to enhance PLS and protect sensitive data against eavesdropping, offering different trade-offs in terms of complexity, and security effectivenes.

A. Adding the Artificial Noise to all APs

The first approach, termed CAN, involves all APs within the network simultaneously broadcasting AN in the null space of the users' channel matrix. This method aims to create interference that confounds potential eavesdroppers, thereby preventing them from intercepting confidential communications without requiring additional antennas or complex beamforming techniques. By fully utilizing the collective capability of all APs, CAN maximizes the distribution of artificial noise across the network, enhancing overall security against passive and active eavesdropping attacks. The CAN method involves adding AN across all APs which is given by

$$x_{m,n} = \underbrace{\sqrt{\delta}\sum_{k=1}^{K} w_{mk,n} s_{k,n}}_{\text{Users' Data}} + \underbrace{\sqrt{1-\delta} v_{m,n} \bar{s}_{m,n}}_{AN} \tag{4}$$

where $\mathbb{E}\left\{\|\bar{\mathrm{s}}\|^2\right\} = 1$, $v_{m,n}$ is the AN precoding vector added for the m^{th} AP on the n^{th} sub-channel and it satisfies the condition $\forall k \in \{1, \dots, K\}$, $\sum_{m=1}^{M} g_{km,n} v_{m,n} = 0$, and to have a fair comparison, we set a proportional power coefficients δ to the desired data and $1-\delta$ is the AN power. Therefore, the received signals at all UEs can be described by the same expression as given in (2). However, the signal intercepted by a hidden Eve is intentionally distorted by the AN introduced by the system, making it challenging for the eavesdropper to accurately reconstruct the original transmission. Then, the received signal at the i^{th} Eve is given by:

$$\begin{aligned} r_{i,n}^{e} = \sqrt{\delta} \sum_{m=1}^{M} g_{im,n} \sum_{k'=1}^{K} w_{mk',n} s_{k',n} \\ + \sqrt{1-\delta} \sum_{m=1}^{M} g_{im,n} v_{m,n} \bar{s}_{m,n} + z_{i,n} \end{aligned} \tag{5}$$

B. Partitioned Access Point Strategy: Some Transmit Artificial Noise, Others Transmit Data Signals

The second approach, known as PAN, employs a refined strategy by dividing the APs into two distinct groups. One group is tasked with cooperatively transmitting AN to disrupt eavesdroppers' ability to intercept communications, while the other group focuses on delivering data signals to legitimate users. This partitioned approach enables a more strategic deployment of AN, effectively balancing the need to maintain high-quality service for legitimate users while thwarting potential eavesdropping attempts. The flexibility of the PAN approach in resource allocation makes it particularly beneficial in scenarios where both security and service quality need to be carefully managed. As shown in Fig. 2, APs with black dashed lines are solely responsible for transmitting AN. The m^{th} AP in the first subset sends the data $x_{m,n} = \sum_{k=1}^{K} w_{mk,n} s_{k,n}$, and the j^{th} AP in the second subset transmits the AN $x^e_{j,n} = v_{j,n}\bar{s}_{j,n}$, following the condition $\sum_{j=1}^{M'} g_{kj,n} v_{j,n} = 0$ for $k \in \{1 \dots K\}$, where M' is the number of APs in the second subset and $M' > K$, resulting in the received signal at the k^{th} UE

$$
\begin{aligned}
r_{k,n} &= \sum_{m=1}^{M-M'} g_{km,n} x_{m,n} + \sum_{j=1}^{M'} g_{kj,n} x^e_{j,n} + z_{k,n} \\
&= \sum_{m=1}^{M-M'} g_{km,n} \sum_{k'=1}^{K} w_{mk',n} s_{k',n} + \sum_{j=1}^{M'} g_{kj,n} v_{j,n} \bar{s}_{j,n} + z_{k,n} \qquad (6)
\end{aligned}
$$

Finally, the received signal at the i^{th} Eve is denoted by

$$
r^e_{i,n} = \sum_{m=1}^{M-M'} g_{im,n} \sum_{k'=1}^{K} w_{mk',n} s_{k',n} + \sum_{j=1}^{M'} g_{ij,n} v_{j,n} \bar{s}_{j,n} + z_{i,n} \qquad (7)
$$

C. Feasibility Condition for AN vector

To transmit AN into the users' null space, the AN streams are pre-coded using a vector $\mathbf{v}_n$, which is derived from the columns of the null space of the channel matrix $\mathbf{G}_n$. The null space of $\mathbf{G}_n$ exists when the number of transmitting antennas exceeds the number of receiving antennas. In CF-mMIMO systems, this condition typically occurs when the number of APs, denoted as M, is significantly greater than the number of users, denoted as K. Furthermore, to effectively beamform the AN, the design leverages this difference in the number of APs and users to ensure that the artificial noise does not interfere with the intended communication signals. It is also important to carefully satisfy this condition in the second method (PAN) when selecting the subset of APs designated to transmit AN, ensuring that the subset configuration does not compromise the security or performance of the system [16].

D. Passive vs Active Eavesdroppers

Passive Eves pose a security threat due to the open and distributed nature of CF-mMIMO systems. These eavesdroppers silently intercept communications without actively engaging with the network, making them difficult to detect. While passive Eves can compromise the confidentiality of transmitted data, their impact is generally limited to overhearing communications without altering the network's operation. In contrast, active eavesdroppers are more aggressive and pose a greater threat. They can mimic legitimate nodes or create interference, allowing them to manipulate the network environment and potentially access more confidential information. A major threat from active Eves is their ability to conduct pilot spoofing attacks, where they transmit false pilot sequences to contaminate the CSI used by legitimate users. This contamination degrades the quality of the received signal and increases the likelihood of data interception. In our system model, we address the threat of active eavesdroppers by simulating the effects of pilot spoofing attacks, including the resulting pilot contamination. We introduce adjustment factors to model the degradation in channel estimation accuracy, providing a more realistic evaluation of system performance and security in the presence of both passive and active eavesdroppers.

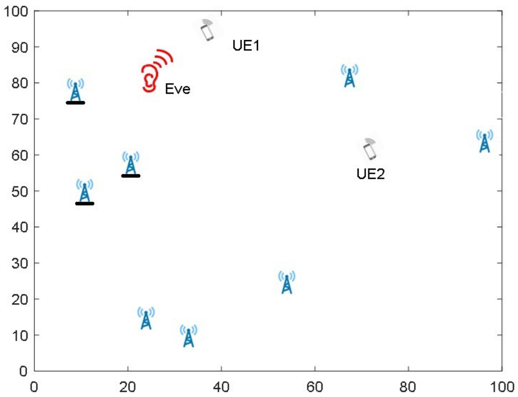


Fig. 2: A CF-mMIMO system with 2 single antenna users, a single antenna Eve and 8 single antenna APs.

IV. Numerical Result and Discussion

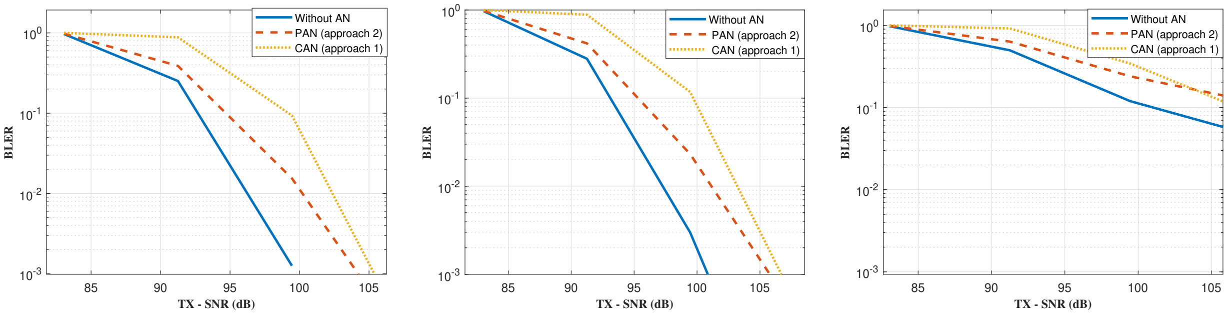
A. Parameters and Setup

We consider a CF-mMIMO system with a simplified setup of 8 single-antenna APs, 2 single-antenna UEs, and 1 single-antenna Eve, all randomly distributed within a $100\text{m} \times 100\text{m}$ area, as shown in Fig. 2. This small configuration is specifically chosen because our link-level simulations account for all the detailed aspects of coding, modulation, and channel effects, which makes the simulations highly accurate but also computationally intensive. By using this limited setup, we can thoroughly explore the performance and security characteristics of the system while managing the considerable computational demands of such detailed simulations. The small-scale fading channel parameters, as well as the basic setup for the PDSCH and carrier, are detailed in Table I.

TABLE I: System Parameters for the Simulation

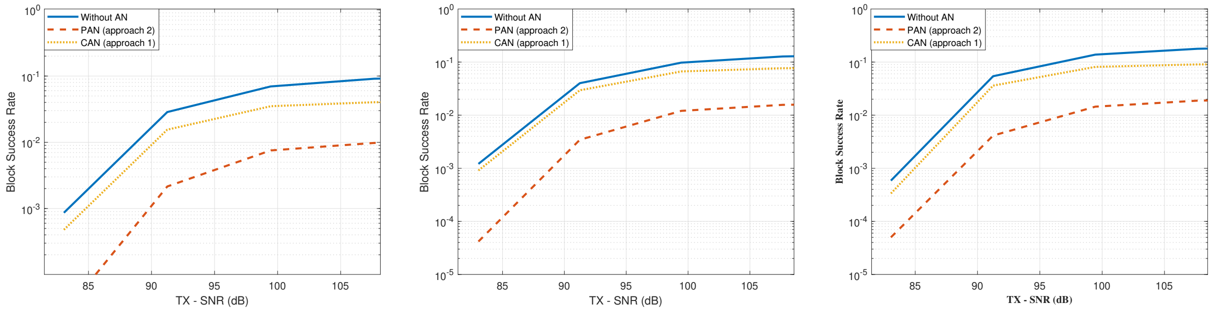
Modulation - Code rate	QPSK - 120/1024
Transport block size	3912
Subcarrier spacing	15 KHz
Delay profile	TDL-B
Delay spread	30 ns
Maximum doppler shift	10
Noise figure (NF)	9 dB
Noise temperature	290 K

The noise power, N, is calculated using the formula $N = k \times B \times T_e$, where $k = 1.3807 \times 10^{-23}$ J/K is the Boltzmann constant, and B represents the bandwidth. The equivalent noise temperature, T_e, is determined by $T_e =$



(a) MMSE precoder (b) ZF precoder (c) MRT precoder

Fig. 3: BLER versus TX-SNR for legitimate UE in a system setup with passive Eves, using MMSE, ZF, and MRC precoders.



(a) MMSE precoder (b) ZF precoder (c) MRT precoder

Fig. 4: BLSR versus TX-SNR for illegitimate UE in a system setup with passive Eves, using MMSE, ZF, and MRC precoders.

$T_{\text{Ant}} + 290 \times (\text{NF} - 1)$, where $T_{\text{Ant}} = 290$ denotes the input noise temperature.

B. Large-Scale Fading Model

We use the 3GPP path loss model and uncorrelated shadow fading from [14] to calculate the large-scale fading coefficient. In our setup, defining the SNR is challenging because the signal from a UE is received by different APs over links of varying lengths. This variability in link distances results in different levels of signal attenuation and noise at each AP. To address this, we use the TX-SNR, defined as the ratio of the signal power at the transmitter (APs) to the noise power at the receiver (UEs). This approach compensates for high path loss by setting a sufficiently large TX-SNR, ensuring that the overall system performance is accurately evaluated across various transmission scenarios.

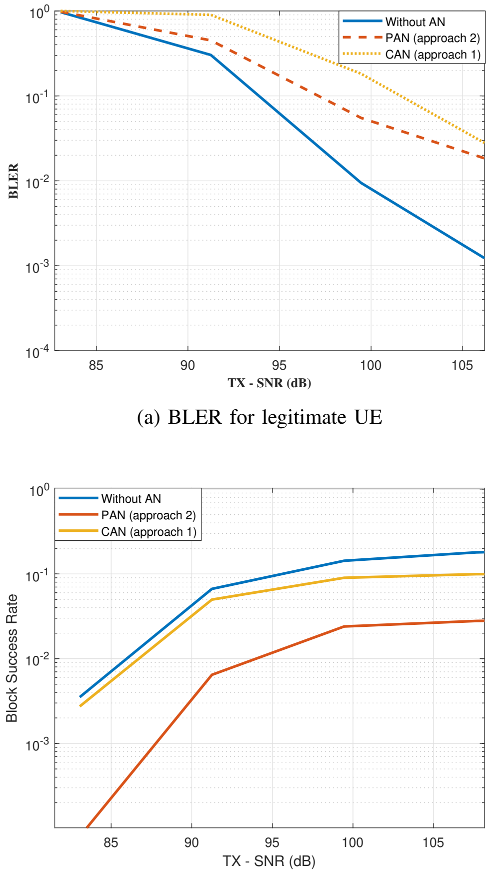
C. Numerical Results

Figure 3 shows the impact of different PLS approaches on the BLER for a legitimate user in the presence of passive Eves, using MMSE, ZF, and MRT precoding schemes. While a lower BLER indicates better performance, introducing PLS techniques like CAN and PAN causes some degradation in the legitimate user's performance. However, this degradation is less significant with the PAN approach, particularly when compared to CAN. Furthermore, MMSE and ZF precoding schemes show a minimal performance trade-off in BLER compared to MRT. Figure 4 presents the BLSR versus TX-SNR for an eavesdropper in a system with passive eavesdroppers, using MMSE, ZF, and MRT precoding schemes. A lower BLSR reflects better security, as it indicates a reduced success rate for eavesdropping. With MMSE precoding, both PAN and CAN effectively lower the BLSR, with PAN offering the best performance in minimizing the eavesdropper's success. This trend is consistent across ZF and MRT precoding schemes, with PAN consistently achieving the lowest BLSR at most TX-SNR levels, demonstrating its effectiveness in enhancing system security. Taken together, Figures 3 and 4 highlight the trade-off between security and performance: while adding AN through PAN and CAN approaches improves security by reducing the BLSR for eavesdroppers, it results in a slight increase in BLER for legitimate users. This underscores the need to balance enhanced security against eavesdropping with maintaining optimal communication performance for legitimate users. Specifically, with the MMSE precoder, both CAN and PAN significantly reduce the BLSR of Eves, from approximately 0.1 without AN to 0.02 and 0.01, respectively. However, this improvement in security comes at the cost of performance for legitimate UEs, as indicated by an increase in BLER from 0.001 without AN to 0.01 with PAN and 0.1 with CAN.

Figure 5 illustrates the BLER and BLSR versus TX-SNR for both legitimate users and Eves in a setup with active eavesdroppers and an MMSE precoder. In Figure 5a, which shows the BLER for legitimate users, the system without AN has the lowest BLER across all TX-SNR levels. For instance, at a TX-SNR of 95 dB, the BLER without AN is about 0.06, while it increases to around 0.2 with PAN and 0.5 with CAN. Conversely, Figure 5b indicates that the BLSR for eavesdroppers is higher without AN, implying less security. At a TX-SNR of 95 dB, the BLSR without AN is approximately 0.1, compared to around 0.06 with PAN and 0.01 with CAN, demonstrating that adding AN effectively reduces the eavesdropper's success rate, albeit with a slight trade-off in performance for legitimate users.

V. Conclusions

In this paper, we have investigated the vulnerability of downlink transmissions in CF-mMIMO systems to both passive and active eavesdropping within a 5G NR framework. To counter these eavesdropping threats, we proposed two innovative methods based on cooperative AN. The first approach involves all access APs broadcasting AN in the null space of the users' channel matrix, while the PAN method divides APs into two groups, with one group transmitting AN and the other serving legitimate users. Our link-level simulations, conducted under various frequency-selective fading scenarios and noise conditions using 3GPP TR 38.901 channel models, show that these strategies can significantly enhance the security of downlink transmissions. Notably, the PAN approach demonstrates a superior ability to reduce the BLSR of eavesdroppers, achieving a reduction from 0.2 without AN to 0.1 with CAN and further down to 0.025 with PAN. Despite the promising results, our study was limited to ideal channel conditions without considering the effects of practical channel estimation errors. As future work, we intend to incorporate practical channel estimation effects into our results to better reflect real-world scenarios. Additionally, we will explore optimization techniques to find the best trade-offs between security performance and system resources, potentially enhancing the effectiveness of our proposed methods in diverse deployment environments.



(a) BLER for legitimate UE

(b) BLSR for Eve

Fig. 5: BLER and BLSR versus TX-SNR for legitimate UE and eavesdropper in a system setup with active eavesdroppers, using an MMSE precoder.

References

[1] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1834–1850, 2017.

[2] H. Q. Ngo, G. Interdonato, E. G. Larsson, G. Caire, and J. G. Andrews, "Ultradense cell-free massive MIMO for 6G: Technical overview and open questions," *Proceedings of the IEEE*, 2024.

[3] M. Rahmani, M. Bashar, M. J. Dehghani, A. Akbari, P. Xiao, R. Tafazolli, and M. Debbah, "Deep reinforcement learning-based sum rate fairness trade-off for cell-free mMIMO," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 5, pp. 6039–6055, 2022.

[4] J. Zheng, J. Zhang, H. Du, D. Niyato, B. Ai, M. Debbah, and K. B. Letaief, "Mobile cell-free massive MIMO: Challenges, solutions, and future directions," *IEEE Wireless Communications*, 2024.

[5] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2016.

[6] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: Optimal power control against active eavesdropping," *IEEE Transactions on Communications*, vol. 66, no. 10, pp. 4724–4737, 2018.

[7] Y. Zhang, W. Xia, G. Zheng, H. Zhao, L. Yang, and H. Zhu, "Secure transmission in cell-free massive MIMO with low-resolution DACs over rician fading channels," *IEEE Transactions on Communications*, vol. 70, no. 4, pp. 2606–2621, 2022.

[8] X. Ma, X. Lei, X. Zhou, and X. Tang, "Secrecy performance evaluation of scalable cell-free massive MIMO systems: A stochastic geometry approach," *IEEE Transactions on Information Forensics and Security*, 2023.

[9] X. Gao, Y. Li, W. Cheng, L. Dong, and P. Liu, "Secure optimal precoding for user-centric cell-free massive MIMO system," *IEEE Wireless Communications Letters*, vol. 12, no. 1, pp. 31–35, 2022.

[10] X. Xia, Z. Fan, W. Luo, A. Lu, D. Wang, X. Zhao, and X. You, "Joint uplink power control, downlink beamforming, and mode selection for secrecy cell-free massive MIMO with network-assisted full duplexing," *IEEE Systems Journal*, vol. 17, no. 1, pp. 720–731, 2022.

[11] Y. Chen, X. Zhang, F. Yao, K. An, G. Zheng, and S. Chatzinotas, "Pilot assignment and power control in secure UAV-enabled cell-free massive MIMO networks," *IEEE Internet of Things Journal*, 2023.

[12] Y. S. Atiya, Z. Mobini, H. Q. Ngo, and M. Matthaiou, "Secure transmission in cell-free massive MIMO under active eavesdropping," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2024.

[13] A. Tahreem, D. Tubail, and S. Ikki, "Impact of hardware impairments on physical layer security of cell-free massive MIMO," in *2024 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2024, pp. 246–251.

[14] 3GPP, "Study on channel model for frequencies from 0.5 to 100 GHz," *ETSI, TR 38.901 version 17.0.0*, 2022.

[15] L. Miretti, E. Björnson, and D. Gesbert, "Team MMSE precoding with applications to cell-free massive MIMO," *IEEE Transactions on Wireless Communications*, vol. 21, no. 8, pp. 6242–6255, 2022.

[16] D. A. Tubail, M. Alsmadi, and S. Ikki, "Physical layer security in downlink of cell-free massive MIMO with imperfect CSI," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2945–2960, 2023.