A Survey on Artificial Noise for Physical Layer Security: Opportunities, Technologies, Guidelines, Advances, and Trends

Hong Niu, Yue Xiao, Xia Lei, Jiangong Chen, Zhihan Xiao, Mao Li, and Chau Yuen

Due to the broadcast nature of wireless communications, physical-layer security has attracted increasing concerns from both academia and industry. Artificial noise (AN), as one of the promising physical-layer security techniques, is capable of utilizing the spatial degree-of-freedom of channels to effectively enhance the security of wireless communications. In contrast to other physical-layer security techniques, the key distinguishing feature of AN is to generate specific interfering signals according to channel characteristics, increasing the secrecy capacity by reducing the wiretap channel capacity without affecting the legitimate channel capacity. Hence, this paper provides the latest survey of AN, including its evolution, modeling, backgrounds, applications, and future trends. Initially, we introduce the development, fundamentals, and backgrounds of AN. Subsequently, we highlight a comprehensive survey of the current state of research on various AN-empowered scenarios and AN-combined technologies. Finally, we discuss some technical challenges to tackle for AN-aided wireless security in the future.

***Index Terms*—Artificial noise (AN), physical-layer security, wireless communications, resource allocation.**

List of Abbreviations

2D	Two-dimensional
3D	Three-dimensional
5G	Fifth-generation
6G	Sixth-generation
AD	Alternating direction
AF	Amplify-and-forward
AFF	Artificial fast fading
AG	Air-ground
Alice	Legitimate transmitter
AN	Artificial noise
ANE	Artificial noise elimination
ANH	Artificial noise hopping
AN-SM	Artificial-noise-aided spatial modulation
ANSR	Artificial noise to signal ratio
ARQ	Automatic-repeat-request
AWGN	Additive white Gaussian noise
BCD	Block coordinate descent
BD	Block diagonalization
BER	Bit-error rate
Bob	Legitimate receiver
BS	Base station
CB	Cooperative beamforing
CBS	Cognitive base station
CJ	Cooperative jammer
CP	Cyclic prefix
CPS	Cyber physical system
CR	Cognitive radio
CRN	Cognitive radio network
CSI	Channel state information
CU	Cognitive user
D2D	Device-to-device
DCAN	Data carrying artificial noise
DF	Decode-and-forward
DFRC	Dual-functional Radar Communication
DM	Directional modulation
DNN	Deep neural network
DoF	Degree-of-freedom
DQSM	Differential quadrature spatial modulation
DRFC	Dual-functional radar-communication
EH	Energy harvesting
ER	Energy receiver
ESR	Ergodic secrecy rate
Eve	Eavesdropper
FD	Full-duplex
FDMA	Frequency-division multiple access
FFT	Fast Fourier Transform
FH	Frequency hopping
GPI	General power iterative
GSM	Generalized spatial modulation
HD	Half-duplex
IA	Interference alignment
IFFT	Inverse fast Fourier transform
IoT	Internet of things
IOS	Intelligent omni surface
IQ	In-phase and quadrature
ISAC	Integrated sensing and communication
LED	Light-emitting diode
LoS	Line-of-sight
MAC	Medium-access control
MEC	Mobile-edge computing
MIMO	Multiple-input multiple-output
MIMOME	Multiple-input multiple-output multiple-antenna-eavesdropper
MIMOSE	Multiple-input multiple-output single-antenna-eavesdropper
MISO	Multiple-input single-output
MISOME	Multiple-input single-output multiple-antenna-eavesdropper
MISOSE	Multiple-input single-output single-antenna-eavesdropper
MLI	Main-lobe-integration
MM	Majorization-minimization
MMA	Multiple multiple-antenna
mMIMO	Massive multiple-input multiple-output
mmWave	Millimeter wave
MRC	Maximal ratio combining
MRT	Maximal ratio transmission
MSA	Multiple single-antenna
MSE	Mean squared error
MU	Multi-user
nLoS	Non-light-of-sight
NOMA	Non-orthogonal multiple access
NR	Non-regenerative
OFDM	Orthogonal frequency division multiplexing
OM	Oblique manifold
OSI	Open system interconnection
OSTBC	Orthogonal space-time block code
PAM	Pulse amplitude modulation
PAPR	Peak-to-average power ratio
PLS	Physical-layer security
PMAN	Power minimized artificial noise
PU	Primary user
PLA	Physical layer authentication
PZ	Protected zone
QoMS	Quality of multicast service
QoS	Quality of service

H. Niu, Y. Xiao, X. Lei, J. Chen, Z. Xiao, and M. Li are with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, 611731, Sichuan, China (Email: niuhong@std.uestc.edu.cn; xiaoyue@uestc.edu.cn; leixia@uestc.edu.cn; jg_chen@std.uestc.edu.cn; 202221220122@std.uestc.edu.cn; 2385353188@qq.com).

C. Yuen is with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore 639798 (email: chau.yuen@ntu.edu.sg; Corresponding author: C. Yuen).

QVP	Quality of violation probability
RCI	Regularized channel inversion
RF	Radio frequency
RIS	Reconfigurable intelligent surface
RLC	Rateless codes
SCA	Successive convex approximation
SDP	Semidefinite program
SDR	Semidefinite relaxation
SEE	Secrecy energy efficiency
SEEM	Secrecy energy efficiency maximization
SIC	Self-interference cancellation
SIMOME	Single-input multiple-output multiple-antenna-eavesdropper
SIMOSE	Single-input multiple-output single-antenna-eavesdropper
SER	Symbol error rate
SINR	Signal to interference plus noise ratio
SISO	Single-input single-output
SISOME	Single-input single-output multiple-antenna-eavesdropper
SISOSE	Single-input single-output single-antenna-eavesdropper
SKG	Secret key generation
SM	Spatial modulation
SMA	Single multiple-antenna
SNR	Signal to noise ratio
SOP	Secrecy outage probability
SRM	Secrecy rate maximization
SSA	Single single-antenna
SSR	Secrecy sum rate
STBC	Space time block code
STLC	Space time line code
STM	Secrecy throughput maximization
SU	Secondary user
SVD	Singular value decomposition
SWIPT	Simultaneous wireless information and power transfer
TAS	Transmit antenna selection
TDD	Time division duplexing
THP	Tomlinson-Harashima precoder
THz	Terahertz
TSPS	Time-switching power-splitting
UAV	Unmanned aerial vehicle
UC-SM	Unitary coded spatial modulation
UTWR	Untrusted two-way relay
VAA	Virtual antenna array
VLC	Visible light communication
WPT	Wireless power transfer
ZF	Zero-forcing

I. Introduction

DURING the last decades, wireless communications have been proliferating with the maturity commercialization of the fifth-generation (5G) and the forthcoming development of the sixth-generation (6G) technologies [1]. Due to the nature of broadcast propagation, the data transmission in wireless communication suffers from a critical threat of information leakage, which calls for the paramount importance of improving wireless communications security [2]. As a widely used protocol architecture for wireless communications, the open system interconnection (OSI) model [3] consists of the application layer [4], presentation layer [5], session layer, transport layer [6], network layer [7], medium-access control (MAC) layer [8], and physical layer [9]–[24] from top to bottom. In order to comprehensively and effectively ensure the security of wireless communications, relevant security threats and vulnerabilities in each protocol layer are individually protected to meet the security requirements of authenticity, confidentiality, integrity, availability, and so on [25]. Generally above the network layer, the information security has been conventionally guaranteed by using pre-shared keys [26]. Although the cryptographic mechanism indeed enhances the secrecy performance of communications, it suffers from the redundant secret key distribution and management process, especially in high-speed and low-latency dynamic wireless communications. Hence, cryptography requires additional computational power and endures an increasing latency with the rapid growth of large-scale resource-constrained wireless devices. More fatally, all encryption measures are based on the premise that decrypting is impossible without the knowledge of key, which may be invalid with the relentless growth of computational power.

During recent decades, physical-layer security (PLS) has been heralded as a potential direction for information-theoretic security of wireless communications against eavesdropping, as a complement to upper-layer encryption mechanisms. The fundamental principle of PLS was initially studied by Wyner [27], where the key principle is to exploit the inherent randomness of noise or channels to limit the amount of information intercepted by unauthorized receivers. In [27], the gap of channel capacity between the legitimate user and unauthorized eavesdropper is defined as the secrecy capacity and it is proved that secure transmission can be achieved as long as the secrecy capacity is positive. Following this concept, the artificial noise (AN) technology has been widely investigated as a typical PLS technique due to its ability to utilize channel state information (CSI) to enhance the secrecy performance. The AN technique is usually implemented at the legitimate transmitter (Alice), leveraging the spatial degree-of-freedom (DoF) of channels to ensure secure communications. By invoking the AN into the null space[1]of channels of legitimate receiver (Bob), it is able to further enhance the secrecy performance by reducing the channel capacity of eavesdropper (Eve) without seriously affecting that of Bob due to the channel differences between them. Compared with the conventional cryptographic mechanism, AN has the following core features:

Information-theoretic security: AN realizes the PLS by exploiting the characteristic of channels, where the secrecy performance can be theoretically analyzed and information-theoretic security can be constructed.

Acceptable power consumption: Although the deployment of AN may occupy additional power, the performance loss of Bob is acceptable in contrast to that of Eve. Additionally, in some specific systems, the optimized AN may not invoke power consumption.

Software programmable: AN can realize real-time and dynamic regulation with the variation of channel response.

Excellent compatibility: As a beamforming technology for security, AN can be easily compatible with various systems in wireless propagation environments.

In a nutshell, AN has significant potential to become a crucial PLS technique for wireless communications. However, the state-of-art research reported in the literature has not conducted a comprehensive survey on AN, which is the original motivation for writing this paper. Although several noteworthy surveys have been published in the domain of PLS,

[1]The null space is the set of all vectors that are mapped to the zero vector when the transformation is applied. In the context of AN, the null space is used to design the AN signal that has no influence on the information-bearing signal, allowing for secure communication while obscuring information from eavesdroppers (refer to Section II.C.).

there is still an insufficient focus on the AN and the coverage of its applications. As summarized in Table I, existing surveys mainly focus on the PLS rather than the AN technology, thus somewhat neglecting the introduction of AN principles, system models, related applications, and future directions. Additionally, due to the excessive number of technologies involved in PLS and different focuses, some applications have been omitted in the existing surveys.

Against this backdrop, the main contributions of this paper are divided into two folds. On the one hand, we focus on the AN technology to fill the gap in existing surveys. On the other hand, we provide more comprehensive applications in terms of AN-empowered scenarios and AN-combined technologies. Through our efforts, readers are expected to quickly figure out the principles, research status, design features, and future challenges of AN in their interested topics.

To this end, the remainder of this paper is organized as follows.

- In Section II, the evolution and fundamentals of AN are introduced, along with common design guidelines.
- In Section III, a comprehensive survey of the current state of research on AN-empowered scenarios is presented.
- In Section IV, a comprehensive survey of the current state of research on AN-combined technologies is provided.
- In Section V, the most significant challenges worth future tackling are discussed.
- In Section VI, a brief conclusion is drawn.

II. AN Evolution and Modeling

A. AN Evolution

The theoretical framework of AN was academically mentioned by Goel and Negi in 2005 [28] and 2008 [29] to guarantee the secrecy performance of multiple-input single-output (MISO)/ multiple-input multiple-output (MIMO) systems by mixing the information-bearing and AN signals at Alice[2]. Since the AN lies in the null space of Bob's channel, it has no influence on the signal detection of Bob. However, due to the channel difference between Bob and Eve, the received signal at Eve will be severely affected by the AN, which can be regarded as the degradation of Eve's channel. In addition, the existence of null space requires satisfying the constraint that the number of Alice's antennas is larger than that of Bob, which can be seen as using the spatial DoF to generate AN [32].

Later on, some investigation on the performance analysis of AN sprang up, with the purpose of illustrating the secrecy performance of AN [33]–[36]. For example, in [33], the closed-form expressions of the connection and secrecy outage probabilities (SOPs) were derived for multi-antenna small-cell networks, where the results show that in a low cell-load case, deploying more base stations (BSs) will improve the connection and secrecy outage performance, and deploying more transmit antennas at each BS will only improve the connection outage performance. In [34], the closed-form expression for the ergodic secrecy sum rate (SSR) was derived for the large system in the multiuser downlink, and the power allocation between information-bearing signals and the AN was optimized by maximizing the SSR. It shows that more power needs to be used for AN when Eve has more antennas and when the system serves fewer users. In [35], the upper and lower bounds of the leakage rate to the eavesdropper in the high signal to noise ratio (SNR) regime were represented by a single compact expression as a function of the number of Eve's antennas, the dimensionality of signal space, and the channel coherence time, which offers useful insights in exploiting the secrecy potential of the AN-assisted massive multiple-input multiple-output (mMIMO) systems. In [36], the SOP and mean secrecy rate were derived for the large-scale broadcast channels. Analytical results show that i) when the AN is adopted, the SOP exponentially decays with the number of transmission antennas, ii) in most of the power allocation cases, the per-user secrecy rate can be improved significantly, e.g., there is an almost 2.7 times of improvement for the particular transmission antennas number.

In order to further expand the usage scope of AN, in 2012, the authors of [37] first studied a new form of AN by removing the limitation of null space, which is also known as generalized AN [38]. The authors of [37] and [38] investigated the secrecy rate optimization problems of generalized AN in multiple-input multiple-output single-antenna-eavesdropper (MIMOSE) and multiple-input single-output single-antenna-eavesdropper (MISOSE) systems, respectively, where the conventional AN based on null space is demonstrated to be strictly sub-optimal. Then the authors of [39] addressed the generalized AN to the discriminatory channel estimation for multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) systems, in which the AN covariance matrix, the pilot signal power, and the linear estimator are jointly determined to minimize the channel estimation error. Moreover, the authors of [40] focused on the generalized AN generation in MIMOME Rician channels using the complex non-central Wishart distribution, while the authors of [41] paid attention to the generalized AN with the CSI of the eavesdropping channel for MIMOME systems. Recently, the authors of [42] pointed out that the optimality of generalized AN in [38] is valid only under some ideal assumptions such as perfect channel estimation and spatially uncorrelated channels. To break through this limitation, the authors of [42] first exploited a deep neural network (DNN) to jointly design and optimize the precoders for the information signal and the AN, which is called the deep AN scheme.

In 2014, the researchers of [43] proposed a time-domain AN generation technique to orthogonal frequency division multiplexing (OFDM) systems when the null space in the spatial domain may not exist, and showed that this technique requires a longer cyclic prefix (CP). In 2016, the combination of AN and secret key generation (SKG) was first named data carrying artificial noise (DCAN) in [44] to summarize the

[2]AN and friendly jamming are both techniques designed to improve communication security by thwarting eavesdropping. The AN seeks to obscure the intended signal by introducing random noise that primarily impacts potential Eves, whereas friendly jamming actively disrupts an Eve's ability to intercept communications by creating intentional interference. Although both strategies aim to protect legitimate communication, they are distinct technologies with different foundational principles and implementation methods. AN is a technique that introduces randomness at the transmitter, whereas friendly jamming requires cooperative nodes to create the interference [16], [30], [31].

TABLE I
SUMMARY OF SURVEYS RELATED TO AN

Main Topics	Related Scenarios								Related Technologies							Main Contributions
Reference (year)	HetNet[1]	IoT	mmWave	MU	Relay	Satellite	UAV	VLC	Coding	DM	mMIMO	NOMA	OFDM	RIS	SM	
[9] (2014)				✓					✓							PLS in MU networks
[10] (2017)	✓			✓	✓											Multiple-antenna techniques for PLS
[11] (2017)				✓		✓										PLS in satellite systems
[12] (2018)	✓		✓						✓		✓	✓				PLS for 5G
[13] (2018)								✓								PLS for optical wireless communications
[14] (2019)	✓	✓	✓		✓		✓	✓	✓			✓				Classifications and applications of PLS
[15] (2019)				✓	✓											Optimization approaches for PLS
[16] (2019)	✓				✓						✓	✓				Cooperative relaying and jamming for PLS
[17] (2019)	✓		✓								✓					PLS for 5G
[18] (2020)	✓	✓				✓										PLS in space information networks
[19] (2020)			✓					✓								PLS for VLC
[20] (2021)		✓														PLS for IoT
[21] (2022)							✓									PLS for UAV
[22] (2022)		✓			✓											PLS in satellite networks
[23] (2023)							✓									PLS for UAV
[24] (2024)														✓		RIS-assisted PLS
This survey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	AN-assisted PLS with wider coverage

[1]Heterogeneous networks, including CRN, D2D, SWIPT, etc.

case that Bob uses the pre-shared knowledge of AN and SKG to mitigate the influence. On one hand, finding a balanced trade-off for power allocation between the information-bearing signal and the AN has attracted wide attention. For example, the authors of [45] investigated the power allocation by maximizing a lower bound of ergodic secrecy rate (ESR) for MIMOME in 2018. On the other hand, the optimization for a new form of AN is desired to reduce the power consumption and enhance the jamming effect of AN. Specifically, in 2020, an Euclidean distance optimized AN scheme was proposed by minimizing the Euclidean distance between the transmit signal and a random jamming signal, which introduces no waste of transmit power and provides a stronger jamming intensity to eavesdroppers in contrast to conventional AN scheme using complex Gaussian random matrix [46].

In general, the AN has been progressively evolving towards broader application scenarios, enhanced energy efficiency, and improved jamming effectiveness.

B. Modeling of AN-assisted Wireless Communications

As depicted in Fig. 1, most wireless secrecy communication systems consist of an Alice with N_a antennas, a Bob with N_b antennas, and an unauthorized Eve with N_e antennas, wherein Alice wishes to convey a private message to Bob under the wiretapping of a passive Eve. While transmitting the information-bearing signal, Alice is able to generate specific interfering signals termed AN so that only Eve is adversely affected by the interfering signals, while Bob remains slightly unaffected. The transmit signal at Alice can be modeled as

$$\mathbf{x} = \mathbf{W}\mathbf{s} + \mathbf{V}\mathbf{r}, \tag{1}$$

where $\mathbf{W}\mathbf{s}$ and $\mathbf{V}\mathbf{r}$ denote the information-bearing signal and AN, respectively. In practice, the precoding/beamforming matrix $\mathbf{W}\in^{N_a\times N_s}$ attempts to enhance the transmission quality of the information-bearing vector $\mathbf{s} \in \mathbb{C}^{N_s}$ and N_s denotes the number of data stream, while the AN matrix $\mathbf{V} \in \mathbb{C}^{N_a\times(N_a-N_b)}$ tries to reduce the impact of AN vector $\mathbf{r} \in \mathbb{C}^{(N_a-N_b)}$ for Bob. The transmit signal is conveyed to Bob via an MIMO channel $\mathbf{H} \in \mathbb{C}^{N_b\times N_a}$ and also received by Eve via a wiretap channel $\mathbf{G} \in \mathbb{C}^{N_e\times N_a}$. Hence, the received signals at Bob and Eve can be expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{W}\mathbf{s} + \mathbf{H}\mathbf{V}\mathbf{r} + \mathbf{u}, \tag{2}$$

$$\mathbf{z} = \mathbf{G}\mathbf{W}\mathbf{s} + \mathbf{G}\mathbf{V}\mathbf{r} + \mathbf{v}, \tag{3}$$

where $\mathbf{u} \in \mathbb{C}^{N_b}$ and $\mathbf{v} \in \mathbb{C}^{N_e}$ stand for complex additive white Gaussian noise (AWGN) with elements obeying i.i.d. $\mathcal{CN}(0,\sigma_u^2)$ and $\mathcal{CN}(0,\sigma_v^2)$, respectively.

1) Orthogonal AN

With the CSI of Bob, an orthogonal AN can be conducted using null-space projection. Specifically, assuming $\mathbf{V}$ is the null space of $\mathbf{H}$, i.e., $\mathbf{H}\mathbf{V} = \mathbf{0}$, the influence of AN can be mitigated at Bob as

$$\mathbf{y} = \mathbf{H}\mathbf{W}\mathbf{s} + \mathbf{u}. \tag{4}$$

It is worth mentioning that the null space $\mathbf{V}$ can be obtained by the singular value decomposition (SVD) of $\mathbf{H}$ as

$$\mathbf{H} = \mathbf{U}\begin{bmatrix}\mathbf{D} & 0\end{bmatrix}\begin{bmatrix}\mathbf{V}_1 & \mathbf{V}\end{bmatrix}^H, \tag{5}$$

where $\mathbf{U} \in \mathbb{C}^{N_b\times N_b}$ denotes a unitary matrix composed of left singular vectors of $\mathbf{H}$, $\mathbf{D} \in \mathbb{C}^{N_b\times N_b}$ represents a diagonal matrix whose entries are the singular values of $\mathbf{H}$, $\mathbf{V}_1 \in \mathbb{C}^{N_a\times N_b}$ consists of the first N_b right singular vectors of $\mathbf{H}$, spanning the subspace corresponding to the information-bearing, and $\mathbf{V} \in \mathbb{C}^{N_a\times(N_a-N_b)}$ contains the remaining $N_a - N_b$ right singular vectors, spanning the null space associated with the noise component. Another more straightforward way to obtain the null space of $\mathbf{H}$ is

$$\mathbf{V} = \mathbf{I} - \mathbf{H}^{\mathrm{H}}(\mathbf{H}\mathbf{H}^{\mathrm{H}})^{-1}\mathbf{H}. \tag{6}$$

2) Non-orthogonal AN

Orthogonal AN may not be optimal when the CSI of Eve is known. An intuitive explanation is that one can further interfere with Eve by sacrificing part of Bob's communication quality. Mathematically, a generalized optimization problem

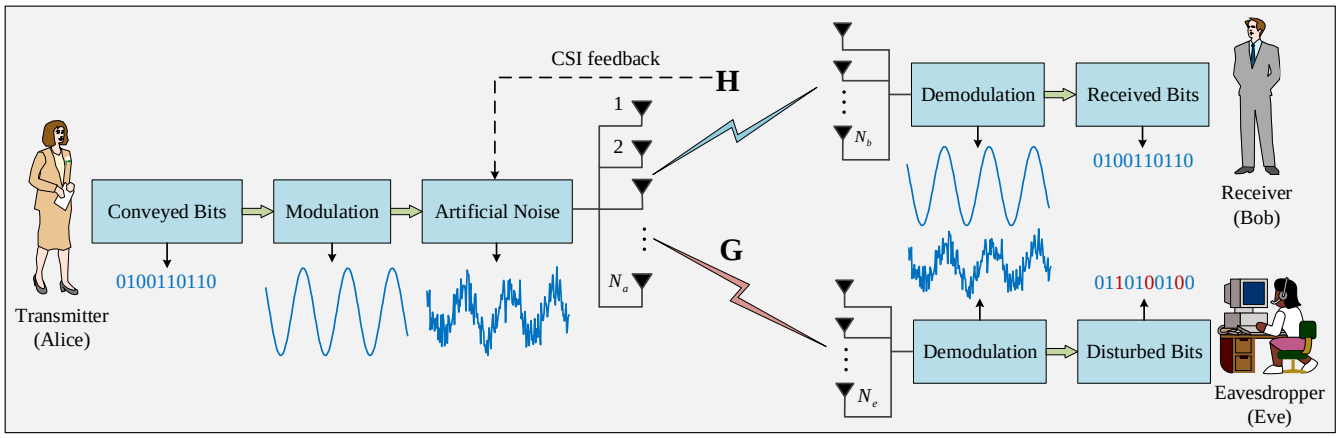

Fig. 1. Framework of AN-assisted wireless communications.

can be cast to design the beamforming matrix and the AN to improve the secrecy performance, which can be given by

$$\max / \min f(\mathbf{W}, \mathbf{V}, \mathbf{r}) \tag{7a}$$
$$\text{s.t. } \|\mathbf{x}\|^2 \leqslant 1, \tag{7b}$$
$$\mathbb{P}_{out} \leqslant \mathbb{P}_{\gamma}, \tag{7c}$$
$$R_b \geqslant \gamma_b, \tag{7d}$$
$$R_e \leqslant \gamma_e, \tag{7e}$$

where f denotes a specific secrecy-related objective function such as secrecy rate, secrecy capacity, or SOP. For instance, a maximization problem can be formulated as $\max R_s$, which aims to maximize the secrecy rate by enhancing Bob's achievable rate while suppressing Eve's. Conversely, a minimization problem may take the form $\min \mathbb{P}_{out}$, which attempts to minimize the SOP under the given constraints. Moreover, $\|\mathbf{x}\|^2 \leqslant 1$ represents the power constraint triggering the issue of power allocation between information-bearing signal and AN, $\mathbb{P}_{out} \leqslant \mathbb{P}_{\gamma}$ means that the SOP is restricted below a certain threshold, $R_b \geqslant \gamma_b$ indicates that the quality of service (QoS) of Bob is desired to exceed a certain threshold, while $R_e \leqslant \gamma_e$ implies that of Eve is lower than a certain threshold.

3) AN through Symbol-level Precoding

Different from the aforementioned orthogonal and non-orthogonal AN design at the channel fading rate, AN can also be conducted at the symbol rate with symbol-level precoding techniques [47]–[51]. As shown in Fig. 2, the effect of AN can be divided into constructive and destructive types. Thus, AN can be designed as constructive interference towards Bob for transmit power saving. Meanwhile, when the CSI of Eve is available, AN can be designed as destructive interference towards Eve. A general optimization for AN design in multi-user MISO $\mathcal{M}$-PSK transmissions through symbol-level precoding can be cast as

$$\min_{\mathbf{x}} \|\mathbf{x}\|_2^2 \tag{8a}$$
$$\text{s.t. } \left[\Re(\lambda_{n_\text{b}}) \sqrt{\Gamma_{n_\text{b}} \sigma_u^2}\right] \tan\theta_\text{th} \geq |\Im(\lambda_{n_\text{b}})|, \tag{8b}$$
$$\left[\Re(\lambda_{n_\text{e}}) - \sqrt{\Gamma_{n_\text{e}} \sigma_v^2}\right] \tan\theta_\text{th} \leq |\Im(\lambda_{n_\text{e}})|, \tag{8c}$$
$$1 \leq n_\text{b} \leq N_\text{b},\ 1 \leq n_\text{e} \leq N_\text{e}, \tag{8d}$$

where we have $\mathbf{h}_{n_\text{b}}^\text{T}\mathbf{x} = \lambda_{n_\text{b}} s_{n_\text{b}}$ and $\mathbf{h}_{n_\text{e}}^\text{T}\mathbf{x} = \lambda_{n_\text{e}} s_{n_\text{e}}$. s_{n_b} and s_{n_e} denote the expected receive PSK signals at the n_b-th Bob and n_e-th Eve, respectively, λ_{n_b} and λ_{n_e} represent the scalar factor for the n_b-th Bob and n_e-th Eve, respectively, $\mathbf{h}_{n_\text{b}}$ and $\mathbf{h}_{n_\text{e}}$ are the CSI for the n_b-th Bob and n_e-th Eve, respectively, Γ_{n_b} and Γ_{n_e} denote the SINR of the n_b-th Bob and n_e-th Eve, respectively, $\Re(\cdot)$ and $\Im(\cdot)$ represent the operations on taking the real and imaginary parts of complex numbers, respectively, and $\theta_\text{th} = \pi/\mathcal{M}$ stands for the phase deviation between adjacent PSK symbols.

From the perspective of secrecy performance, the non-orthogonal AN can provide a higher secrecy rate in contrast to the orthogonal one due to the intuitive objective function of the optimization problem. However, from the implementation perspective, the non-orthogonal AN requires Eve's CSI, which is unavailable as the passive receiver has no cooperation with Alice to perform the channel feedback. Although relevant papers may relax this restriction to only know the location range of Eve, the essence of requiring the CSI of Eve is unchanged. By contrast, the orthogonal AN, as a security technique that only requires the CSI of Bob, benefits from better feasibility. Furthermore, the orthogonal AN has no additional interference to Bob in comparison with the non-orthogonal one, hence maintaining the hardware requirements and detection technology for Bob. Finally, AN based on symbol-level precoding can improve secure transmission performance by designing the AN as constructive interference for Bob and destructive interference for Eve. For example, the authors of [51] investigated such AN in generalized spatial modulation (GSM) systems, resulting in both power saving and security enhancement.

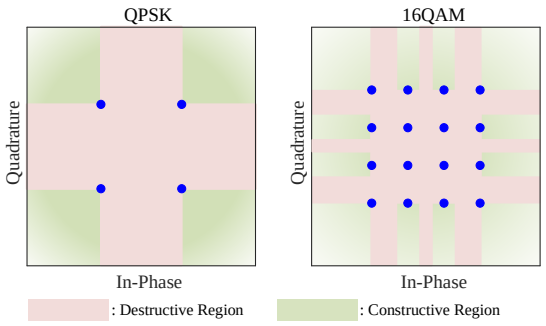

Fig. 2. Constructive and destructive interference illustration for QPSK and 16QAM constellations.

C. Technical Background

In order to provide researchers with a smoother reading experience, we first address some common issues, such as why AN technology is effective, what is the required workflow, and what are the minimum hardware requirements.

Why AN Is Effective?

AN is tailored to the characteristics of the legitimate channel, enabling it to disrupt Eve while allowing Bob to effectively extract the information. By masking the information-bearing signal with customized AN, the distinction between the legitimate channel and the wiretap channel prevents Eve from successfully eavesdropping. Specifically, the presence of random AN lowers the SNR at Eve, complicating the extraction of the information and increasing the likelihood of decoding errors. When AN is designed to align with the null space of the legitimate channel, it minimizes the impact on Bob's signal detection.

What Is the Complete Workflow?

The complete AN transmission workflow consists of the following three main steps.

1) Channel Assessment:

Evaluate the CSI of the legitimate channel via channel estimation and channel feedback.

2) AN Design and Integration:

Design the AN to match the specific characteristics of the legitimate channel, ensuring it effectively obscures the signal for Eves without significantly impacting Bob. Combine the AN with the information-bearing signal before transmission.

3) Transmission and Reception:

Transmit the combined signal over the legitimate channel to Bob and over the wiretap channel to Eve. Since the AN is tailored to the legitimate channel, Bob can successfully demodulate the information, while the detection of Eve is hindered by AN.

From the above steps, the prior information that Alice and Bob need to share includes the pilot signals, the CSI feedback mechanism, and the synchronization parameters.

Note that a capable Eve may estimate the CSI of the wiretap channel based on the pilot signal sent by Alice. However, due to the inherent difference between the wiretap channel and the legitimate channel, the random AN continues to interfere with Eve's reception. In practice, the differences between the wiretap channel and the legitimate channel are common due to the distinct placements of Bob and Eve, allowing Alice to design the AN solely based on the characteristics of the legitimate channel.

What Are the Minimum Hardware Requirements?

The minimum hardware requirements for implementing AN consist of signal processing units, modulators, demodulators, channel estimation tools, synchronization components, and power control modules. These components collaborate to generate, transmit, and process the AN effectively. Furthermore, the minimum number of RF chains varies depending on specific cases.

In scenarios where the deployment of AN has no influence on Bob, Alice are required to have more RF chains than Bob. This spatial-domain requirement typically applies to MISO and MIMO systems. However, in SISO systems, this restriction can be relaxed by sacrificing some frequency or time domain resources. For instance, in OFDM systems, the CP matrix offers time-domain DoF, which can reduce the number of RF chains needed by Alice. Similarly, in time-domain multiplexing systems, increasing the number of time slots also lessens Alice's RF chain requirements. Additionally, a mutual retransmission mechanism between Alice and Bob can also decrease the RF chain requirements.

In scenarios where the deployment of AN impacts Bob, the requirement for the number of RF chains becomes irrelevant. Here, effective AN design necessitates that the interference to Eve exceeds the interference to Bob. This requirement is often represented in research through quantitative metrics, such as secrecy capacity and secrecy rate, etc. However, these metrics rely on the channel CSI of the wiretap channel, challenging their implementation.

In a nutshell, the AN design generally requires Alice to have more RF chains than Bob. However, this requirement can be relaxed by sacrificing some frequency/time-domain resources or establishing a retransmission mechanism in advance between Alice and Bob.

Subsequently, we explain the meaning of some basic technical concepts.

Null Space: Given a channel matrix $\mathbf{H}$, its null space $\mathbf{V}$ is the combination of all orthogonal basis vectors such that

$$\mathbf{HV} = \mathbf{0}. \tag{9}$$

By deploying the AN in the null space of the legitimate channel, the legitimate receiver will not be interfered with, thus it is also called orthogonal AN. Although non-orthogonal AN is also mentioned in many papers, it is not as well-known as orthogonal AN as it may require the CSI of Eve. In technical implementation, the null space can be generated by performing the SVD or orthogonal projection on channel matrix $\mathbf{H}$ as shown in (5) or (6).

Spatial DoF: In general, the DoF refers to the number of independent parameters or variables that can vary in a system without violating any constraints. It is a measure of the number of independent directions or dimensions in which a system can move or be manipulated.

In AN technology, the elements of the random vector $\mathbf{r}$ are such independent parameters. The reason is that by multiplying

the random vector $\mathbf{r}$ at the right side of the null space matrix , the AN $\mathbf{Vr}$ will not affect Bob no matter how the random vector $\mathbf{r}$ changes. The dimension of the random vector $\mathbf{r} \in \mathbb{C}^{(N_a - N_b)}$ implies that the existence of spatial DoF requires Alice to have more antennas than Bob.

Secrecy capacity:

$$C_s \triangleq \max_{p(\mathbf{s})} \{I(\mathbf{s};\mathbf{y}) - I(\mathbf{s};\mathbf{z})\}. \tag{10}$$

The definition of secrecy capacity was firstly proposed in [27] as the gap of channel capacity between Bob and Eve. In [28] and [29], the expression for secrecy capacity under the AN technology was derived. Since the closed-form expressions for secrecy capacity are not always available [52], the following secrecy rate is often considered.

Secrecy rate:

$$R_s \triangleq I(\mathbf{s};\mathbf{y}) - I(\mathbf{s};\mathbf{z}). \tag{11}$$

The definition of secrecy rate is the gap of achievable rate between Bob and Eve, whose theoretical upper bound is the secrecy capacity when the distribution of $\mathbf{s}$ satisfies certain conditions. Note that in some literature, the secrecy rate is equivalent to the secrecy capacity because the authors may assume the perfect distribution of the source.

In extensive papers, the optimization problem was formulated to maximize the secrecy capacity or secrecy rate under specific constraints (see [53]–[56]). Moreover, the objective function can be transformed to some similar indicators.

For example, the ESR is the average of the secrecy rate over different channel realizations. This average is taken over the distribution of possible channel conditions, reflecting long-term or statistical performance as [45], [58]

$$R_s^{erg} = \mathbb{E}_{\mathbf{H},\mathbf{G}}[R_s]. \tag{12}$$

The SSR is the sum of the secrecy rates for all users in the system, which provides an aggregate measure of the secure transmission capacity across multiple users as [59]

$$R_s^{sum} = \sum_{k=1}^{K} R_s^k, \tag{13}$$

where k denotes the index of k-th user.

Combing the definitions of ESR and SSR, the ergodic SSR becomes a more comprehensive metric that takes into account the sum of secrecy rate for all users over multiple channel realizations as [34]

$$R_{sum}^{erg} = \mathbb{E}_{\mathbf{H},\mathbf{G}}\left[\sum_{k=1}^{K} R_s^k\right]. \tag{14}$$

When Eve's position appears in a certain area and obeys a certain probability distribution, the mean secrecy rate can be calculated by averaging the secrecy rate with respect to Eve's position l_e as [36], [60]

$$R_s^m = \mathbb{E}_{l_e}[R_s]. \tag{15}$$

Furthermore, some approximations of the secrecy rate, such as its upper bounds [35] or lower bounds [52], [62], [63], were also applied to obtain results with better form.

SOP:

$$\mathbb{P}_{out} \triangleq \mathbb{P}\{R_s < R_t\}. \tag{16}$$

The definition of SOP was firstly proposed in [61] as the probability that the instantaneous secrecy rate is below a target secrecy rate threshold R_t. Commonly, it quantifies the probability of unsafe transmission and can be minimized to guarantee the security of transmission [64], or it can be used as a constraint to optimize other parameters [65].

Power Allocation:

$$\theta = \|\mathbf{Ws}\|^2 / \|\mathbf{x}\|^2. \tag{17}$$

Power allocation between the information-bearing signal and the AN is an important design parameter. Allocating more power to AN will lead to a decrease in the throughput of information-bearing signals, while less AN power will reduce the security of systems. Hence, the problem of finding a balanced trade-off for power allocation has attracted lots of attention. In [45], the power allocation was derived by maximizing a lower bound of ESR for MIMOME without the CSI of Eve. In [62], the power allocation was given by the water-filling algorithm to maximize a lower bound of secrecy rate for MIMOME without the CSI of Eve. In [63], the power allocation was designed to maximize a closed-form lower bound of secrecy capacity and showed that equal power allocation is a simple and generic strategy to achieve near-optimal capacity performance. In [66], the power allocation was optimized by maximizing the SSR for multi-user (MU) downlink without the CSI of Eve. In [67], the power allocation was obtained with constraints for reliability and secrecy level and the corresponding secrecy transmission rate in the presence of network interference for the worst scenario. In [68], the power allocation was studied by minimizing the SOP under a target secrecy rate or maximizing the secrecy rate under an SOP constraint, respectively. In [69], the power allocation was investigated by minimizing the total transmission power in multiple-input single-output multiple-antenna-eavesdropper (MISOME) systems. In [70], the power allocation was designed to ensure a target secrecy probability under QoS constraints at Bob and Eve in MISOME systems without Eve's CSI. In [71], the power allocation was derived as a closed-form solution by maximizing the achievable secrecy rate for MIMOME, where the derived results show that equal power and water-filling power allocations lead to similar solutions and rate loss. In [72], the power allocation was considered to maximize an analytical closed-form expression of an achievable secrecy rate for MISOME.

QoS:

$$\mathrm{SINR}_b = \|\mathbf{HWs}\|^2 / \left(\|\mathbf{HVr}\|^2 + \sigma_b^2\right), \tag{18}$$

$$\mathrm{SINR}_e = \|\mathbf{GWs}\|^2 / \left(\|\mathbf{GVr}\|^2 + \sigma_e^2\right). \tag{19}$$

QoS means the attainable signal quality at Bob or Eve, which can be seen as the requirement of SNR or signal to interference plus noise ratio (SINR). QoS is always used as a constraint to jointly optimize beamforming and AN by minimizing the transmit power [73], [74].

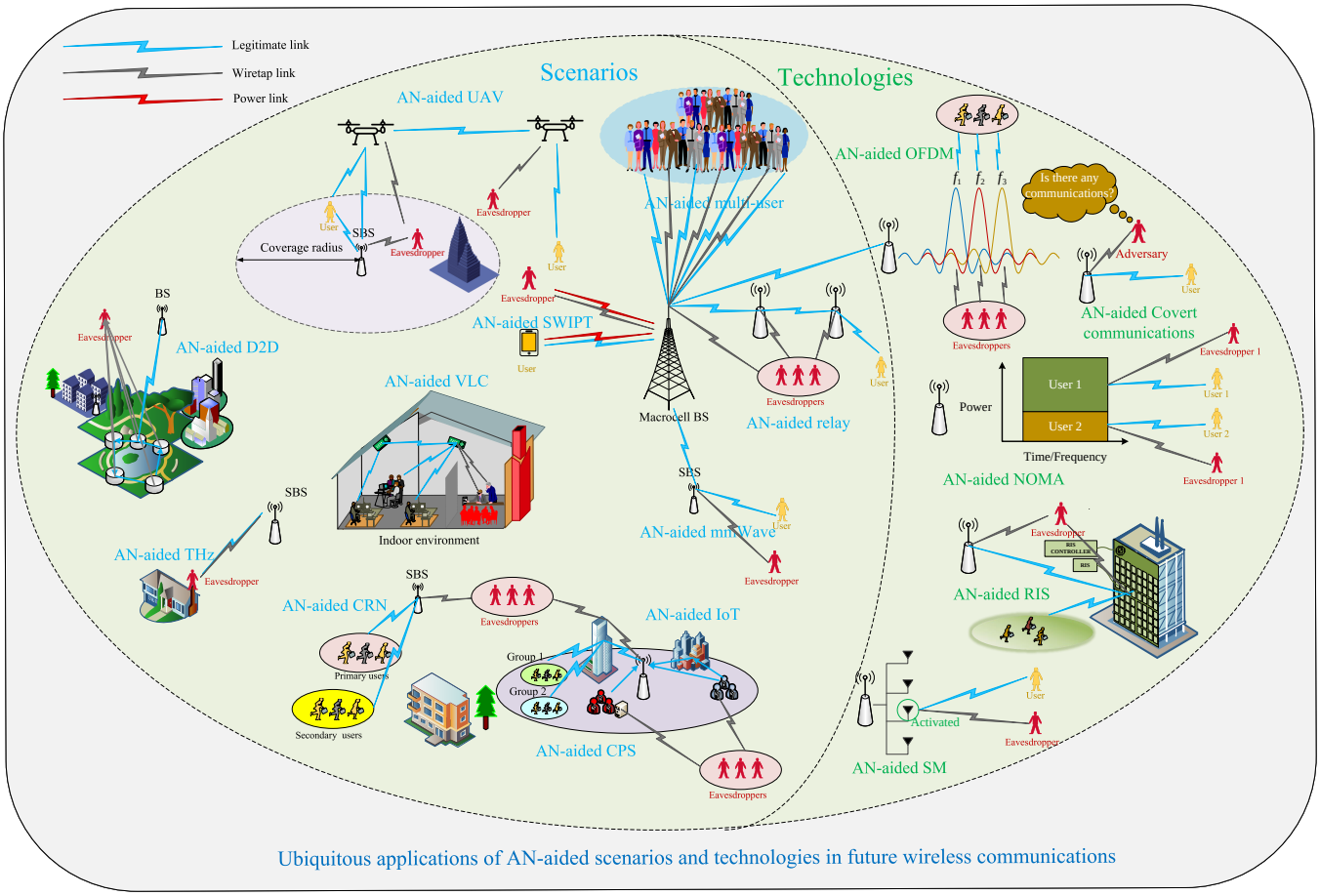

Fig. 3. The applications of AN in future wireless communications.

BER:

$$P_b = \mathbb{E}_{\mathbf{H}}\left(n_b/n\right), \tag{20}$$

$$P_e = \mathbb{E}_{\mathbf{H},\mathbf{G}}\left(n_e/n\right). \tag{21}$$

The bit-error rate (BER) is defined as the ratio of the number of error bits–denoted as n_b for Bob and n_e for Eve–to the number of the total transmitted bits n. The AN technology aims to maintain acceptable BER loss for Bob, while sharply increasing the BER of Eve even when SNR goes to infinity [75]. Specifically, the notion of practical secrecy was proposed in [76] as a new design criterion based on the behavior of the BER of Eve, as its SNR goes to infinity.

III. Overview of AN-empowered Scenarios

As shown in Fig. 3, AN is expected to pervade future wireless networks. Existing works fall into two categories: (i) AN-empowered scenarios; (ii) AN-integrated technologies. This section reviews key scenarios, with Table II summarizing AN types, models, node roles, CSI availability, and contributions.

A. AN-aided CPS

Cyber-physical systems (CPSs) integrate the cyber world, physical processes, and control to enable real-time sensing and dynamic control in large-scale systems. Wireless communication is essential in CPSs, especially in mobile applications like autonomous vehicles, medical monitoring, and robotics, where security remains critical due to the broadcast nature [77], [78].

As pointed out in [77], the main challenge of adding AN to the CPSs is that the AN direction matrix is given in advance as the excitation signals, thus optimizing the AN direction matrix will lead to the re-excitation of CPSs. To solve this problem, the authors of [77] introduced a searchable virtual noise space to design the AN injection direction as

$$S_{\mathbf{V}} = \left\{\mathbf{V}_{-} \in \mathbb{R}^{h\times N} \,|\text{rank}\left(\mathbf{V}_{-}\right) = h\right\}, \tag{22}$$

where $\mathbf{V}_{-}$ denotes a specific virtual noise matrix in the searchable virtual noise space $S_{\mathbf{V}}$. For any $\mathbf{V}_{-} \in S_{\mathbf{V}}$, there exists a direction matrix $\mathbf{E} \in \mathbb{R}^{h\times h}$ such that $\mathbf{V} = \mathbf{E}\mathbf{V}_{-}$ with h denoting the dimension of the virtual noise space and N representing the number of the state data samples. Driven by this searchable virtual noise space, the influence of AN is not amplified for Bob in the CPS.

The authors of [78] focused on the full-duplex communication mode in CPS, which is challenging as the AN is unable to remain in the null space in both forward and reverse channels. Therefore, the optimization problem aims to jointly

TABLE II
OVERVIEW OF AN-EMPOWERED SCENARIOS

References	Scenarios	AN Types	System Models	Bob types	Eve types	CSI of Bob/ Eve	Involved Contributions
[77]	CPS	AN	MIMOME	SMA	SMA	Imperfect/No	Virtual noise space
[78]	CPS	AN	MIMOME	SMA	SMA	Either/Either	AN Optimization for full-duplex
[79]	CRN	AN	MISOSE	MSA	MSA	Perfect/Either	Two SEEM schemes
[80]	CRN	AN	MIMOME	SMA	MMA	Perfect/Perfect	Convergent solution of SRM problem
[81]	CRN	AN	MISOSE	MSA	SSA/MSA	Statistical/Statistical	SRM
[82]	CRN	AN	MISOSE	SSA	SSA	Statistical/Statistical	SRM
[83]	CRN	AN	MISOME	SSA	SMA	Either/Either	SEEM in OFDM-CRNs
[84]	D2D	AN	MISOSE	MSA	SSA	Statistical/Statistical	Three schemes of precoding matrix
[85]	D2D	AN	MISOME	MSA	SMA	Perfect/ No	Secrecy sum rate maximization
[86]	IoT	AN	MISOSE	SSA	SSA	Either/Either	Cooperative beamforming
[87]	IoT	AN	MISOSE	SSA	SSA	Perfect/No	A dual-user two-phase system
[88]	mmWave	Hybrid ANH	MIMOME	SMA	SMA/MMA	Perfect/ No	Minimal hardware complexity
[89]	mmWave	Two-stage AN	MISOME	MSA	MMA	Perfect/ No	Hybrid beamforming for AF relay
[90]	mmWave	Hybrid AN	MISOSE	SSA	MSA	Perfect/ Partial	A secrecy rate lower bound
[91]	mmWave	AN	MISOSE	SSA	SSA	Perfect/ Statistical	Secrecy throughput maximization
[92]	mmWave	AN	MISOSE	SSA	SSA	Perfect/ Partial	SOP minimization
[93]	MU	AN	MISOSE	MSA	MSA	Perfect/ Perfect	AN in service integration
[94]	MU	Robust AN	MISOSE	MSA	MSA	Imperfect/ Imperfect	Imperfect CSI
[95]	MU	AN	MISOSE	MSA	MSA	Either/ Either	Secrecy rate region maximization
[96]	MU	Jammer AN	MISOME	MSA	SMA	Perfect/ No	Opportunistic scheduling OSTBC and AN
[97]	MU	AN with THP	MISOME	MSA	SMA	Either/ No	Nonlinear precoding
[98]	MU	AN	MISOME	MSA	SMA	Imperfect/ No	Closed-form expression of ESR
[99]	MU	AN	MISOSE	MSA	MSA	Perfect/ Either	SRM in joint optimization framework
[100]	MU	Jammer AN	MISOSE	SSA	MSA	Perfect/ Perfect	Optimal multiuser diversity
[101]	MU	Jammer AN	SIMOME	SMA	SMA	Perfect/ Statistical	SOP minimization
[102]	MU	AN	MIMOME	SMA	SMA	Perfect/ No	Joint MU constellations and AN alignment
[103]	MU	Time-domain AN	MISOSE	SSA	SSA	Perfect/ No	AN and secret key aided schemes
[104]	PZ	AN	MISOSE	SSA	SSA	Perfect/ No	Optimization of the protected zone size
[105]	PZ	AN	SISOSE	SSA	MSA	Statistical/ No	Optimal use of AN with a protected zone
[106]	AF relay	AN	MIMOME	SMA	SMA	Perfect/ No	SRM
[107]	AF relay	AN	MIMOME	SMA	SMA	Perfect/ No	AN for IA-based multipair relay networks
[108]	AF relay	AN	MIMOME	SMA	SMA	Perfect/ No	Antenna selection on relay with AN
[109]	AF relay	Bob AN	SISOSE	SSA	SSA relay	Perfect/ Perfect	AN from Bob for untrusted relay
[110]	AF relay	Relay AN	SISOSE	SSA	MSA	Perfect/ Imperfect	SINR maximization
[111]	AF relays	Relay AN	SISOSE	SSA	MSA	Perfect/ No	AN generation from cooperative relays
[112]	AF relays	Relay AN	SISOSE	SSA	MSA	Perfect/ Perfect	SSR maximization through SDR and SCA
[113]	AF relays	Relay AN	SISOSE	SSA	MSA	Perfect/ Perfect	SRM via two-level optimization and SDR
[114]	AF relays	Relay AN	SISOME	SSA	MMA	Perfect/ Imperfect	SRM for MMA relays
[115]	DF relay	Jammer AN	MIMOME	SMA	SMA	Perfect/ No	AN from a cooperative FD jammer
[116]	DF relay	AN and relay AN	MIMOME	SMA	MMA	Perfect/ No	STM under an SOP constraint
[117]	DF relay	Relay PR AN	MISOSE	MSA	MSA	Perfect/ Statistical	Joint NOMA and AN-aided FD relay
[118]	DF relay	Relay AN	SISOSE	SSA	SSA/MSA	Perfect/ No	NOMA-based two-way relay network
[119]	DF relays	Relay AN	SISOSE	MSA	MSA	Perfect/ No	Joint AN and relay selection for CRNs
[120]	DF relays	Relay AN	SISOSE	SSA	SSA	Imperfect/ No	AN-aided two-way relay selection
[121]	DF relays	AN	MISOME	SSA	SMA	Perfect/ Statistical	Joint user and relay selection with AN
[122]	NR relay	Relay AN	SISOSE	SSA	SSA	Imperfect/ Imperfect	Two energy harvesting strategies
[123]	UTWR	AN	MIMOME	SMA	SMA relay	Either/ Either	Maximum SSR for untrusted relay
[124]	Satellite	DCAN	MIMOME	SMA	SMA	Imperfect/Imperfect	Power and time slot allocation
[125]	Satellite	AN	MISOSE	MSA	MSA	Perfect/Perfect	Transmit power minimization
[50]	SWIPT	AN	MISOSE	MSA	MSA	Either/ Either	Total transmit power minimization
[126]	SWIPT	AN	MIMOME	SMA	MMA	Perfect/ No	SEEM for SWIPT
[127]	SWIPT	AN	SISOSE	SSA	SSA	Statistical/ No	AN-aided hybrid TSPS scheme
[128]	SWIPT	AN	MISOSE	MSA	MSA	Perfect / Either	Power minimization for NOMA
[129]	SWIPT	AN	MIMOME	MMA	SMA	Statistical/ No	AN assisted IA scheme with WPT
[130]	SWIPT	AN	MISOSE	MSA	MSA	Either/Either	Multi-cell coordinated beamforming
[131]	SWIPT	AN	MISOME	MSA	MMA	Imperfect/ Imperfect	Cooperative jamming
[132]	SWIPT	AN	MIMOSE	SMA	MSA	Perfect/Statistical	SOP analysis with secondary terminals
[133], [134]	THz	SIC-free AN	MIMOME	SMA	SMA/MMA	Statistical/ No	DNN-powered SIC-free receiver AN
[135]	UAV	AN	MISOSE	SSA	MSA	Statistical/ Statistical	Max-min secrecy, trajectory design
[136]	UAV	AN	SISOSE	SSA	SSA	Perfect/ No	Joint optimization
[137]	UAV	AN	MISOSE	MSA	SSA	Imperfect/No	SEEM for UAV-based NOMA
[138]	VLC	AN	MISOSE	SSA	SSA	Perfect/ Imperfect	Closed-form expression for secrecy rate
[139]	VLC	AN	MISOSE	SSA	MSA	Perfect/ Either	Two sub-optimal low-complexity schemes
[140]	VLC	AN	MISOSE	MSA	SSA	Statistical/ Either	ZF design
[141]	VLC	AN	MISOSE	MSA	SSA	Imperfect/ Imperfect	Power minimization for NOMA
[142]	VLC	Time-domain AN	SISOSE	SSA	SSA	Statistical/ Statistical	Time-domain AN for restricting PAPR

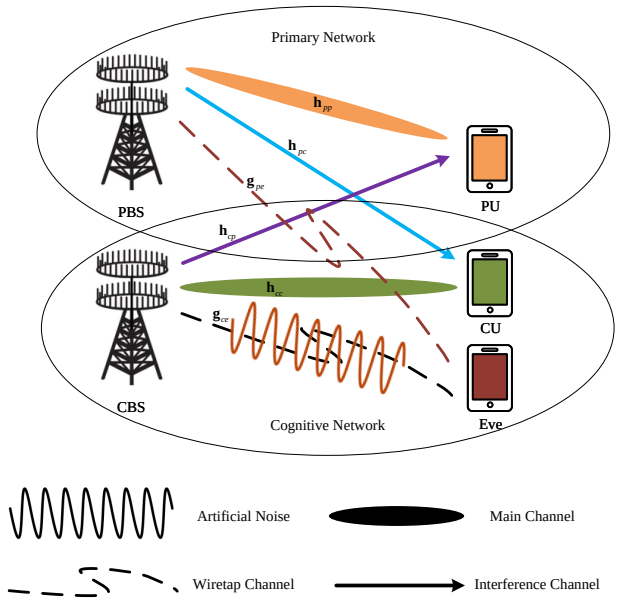

Fig. 4. Framework of the AN-aided CRN wireless secure communications.

optimize the AN and the transmit filter with respect to the QoS constraint, which is formulated as

$$\min_{\mathbf{W},\mathbf{V}} P_t^A + P_t^B, \tag{23a}$$

$$\text{s.t. SINR} \geqslant \gamma, \tag{23b}$$

where P_t^A and P_t^B denote the transmit power for forward and reverse communications, respectively. Additionally, the research has delved into the impact of channel estimation errors and self-interference on the overall system performance, providing a comprehensive explanation of these effects.

AN-aided CPSs face unique challenges in effectively integrating AN to enhance both communication and sensing functionalities without degrading system performance. Key challenges include optimization for performance improvements. Future trends are likely to focus on developing adaptive noise management strategies to dynamically balance performance across diverse operational conditions. These trends will leverage advanced machine learning for real-time adjustments and anomaly detection while enhancing security measures to protect against vulnerabilities introduced by AN. Additionally, innovations will aim to improve energy efficiency and system robustness to support increasingly complex CPS applications.

B. AN-aided CRN

Over the past two decades, cognitive radio networks (CRNs) have rapidly evolved to address spectrum scarcity by allowing cognitive users (CUs) to share licensed spectrum with primary users (PUs) under QoS constraints, as shown in Fig. 4. To enhance the PLS of CRN, extensive analytical studies have been conducted [79]–[83].

In order to address multiple Eves in the network and to improve energy efficiency, the authors of [79] proposed a new optimization framework to maximize the secrecy energy efficiency (SEE) at the cognitive base station (CBS). This was achieved by optimizing the beamforming under the constraints of the secrecy rate for both PU and CU, limitation of PUs interference from CBS, and adhering to the total transmit power constraint for the CBS. The SEE metric is given by

$$\eta_{SEE} = R_{c,\text{sec}}/P_{tot}, \tag{24}$$

where $R_{c,\text{sec}}$ represents the secrecy rate and P_{tot} is the total power consumption. Moreover, a secrecy energy efficiency maximization (SEEM) scheme was proposed by exploiting the instantaneous CSI of Eves. In addition, when the instantaneous CSI is unavailable, the authors proposed an alternative SEEM scheme by exploiting the statistical CSI of Eves. Numerical results demonstrated that the proposed method can achieve a trade-off between schemes that focus solely on secrecy rate and those that focus solely on energy efficiency.

In [55], the authors studied the AN-aided precoding scheme for MIMOME CRNs by solving a secrecy rate maximization problem. Later, the authors of [80] identified and corrected gaps in [55]. To handle the non-convex capacity constraint, the capacity function was reformulated as

$$C_k(\mathbf{W},\mathbf{V}) = \varphi_k(\mathbf{W},\mathbf{V}) - \phi_k(\mathbf{V}), \tag{25}$$

where $\varphi_k(\mathbf{W},\mathbf{V})$ and $\phi_k(\mathbf{V})$ are auxiliary functions. Subsequently, this problem was iteratively solved using successive convex approximation (SCA), with simulations confirming convergence and satisfactory performance.

In [81], an AN-aided cognitive transmit strategy was proposed to maximize the joint secrecy rate of primary and cognitive links under power and primary QoS constraints. In the first slot, the cognitive transmitter listens while an inactive user jams with AN; in the second slot, it relays the primary signal while sending its own data and AN. Specifically, the secrecy rate is formulated as

$$R_{\text{secrecy}} = \left[R_p + R_s^{\text{sum}} - R_e\right]^+, \tag{26}$$

where R_p denotes the achievable rate at the primary receiver, R_s^{sum} represents the sum rate of cognitive network, and R_e stands for the achievable rate at Eve. Furthermore, the authors proposed a computationally efficient approximation method combining semidefinite relaxation (SDR) with a two-step alternating optimization to obtain a local optimum.

Further in [82], an alternative optimization method combined with one-dimensional linear searching was employed to design the optimal beamforming. Furthermore, by confining the AN to the null space of the legitimate channel, a low-complexity secure beamforming scheme was also presented.

The authors of [83] proposed a SEE optimization scheme for OFDM-based cognitive radio downlink transmissions. This was achieved by optimizing the power allocation between information-bearing and AN signals across different OFDM subcarriers subject to the total transmit power constraints for the PBS and CBS while guaranteeing a required secrecy rate for the CU and PU. Additionally, two schemes were proposed for scenarios where the instantaneous CSI or statistical CSI of Eve was available. Since there are no closed-form solutions

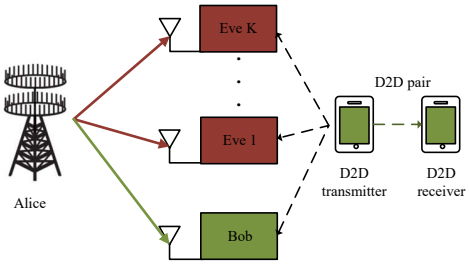

Fig. 5. Framework of the AN-aided D2D wireless secure communications.

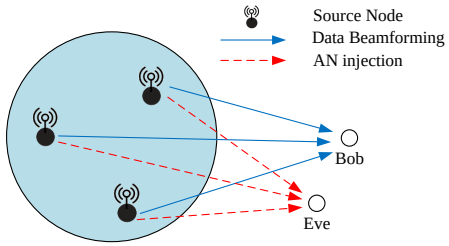

Fig. 6. Framework of the AN-aided IoT wireless secure communications.

for the proposed problems, new two-tier algorithms were proposed to achieve the optimal power allocation solutions to the formulated problems.

In general, AN is generated within the CRN to secure communications of both PUs and CUs. However, as the CRN inherently interferes with the PU, optimal power allocation between the information signal and AN, along with system energy efficiency, emerges as a key challenge, further complicating the optimization problem.

C. AN-aided D2D

Device-to-device (D2D) communication, enabling direct transmission without BS involvement, is a key technology in 5G networks. As illustrated in Fig. 5, scenarios involving multiple Eves targeting both cellular and D2D links have drawn increasing research interest [84], [85].

The authors of [84] devised a secure D2D communication strategy using AN, jamming-aided precoding, and signal precoding to maximize secrecy capacity while sharing downlink resources with cellular users. AN was placed in the null space of interference channels. Three precoding schemes and an optimal power allocation algorithm were developed, all showing strong security improvements in simulations.

In [85], the authors aimed to enhance the SSR for both D2D and cellular users. AN was precoded using the null space of CSI from the BS to both user types, and power was allocated via a one-dimensional search. A pricing-based pairing and power control algorithm was also introduced to match D2D pairs with cellular users, maximizing secrecy throughput.

Due to device limitations, AN is typically generated by the BS over the downlink, making power allocation in D2D communications difficult. In addition, how to pair D2D devices for security improvement is also a great challenge.

D. AN-aided IoT

With the appearance of the Internet of Things (IoT), human-computer interaction technology is more important in our lives. Due to the sharp growth in the number of connected devices, conventional cryptography mechanisms may suffer from the difficulties caused by the key distribution of multiple devices. As shown in Fig. 6, to overcome such critical issues for IoT, AN techniques can be generated cooperatively [86], [87].

To reduce overhead in large-scale IoT networks, the authors of [86] proposed an AN-aided cooperative beamforming (CB) scheme using a virtual antenna array (VAA). The method exploits the statistical properties of CB links to avoid CSI collection and precoding weight sharing. Closed-form secrecy rate expressions were derived with and without CSI errors, and the impact of system parameters like VAA size was analyzed for secure CB system design.

In [87], the authors proposed an AN-aided secure transmission scheme for cooperative non-orthogonal multiple access (NOMA)-based IoT systems with multi-antenna nodes. The BS transmits signals with AN, and strong nodes relay them to weak nodes. Exact SOP expressions were derived, and secrecy diversity analysis showed that system performance is limited by the weaker node's channel quality.

In conclusion, AN in IoT needs to be generated collaboratively by multiple nodes, which indicates that additional coordination and synchronization issues between multiple nodes need to be addressed.

E. AN-aided mmWave

The millimeter wave (mmWave) frequency band is a promising candidate for 5G wireless networks. The narrow and directional beams in mmWave communications have significantly enhanced transmission security. However, eavesdropping remains a potential threat in both indoor and outdoor environments [88]–[92].

In [88], a practical secure transmission scheme called artificial noise hopping (ANH) was proposed for MIMO mmWave systems with single or multiple colluding Eves. ANH avoids symbol-level beam steering and requires only two RF chains-one for data and another one for ANH. Considering LoS-dominant channels and MRC, the scheme achieves low overhead and minimal hardware complexity, with both simulations and experiments confirming its practicality.

The authors of [89] proposed an AN-aided two-stage hybrid beamforming scheme for MU-MISO mmWave relay systems with two passive Eves. In phase I, RF analog beamformers and relay combiners are designed to maximize signal power and suppress interference using codebook-based beam training. In phase II, digital baseband beamforming uses zero-forcing to reduce complexity. The same approach applies to both relay phases, avoiding joint optimization and minimizing feedback.

In [90], a low-complexity AN-aided hybrid analog–digital precoding scheme was proposed for mmWave MISO systems.

Using the joint moment generating function, a lower bound of secrecy rate $\tilde{R}_{\mathrm{Sec}}$ were derived and optimized as

$$\max_{\phi,\mathbf{F}_{\mathrm{RF}},\mathrm{f}_{\mathrm{BB}},\mathbf{U}_{\mathrm{BB}}} \tilde{R}_{\mathrm{Sec}}, \tag{27a}$$

$$\text{s.t. } \mathbf{F}_{\mathrm{RF}} \in \mathcal{F}_{\mathrm{RF}}, \tag{27b}$$

$$\|\mathrm{f}_{\mathrm{BB}}\|^2 = 1, \tag{27c}$$

$$\|\mathbf{U}_{\mathrm{BB}}\|_{\mathrm{F}}^2 = 1, \tag{27d}$$

$$0 \le \phi \le 1 \tag{27e}$$

where $\mathbf{F}_{\mathrm{RF}}$ denotes the analog beamforming matrix, $\mathbf{f}_{\mathrm{BB}}$ represents the digital beamforming vector and AN digital baseband precoder, and ϕ is the power allocation factor. The problem was decomposed into optimizing ϕ and solving a hybrid precoder via eigen-decomposition and projection methods.

The authors of [91] proposed a dynamic parameter transmission scheme for mmWave systems over multipath slow fading channels, aiming to maximize secrecy throughput under an SOP constraint. The CDF of Eve's SINR was derived for SOP analysis, enabling optimal codeword rate and power allocation design. AN beamforming was based on the array responses of Bob and Eve, and the study revealed that secrecy performance heavily depends on the spatial path overlap between them.

The same system model with partial CSI of Eve at Alice was considered in [92] under an on-off transmission scheme. An optimization problem was formulated to maximize the secrecy rate subject to codeword rate and SOP constraints as

$$\max_{\eta,R_t} R_s\left(\gamma^{\circ}\right) \tag{28a}$$

$$\text{s.t. } 0 < R_s\left(\gamma^{\circ}\right) < R_t\left(\gamma^{\circ}\right) \le C_d, \tag{28b}$$

$$\mathcal{P}_{so}\left(\gamma^{\circ}\right) \le \epsilon, \tag{28c}$$

$$0 \le \eta \le 1, \tag{28d}$$

where $\gamma^0 \in \Upsilon$ represents overall channel gain satisfying the transmission constraint, R_s and R_t are defined as the secrecy rate and codeword rate. η is the power allocation factor between useful signal and AN. Using the CDF of Eve's SINR from [91], a closed-form SOP and optimal power allocation $\eta^{\star}$ were derived. Results highlighted that the secrecy outage is more likely to occur when common paths are weak or Eve is close to Alice.

Overall, AN design in mmWave systems needs to consider unique channel characteristics like array response, codebook structure, orthogonality, and sparsity. Despite signal processing challenges, hybrid architectures are essential due to the high overhead of fully digital massive MIMO.

F. AN-aided MU

The application of AN can be easily extended to MU networks with multiple receivers or transmitters. Depending on the characteristics of receivers and transmitters in actual application scenarios, MU can be divided into downlink and uplink. As displayed in Fig. 7, in the downlink, a powerful BS serves multiple users, necessitating high spectral efficiency and secure communication. A heuristic approach is to integrate co-existing services, typically, multicast service and confidential service, into one integral service for one-time transmission,

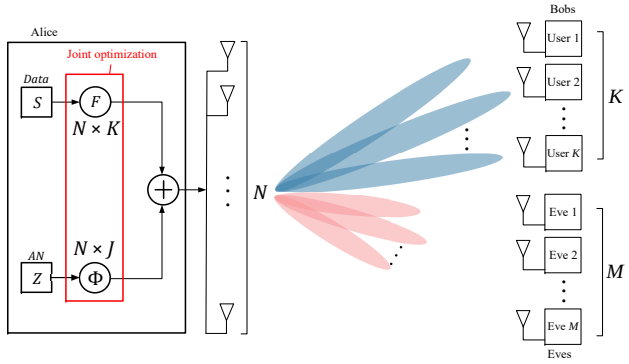

Fig. 7. AN-aided MU wireless secure communications.

where establishing the security of the confidential service while not compromising the public service becomes a crucial problem. The authors of [93]–[95] designed the optimal input of multicast message, confidential message, and AN jointly in this scenario. Furthermore, an appropriate user scheduling strategy can enhance security, as demonstrated by [96]. In the downlink scenario, feedback from the user end is limited. The authors of [97] and [98] addressed this issue by using quantified CSI to complete the design of the corresponding transceiver and transmission framework. In addition, Ref. [99] studied the joint design of precoding and AN, and proposed a new secure precoding algorithm. In the uplink, the performance of the user transmission is limited, making the utilization of the MU feature an important topic. The authors of [100] and [101] used MU diversity to make non-scheduled users in the network generate AN, thereby improving security performance. Ref. [102] studied the power allocation problem of MU constellations and AN in the mMIMO scenario, and provided a new NOMA solution. In addition, time-domain AN can also be combined with the secret key in single-carrier frequency-division multiple access (FDMA) systems to obtain enhanced security [103].

The authors of [93] studied optimal AN-aided transmit design for MU-MISO systems with integrated multicast, confidential messages, and AN, focusing on quality of multicast service (QoMs). They aimed to maximize secrecy rate under QoMs constraints and defined the secrecy rate region boundary. Results showed this beamforming approach effectively enhances security performance.

In [94], a secure MU-MISO transmission design with AN was proposed to serve multicast and confidential messages under imperfect CSI modeled as $\mathbf{h} = \tilde{\mathbf{h}} + \mathbf{e}$ with bounded error. The goal was worst-case secrecy rate maximization (SRM) under sum power and QoS constraints. The problem's hidden convexity was revealed and reformulated into a sequence of semidefinite programs (SDPs).

Building on [94], the authors of [95] showed that transmit beamforming with well-designed AN outperforms existing schemes for confidential message transmission under both perfect and imperfect CSI. They analyzed computational complexity and proposed two suboptimal schemes, including one

with a power splitting factor ρ to decouple multicast and confidential transmissions:

$$\mathrm{Tr}(\mathbf{Q}_c + \mathbf{Q}_a) = \rho P, \quad \mathrm{Tr}(\mathbf{Q}_0) = (1-\rho)P, \tag{29}$$

where $\mathbf{Q}_c$, $\mathbf{Q}_a$, and $\mathbf{Q}_0$ denote covariance of x_c, x_a ,and x_0, respectively, while P represents the total transmission power budget. Numerical results showed AN effectively enlarges secrecy rate regions, and suboptimal methods achieve near-optimal performance with less complexity.

To enhance MU-MISO network security, the authors of [96] proposed an AN relay strategy using orthogonal space-time block code (OSTBC) at the BS and AN transmission from a cooperative relay that avoids the selected legitimate user. Two user scheduling schemes were used for user selection. Exact closed-form expressions for SOP and secrecy throughput were derived, and simulations confirmed the scheme's effectiveness and the impact of varying antenna numbers.

In [97], an AN-aided nonlinear low-complexity transceiver using Tomlinson-Harashima precoding (THP) was proposed for secure MU-MISO communications with limited feedback. The authors derived analytical ESR approximations and near-optimal power allocation via numerical methods.

A secure MU multi-antenna transmission framework using AN-aided linear ZF beamforming with limited CSI feedback from distributed Bobs was proposed in [98]. Users quantize the channel direction as

$$\hat{\mathbf{h}} = \arg\max_{\mathbf{c}\in\mathcal{C}} \left|\tilde{\mathbf{h}}\mathbf{c}^H\right|, \tag{30}$$

where $\mathbf{c}$ is the codeword for feedback. The authors derived a tractable lower bound on ESR and optimized power allocation to maximize it. They analyzed the effects of transmit power and feedback bits, identifying minimum requirements for both to ensure desired performance.

In [99], a joint optimization framework was proposed to maximize the sum secrecy rate in MU-MIMO wiretap channels with multiple Eves by jointly optimizing secure precoders and AN. The non-convex, non-smooth SRM problem was reformulated into a smooth one, defining a joint vector

$$\bar{\mathbf{v}} = \left[\mathbf{f}_1^\top, \mathbf{f}_2^\top, \cdots, \mathbf{f}_K^\top, \mathbf{a}_1^\top, \mathbf{a}_2^\top, \cdots, \mathbf{a}_J^\top\right]^\top, \tag{31}$$

with the channel rate expressed as

$$R_k = \log_2\left(\frac{\bar{\mathbf{v}}^{\mathsf{H}}\mathbf{A}_k\bar{\mathbf{v}}}{\bar{\mathbf{v}}^{\mathsf{H}}\mathbf{B}_k\bar{\mathbf{v}}}\right). \tag{32}$$

Algorithms were developed for both perfect and imperfect CSI, including a null-space projection AN design. The approach achieved faster convergence, required only a small AN subspace, and outperformed existing methods in secrecy rate.

The authors of [100] proposed a user scheduling scheme with AN to enhance security in an MU uplink wiretap network with one desired receiver and multiple Eves. One user transmits data while others generate AN, with the received signal at the desired user given by

$$y = h_n x_n + \sum_{s=1}^{S} h_s \delta_s + z, \tag{33}$$

where x_n denotes the desired data symbol for the n-th user and δ_s represents an independent jamming signal generated by the s-th user. By using threshold-based feedback, the scheme achieves optimal multiuser diversity gain $\log N$ and reduces signaling overhead. Simulations show it outperforms conventional methods with higher average secrecy rates.

Similar to [100], the authors of [101] proposed a secure user scheduling scheme with AN for an MU SIMOME wiretap network, selecting one user for data and another for AN. The scheme requires only Eve's channel statistics, not instantaneous CSI. Closed-form SOP expressions with MRC were derived, showing that AN effectively lowers SOP by degrading Eve's link and is robust to changes in Eve's antenna number.

To secure an energy-based mMIMO system, a joint MU constellation alignment and AN design was proposed in [102] to manage multiuser interference with finite-alphabet inputs and optimize error performance. With large antenna arrays at the BS and passive Eve, and multi-antenna Bobs, the authors designed an energy-efficient pulse amplitude modulation (PAM) constellation and a stepped water-filling algorithm to generate AN vectors unknown to Eve. Simulations showed Bob's error rate vanishes with more antennas, while Eve's error rate remains bounded, highlighting improved security.

In [103], a time-domain AN-aided scheme was proposed for single-carrier-FDMA with eavesdropping, where AN is projected onto the null space of the Alice-Bob channel:

$$\mathbf{R}^{\mathrm{cp}}\mathbf{H}_t^{(k)}\mathbf{V}^{(k)} = 0, \tag{34}$$

where $\mathbf{R}^{\mathrm{cp}}$ is cyclic prefix removal matrix. Analysis showed robustness even when Eve used machine learning detectors, with secrecy rate growing linearly with AN streams. The study also combined AN with a channel-based secret key to further enhance the PLS.

In summary, AN in downlink scenarios are mainly utilized to enhance the quality of confidential service, whereas in uplink scenarios AN are often co-generated by users and employed to secure communications. Multi-user scenarios bring multiple variables that complicate the problem and increase the algorithmic complexity. Consequently, the development of efficient algorithms with minimal performance loss should be a primary focus in current research.

G. AN-aided Protected Zone

The secrecy-protected zone (PZ) is an Eve-free area formed inherently or intentionally, preventing eavesdroppers from accessing it. Installing Alice or Bob in restricted or isolated locations, like high communication towers, ensures such zones. Beyond physical barriers, defining a protected zone near Alice helps prevent Eve's channel from outperforming Bob's, allowing AN to achieve higher secrecy rates [104], [105].

The authors of [104] studied the impact of a nearby Eve by defining a PZ around Alice. A weighted normalized cost function was introduced as

$$\mathrm{CF}(a, b, r_s) = \kappa_1 \frac{a+b}{P_{max}} + \kappa_2 \frac{r_s}{r_{s_{max}}}, \tag{35}$$

where P_{max} and $r_{s_{max}}$ denote the maximum available transmission power and the maximum allowable radius of the PZ,

respectively. $a+b$ represents the total transmitted power and r_s stands for the size of PZ, while κ_1 and κ_2 are the weights, respectively. The study proposed an optimization strategy to smartly allocate power and PZ size, effectively maximizing the probability of achieving a target secrecy rate.

Furthermore, the authors of [105] enhanced secrecy by combining AN and a PZ, considering unknown Eves and jammers. Without CSI, a fixed secrecy rate R_S is set, and the secrecy transmission rate is defined as

$$\mathcal{R} \triangleq (1-\Pr[\mathbb{E}_1])(1-\Pr[\mathbb{E}_2])R_{\mathrm{S}}, \tag{36}$$

where $\mathbb{E}_1$ represents for Bob's inability to decode the codeword at the specified rate and $\mathbb{E}_2$ denotes for the capacity of at least one Eve is higher than the limit. They analyzed how AN, PZ radius, and jammer/Eve density affect performance and derived optimal power allocation in interference-limited networks to maximize $\mathcal{R}$.

The advantage of using the AN for secure communication in the protected zone is that as long as Eve cannot approach Alice, more resources could be allocated to Bob to ensure robust security. Therefore, resource allocation in this scenario becomes a critical issue, which fundamentally explains the impact of Eve channel quality on the PLS boundary.

H. AN-aided Relay

To enhance the PLS of relay networks, various relaying strategies have been explored in the literature, as evidenced in citations like [106]–[123]. The research on AN-aided relay techniques can be categorized into different scenarios, including single amplify-and-forward (AF) relay [106]–[110]; multiple AF relays [111]–[114]; single decode-and-forward (DF) relay [115]–[118]; multiple DF relays [119]–[121]; non-regenerative (NR) relay [122]; untrusted two-way relay (UTWR) [123]. These studies aim to devise effective strategies to bolster the security and performance of relay-assisted communication networks.

In [106], an AN-aided secure MIMOME system with a multi-antenna AF relay was studied under unknown Eve CSI and location. The goal was to maximize the expected secrecy rate, where a penalty method with stochastic decomposition was used. Results showed that secrecy rate improves with more antennas at Bob, and higher AN power becomes optimal as SNR increases. Furthermore, two novel AN algorithms were introduced in [107] for interference alignment (IA)-based multiuser communication systems with a multi-antenna half-duplex (HD) relay and Eve. The goal was to minimize transmit power while ensuring each user's SNR exceeds a threshold.An iterative algorithm with SDP was proposed to solve this problem, leading to four AN-based transmission models balancing sum and secrecy rates.

In [108], three AN-aided MIMOME transmission schemes using a two-way multi-antenna relay were studied with different security–complexity trade-offs. First, secure transmission conditions were derived for relay antenna selection without AN. Then, Alice's AN injection was analyzed under various eavesdropping strategies. Finally, a low-complexity joint antenna selection and AN scheme was proposed. Results showed that joint AN and antenna selection improves secrecy at the cost of increased complexity.

In [109], the concept of AN was applied in an untrusted relay network for single-input single-output (SISO) systems. In the first time slot, Alice sends the information-bearing signal while Bob transmits AN r, resulting in the relay receiving

$$\tilde{y}_R = h_{ar}s + h_{br}r + \tilde{n}, \tag{37}$$

where h_{ar} denotes the CSI between Alice and the relay, h_{br} represents the CSI between Bob and the relay, and $\tilde{n}$ is the AWGN. In the second time slot, the relay amplifies and forwards the combined signal to Bob, who can cancel the AN using prior knowledge. The SER was derived under AWGN, and the optimal AN phase and power allocation were obtained by maximizing the SER. Notably, the study revealed that Gaussian-distributed AN is not always optimal.

The AN was injected at the trusted multi-antenna AF relay for SISO in the presence of multiple single-antenna (MSA) Eves in [110]. Assuming imperfect knowledge of the Eves' channels, the power of Alice, the AF relaying matrix, and the covariance of the AN transmitted by the relay were jointly optimized to maximize the received SINR of Bob under robust secrecy constraints. Furthermore, a penalized difference-of-convex algorithm was proposed to efficiently solve the non-convex SDP with guaranteed convergence.

In [111], the authors employed AN from multiple cooperative relays using MU diversity in SISO systems to combat MSA eavesdroppers. They derived the maximum number of uniformly distributed Eves that can be tolerated under secrecy constraints. For identical path-loss Eves, an exponential number (in system nodes) is tolerable, while for uniformly distributed Eves, sub-linear growth in Eves is supported.

For two-way AF relay networks, a joint design of cooperative beamforming and AN was proposed as [112]

$$\min_{\mathbf{w},\mathbf{\Sigma}} \max_{l\in\mathcal{L}} -\left(R_{B,1}+R_{B,2}-R_{E,l}\right) \tag{38a}$$

$$\text{s.t. } \mathbf{e}_k^T\left(\mathbf{C}\mathbf{w}\mathbf{w}^H+\mathbf{\Sigma}\right)\mathbf{e}_k \leqslant P_{R,k}, \forall k, \tag{38b}$$

where $P_{R,k}$ is the power budget of the k-th relay, $\mathbf{e}_k$ denotes a unit vector, $\mathbf{C}$ represents the covariance matrix of the information-bearing signal, and $\mathbf{\Sigma}$ stands for AN covariance matrix. Based on the SSR maximization criterion, a stationary point was efficiently developed by utilizing SDR and SCA techniques. The proof was also given to show that SDR is always tight and yields a rank-one solution.

In [113], the joint cooperative beamforming and AN strategy was employed for a set of single-antenna AF relays in the presence of a single-antenna Alice, a single-antenna Bob, and MSA Eves. Under both the total and individual relay power constraints, an optimal joint cooperative beamforming and AN design based on SRM was proposed as

$$\max_{\mathbf{w},\mathbf{\Sigma}} R_s \tag{39a}$$

$$\text{s.t.}\mathbf{w}^H\mathbf{C}\mathbf{w}+\mathrm{Tr}\left(\mathbf{\Sigma}\right)\leqslant P, \mathbf{\Sigma}\succeq\mathbf{0}, \tag{39b}$$

$$\mathbf{e}_k^T\left(\mathbf{C}\mathbf{w}\mathbf{w}^H+\mathbf{\Sigma}\right)\mathbf{e}_k \leqslant P_{R,k}, \forall k, \tag{39c}$$

where $\mathbf{e}_k$ denotes a unit vector with the k-th entry being one. The SRM problem was treated by a combination of two-level

optimization and SDR. For the latter, it was proved that SDR always has a rank-one solution for the SRM problem, which identifies that SDR is optimal.

The authors of [114] tackled an optimization problem in a two-hop relay single-input single-output multiple-antenna-eavesdropper (SISOME) system, wherein multiple multiple-antenna (MMA) AF relays collaboratively transmit information-bearing and AN signals from a single-antenna Alice to a single-antenna Bob in the presence of MMA Eves. More specifically, under the the spherical uncertainty model of wiretap channel $\|\mathbf{g}_m - \bar{\mathbf{g}}_m\| \leqslant \varepsilon_m$, the worst achievable rate of Eve is expressed as

$$\max_{\mathbf{g}_m} C_{e,m} = \log\left(1 + P_s(\|\bar{\mathbf{g}}_m\| + \varepsilon_m)^2 + \mathbf{\Lambda}_m\right), \tag{40}$$

where ε_m reflects the accuracy for the knowledge of Eves' CSI and $\mathbf{\Lambda}_m$ represents the SINR under the accurate CSI. The SRM problem was solved via a two-level polynomial-time approach using SDR, which was proven optimal through reformulation and Karush-Kuhn-Tucke analysis. AN played a key role in ensuring the SDR solution's optimality.

In [115], the AN was generated by a cooperative FD jammer for MIMOME with a multi-antenna FD relay, where the cooperative jammer (CJ) was assumed to be an FD node that is solely charged by the ambient RF transmissions. Without the CSI of Eve, the authors of [115] investigated the self-energy recycling at the CJ and derived a sufficient condition for the CJ to operate as a node, expressed as

$$B_J \geqslant (P_J + P_p)\, T, \tag{41}$$

where B_J denotes the battery energy of the CJ, P_J represents the signal power transmitting information-bearing signal and AN, P_p stands for the signal processing power consumption for DF, and T is the activation duration. It reveals that the battery state increases with time. Finally, the numerical results demonstrated that the introduction of AN-aided CJ achieves a significant average secrecy rate improvement.

The authors of [116] designed a relay-aided secure transmission scheme for MIMOME. By assuming that both Alice and the relay transmit AN alongside information-bearing signals, a closed-form expression for the transmission outage probability and SOP were derived as

$$\begin{aligned} P_{to} &= 1 - (1 - F_{\gamma_{sr}}(\tau_b))(1 - F_{\gamma_{rd}}(\tau_b)), \\ P_{so} &= 1 - \exp(-2\lambda(J_1 + J_2 - J_3)), \end{aligned} \tag{42}$$

where γ_{sr} and γ_{rd} stand for the SINR from S to R and from R to D, respectively, $F_\gamma(\tau)$ denotes the CDF of γ, while J_1, J_2, and J_3 are calculated by the CDF of Eve's SINR. Asymptotic analysis with a large number of Alice's antennas led to the secrecy throughput expression

$$T_s = (R_b - R_e)(1 - P_{to}). \tag{43}$$

By solving the secrecy throughput maximization (STM) problem under the SOP constraint, the system and channel parameters were determined for practical deployment.

Based on a pseudo-random sequence known to Bob, an AN scheme was investigated in [117] for NOMA FD relay networks. In this scheme, the optimal power allocation between the information-bearing and the AN signals was determined to minimize the SOP

$$\theta^* = \arg\min_{0 \leqslant \theta < 1} P_{so}. \tag{44}$$

A closed-form SOP expression showed that combining FD and AN at relays significantly improves physical layer secrecy in NOMA cooperative networks.

In [118], a NOMA-based two-way relay network was developed where a trusted relay assists two users in exchanging messages while continuously transmitting AN to impair SSA/MSA Eves. The relay's signals in phases 1 and 2 are given by

$$\begin{aligned} \mathbf{x}_R^{(1)} &= \mathbf{V}\sqrt{\frac{P_R}{(N_R - 2)}}\mathbf{r}^{(1)}, \\ \mathbf{x}_R^{(2)} &= \mathbf{W}\sqrt{\frac{\theta P_R}{2}}\begin{bmatrix} s_B \\ s_A \end{bmatrix} + \mathbf{V}\sqrt{P_R/(N_R - 2)}\mathbf{r}^{(2)}, \end{aligned} \tag{45}$$

where $\mathbf{x}_R^{(1)}$ and $\mathbf{r}^{(1)}$ denote the transmit signal and random vector during the phase 1, while $\mathbf{x}_R^{(2)}$ and $\mathbf{r}^{(2)}$ represent that during phase 2. The relay and users employ FD to enhance efficiency and secrecy. Successive interference cancellation-based decoding schemes were proposed, and closed-form ESRs were derived under both SSA and MSA Eve scenarios.

The authors of [119] proposed a novel cooperative AN scheme for underlay cognitive DF relay networks, where a secondary transmitter communicates with an SU via multiple cognitive DF relays while MSA passive Eves attempt interception. Without Eves' CSI, two relay selection schemes were introduced as

$$\begin{aligned} k^* &= \arg\max_{k \in K} |h_{kB}|^2, \\ k^o &= \arg\max_{k \in K} R_s, \end{aligned} \tag{46}$$

where h_{kB} denotes the CSI between the k-th relay and the SU, while k^* and k^o represent the indices of selected relays. The conventional scheme uses only main channel CSI, while the best relay scheme also considers interference CSI. Closed-form SOP expressions for both schemes were derived.

To secure source nodes communicating via multiple two-way DF relays in the presence of an Eve, an AN-aided two-way opportunistic relay selection scheme was conceived as [120]

$$o = \arg\max_{k \in K}\left[\min\left(|h_{kA}|^2, |h_{kB}|^2\right)\right] \tag{47}$$

where o denotes the selected relay, while h_{kA} and h_{kB} are the channels between the relay k to the users A and B, respectively. The scheme's outage and intercept probabilities were analyzed to characterize security and reliability, with a security-reliability trade-off compared against direct transmission and one-way relaying.

A joint user and relay selection scheme was proposed to enhance PLS in an MU multi-relay network, where the best pair of the user and relay maximizing the user-to-destination SINR is jointly selected in [121] as

$$(m^*, n^*) = \arg\max_{m,n} \min(\gamma_{m,n}, \gamma_n), \tag{48}$$

where $\gamma_{m,n}$ and γ_n are the SINR of the relay and destination, respectively. In addition, the authors analytically examined the SOP of this scheme, based on which the optimal power allocation between the information-bearing signal and AN at the users was determined to minimize the SOP. To avoid the high complexity of the joint selection, a separate user and relay selection scheme was also proposed, where a relay is first selected to maximize the relay-to-destination SINR, and a user is then selected to maximize the SINR from the user to the selected relay as

$$\begin{aligned} n^* &= \arg\max_n \gamma_n, \\ m^* &= \arg\max_m \gamma_{m,n^*}. \end{aligned} \tag{49}$$

Moreover, the authors also derived the SOP and optimal power allocation for the separate selection scheme. While the joint user-relay selection outperforms the separate scheme, the low-complexity separate scheme achieves similar secrecy performance under certain conditions, such as when the number of users far exceeds relays or when the user-to-relay SNR is much higher than relay-to-destination SNR.

The authors of [122] investigated a non-regenerative relay network supporting simultaneous wireless information and power transfer, in which the energy harvesting relay is powered by RF signals from Alice. Assuming imperfect CSI from the Alice/relay to the Bob/Eve, the authors investigated the AN-aided secure robust beamforming that minimizes the transmission power at the relay, while guaranteeing the secrecy rate constraint and the transmit power constraint at the relay. In particular, two energy harvesting strategies, namely power splitting and time switching, were studied. Numerical results showed power-splitting outperforms time switching.

For a UTWR, Ref. [123] aimed to maximize the secrecy sum rate by jointly designing the sources' signal precoder $\mathbf{W}_i$, AN matrix $\mathbf{V}_i$, and the relay's precoder $\mathbf{F}$ as

$$\max_{\mathbf{F},\mathbf{W}_i,\mathbf{V}_i} \left(R_1 + R_2 - R_r\right)^+ \tag{50a}$$

$$\text{s.t. } \|\mathbf{W}_i\|^2 + \|\mathbf{V}_i\|^2 \leqslant P_i, i = 1, 2, \tag{50b}$$

$$\sum_{i=1}^{2} \left(\|\mathbf{F}\mathbf{H}_i\mathbf{W}_i\|^2 + \|\mathbf{F}\mathbf{H}_i\mathbf{V}_i\|^2 \right) + \sigma_r^2 \|\mathbf{F}\|^2 \leqslant P_R, \tag{50c}$$

where R_1, R_2, and R_r denote the achievable rates at source 1, source 2, and UTWR, respectively. Under perfect CSI, the problem was reformulated as a difference-of-convex program and solved iteratively for a local optimum, with asymptotic analysis guiding precoder design at high relay power. Under imperfect CSI, channel uncertainties were handled via a worst-case model, and a weighted minimum mean square error approach was developed for robust secure precoding.

In a nutshell, applying the AN in relay systems faces several challenges, including optimizing noise power allocation, balancing security with signal quality, and managing increased computational complexity. Ensuring adaptability to dynamic conditions and mitigating interference are also critical concerns. Future directions involve developing advanced optimization and adaptive algorithms, integrating emerging technologies like 5G, enhancing interference mitigation and energy efficiency, and improving robustness and real-time implementation. Addressing these challenges through innovative research and technology can enhance the effectiveness of AN in improving security and performance in relay networks.

I. AN-aided Satellite Communications

As a result of extended communication range, wide coverage, and adaptable networking capabilities, satellite communication systems offer extensive utility in both military and civilian domains, encompassing broadcasting, navigation, and emergency communication, each benefiting from their distinctive attributes. To enhance the PLS of satellite communications, some AN methods were put forth in [124], [125].

A power and time slot allocation method was proposed in [124] to secure satellite transmission. The authors first proposed a DCAN method based on weighted fractional Fourier transform (WFRFT), outperforming conventional AN methods under imperfect CSI. An optimized allocation method using fractional and convex differential programming addressed secrecy degradation with more signals. Simulations showed improved performance, especially with imperfect CSI, and maximized total secrecy capacity.

In [125], a secure AN-assisted beamforming scheme was proposed for cognitive satellite-ground networks, where the satellite shares spectrum with multi-cell terrestrial networks amid multiple unauthorized Eves. The goal is to minimize the total transmit power of the satellite and BSs while meeting secrecy rate constraints C_p for satellite users and SNR constraints $\mathrm{SINR}_{n,m}$ for terrestrial users as

$$\min_{\mathbf{w}_0,\mathbf{w}_{n,m}} \|\mathbf{w}_0\|^2 + \sum_{n=1}^{N} \sum_{m=1}^{M_n} \|\mathbf{w}_{n,m}\|^2 \tag{51a}$$

$$\text{s.t. } C_p \geqslant R, \tag{51b}$$

$$\mathrm{SINR}_{n,m} \geqslant \gamma_{n,m}, \tag{51c}$$

where a low-complexity ZF method was employed to obtain a suboptimal solution.

In summary, the precision of CSI and power constraints are crucial concerns in implementing AN for satellite communication. Inaccurate CSI may lead to the leakage of AN into the main channel, affecting the intended receiver. Furthermore, integrating AN into transmitted signals demands extra power, which is a scarce resource on satellites.

J. AN-aided SWIPT

The simultaneous wireless information and power transfer (SWIPT) has garnered significant interest in recent years due to its potential to enhance the energy efficiency of networks. It is particularly appealing in scenarios with low energy demands, where it can power wireless devices with limited battery capacity, often in situations where battery replacement or recharging is impractical. However, SWIPT is susceptible to eavesdropping, primarily because energy receivers (ERs) can not only harvest energy but also intercept information-bearing messages intended for Bobs, as noted in [50]. To mitigate this vulnerability, the introduction of AN can further enhance the PLS in SWIPT, as discussed in [126]–[132].

The authors of [126] focused on an SEEM problem for a SWIPT-based MIMOME wiretap channel. Concentrating the optimization of the transmit and AN covariance matrix $\mathbf{Q}_c, \mathbf{Q}_a$, an SEEM problem was cast and sloved by applying fractional programming to simplify the objective, followed by exploiting its primal decomposability.

The authors of [127] proposed an AN-aided time-switching power-splitting (TSPS) scheme for AN-assisted SWIPT in OFDM systems. This scheme exploits the temporal degrees of freedom from the CP structure to degrade Eve's signal while providing power to Bob. The AN precoder is designed to cancel interference at Bob. An SRM problem was formulated over CP length, time switching, and power splitting parameters, subject to energy harvesting constraints. Numerical results demonstrated that the TSPS scheme achieves higher average secrecy gain than pure power splitting.

In [128], a downlink MISO NOMA CRNs network with SWIPT was studied, where a primary BS sends confidential signals to PUs across clusters, and NOMA enhances power efficiency in the secondary network. The authors formulated security and energy harvesting constraints for power minimization and designed beamforming under both perfect and bounded CSI error models using SDR and cost-function algorithms. Simulations showed the AN-aided cooperative scheme reduces transmission power in MISO-NOMA SWIPT systems.

In [129], the authors proposed an AN-assisted interference alignment (IA) scheme with wireless power transfer for interference networks with K users. Each user's transmission involves unitary precoding/decoding matrices to manage signals and AN, while conventional systems require canceling interference and AN at legitimate receivers through specific zero-interference conditions.

The authors of [130] treat AN and interference as redundant energy rather than interference to be removed. Using power splitting, received power is divided between information decoding and energy harvesting. Their precoding and decoding algorithm aligns and cancels AN and interference at legitimate receivers. To enhance performance, they maximize total AN transmit power by jointly optimizing information transmit power and power-splitting coefficient. Since the coupled effect between SINR and EH variables $P_t^{[k]}$ and $\rho^{[k]}$, the constraint is non-convex. Due to the coupling between SINR and EH, this non-convex problem was reformulated into a convex form (as in [129]) and solved by CVX, with a low-complexity suboptimal closed-form solution also derived.

The authors of [130] studied AN-aided multi-cell coordinated beamforming for SWIPT under a non-linear energy harvesting (EH) model. They formulated power-minimization problems to design transmit beamforming vectors and AN covariance matrices at all BSs, ensuring SINR and harvested energy thresholds for authorized users while limiting eavesdroppers' SINR. Key variables include beamforming vectors, power splitting factors between information decoding and EH, and AN covariance matrices. Under perfect CSI, the non-robust design was solved via SDR under imperfect CSI, including worst-case and statistical robust designs by S-Procedure and Bernstein-type inequality. Additionally, a distributed ADMM-based AN-aided multi-cell beamforming framework was proposed, enabling each BS to optimize using only local CSI, greatly reducing overhead compared to centralized designs.

To enhance secrecy robustness, [131] incorporated cooperative jamming into AN-SWIPT. They jointly optimized the transmit beamformer, AN and CJ covariance matrices, and power splitting ratio under imperfect CSI with norm-bounded uncertainty. The semi-infinite problem was tackled in two steps: reformulated into SDPs using the S-Procedure and Schur complement, then reduced to a single-variable optimization solved via one-dimensional line search.

In [132], the authors analyzed secrecy outage in AN-aided cognitive radio SWIPT systems with randomly located non-colluding Eves. They proposed a MIMO CR-SWIPT system with AN over Rayleigh fading and selection combining at Bob. A closed-form SOP expression was derived using Gauss-Laguerre quadrature, and asymptotic analysis revealed the secrecy diversity order and array gain at high SNR.

Overall, due to the additional constraints brought by EH, the design of AN in SWIPT systems is more complex compared to conventional systems. Furthermore, in SWIPT systems, AN can simultaneously serve as an energy signal for EH devices, which is a feature not present in traditional AN systems.

K. AN-aided THz

Due to the enticing data rate brought by the abundant bandwidth resource, the potential of PLS of Terahertz (THz) communications needs in-depth analysis. Despite the narrow beam of THz communications, the PLS in the THz band is challenging when eavesdroppers are inside the beam radiation sector [133], [134].

To enhance THz secure communications, [133] and [134] proposed a self-interference-cancellation (SIC)-free AN-assisted receiver scheme leveraging the distinct temporal broadening of AN at Eve. By introducing a time delay in Bob's AN pulses, Eve experiences pulse overlap, degrading her reception. This eliminates the need for complex SIC at Bob. The authors further optimized system parameters via a DNN to maximize secrecy rate. Results showed the proposed method achieves 4 bps/Hz with lower hardware and computational complexity than SIC-based designs.

In summary, due to the narrow beamwidth in THz scenarios, traditional spatial AN is no longer suitable for interfering with Eves within the beam. Therefore, temporal broadening effect has become the new choice for AN in terahertz scenarios.

L. AN-aided UAV

Recently, unmanned aerial vehicle (UAV)-aided wireless communications have attracted significant research interest. UAVs offer unique attributes, including flexible deployment, dominant line-of-sight (LoS) and air-ground (AG) channels, and controlled mobility in three-dimensional (3D) space. Consequently, UAVs can serve as flying BSs, aerial radio access points, or aerial relays, establishing AG links to extend coverage, ensure seamless connectivity, and support high-rate communications. However, the open nature of AG links inevitably renders such systems vulnerable to eavesdropping

attacks, and hence, safeguarding UAV communication is of significant importance [135].

Currently, the form of AN employed in UAV resembles a shared jamming signal at both Alice and Bob, which can also be seen as a pre-shared key in cryptography mechanisms and differs from space-domain AN [135]–[137]. In UAV-aided wireless networks, the joint optimization of power allocation and trajectory for AN-aided UAV has emerged as a new challenge [135], [136]. Furthermore, the joint optimization of resources, trajectory, and AN was explored in [137] for a dual-UAV-based NOMA scenario with imperfect CSI.

In [135], a secure UAV-based data dissemination system was proposed, where the UAV transmits both information and pre-known AN. To maximize the average minimum secrecy rate η, the user scheduling, power splitting, and UAV trajectory were jointly optimized. The resulting non-convex problem was tackled using an iterative algorithm based on alternating and successive convex optimization.

For UAV-aided wireless networks, a secure two-phase transmission protocol was introduced in [136], where Alice shares AN with Bob beforehand for cancellation during data transmission. The UAV's trajectory, transmit power, and AN power allocation were jointly optimized to enhance secrecy rate. To handle the non-convex problem, the authors decomposed it into four subproblems and solved it using a successive convex approximation-based iterative algorithm.

In [137], joint optimization of resource allocation, trajectory, and AN was studied for a dual-UAV NOMA system under imperfect CSI. Probabilistic constraints were handled using the Markov inequality and Marcum Q-function, enabling a reformulation into deterministic constraints. The communication UAV's trajectory was optimized using slack variables and Taylor expansion.

In UAV secure transmission systems, it is important to jointly optimize the power allocation of AN, other resource allocation, and the UAV's trajectory. This typically requires complex optimisation methods, and finding a low-complexity algorithm remains a significant challenge.

M. AN-aided VLC

The visible light communication (VLC), primarily based on light-emitting diodes (LEDs) and photo diodes, has been regarded as one of the most promising wireless communication technologies due to its impressive data rate and unregulated wide bandwidth. By combining communication and illumination, VLC is well-suited for future indoor access scenarios, which, however requires security, particularly in the presence of potential wiretapping threats. To fulfill secure VLC communications, AN has been introduced into the MISO VLC wiretap channels to protect against a single Eve [138] or multiple Eves [139]. In addition, AN-aided precoding design for multi-user VLC channels was addressed in [140], and this concept was extended to NOMA in [141]. Furthermore, it found application in indoor SISO direct-current-biased optical OFDM systems in [142]. In general, when adding the AN $\mathbf{v}$ to the VLC, an additional concern is the influence of the direct current bias I_D in the transmit signal

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{W}_k \mathbf{s}_k + \mathbf{v} + I_D \mathbf{1}_N, \tag{52}$$

where $\mathbf{W}_k$ and $\mathbf{s}_k$ denote the precoding matrix and transmit signal towards the k-th user.

Due to the unique nonlinear transfer characteristic of the LEDs, the power of transmit signal must be constrained within a certain range, which inspires new requirements regarding the power allocation of AN

$$\sum_{k=1}^{K} \|\mathbf{W}_k\|_1 + \rho \|\mathbf{V}\|_1 \leqslant \Delta_n, \tag{53}$$

where $\Delta_n = \min\left(I_n^{DC} - I_{\min}, I_{\max} - I_n^{DC}\right)$ is the direct current limitation with $[I_{\min}, I_{\max}]$ bounding the allowable range of current.

For the MISO VLC wiretap channel, the authors of [138] employed an AN-based beamforming approach to maximize an upper bound of secrecy rate. The upper bound of secrecy rate is expressed as

$$R_u\left(\mathbf{h}_E\right) = \frac{1}{2} \log \left[\frac{1 + NA^2 \left(\mathbf{h}_B^T \mathbf{e}\left(\mathbf{h}_E\right)\right)^2 / \sigma_B^2}{1 + NA^2 \left(\mathbf{h}_B^T \mathbf{e}\left(\mathbf{h}_E\right)\right)^2 / \sigma_E^2} \right], \tag{54}$$

where N denotes the number of LED fixtures, A represents the peak-power constraint for transmit signals, and $\mathbf{e}\left(\mathbf{h}_E\right)$ is the only one active orthonormal eigenvector of the matrix $\mathbf{h}_B \mathbf{h}_B^T / \sigma_B^2 - \mathbf{h}_E \mathbf{h}_E^T / \sigma_E^2$.

In [139], the authors explored the design of PLS in VLC systems with multiple Eves. They employed AN-assisted precoding in scenarios where the CSI of Eves was both known and unknown. The primary objective of the design is to minimize the total transmission power, subject to specific constraints on the SINR for both Bob and Eves as

$$\min_{\mathbf{v},\mathbf{W}} \|\mathbf{W}\|_2^2 + \|\mathbf{v}\|_2^2 \tag{55a}$$

$$\text{s.t. SINR} \geqslant \gamma, \tag{55b}$$

$$|[\mathbf{v}]_n| + \left\| [\mathbf{W}]_{n,:} \right\|_1 \leqslant \Delta_n, \tag{55c}$$

where n denotes the index of n-th Eve and Δ_n is defined in (53). In the case of unknown Eve's CSI, the AN was strategically placed in the null space of Bob's channel, simplifying the design problem. When Eve's CSI is known, the problem became non-convex due to constraints imposed by the Eves' SINR. To address this, the authors investigated two different sub-optimal but low-complexity approaches: a concave-convex process and SDR.

The AN-aided precoding designs with respect to Bobs' and Eves' SINR performances for multi-user VLC wiretap channels were discussed in [140]. In the case of passive Eves, the AN was strategically designed to occupy the null space of the Bobs' aggregate channel matrix. When dealing with active Eves, the design objective is to limit the Eves' SINR to be below a certain threshold, thereby enhancing security.

Aside from the general precoding design, the authors explored a specific design of $\mathbf{W}$ as

$$\mathbf{W} = \left(\mathbf{H}^{\dagger} + \left(\mathbf{I} - \mathbf{H}^{\dagger}\mathbf{H}\right)\mathbf{R}\right) \text{diag}\left\{\sqrt{\mathbf{p}}\right\}, \tag{56}$$

which employs the ZF technique as the fundamental precoding scheme for Bobs, effectively decoupling the multi-user channel into multiple subchannels. This decoupling facilitated confidentiality among Bobs and contributed to securing the communication in multi-user VLC scenarios.

For a MISO VLC system with NOMA, a robust AN-aided secure beamforming design was optimized in [141], formulated by

$$\min_{\mathbf{W}_k, \mathbf{V}} \text{Tr}\left(\sum_{k=1}^{K} \mathbf{W}_k + \mathbf{V}\right) \tag{57a}$$

$$\text{s.t. } R_{B,k}^{L} \geqslant \gamma_b, \tag{57b}$$

$$R_{E,k}^{U} \leqslant \gamma_E, \tag{57c}$$

$$\text{Tr}\left(\sum_{k=1}^{K} \mathbf{W}_k \mathbf{e}_n \mathbf{e}_n^T\right) \leqslant \Delta_n^2, \tag{57d}$$

$$\mathbf{W}_k \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, \tag{57e}$$

where $\mathbf{W}_k$ and $\mathbf{V}$ denote the precoding matrix for k-th user and the AN matrix, respectively. $\mathbf{e}_n$ represents the n-th column of the identity matrix and Δ_n is defined in (53). The optimization leveraged SDP relaxation to minimize transmit power under QoS and Eve's rate constraints. Simulations showed that the AN-aided beamforming improved security and efficiency, though CSI imperfections led to conservative resource use and limited performance gains.

In [142], the authors focused on indoor SISO direct-current-biased optical OFDM systems. They proposed a precoding scheme using time-domain AN to exploit the DoF provided by the CP of OFDM, i.e.,

$$\mathbf{R}^{cp}\mathbf{H}\mathbf{V} = \mathbf{0}. \tag{58}$$

The authors proposed a convex optimization approach to limit PAPR while maximizing secrecy rates. Results showed improved secrecy and reduced PAPR. For further details on time-domain AN, refer to the AN-OFDM chapter.

In a nutshell, the use of AN in VLC needs to fully comply with the requirements of the LED constrained power range, and the influence of direct current bias should be paid attention to by researchers.

N. AN-aided ISAC

Integrated sensing and communications (ISAC), a key 6G feature, faces risks of information leakage from both communication and sensing. To address this, AN has been widely studied as a promising PLS technique for secure ISAC transmission. [143]–[146].

In [143], a secure beamforming scheme for dual-functional radar-communication (DFRC) systems was proposed, where radar beams act as AN to suppress eavesdropping. The system jointly optimizes communication and radar beamformers to maximize the sum secrecy rate while maintaining a desired radar beampattern and limiting Eve's SINR. To solve the non-convex problem, a ZF-based strategy and SDR with eigenvalue decomposition were used. Additionally, a jamming power maximization problem was formulated to reduce complexity. Simulations confirmed that both SRM and JRM approaches enhance security without requiring Eve's CSI.

Refs. [144] and [145] introduced AN in DFRC systems to enhance secure transmission. The transmitter, equipped with a uniform linear array, serves multiple Bobs and detects a single-antenna Eve. A joint design of transmit beamforming and AN was proposed to optimize the radar beampattern while minimizing Eve's SNR and ensuring Bobs' SINR constraints. The problem was solved using SDR, Dinkelbach's method, and quadratic transform, with extensions for angle uncertainty and imperfect CSI. Additionally, from a symbol-level precoding view, AN was shown to act as constructive interference for Bobs, achieving superior radar SINR.

In [146], the authors studied an ISAC system combining an MU-MISO downlink and a colocated MIMO radar. The BS with a ULA serves multiple single-antenna users in the presence of eavesdroppers, while the radar detects a target. A joint design of BS and radar beamforming, along with AN, was proposed to minimize Eve's SINR while meeting communication and radar SINR constraints. The optimization was solved via BCD, fractional programming, and SDR. AN was also incorporated from both BS and radar to further degrade Eve's reception. Simulations confirmed that the proposed schemes significantly reduced Eve's SINR versus baselines.

In a nutshell, AN-aided ISAC must balance tradeoffs among communication throughput, sensing accuracy, and AN design complexity. Future work will explore adaptive algorithms, ML-enhanced signal processing, energy-efficient designs, and application-specific, secure solutions.

IV. Overview of AN-combined Technologies

In this section, an overview of the AN-combined technologies is provided and the technical contributions of related papers are summarized in Table III.

A. AN-aided Coding

Over the past few decades, several coding technologies have been extensively explored to improve communication quality. The property of channel characteristic enables them to combine with AN for PLS, which includes but is not limited to the AN-aided space time block code (STBC) [147], space time line code (STLC) [148], rateless codes (RLC) [149], and polar code [150].

In [147], a secure STBC scheme was presented for MIMO systems when Alice has the CSI of Bob but without that of Eve. To bolster security, the authors introduced AN symbols v_1 and v_2 at the first slot, which are carefully aligned with each other, yielding

$$\begin{aligned} v_1 &= \eta\left[\bar{h}_1\left(c_1^* - c_2^*\right) + \bar{h}_2\left(c_3^* - c_4^*\right)\right], \\ v_2 &= \eta\left[\bar{h}_3\left(c_1^* - c_2^*\right) + \bar{h}_4\left(c_3^* - c_4^*\right)\right], \end{aligned} \tag{59}$$

where $\bar{h}_1$, $\bar{h}_2$, $\bar{h}_3$, and $\bar{h}_4$ are equivalent parameters composed of CSI, while η is a defined power constraint parameter.

TABLE III
OVERVIEW OF AN-COMBINED TECHNOLOGIES

References	Technologies	AN Types	System Models	Bob types	Eve types	CSI of Bob/ Eve	Involved Contributions
[147]	STBC	AN	MIMOME	MMA	SMA	Imperfect/ No	Aligned AN symbols
[148]	STLC	AN	MIMOME	SMA	SMA	Perfect/ No	Lower bound of SSR
[149]	RLC	Jammer AN	MISOME	SSA	SMA	Perfect/ No	TAS for reducing QVP
[150]	Polar codes	AN	SISOSE	SSA	SSA	Perfect/ Perfect	Jamming positions selecting
[151]	Covert	AN	SISOSE	SSA	MSA	Statistical/ Statistical	AN from the closest friendly node
[152]	Covert	AN	SISOSE	SSA	MSA	Statistical/ Statistical	Increased covert transmission bits
[153]	Covert	Jammer AN	SISOSE	SSA	SSA	Statistical/ Statistical	AN from a friendly jammer
[154]	Covert	AN	MISOSE	MSA	MSA	Perfect/ Statistical	AN for D2D cellular network
[155]	Covert	AN	MISOSE	MSA	MSA	Statistical/ Statistical	Stackelberg game formulation for IoT
[157]	DM	Analog AN	MISOSE	MSA	SSA	Perfect/No	Analog AN far-field beampattern design
[158], [159]	DM	Analog AN	MISOSE	MSA	SSA	Perfect/No	Simplified AN design for dynamic DM
[160]	DM	AN	MISOSE	MSA	SSA	Perfect/No	GPI-based precoding for SRM
[161]	DM	AN	MISOME	MSA	SSA	Either/Either	Robust multi-beam for broadcasting
[162]	DM	AN	MISOME	MSA	SSA	Either/Either	MLI-based SINR maximization for MU
[164]	FH	AN	SISOSE	SSA	SSA	No/ No	Pre-stored AN for FH
[165]	FH	AN	SISOSE	SSA	MSA	No/ No	Storage AN for IQ balances
[166]	FH	AN	SISOSE	SSA	MSA	No/ No	Secrecy analysis and power allocation
[167]	MISO	AN	MISOSE	SSA	SSA	Perfect/ No	Channel correlation
[168]	MISO	Robust AN	MISOSE	SSA	SSA	Partial/ Partial	Imperfect CSI
[169]	MISO	Generalized AN	MISOSE	SSA	SSA	Perfect/ Statistical	SRM
[170]	MISO	AN	MISOSE	SSA	SSA	Perfect/ Statistical	On-off and adaptive schemes
[171]	MISO	AN	MISOME	SSA	SMA	Perfect/ Statistical	SOP minimization
[172]	MISO	Generalized AN	MISOME	SSA	SMA	Perfect/ Statistical	SRM
[173]	MISO	AN	MISOME	MSA	SMA	Perfect/ No	Three AN schemes for CRNs
[174]	MISO	AN	MISOME	SSA	SMA	Perfect/ Statistical	On-off and adaptive schemes
[175]	MISO	AN-AFF	MISOME	SSA	SMA	Perfect/ No	Hybrid AN-AFF scheme
[176]	MISO	Robust AN	MISOSE	SSA	MSA	Perfect/ Imperfect	SRM
[177]	MISO	Generalized AN	MISOSE	SSA	MSA	Perfect/ Imperfect	A safe convex approximation
[178]	MISO	AN	MISOSE	SSA	MSA	Perfect/ No	SOP-based security region
[179]	MISO	Generalized AN	MISOSE	SSA	MSA	Perfect/ Statistical	Semiadaptive scheme for STM
[180]	MISO	Generalized AN	MISOME	SSA	MMA	Perfect/ Either	SRM
[181]	mMIMO	AN	MISOME	MSA	SMA	Either/ Either	SRM under different CSI accessibility
[182]	mMIMO	AN	MISOME	MSA	SMA	Imperfect/ No	Three AN precoders and analysis
[183]	mMIMO	AN	MISOME	MSA	SMA	Imperfect/ No	Two AN schemes in two phases
[184]	mMIMO	AN	MISOME	MSA	SMA	Statistical/ No	Low-complexity AN over Ricean channel
[185]	mMIMO	AN	MISOSE	MSA	SSA	Imperfect/ No	SSR maximization for NOMA
[186]	NOMA	Two-phase AN	SIMOSE	SMA/SSA	SSA	Perfect/ No	Two-phase AN and relay selection
[187]	NOMA	Bob AN	SISOSE	MSA	SSA	No/ No	Pseudo random AN from FD Bobs
[188]	NOMA	AN	MISOSE	MSA	SSA	Perfect/ Perfect	SRM via AO for RIS-NOMA
[189]	NOMA	AN	MISOME	MSA	SMA	Perfect/ No	Closed-form SOP for MISO-NOMA
[190]	OFDM	Temporal AN	SISOSE	SSA	SSA	Perfect/ Either	Temporal AN for OFDM
[191]	OFDM	Time-domain AN	SISOSE	SSA	SSA	Perfect/ Perfect	Time-domain AN with discrete inputs
[192]	OFDM	Time-domain AN	MISOME	MSA	SMA	Perfect/ Perfect	Time-domain AN for multiuser
[193]	OFDM	Time-domain AN	SISOSE	SSA	SSA	Perfect/ Perfect	Time-domain AN for AF relay
[194]	OFDM	Hybrid AN	MIMOME	SMA	SMA	Perfect/ No	Closed-form expressions for secrecy rate
[195]	OFDM	Hybrid AN	MIMOME	SMA	MMA	Perfect/ Perfect	Hybrid spatial and temporal AN
[196]	OFDM	Frequency AN	SISOSE	MSA	MSA	Perfect/ Perfect	Frequency-domain AN for SWIPT
[197]	OFDM	Bob AN	SISOSE	SSA	MSA	Perfect/ No	Hybrid parallel power-line/wireless OFDM
[198]	PLA	AN	MIMOME	SMA	SMA	Imperfect/ No	AN fingerprint embedding authentication
[199]	PLA	AN	SISOSE	SSA	SSA	No/ No	AN-aided message authentication codes
[200]	PLA	Tikhonov AN	SISOSE	SSA	SSA	Perfect/ No	OFDM challenge-response authentication
[201]	PLA	Two frame AN	SISOSE	SSA	SSA	Perfect/ No	Authentication over time-variant channels
[202]	RIS	AN	MISOSE	SSA	MSA	Perfect/ Perfect	Performance validation of AN-RIS
[203]	RIS	AN	MIMOME	SMA/MMA	SMA	Perfect/ Perfect	BCD for RIS-MIMO
[204]	IOS	AN	MIMOME	SMA	SMA	Perfect/ Perfect	Complexity reduction for refractive RIS
[205]	RIS	AN	MISOSE	MSA	MSA	Perfect/ Perfect	RIS and AN assisted MEC systems
[206]	RIS	AN	MISOSE	SSA	SSA	Perfect/ No	Efficient OM and MM algorithms
[207]	RIS	AN	MISOSE	SSA	SSA	Perfect/ No	Computational complexity reduction
[208]	SISO	Time-domain AN	Multi-path	SSA	SSA	Perfect/ No	Inter-symbol interference compensation
[209]	SISO	Adaptive AN	SISOSE-ARQ	SSA	SSA	Perfect/ No	PAPR and out-of-band emission reduction
[210]	SISO	Time-domain AN	TDD SISOSE	SSA	SSA	Perfect/ No	Repetition coding in two time slots
[211]	SISO	Two-phase AN	HD SISOSE	SSA	SSA	No/ No	Broadcasting and forwarding of AN
[212]	SISO	Reference-free AN	SISOSE	SSA	SSA	No/ No	AN reconstruction from received signals
[213]	SM	AN	MISOSE	SSA	SSA	Perfect/ No	Single RF chain
[214]	SM	AN	MISOSE	SSA	SSA	Imperfect/ Imperfect	Closed-form expression of ESR
[215]	DQSM	Jammer AN	MISOSE	SSA	SSA	Perfect/ Either	AN from a CJ
[216]	SM	AN	MISOSE	SSA	SSA	Perfect/ No	Antenna selection for two RF chains
[51]	GSM	AN	MIMOME	SMA	SMA	Perfect/ No	PMAN and BER analysis
[217]	GSM	AN	MIMOME	MMA	SMA	Perfect/ No	Multi-user GSM with AN and BD

In [148], the STLC with AN was proposed for enhancing the PLS in a time division duplex (TDD) mode. Note that the AN symbols are injected in two time slots, i.e.,

$$\begin{aligned}\begin{bmatrix} v_{1,1}^* \\ v_{2,1}^* \end{bmatrix} &= \frac{\|\mathbf{h}_2\|}{\|\mathbf{h}_1\|}\begin{bmatrix} h_{1,1} & h_{2,1}^* \\ h_{2,1} & -h_{1,1}^* \end{bmatrix}\mathbf{r}, \\ \begin{bmatrix} v_{1,2}^* \\ v_{2,2}^* \end{bmatrix} &= \frac{-\|\mathbf{h}_1\|}{\|\mathbf{h}_2\|}\begin{bmatrix} h_{1,2} & h_{2,2}^* \\ h_{2,2} & -h_{1,2}^* \end{bmatrix}\mathbf{r}.\end{aligned} \tag{60}$$

Moreover, the authors derived the lower bound for the SSR under various scenarios: without AN, with AN, and with AN in the presence of imperfect CSI.

Ref. [149] investigated a secure transmission scheme using RLC in a delay-constrained system. By using RLC, secrecy is achieved if Bob can accumulate the required number of packets before Eve does. To achieve this, the authors employed transmit antenna selection (TAS) at Alice to improve the main channel quality as

$$h_S = \max_{k\in\{1,2,\ldots,N_a\}} |h_k|, \tag{61}$$

and the AN based on the null space was generated to degrade Eve's channel.

Ref. [150] proposed an AN-aided polar coding algorithm to improve the secrecy rate. Specifically, a secure coding model based on AN was presented, where the AN is pre-shared by transceivers and injected into the current codeword

$$\mathbf{x} = \mathbf{s} \oplus \mathbf{v}, \tag{62}$$

where $\oplus$ is the module-2 sum. With the knowledge of AN $\mathbf{v}$, Bob can mitigate its impact and detecting codewords.

In general, the combination of AN and coding is practical and feasible. However, the difficulty that researchers need to show solicitude for is how to utilize the characteristics of different coding methods.

B. AN-aided Covert Communications

Due to its ability to create interference towards the adversary, the AN technology can be considered as an implementation method for covert communications, which is also known as low probability of detection (LPD) communications. [151]–[155]. As depicted in Fig. 8, the main concept of covert communications is to confuse the judgment of the adversary, making it hard to determine whether Alice and Bob are communicating. With the aid of AN, this goal can be achieved more easily, making it more difficult for the adversary to detect the conduct of communications.

The authors of [151] explored network scenarios with friendly nodes generating AN to enable covert communication, suggesting that the node nearest the adversary should do so to satisfy the error probability constraint

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} \geqslant 1 - \varepsilon, \forall \varepsilon, \tag{63}$$

where $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ denote false alarm and miss detection probabilities, respectively, and ε is small positive constant indicating the maximum deviation from perfect covertness.

The authors of [152] focused on the scenario where other friendly nodes were distributed according to a 2D Poisson point process with a specific density. They proposed an AN generation strategy from the friendly node closest to Eve, and demonstrated that compared to the conventional work that can only transmit $\mathcal{O}(\sqrt{n})$ bits in n channel uses, the method in [152] allows Alice to reliably send increased $\mathcal{O}\left(\min\left\{n, m^{\gamma/2}\sqrt{n}\right\}\right)$ bits to Bob.

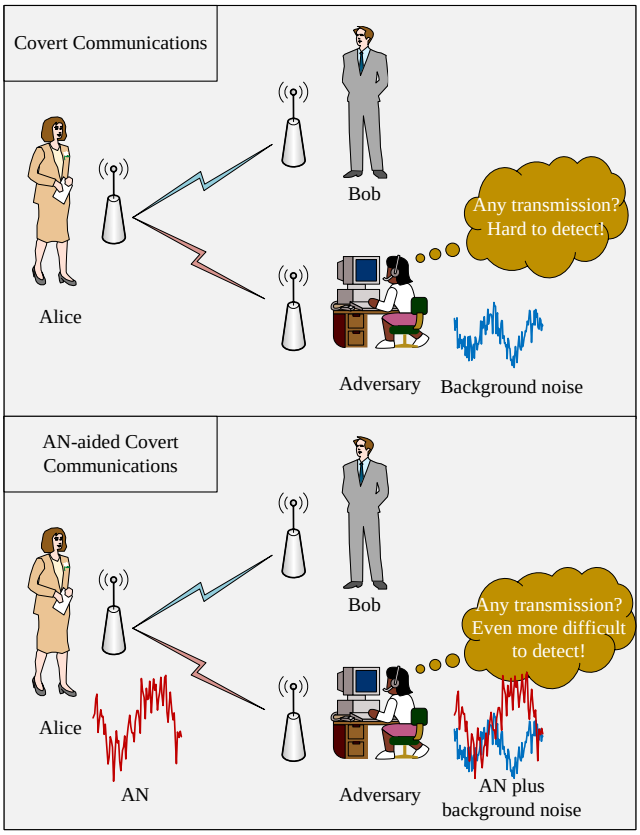

Fig. 8. The effect of AN in covert communications.

The authors of [153] studied a wireless covert communication system, where a friendly jammer generates intermittent AN to confuse Eve. The transmission probabilities of information and AN were jointly optimized to maximize the communication covertness under a throughput requirement. Then, closed-form optimal solutions are obtained by simplifying the original problem to a one-dimensional problem.

To confuse Eve in a D2D underlying cellular network, the AN-aided covert signals were used at Alice in [154]. To evaluate performance, the achievable D2D communication rate is defined as the product of the covert signal desirable communication rate R_d, the cellular link connection probability $1 - \mathbb{P}_{co}$, and the D2D link connection probability $1 - \mathbb{P}_{do}$. By maximizing the achievable D2D communication rate under the constraints of error probabilities (including false alarm and mis-detection probability), the optimization problem was formulated as

$$\max_{P_t} R_d\left(1 - \mathbb{P}_{co}\right)\left(1 - \mathbb{P}_{do}\right) \tag{64a}$$

$$\text{s.t. } \mathbb{P}_{FA}^k + \mathbb{P}_{MD}^k \geqslant 1 - \varepsilon. \tag{64b}$$

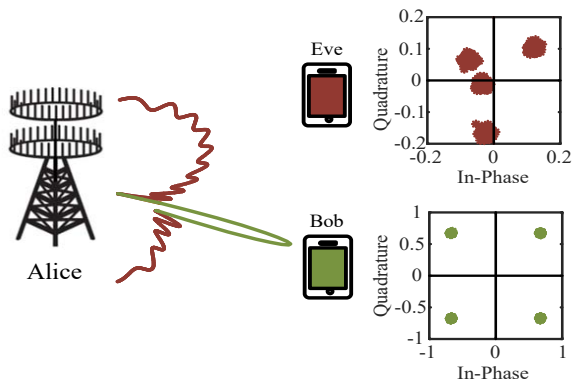

Fig. 9. Framework of the AN-aided DM wireless secure communications.

By applying uplink power control and AN scheme, a covert IoT system was studied in [155]. Specifically, the AN is transmitted by in-band FD IoT gateways as a jamming operation to intends to hide the legitimate transmission from the observant Eves. Moreover, a Stackelberg game was formulated to study the interaction between the Eves and Bobs as

$$\max_{p,q} \mathbb{P}\left(\text{SINR}_b \geqslant \gamma_b \,|\mathcal{L}_1\right) u_b \tag{65a}$$

$$\text{s.t.} \quad -\mathbb{P}\left(\text{SINR}_e \geqslant \gamma_e \,|\mathcal{L}_1\right) u_e - v_D p \tag{65b}$$

$$\mathbb{P}_{FA}^k + \mathbb{P}_{MD}^k \geqslant 1-\varepsilon, \tag{65c}$$

$$p^L \leqslant p \leqslant p^U, q^L \leqslant q \leqslant q^U, \tag{65d}$$

where p and q are the power of information-bearing signal and AN bounded by $\left[p^L, p^U\right]$ and $\left[q^L, q^U\right]$, respectively, u_b and u_b are the reward of guaranteeing the transmission reliability, while $v_D p$ is the power cost for the IoT device.

Objectively speaking, the AN significantly enhances the performance of covert communications. However, the main concern that researchers need to be aware of is that the calculation of error probabilities for the adversary, i.e., $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$, includes the knowledge of its CSI, which may contradict the fact that Alice and adversary cannot collaborate to perform channel estimation in the practical scenarios.

C. AN-aided DM

As shown in Fig. 9, directional modulation (DM) is capable of conducting beamforming towards the legitimate user while projecting AN to eavesdroppers in other directions, resulting in a standard constellation appearing only in the desired direction of legitimate users. As a multi-antenna-based PLS technique, DM extensively incorporates the notion of AN [156]–[162].

The earliest utilization of AN in DM was proposed in [157], where the interference pattern for introducing AN was designed separately from information patterns by the far-field pattern null steering method. Specifically, the information beampattern towards the direction of Bob was first constructed with the array excitation $\mathbf{w}$, after which the orthogonal null-space interference beampattern towards the i-th sidelobe $\mathbf{v}_i$

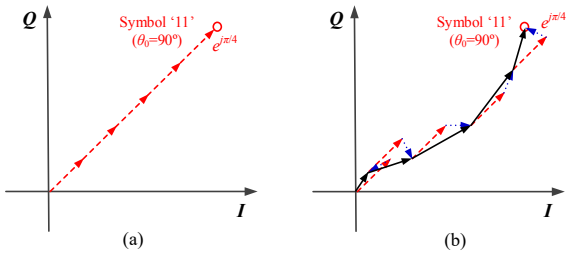

Fig. 10. Vector paths along the boresight for one QPSK symbol: (a) without AN; (b) with AN [157].

was constructed using an orthogonal projection matrix of the array response of Bob $\mathbf{h}$. Therefore, the transmission can be synthesized as

$$\mathbf{x}_m = \mathbf{w}s_m + \sum_{n=1}^{N-1} (\mathbf{v}_i r_i), \tag{66}$$

where the interference beampattern is given by

$$\mathbf{v}_i = \left[\mathbf{I}_N - \mathbf{h}^{-1}\mathbf{h}\right] \mathbf{w}_i^{\text{sl}}, \tag{67}$$

with $\mathbf{w}_i^{\text{sl}}$ being the excitation of beampattern towards the ith sidelobe. Although this method was operated at the analog RF level, the main idea is consistent with the digital AN.

This approach underwent refinement in [158] and [159], where an innovative orthogonal vector representation for AN was employed for the so-called dynamic DM. The authors intuitively explained the diversity of AN through the geometric process of vector synthesis as shown in Fig. 10.

It can be observed that the different vector paths form the same constellation points in the boresight direction, which means that these vector paths have the same transmission effect for the legitimate receiver. On the contrary, for eavesdroppers in other directions, these different vector paths have different degrees of influence on the transmission effect.

To maximize the secrecy rate in a single-user MISO-DM system, the authors of [160] proposed a general power iterative (GPI)-based DM precoding, which optimizes the beamforming vector and AN projection matrix iteratively in an alternating manner. With the given AN projection matrix $\mathbf{V}$, the beamforming optimization can be cast as

$$\max_{\mathbf{w}} \frac{\mathbf{w}^{\text{H}}\left(\mathbf{H} + A_{\text{B}}\mathbf{I}_N\right)\mathbf{w}}{\mathbf{w}^{\text{H}}\left(\mathbf{G} + A_{\text{E}}\mathbf{I}_N\right)\mathbf{w}} \tag{68a}$$

$$\text{s.t.} \mathbf{w}^{\text{H}}\mathbf{w} = 1, \tag{68b}$$

where $\mathbf{w}$ denotes the beamforming vector, while $\mathbf{H} = \mathbf{h}\mathbf{h}^{\text{H}}$ and $\mathbf{G} = \mathbf{g}\mathbf{g}^{\text{H}}$ represent the channel covariance matrices for Bob and Eve, respectively.

For broadcasting MU-MISO systems, a robust multi-beam DM synthesis was explored in [161]. The beamforming vector was obtained by maximizing signal-to-leakage-noise ratio.

For performance improvement, the authors of [162] expanded the algorithm in [161] to an MU-MISO scenario. Specifically, a main-lobe-integration (MLI)-based SINR maximization problem was cast and solved by the generalized

Rayleigh-Ritz theorem to obtain the beamforming vector for the MU-MISO-DM system in both perfect and imperfect knowledge of desired directions scenarios. Recently, an analog DM precoding was proposed in [163] for near-field secure transmission in both angle and distance dimensions, significantly improving the secure capbility of AN.

From the perspective of maximizing the secrecy rate, AN has been applied comprehensively in DM systems, including orthogonal and non-orthogonal AN. However, these methods tend to require high computational complexity, which may not be suitable for resource-limited DM systems. Additionally, the current application of AN is limited to projection in the angular domain, restricting DM to secure transmission solely in the directional dimension. Expanding AN to other domains is crucial for enhancing the security capabilities of DM.

D. AN-aided FH

Through changing the carrier frequencies, the frequency hopping (FH) technique has surged to avoid electromagnetic interference. To address both electromagnetic interference and wiretapping, one appealing research idea is to jointly utilize FH and AN techniques to provide rigorous security. Song et al. discovered that the wide hopping bandwidth will raise a non-negligible in-phase and quadrature (IQ) imbalance at transceiver oscillators, yielding significant signal distortions during IQ mixing [164]–[166].

To further protect FH systems against severe wiretapping, an architecture of AN-shielded FH systems was proposed in [164], wherein AN cancellation architecture is utilized at Bob in the presence of Eve. Specifically, AN reconstruction and cancellation were employed to depict the residual AN, where the time delay and channel fading were supposed to be perfectly estimated. In the focus of the impact of frequency deviation, the estimated normalized frequency offset was assumed to be $\hat{F}_{d_r} = F_{d_r} - \Delta F_{d_r}$, where ΔF_{d_r} denotes the frequency deviation after synchronization. Under this estimation, the AN can be reconstructed as

$$\hat{c}_{\mathrm{ref}}(n) = \tilde{h}_r c(n - D_r) \mathrm{e}^{\mathrm{j}2\pi n \hat{F}_{d_r}} g(n - D_r - iL), \tag{69}$$

where h_r, $c(n)$, D_r, and $g(n)$ denote the complex channel gain, AN signal, normalized propagation delay, and shaping signal. Theoretical and simulation results confirmed that frequency deviation in practical FH systems will degrade both AN cancellation and system secrecy performance, and shorter hop length or proper power allocation for secret data and AN can mitigate the negative impact of frequency deviation, which in turn guides the practical transceiver design.

To alleviate signal distortion from IQ imbalances, the authors modeled signal distortions for AN-shielded FH systems [165]. In order to measure the quality of the obtained signal after AN cancellation, the signal-to-distortion-plus-noise ratio for Bob's residual signal and n-th Eve's composite signal are presented. Subsequently, the secrecy capacity was derived to evaluate system secrecy under multiple Eves as

$$C_s = 1/2 \log_2 (1 + \Lambda_r) - \max_n \left\{ 1/2 \log_2 (1 + \Lambda_e^n) \right\}, \tag{70}$$

where Λ_r and Λ_e^n are the signal to AN plus noise ratio at Bob and n-th Eve.

To protect military broadcasting against both hostile interference and eavesdropping, an AN-sheltered FH broadcasting architecture was proposed in [166], and the secrecy capacity in (70) was employed to measure its secrecy performance. Besides, the optimal transmitting power allocation for the information-bearing signal and AN was provided in a closed-form to maximize secrecy capacity in the presence of frequency mismatch. Specificialy, the power allocation problem was first cast as

$$\max_{\alpha} C_s = \frac{1}{2} \log_2 \frac{(a\alpha + b)(c\alpha + 1)}{(a\alpha + 1)(c\alpha + c)} \tag{71a}$$

$$\text{s.t. } \gamma_r > \gamma_e \tag{71b}$$

$$\alpha \geq 0, \tag{71c}$$

where α denotes the power allocation factor between the confidential information signal and AN. a, b, c, and d are four constant variables with respect to channel, frequency mismatch, and normalized power budget. The closed-form optimal solution for this problem is given by

$$\alpha^* = \begin{cases} \alpha_1, & \text{if } ac + c < a + bc \ , \ ab + b \leq a + bc, \\ 0, & \text{if } a + bc < ab + b \ , \ b > c, \\ \phi, & \text{if } ac + c \geq a + bc \ , \ b \leq c, \end{cases} \tag{72}$$

where α_1 is expressed as

$$\alpha_1 = \frac{a(b - c) - \sqrt{a(b-1)(c-1)(a-b)(a-c)}}{a(ac + c - a - bc)}. \tag{73}$$

Conclusively, AN-aided FH systems can avoid electromagnetic interference and guarantee security simultaneously. However, imperfect analog components are major challenges in such systems since the legitimate receivers need to perform FH synchronization, AN reconstruction and cancellation operations. This process is sensitive to analog component issues, such as IQ imbalance, power amplifier nonlinearity, phase noise, and frequency deviation. Considering these issues, the performance analysis and transmission design of AN-aided FH systems will be more accurate and meaningful.

E. AN-aided MISO

Since the null space of the channel involved in the AN technology exists under the condition that the number of transmit antennas exceeds the number of receive antennas, the MISO channel naturally aligns with this condition, making them compatible. As depicted in Fig. 11, the framework of AN-aided MISO wireless communications consists of a multiple-antenna Alice and a single-antenna Bob, which communicate in the presence of single or multiple Eves. For a fair comparison, most of the papers assume SSA Eve [167]–[170]. In order to achieve a stronger secrecy performance, some papers focused on the scenarios involving single multiple-antenna (SMA) Eve [171]–[175], MSA Eves [176]–[179], or MMA Eves [180].

For the MISOSE system, the authors of [167] studied how the correlation of the wiretap channel affects the secrecy rate

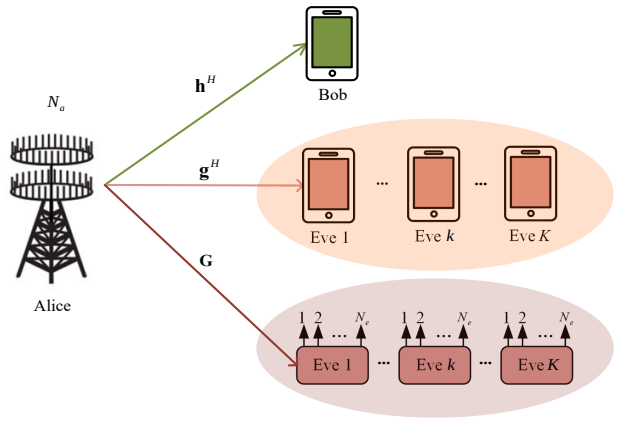

Fig. 11. Framework of the AN-aided MISO wireless secure communications.

of the AN scheme. Specifically, a simple but tight lower bound on the ESR of the AN scheme was developed as

$$\begin{aligned} R_s \geq & \log\left(1+\phi P(N_A-1)\right) \\ & - \left[\log\left(\sigma_e^2+\rho\phi P N_A+(1-\rho)P\right)\right. \\ & \left. - \log\left(\sigma_e^2+(1-\rho)(1-\phi)P\frac{N_A-2}{N_A-1}\right)\right]. \end{aligned} \tag{74}$$

Utilizing the derived bound, the influence of correlation on the secrecy rate was investigated.

Under two uncertainty models that Alice only has the imperfect CSI of Bob and Eve, the authors of [168] designed a robust AN for MISOSE. For the deterministic uncertainty model, the channel errors are assumed to be bounded by

$$\|\mathbf{\Delta h}\| \leq \epsilon_b, \|\mathbf{\Delta g}\| \leq \epsilon_e. \tag{75}$$

For the stochastic uncertainty model, the channel errors are zero-mean Gaussian random variables

$$\mathbf{\Delta h} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_b^2\mathbf{I}\right), \mathbf{\Delta g} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_e^2\mathbf{I}\right). \tag{76}$$

Considering the AN not constrained to be orthogonal to the information-bearing signal, the authors of [169] proposed a generalized AN scheme for MISOSE. To construct the AN-aided transmit signal, Alice generates an orthogonal basis $\mathbf{U} = [\mathbf{u}_1, \mathbf{U}_{\rm c}]$, where $\mathbf{u}_1$ denotes the direction of the main channel and $\mathbf{U}_{\rm c}$ represents the orthogonal complementary space of $\mathbf{u}_1$. The power of AN is distributed both in the space of $\mathbf{U}_{\rm c}$ and the direction of $\mathbf{u}_1$, yielding

$$\mathbf{x} = \sqrt{P\phi}\mathbf{u}_1\left(\sqrt{\theta}s+\sqrt{1-\theta}v\right)+\sqrt{P(1-\phi)}\mathbf{U}_{\rm c}\mathbf{r}. \tag{77}$$

Furthermore, the SRM problem under the constraint of SOP was addressed with perfect CSI of the main channel and the distribution of a complex Gaussian random wiretap channel. However, numerical results showed that the optimal AN is always orthogonal to the information-bearing signal.

The authors of [170] explored two AN transmission schemes for MISOSE: (i) An on-off transmission scheme with a constant secrecy rate for all transmission periods. (ii) An adaptive transmission scheme with a varying secrecy rate during each transmission period. The transmitted signal is given by

$$\mathbf{x} = \mathbf{W}\left[t_{\rm IS}^T\ \mathbf{t}_{\rm AN}^T\right]^T = \mathbf{w}_{\rm IS}t_{\rm IS}+\mathbf{W}_{\rm AN}\mathbf{t}_{\rm AN}, \tag{78}$$

where $\mathbf{w}_{\rm IS}$ is used to transmit the information-bearing signal $t_{\rm IS}$ and $\mathbf{W}_{\rm AN}$ is used to transmit the AN $\mathbf{t}_{\rm AN}$. In order to degrade the quality of the received signals at Eve by transmitting AN in all directions except towards Bob, $\mathbf{w}_{\rm IS}$ is chosen as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{hh}^H$, while $\mathbf{W}_{\rm AN}$ is comprised of the remaining $N-1$ eigenvectors of $\mathbf{hh}^H$.

In the context of MISOME, the problem of optimal power allocation was tackled in [171] by minimizing the SOP under the secrecy rate constraint. In this scenario, Alice knows the perfect CSI of Bob and the statistical CSI of Eve. The authors studied the problem of minimizing the secrecy outage probability given the secrecy rate and proved that the optimal power allocation can be conveniently obtained by using the method of bi-section search.

Meanwhile, the authors of [172] started with a generalized AN scheme for MISOME by solving an SOP-constrained SRM problem. Unlike many existing works, which directly adopted the traditional null-space AN scheme, the authors started with a general assumption on the structure of the transmit signal $\mathbf{x}$. Specifically, Alice generates an orthogonal basis $\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N]$ and transmits the signal formulated as

$$\mathbf{x} = \sqrt{p_1}\mathbf{u}_1(\sqrt{\theta}s+\sqrt{1-\theta}r_1)+\sum_{i=2}^{N}\sqrt{p_i}\mathbf{u}_i r_i, \tag{79}$$

where s and r_i denote the information-bearing signal and the AN signal in the direction of $\mathbf{u}_i$, respectively, p_i denotes the transmit power in the direction of $\mathbf{u}_i$. Through generalizing several previously established findings related to scenarios with a single-antenna Eve, they demonstrated that the conventional null-space AN scheme remains optimal for an arbitrary number of Eve's antennas in terms of secrecy outage.

In the context of MISOME-CRNs, three AN-assisted beamforming schemes were designed in [173], where Alice aims to transmit confidential information to two Bobs, namely legitimate PU and secondary user (SU) receivers, in the presence of SMA Eve in fast-fading environments. By maximizing the achievable ESR in the large-antenna regime, the optimal power allocation was derived, and the performance in terms of the secrecy outage probability was also studied. In particular, it was shown that the interference threshold at the PU plays an important role in the beamforming design.

As an extension from MISOSE to MISOME, two AN transmission schemes were further introduced in [174] based on [170], namely the on-off and adaptive transmission schemes. In the on-off transmission scheme, a channel-realization-independent secrecy rate was utilized for all transmission periods, leading to closed-form expressions for secure transmission probability, hybrid outage probability, and effective secrecy throughput. Conversely, in the adaptive transmission scheme, a channel-realization-dependent secrecy rate was employed for each transmission period, yielding closed-form expressions for secure transmission probability, the SOP, and

effective secrecy throughput. Using these closed-form expressions, the authors optimized the power allocation and secrecy rate for both schemes to maximize the secure transmission probability and effective secrecy throughput.

In [175], a randomized beamforming scheme named artificial fast fading (AFF) was proposed for MISOME. The AFF scheme employs a unique randomized weighting of information symbols across Alice's transmit antennas as

$$\mathbf{x} = \mathbf{w}^H s, \tag{80}$$

where $\mathbf{w}^H = [w_1, w_2, \cdots, w_{N_a}]$ denotes the weighted coefficient vector. Note that the first $N_a - 1$ coefficients w_n $(n = 1, 2, \cdots, N_a - 1)$ are randomly generated, while the last coefficient is calculated to compensate for the received signal at Bob to maintain the intended symbol s, yielding

$$x_{N_a}^* = 1 - \sum_{n=1}^{N_a - 1} h_n w_n^*. \tag{81}$$

The AFF scheme facilitated the derivation of an exact secrecy rate expression for the single-antenna-Eve scenario, and a lower bound of the secrecy rate was derived for the multi-antenna-Eve case. Furthermore, a comparison between the AFF scheme and the AN scheme revealed that their relative advantages depended on the number of antennas held by Alice and Eve, i.e., when Eve has more antennas than Alice, the AFF scheme achieves a larger secrecy rate; otherwise, the AN scheme outperforms AFF.

A robust AN-aided SRM problem was considered in [176], assuming perfect CSI of Bob's channel but imperfect CSI of non-colluding MSA Eves. This scenario led to the formulation of an SRM problem with the objective of maximizing the worst-case secrecy rate by jointly designing the signal covariance $\mathbf{W}$ and the AN covariance $\mathbf{\Sigma}$ as

$$\max_{\mathbf{W},\mathbf{\Sigma}} \min_{k} R_b - \max_{\|\mathbf{\Delta g}_k\| \leq \epsilon_e} R_{e,k} \tag{82a}$$

$$\text{s.t. } \mathrm{Tr}\left(\mathbf{W} + \mathbf{\Sigma}\right) \leqslant P, \tag{82b}$$

$$\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}, \tag{82c}$$

where $\mathbf{\Delta g}_k$ represents the deterministic uncertainty model for k-th Eve similar in (75). To overcome the challenge brought by the CSI uncertainty, a reformulation was employed and the worst-case SRM problem was tackled by implementing a one-dimensional line search.

An AN-aided SRM problem was addressed in [177], assuming perfect CSI of Bob but imperfect CSI of non-colluding MSA Eves. The authors considered the design of the transmit covariance $\mathbf{W}$ and AN covariance $\mathbf{\Sigma}$ under an achievable secrecy rate maximization formulation. Unlike the approach in [176], the stochastic CSI uncertainties associated with Eves in [177] were handled using an outage-based formulation.

In the study presented in [178], the SOP was employed as a metric to characterize the secrecy performance. This study assumed the perfect CSI of Bob but lacked the CSI of non-colluding MSA Eves. Based on the SOP, a security region was defined, offering a spatial perspective on security.

In [179], a semi-adaptive generalized AN scheme was proposed for MISOSE with the instantaneous CSI of Bob and the statistical CSI of non-colluding MSA Eves. The semi-adapative scheme fixes the achievable rate for Bob while it adaptively adjusts the secrecy rate and the power-allocation ratio based on the legitimate channel's CSI in order to maximize the secrecy rate.

The authors of [180] addressed the scenario of MISOME, where perfect CSI of Bob is available, along with either perfect or imperfect CSI of non-colluding MMA Eves. They focused on the SRM problem by jointly optimizing the transmit and AN covariance matrices. With the perfect CSI of Eves, the SRM problem was formulated as

$$\max_{\mathbf{W}\succcurlyeq\mathbf{0},\mathbf{\Sigma}\succcurlyeq\mathbf{0},\beta\geqslant 1} C_b(\mathbf{W},\mathbf{\Sigma}) - \log\beta \tag{83a}$$

$$\text{s.t.} C_{e,k}(\mathbf{W},\mathbf{\Sigma}) \leqslant \log\beta, \quad \forall k \in \mathcal{K}, \tag{83b}$$

$$\mathrm{Tr}(\mathbf{W}+\mathbf{\Sigma}) \leqslant P, \tag{83c}$$

$$\mathrm{Tr}(\mathbf{\Phi}_l(\mathbf{W}+\mathbf{\Sigma})) \leqslant \rho_l, \forall l \in \mathcal{L}, \tag{83d}$$

where β is the introduced slack variable.

In summary, in MISO systems, the existence of null space provides convenience for the generation of orthogonal AN, but the design of non-orthogonal AN based on the knowledge of wiretap channel is still worthy of attention and research.

F. AN-aided mMIMO

Due to the fact that the growth in the number of antennas at Alice enhances the DoF for AN, the AN-aided secure downlink transmission in mMIMO systems has sparked great research enthusiasm [181]–[185].

To address the SRM problem for mMIMO systems, an AN-assisted scheme was proposed in [181] through optimizing the power allocation strategies for two distinct cases, which is, the case both Alice and Eve know the CSI of Bobs and the opposite case. The k-th Bob allocates a portion of α_k of its power to transmit the information-bearing signal, while the rest is used for AN transmission. Additionally, the authors proposed the optimization problem of power allocation between AN and data symbols with the objective of maximizing the secrecy rate. Within each case, the authors also considered whether the accurate position of Eve is known to Alice. Furthermore, the study delved into the impacts of the non-ideal factors, including the channel estimation error and the uncertainty of Eve's position, on the power allocation strategies.

In a multicell mMIMO system, the study in [182] focused on secure downlink transmission scenarios where the numbers of Alice's, Bobs', and Eve's antennas tend toward infinity. It is assumed that Eve's CSI is not available at Alice, so linear data precoding and AN are used to enhance confidentiality. Furthermore, to balance complexity and performance, they proposed linear precoder $\mathbf{F}_n$ for n-th BS based on matrix polynomials as

$$\mathbf{F}_n = \frac{1}{\sqrt{N_T}} \hat{\overline{\mathbf{H}}}_{nn}^H \sum_{i=0}^{\mathrm{J}} \mu_i \left(\hat{\overline{\mathbf{H}}}_{nn} \hat{\overline{\mathbf{H}}}_{nn}^H \right)^i, \tag{84}$$

where $\hat{\overline{\mathbf{H}}}_{nn} = \hat{\mathbf{H}}_{nn}/\sqrt{N_T}$, and $\boldsymbol{\mu} = [\mu_0, \ldots, \mu_{\mathcal{J}}]^T$ are the real-valued coefficients of the precoder matrix polynomial which were optimized to minimize the sum of mean-squared

errors and AN leakage to Bobs in the cell by using tools from free probability and random matrix theory. Finally, the analytical and simulation results provided interesting insights for the design of secure multicell massive MIMO systems and revealed that the proposed polynomial data and AN precoders closely approach the performance of selfish RCI data and null-space-based AN precoders, respectively.

In [183], two AN-aided schemes were proposed to secure a mMIMO network with the imperfect CSI of Bob and without the CSI of Eve. In the first scheme, AN was injected into the downlink training signals to prevent Eve from accurately estimating its channel. In the second scheme, AN was utilized in both the downlink training phase and the payload data transmission phase to further deteriorate Eve's channel quality. It was found that deploying AN in the downlink training phase of massive MIMO networks has no impact on the channel estimation process at Bobs while suppressing the channel estimation process at Eve. Besides, implementing AN in both phases provided a flexible solution to improve its secrecy performance, albeit at the price of higher complexity.

For the sake of minimizing system complexity and reducing channel estimation overhead, a low-complexity beamforming and AN scheme was presented in [184] for mMIMO systems over the Ricean fading channel. The AN scheme using only the specular component is described as

$$\mathbf{x} = \sqrt{p}\mathbf{W}\mathbf{s} + \sqrt{q}\mathbf{V}\mathbf{z} = \sum_{i=1}^{K} \sqrt{p}\mathbf{w}_i s_i + \sum_{i=1}^{M-K} \sqrt{q}\mathbf{v}_i z_i, \quad (85)$$

where p and q are the transmit data power and AN signal power. In addition, a tractable closed-form lower bound for the achievable ESR was derived, while the optimal power allocation was determined through asymptotic analysis with the aim of maximizing the achievable ESR. The analytical results revealed that the ESR improves as the increase of Ricean factor increases and converges to a specific constant as the number of antennas at Alice increases.

In the context of mMIMO-NOMA networks, the authors of [185] examined an AN scheme utilizing minimum mean-squared-error estimated CSI. In the training phase, the BS uses the minimum mean-squared-error estimated technique to estimate the CSI. After the training phase, the precoder vector and the null-space AN vector are obtained through the estimated CSI. Following this, the authors proceeded to derive the ESR and proposed a joint power allocation strategy to maximize the ESR. The results indicated that the combination of the mMIMO technique and AN significantly enhances the secrecy performance of NOMA networks.

In summary, in mMIMO systems, AN-assisted downlink transmission techniques are widely used because the substantial increase in the number of transmit antennas provides a large number of spatial degrees of freedom, among which the design of precoding matrices and the optimization of power allocation need to be widely studied.

G. AN-aided NOMA

NOMA has been envisioned as a promising multiple-access technique to improve spectral efficiency and support extensive connectivity in forthcoming wireless networks. To tackle the security concerns inherent in NOMA, the integration of AN with NOMA has garnered growing interest, as highlighted in various studies such as [186]–[189]. As shown in Fig. 12, a specific user treats the remaining users' signals as interference and performs the successive interference cancellation to demodulate its own signal. At the same time, the AN is injected into the null space of the overall channel to avoid overlapping effects on the demodulation of multiple users.

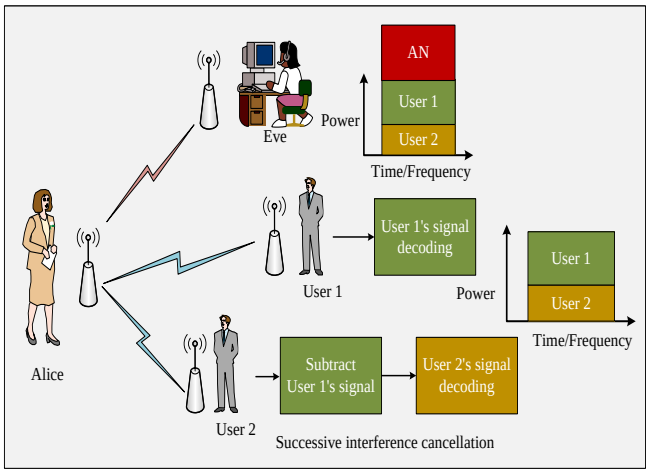

Fig. 12. The principle of AN-aided NOMA.

Concretely, Ref. [186] proposed a new two-phase FD-based AN scheme for NOMA in single-input multiple-output single-antenna-eavesdropper (SIMOSE) systems, with various relay selection methods, enabling simultaneous communicate with both a multi-antenna near-user and a far-user, where multiple FD DF relays are employed. In the first phase, using the NOMA technique, Alice conveys the information-bearing signal $s = \sqrt{\alpha_1}s_1 + \sqrt{1-\alpha_1}s_2$ to the near-user, where s_2 is the signal for the far-user that cannot be directly delivered. Meanwhile, the chosen relay R_i emits the AN v to confuse Eve with power P_1

$$\begin{aligned} \mathbf{y}_1 &= \sqrt{P_s}\mathbf{h}_{ab_1}s + \sqrt{P_1}\mathbf{h}_{ib_1}v + \mathbf{n}_{b_1}, \\ z_1 &= \sqrt{P_s}g_{ae}s + \sqrt{P_1}g_{ie}v + n_e, \end{aligned} \quad (86)$$

where $\mathbf{h}_{ab_1}$ denotes the CSI between Alice and the near-user, $\mathbf{h}_{ib_1}$ represents that between the chosen relay and the near-user, g_{ae} denotes that between Alice and Eve, and g_{ie} represents that between the chosen relay and Eve. In the second phase, the selected relay performs exclusive OR (XOR) operation on the message intended for the far-user and the AN before broadcasting the combined signal

$$\begin{aligned} y_2 &= \sqrt{P_2}\mathbf{h}_{ib_2}\left(s_2 \oplus v\right) + n_{b_2}, \\ z_2 &= \sqrt{P_2}g_{ie}\left(s_2 \oplus v\right) + n_e, \end{aligned} \quad (87)$$

where $\mathbf{h}_{ib_2}$ denotes the CSI between the chosen relay and the far-user. By utilizing the null-space beamforming, self-interference cancellation techniques, and the DF-XOR cooperative protocol, the scheme efficiently eliminated the AN at the

near-user, far-user, and the selected relay, while simultaneously impairing the decoding capability of Eve.

Moreover, an examination of the SOP was conducted in [187] for a large-scale downlink system featuring FD NOMA transmission supported by AN, where MSA Bobs are randomly distributed according to a homogeneous Poisson point processes in the presence of a certainly located single-antenna Eve. A secure cooperative communication scheme was proposed, in which nearby NOMA users operating in FD mode served as jammers, generating pre-shared pseudo random AN to enhance the PLS. Closed-form expressions in terms of the SOP for a user pair were acquired.

Additionally, the authors of [188] explored the integration of reconfigurable intelligent surface (RIS) and NOMA. Since Eve may enjoy similar performance gains brought by RIS as Bobs, an AN strategy was proposed to maximize the secrecy rate. The study revealed that the proposed strategy offers superior secrecy performance while requiring less AN power in comparison to the benchmark schemes. Meanwhile, the authors observed that increasing the number of RIS elements could reduce AN power, although this effect diminished as the number of RIS elements grew sufficiently large. Furthermore, they noted that an increase in the number of transmit antennas reduce AN power when Eve is in close proximity to Alice, but AN power increases when Eve is at a greater distance.

Furthermore, the study presented in [189] delved into an AN-aided beamforming scheme for MISO-NOMA systems as

$$\begin{aligned} y_i &= \mathbf{h}_i \mathbf{w}_i x + n_i,\ i = 1,\ 2, \\ \mathbf{y}_e &= \mathbf{G}\mathbf{w}_1 x + \mathbf{G}\mathbf{V}\mathbf{r} + n_e, \end{aligned} \tag{88}$$

where $x = \sqrt{\alpha_1 \phi} s_1 + \sqrt{(1-\alpha_1)\,\phi} s_2$, $\mathbf{w}_1$ denotes the beamforming for transmit signal, $0 < \phi < 1$ represents the power allocation for information-bearing signal, $1-\phi$ is the power of AN $\mathbf{Vr}$, while α_1 and $1-\alpha_1$ stand for the power coefficients for users 1 and 2, respectively. Emphasizing the practical scenario of the imperfect worst-case successive interference cancellation which is a distinctive characteristic in NOMA transmission, the authors derived a closed-form expression for the SOP to quantitatively represent the secrecy performance.

Generally, the deployment of AN in NOMA not only requires balancing the trade-off between the information-bearing signal and AN, but also demands allocating the power of different symbols for multiple users to satisfy the well-known successive interference cancellation technology.

H. AN-aided OFDM

Despite its utility, many AN techniques cannot be applied to MIMO systems when Alice has fewer antennas than Bob, which is due to null space constraints. However, in scenarios where the spatial DoF is non-existent, AN can be implemented in the time domain, a concept extensively explored in OFDM systems. Specifically, a time-domain AN generation technique was considered in [190] for SISO-OFDM systems, which assumes OFDM as the transmission scheme, and generates AN in a different time slot by exploiting the redundancy derived from CP. This approach was extended to MIMO-OFDM in [43], where the time-domain AN also resides in a null space of the time-domain channel, which can be expressed as a Toeplitz matrix. Since this method uses the DoF derived from the CP, the constraint becomes $N_a\,(1 + N_{CP}/N) > N_b$, where N_{CP} is the length of CP, and N is the number of inverse fast Fourier transform points. For the design of time-domain AN, researchers in [191]–[193] explored cases involving discrete inputs, multi-user OFDM channels, and AF relay systems, respectively. Moreover, note that time-domain and spatial-domain AN techniques can be combined in MIMO-OFDM systems [194] to introduce additional optimization dimensions [195]. Furthermore, the authors of [196] proposed a frequency-domain AN-aided key generation transmission strategy for SWIPT in OFDM access systems, while the authors of [197] assumed a shared AN signal scheme for hybrid parallel power-line/wireless OFDM communication systems.

In [190], AN-aided PLS was studied for SISO-OFDM systems, where temporal AN is injected in the time domain by exploiting the cyclic prefix CP. The impact of channel delay spread, CP length, power allocation, and precoder design on secrecy performance was analyzed. Notably, even without Eve's instantaneous CSI, the proposed scheme achieved secrecy rates close to the full-CSI scenario.

Ref. [191] studied an AN design for OFDM wiretap channels with discrete inputs. The authors formulated an SRM problem under a power constraint and showed how subcarrier power could be optimized accordingly. To further improve secrecy, a novel time-domain AN scheme was proposed, leveraging the CP to inject AN within the null space of the legitimate channel, effectively exploiting temporal degrees of freedom without affecting Bob's reception.

The authors of [192] introduced a time-domain AN to an OFDM wiretap channel with multiple Bobs and a single-antenna Eve. The authors formulated a SSR maximization problem involving subcarrier allocation, power allocation, and AN design. They first optimized subcarrier allocation, then used a low-complexity Lagrange dual method for joint power and AN optimization. Simulation results validated the effectiveness of the proposed approach.

In [193], a time-domain AN scheme was proposed for an OFDM relay system, where Alice transmits AN-bearing signals to the relay, while the destination simultaneously sends jamming signals to disrupt eavesdropping. In the amplify-and-forward phase, the relay forwards the received signal to the destination. To maximize secrecy rate, joint power allocation for Alice and the destination was optimized. An iterative inner convex approximation algorithm was developed to efficiently solve the resulting non-convex problem.

For MIMO-OFDM systems in the presence of SMA Eve, hybrid AN injection along the temporal and spatial dimensions was investigated in [194]. In the novel hybrid spatial and temporal AN design, the data is precoded in the frequency domain, and then data-spatial AN is injected into the direction orthogonal to the data vector. After performing IFFT variations and adding CP to the data-spatial AN, the signal sent by Alice was formulated by

$$\mathbf{s}_A = \mathbf{T}^{cp}\mathbf{F}^H \mathbf{P}_{N_A}(\mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{d}^s) + \mathbf{Q}\mathbf{d}^t, \tag{89}$$

where $\mathbf{P}_{N_A}$ is a permutation matrix that rear-ranges the precoded subcarriers, $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{Q}$ are the precoders of information-bearing signal, spatial AN, and temporal AN. $\mathbf{d}^s$ and $\mathbf{d}^t$ are the spatial AN vector and the temporal AN vector modeled as complex Gaussian random vectors. Assuming that Alice knows the perfect CSI of Bob but does not know the instantaneous CSI of the passive Eve, the closed-form expressions for the secrecy rate and average secrecy rate are derived, focusing on the asymptotic case with a large number of transmit antennas.

In the presence of MMA passive Eves, an existing AN technique was extended to MIMO-OFDM systems in [195]. A multi-carrier optimization problem was formulated to jointly design the transmit beamforming and AN covariance matrices, ensuring reliable transmission to the legitimate user while limiting information leakage to Eves.

Ref. [196] proposed a frequency-domain AN strategy for OFDM-based SWIPT systems to enhance PLS while ensuring energy harvesting at energy receivers. The authors formulated a weighted sum secrecy rate maximization problem involving power allocation, subcarrier assignment, and power splitting. Due to the non-convexity of the problem, they developed a Lagrange duality-based solution along with a low-complexity suboptimal algorithm.

The authors of [197] introduced a novel AN scheme for indoor hybrid power-line/wireless OFDM systems, where Bob shares AN with Alice to enhance security against SSA Eve. Bob first transmits low-SNR AN to Alice, which is then amplified and combined with data for transmission back to Bob over high-SNR subchannels. The study also examined how transmit power and power allocation affect secure throughput under both one-link and two-link eavesdropping scenarios.

In summary, for OFDM systems, the introduction of time-domain AN promotes the diversity of AN generation methods. Furthermore, the combination of spatial-domain AN and time-domain AN deserves the attention of scholars in the future.

I. AN-aided PLA

Authentication technology plays a crucial role in maintaining secure communication, particularly in wireless environments, by allowing trusted users to verify the source of received transmissions. However, conventional authentication methods are typically implemented through cryptographic protocols in the MAC layer or above, which suffer from the disadvantage of the need for secret keys, the absence of information-theoretic guarantees, and the inability to provide covertness in contrast to physical layer authentication (PLA). The authors of [198] highlighted the potential of using AN to further obscure the message authentication code tag, thereby achieving information-theoretic security in PLA. They observed that AN significantly enhances security, with diminishing returns when the quality of CSI knowledge is poor. Additionally, the authors of [199] demonstrated that AN-aided message authentication code can effectively resist key recovery attack, and they also proposed an AN-aided physical-layer phase challenge-response authentication scheme for practical OFDM transmission in [200]. Furthermore, the authors of [201] explored the use of AN added to received signals in message frames to enhance authentication performance in the presence of time-variant channels.

In the fingerprint embedding authentication framework, the authors of [198] explored whether AN still improves security with only imperfect CSI available at Alice and Bob. Their findings indicated that diminishing returns in terms of security improvements when the quality of CSI knowledge is poor.

To construct new message authentication codes, the authors of [199] introduced AN-aided message authentication codes. By formulating key recovery as a channel coding problem, the tag generation process is viewed as encoding a shared key using a message-specified code. The authors showed that AN can effectively resist key recovery attacks, even in scenarios where Eve has unlimited computational resources.

Ref. [200] proposed an AN-aided physical layer phase challenge-response authentication scheme for OFDM systems. Using Tikhonov-distributed AN to protect phase-modulated keys, this scheme involves Alice sending a plot signal for Bob to estimate subcarrier phases, followed by Bob responding with a tagged signal embedding both the key and AN.

The authors of [201] presented a CSI-based PLA method to counter spoofers with distinct spatial features. Under time-invariant channels, binary hypothesis testing was performed via power spectral density comparisons, while the use of AN was explored to enhance robustness in time-varying scenarios.

In a nutshell, in PLA systems, the role of AN is to increase the number of times that a single shared key can be used before being compromised. However, in practice, imperfect CSI caused by channel estimation errors, channel-constrained feedback, and delayed feedback may make AN generation more complicated.

J. AN-aided RIS

The RIS, also known as the intelligent reflecting surface, has arisen as a potential candidate for the upcoming 6G wireless communications. Since the reflecting elements on RIS can manipulate the phase shifts of reflected signals, RIS benefits from considerable multi-path diversity gains without the expense of expensive hardware requirements. With the integration of RIS, AN can improve secrecy performance more effectively. As can be inferred from Fig. 13, due to the introduction of RIS reflecting link, the joint design of transmit beamforming with AN and RIS phase shifts becomes a novel question for the AN-RIS systems [202]–[207].

First of all, the authors of [202] examined the effectiveness of AN in improving secrecy rates in RIS-assisted systems, where a RIS near single-antenna Bob helps SMA Alice communicate securely in the presence of multiple-antenna Eves. A joint optimization problem of transmit beamforming, AN, and RIS phase shifts was formulated and solved via an AO algorithm. Results showed that AN significantly enhances secrecy, especially when many Eves are located near the RIS.

In [203], a RIS-assisted AN-aided secure MIMO system was studied, where Alice, Bob, and Eve have multiple antennas and full CSI is known at Alice. The secrecy rate maximization problem was solved by jointly optimizing the

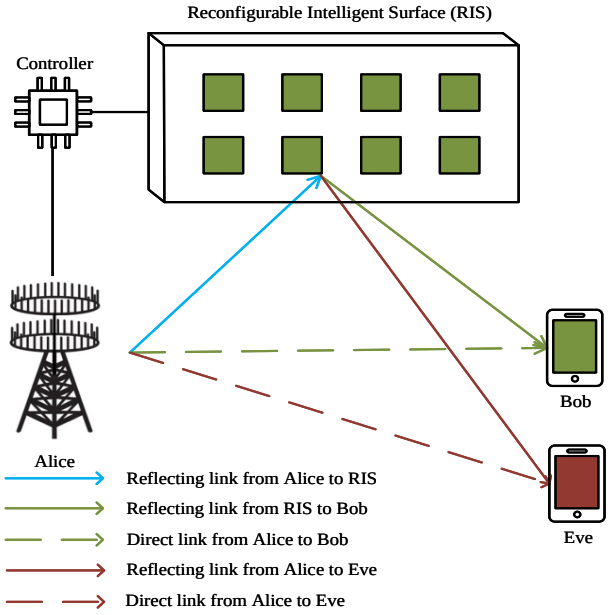

Fig. 13. Framework of the AN-aided RIS wireless secure communications.

transmit precoding, AN covariance, and RIS phase shifts using a BCD algorithm, with Lagrangian and majorization-minimization (MM) methods for subproblems. The approach was also extended to a multi-Bob scenario.

To enhance the security of intelligent omni surfaces (IOS), which support both reflection and refraction, AN-aided beamforming was proposed in [204]. The SRM problem involving beamforming, AN, and IOS phase shifts was formulated under power and unit-modulus constraints. A BCD algorithm was used to solve it, with the Lagrangian dual method for beamforming and AN design, and QCQP for IOS phase shifts.

Additionally, the authors of [205] enhanced security in RIS- and AN-assisted mobile-edge computing (MEC) for IoT. By optimizing RIS phase shifts, receive beamforming, AN covariance, offloading time, transmit power, and local computing, they minimized Bobs' secure energy consumption. The nonconvex problem was solved via alternating optimization combining SDR and Dinkelbach's method.

In [206], the authors studied RIS-assisted MISO systems without Eve's CSI. To enhance security under a total power constraint, they proposed a joint beamforming and jamming scheme. The optimization involved minimizing Alice's transmit power while ensuring Bob's QoS, formulated by

$$\min_{\mathbf{w},\mathbf{\Phi}} P_T \tag{90a}$$

$$\text{s.t.} \left| \left(\mathbf{h}_{IB}^H \mathbf{\Phi} \mathbf{H}_{AI} + \mathbf{h}_{AB}^H\right) \mathbf{w}\right|^2 / {\sigma_b}^2 \geqslant \gamma, \tag{90b}$$

where $\mathbf{w}$ is the beamforming vector, $\mathbf{\Phi}$ is the phase shift matrix of RIS. $\mathbf{h}_{IB}$, $\mathbf{h}_{AB}$, $\mathbf{H}_{AI}$ represent the channel from RIS to Bob, from Alice to Bob, and from Alice to RIS, respectively. σ_b^2 denotes the noise power at Bob side. This non-convex problem was addressed by using maximum ratio transmission (MRT) beamforming to maximize Bob's channel gain, solved via oblique manifold (OM) or MM algorithms. The leftover power at Alice was then used to generate AN in Bob's null space. Simulation results showed both algorithms have complexity $\mathcal{O}\left(N^2\right)$ per iteration, with OM requiring more iterations but achieving better performance.

In the context of RIS-MISO systems where Eve's CSI is unavailable, an AN-aided beamforming scheme was considered in [207]. Similar to [206], the MRT beamforming was adopted in [207], and the channel gain maximization problem was cast to optimize the phase shift matrix of RIS as

$$\max_{\phi_n} \left\| \mathbf{h}^H \mathbf{\Phi} \mathbf{H} + \mathbf{g}^H \right\|^2, \tag{91a}$$

$$\text{s.t.} \left| e^{j\phi_n} \right| = 1, \tag{91b}$$

where $\mathbf{h}$, $\mathbf{H}$, and $\mathbf{g}$ represent the reflect and direct channel. For the sake of alleviating the computational complexity, an alternating direction (AD) algorithm was invoked by determining a specific RIS unit through a closed-form solution while keeping the other configurations fixed. By taking the first-order derivative of (91), the closed-form expressions for the optimal phase shift can be given by

$$\phi_n^1 = \arctan\left[(C-D)/(E+F)\right], \tag{92}$$

$$\phi_n^2 = \arctan\left[(C-D)/(E+F)\right] + \pi, \tag{93}$$

where the specific expression of C to E can be found in [207]. The results from numerical simulations demonstrated that the AD algorithm exhibits faster and more stable convergence compared to the OM method, while maintaining the same level of computational complexity as OM for each iteration.

In a nutshell, the challenge of deploying AN in RIS lies in optimizing its use to enhance security without compromising system performance. Although AN improves communication privacy, it requires precise control to avoid degrading signal quality. Future trends are likely to focus on developing advanced algorithms and machine learning techniques to dynamically adapt real-time network conditions. This will ensure that RIS can effectively balance security and performance while adapting to varying communication needs.

K. AN in SISO

Since the SISO systems dissatisfy the requirement of equipping more antennas at the transmitter than at the receiver, the null space of the channel is non-existent, so that the space-domain AN cannot be directly used [208]–[212]. Therefore, common AN schemes in SISO may adopt novel protocols to relieve the impact of AN on Bob, including retransmission operations [208]–[210] or improving the signal processing capability of Bob [211], [212].

In [208], a novel time-domain AN strategy was proposed for single-antenna point-to-point systems over multi-path fading channels. This strategy was designed for not only confusing Eve, but also compensating inter-symbol interference arising from the multi-path propagation effects, i.e.,

$$\sum_{l=1}^{L} |h_l|^2 r_n + \text{ISI}_n = 0, n = 1, 2, \cdots, N, \tag{94}$$

where N denotes the total number of symbols in a frame, while h_l represents the CSI of the l-th fading path. The study evaluated the performance of this AN strategy by analyzing its impact on effective capacity and spectral efficiency. Additionally, it considered the tradeoff between these two metrics to formulate the achievable data rate of the proposed scheme, enabling the optimization of the design of the CP for enhanced system performance.

The authors of [209] proposed a joint physical/MAC layer security scheme combined automatic-repeat-request (ARQ) with adaptive AN that does not rely on null-space constraints. Upon retransmission requests, an AN-canceling signal is added to enable suppression via MRC. The authors derived secure throughput formulas and showed the scheme also reduces PAPR and out-of-band emissions in OFDM systems.

In [210], a joint AN and repetition coding scheme with TDD protocol was designed for single-input single-output multiple-antenna-eavesdropper (SISOSE) systems. The transmission of the private information is divided into two time slots, where Alice sends a jamming-injected signal in the first slot and sends another well-designed jamming-injected signal in the second slot as

$$r_2 = -h_1 r_1 / h_2. \tag{95}$$

By combining two signals at Bob, the influence of AN can be removed. Besides, the achievable secrecy rate was maximized by deriving the optimal power allocation with the proposed scheme.

For SISOSE over quasi-static fading channels, a novel AN injection scheme was proposed in [211], in which an HD Bob broadcasts pseudo-random AN r to Alice in phase 1 as

$$y_{a,1} = \sqrt{P_b} h_b r + n, \tag{96}$$

while Alice forwards the received signal from phase 1 along with the information-bearing signal to Bob in phase 2 as

$$x = \sqrt{\alpha} s + \sqrt{1-\alpha} y_{a,1} / \left| y_{a,1} \right|, \tag{97}$$

where $y_{a,1}$ denotes the signal received by Alice from phase 1, α represents the power allocation parameter between the information-bearing signal and the AN, h_b stands for the CSI in phase 1, while s and r are information-bearing signal and the AN, respectively. Since Bob knows the AN he generated in phase 1, he can cancel its effect in phase 2. The scheme's performance was analyzed via SNR, SOP, outage probability, and throughput, with optimal power allocation derived to maximize throughput under SOP and outage constraints.

The authors of [212] proposed a reference-free AN waveform design and cancellation scheme for SISOSE. Specifically, the reference-free AN was generated at Alice by extracting the sign information of each information-bearing signal as

$$r = \sqrt{P_r/2} \left\{ \text{sign}\left[\text{Im}\left(s\right)\right] + j\text{sign}\left[\text{Re}\left(s\right)\right] \right\}, \tag{98}$$

where $\text{sign}\left(\cdot\right)$ represents the sign function of a real number, while $\text{Im}\left(\cdot\right)$ and $\text{Re}\left(\cdot\right)$ denote the imaginary and real parts of a complex number, respectively. Bob can reconstruct and cancel this reference-free AN by subtracting it from the received signal. The authors derived the AN cancellation performance and secrecy capacity at Bob, along with their upper bounds.

In a word, since SISO cannot provide enough spatial DoFs, the application of AN in SISO is primarily categorized into two approaches, namely, adding AN in different time slots or pre-sharing the knowledge of AN to Bob. Therefore, researchers are expected to address the ensuing problems of reduced spectral efficiency and increased computational complexity.

L. AN-aided SM

The spatial modulation (SM) is heralded as an emerging MIMO approach, which activates only an antenna in each time slot and uses the index of the activated antenna to convey additional information, which owns the merit of reduced implementation complexity. As a PLS of the spatial domain, the AN has the potential to combine with the SM, which has also been investigated in several literature [213]–[216].

Due to the incompatibility between AN and SM in antenna usage modes, the research of artificial-noise-aided spatial modulation (AN-SM) encounters many difficulties. Specifically, in order to improve the security of SM, a secure unitary coded spatial modulation (UC-SM) scheme was proposed in [213]. However, the UC-SM scheme only supports a single receive antenna and transmits the same information in two time slots to eliminate the interference of AN, which lowers the spectral efficiency. Hence, an AN-SM scheme was proposed in [214]. In the conventional SM scheme, only one antenna is activated, thus only one active RF chain is required at the transmitter. In order to improve the security of SM, AN was added to all the transmit antennas, which means that the AN-SM has to activate all the transmit antennas otherwise it cannot eliminate the interference of AN. Furthermore, the scheme was optimized in [216] for MISO transmission by activating two antennas, where only an antenna is additionally activated. To address the incompatibility between AN and conventional SM, the combination of AN and GSM has emerged [51], [217]. As the extension of SM, the GSM activates more than one transmit antenna, which naturally solves the original incompatibility problem.

In order to prevent eavesdropping in MISO systems, a secure UC-SM was proposed in [213] to achieve a second-order transmit diversity by using a single RF chain at two time slots. Specifically, SM combined with unitary codes was designed to provide a second-order diversity at the desired receiver, where the AN in two time slots α_1 and α_2 satisfies the cancellation criterion, i.e.,

$$h_{t_1}\alpha_1 + h_{t_2}\alpha_2 = 0. \tag{99}$$

It was shown that the proposed scheme outperforms the existing secure SM scheme at the cost of spectral efficiency as transmitting the same signal at two time slots.

In [214], the secrecy performance of AN-SM over Rayleigh channels with imperfect CSI was analyzed. Closed-form lower bounds and approximations for ESR were derived. Results showed imperfect CSI reduces ESR due to estimation errors. However, unlike conventional SM, AN-SM activates all transmit antennas, increasing RF chain requirements.

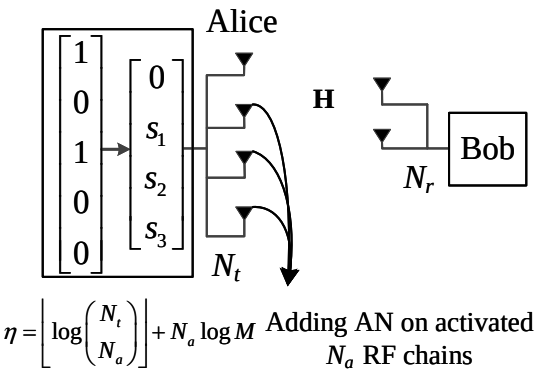

Fig. 14. Framework of AN-aided GSM wireless secure communications.

The authors of [215] studied a secure transmission using differential quadrature spatial modulation (DQSM) with a multi-antenna CJ for MISO wiretap channels. Alice uses a single RF chain, shifting antenna costs to the CJ, requiring perfect synchronization. The authors derived closed-form expressions for SOP and secrecy throughput under passive and active Eve scenarios. Simulations showed that increasing transmit power at Alice or CJ improves secrecy up to a point, beyond which performance degrades.

Ref. [216] proposed a combination of AN and antenna selection for the SM system. Specifically, Alice first chooses antennas for SM, and then, Alice transmits an AN through the active antenna. At the same time, another one of the remaining antennas was activated to transmit another AN. The ANs were designed by exploiting the CSI of Bob, and can only be canceled at Bob as

$$h_j \beta_1 v + h_i \beta_2 v = 0, \tag{100}$$

where v is zero-mean unit-variance complex Gaussian AN, h_j and h_i denotes the CSI for the j-th and i-th antennas, respectively, while the coefficient $\beta_2 = -h_j/h_i$ is designed to cancel the AN at Bob. Furthermore, the secrecy rate of the proposed scheme was analyzed. Note that the proposed scheme just requires two activated transmit antennas, which means the incompatibility between AN and conventional SM still exists because the single RF chain required by SM is unattainable.

For the sake of alleviating the incompatibility between AN and conventional SM, the AN was first introduced to GSM systems [51]. As the extension of SM, the GSM activates more than one transmit antenna, which naturally solves the original incompatibility problem by introducing a sparse null-space matrix corresponding to the index of activated antennas

$$\mathbf{V}\left(\mathbf{x}_{l_x}, :\right) = \mathbf{V}_0, \tag{101}$$

where $\mathbf{x}_{l_x}$ denotes the indices of activated antennas and $\mathbf{V}_0$ is the null space of the active antenna channel.

As shown in Fig. 14, GSM systems activate N_a antennas and are similar to SM using the index to convey additional information bits. Thus, the AN is only added on the activated antennas, which avoids the incompatibility problem in SM.

Besides, a novel power minimized artificial noise (PMAN) was proposed in [51] to improve the power efficiency while maintaining the jamming effect of AN as

$$\mathbf{r} = -\mathbf{V}_0^H \mathbf{s}^i. \tag{102}$$

where $\mathbf{s}^i$ denotes the GSM-modulated information-beraing signal. The power optimization ratio of PMAN was analyzed, while the theoretical bounds of the BER for both Bob and Eve were derived.

Based on a BD algorithm, a secure downlink multi-user GSM system with AN was investigated in [217]. Specifically, the AN matrix was expressed as

$$\mathbf{V} = [\mathbf{I}_{N_t} - \mathbf{H}^H \left(\mathbf{H}\mathbf{H}^H\right)^{-1} \mathbf{H}]. \tag{103}$$

Particularly, the proposed MU-GSM system can achieve satisfying security performance even without AN, which is different from the single-user scenario. Finally, the simulation results showed that with AN protection and BD, the PLS can be significantly enhanced when compared with the random noise scheme and the multi-user precoding-aided SM.

In summary, the introduction of AN in the SM system may require an increased RF chains at the Alice, which needs attention from relevant researchers.

V. Challenges and Road Ahead

A. Limited Training and Feedback

1) Challenge

As indicated in [29], the AN technology desires for the perfect CSI between Alice and Bob, which requires Bob to achieve perfect channel estimation based on pilot training and provide perfect channel feedback based on infinite feedback resources. However, both perfect training and perfect channel feedback are unattainable in practical applications and bring vitality to the research of limited training and limited channel feedback. In practice, CSI is usually obtained through training-based receiver channel estimation and fed back to Alice, which is not perfect due to the estimation error.

2) Current Status

In such scenarios, it is important to investigate the optimal resource tradeoff between the training phase and data transmission phase to maximize the secrecy rate [218]. By maximizing the achievable secrecy rate, the power allocation between signal and AN in both training and data transmission phases can be proposed for AN-assisted training-based schemes [219].

Similarly, the channel estimation error [220] and quantized channel feedback [221] always bring imperfect CSI. For instance, with the statistics CSI of Eve, the authors of [52] proposed a lower bound on ergodic secrecy capacity of the MIMOME wiretap channel. Their analysis showed the lower bound asymptotically matches the secrecy capacity as feedback bits and AN power approach infinity.

Furthermore, it has been observed in [222] that enforcing stringent secrecy outage constraints puts higher requirements in terms of the number of feedback bits and the strength

of the intended channel. For the sake of revealing the impact of the quantized channel feedback [223], several studies focused on the AN schemes with limited feedback [224]–[228]. Specifically, the authors of [223] revealed that only when quantized channel direction is available, the AN that was originally intended to jam Eve may not leak into Bob's channel. In addition, the study in [224] emphasized that the channel estimation error can drastically reduce the secrecy sum-rate, and more power needs to be allocated for AN when the channel estimation error grows larger.

The impact of quantized channel feedback on the secrecy capacity achievable with AN was studied [221], revealing that the number of feedback bits must increase logarithmically with the transmission power to maintain consistent performance levels. Encouragingly, the authors of [225] demonstrated that, for sufficiently high transmit power, a positive secrecy capacity can still be attained, thereby addressing the challenge of unfavorable CSI at Bob compared to Eve.

In order to enhance the secrecy performance with limited feedback, researchers in [226] proposed a novel on-off transmission scheme to perform secure transmission and derive a closed-form expression for the secrecy throughput. Moreover, the authors of [227] presented an adaptive transmission strategy that judiciously selects the wiretap coding parameters, as well as the power allocation between the AN and the information signal. Their simulation results indicated that allocating approximately 20% of the feedback bits to quantize channel gain information, with the remainder for channel direction quantization, yields robust performance irrespective of secrecy outage constraints. Additionally, they found that 8 feedback bits per transmit antenna achieve approximately 90% of the throughput achievable with perfect feedback. In the context of multi-cell multi-antenna networks, coordinated beamforming was employed in [228] for multiple BSs with the assistance of limited feedback AN beamforming.

3) Future Direction

However, current methods primarily emphasize resource allocation challenges in the context of conventional AN scheme, whereas neglect the exploration of near-optimal channel estimation approaches and the associated optimization problems for AN. Consequently, there is a pressing need to address these underexplored areas, particularly focusing on the development of low-complexity yet near-optimal channel estimation methods within the framework of AN. Furthermore, the AN optimization in the presence of channel estimation errors should be paid more attention, along with the theoretical analysis on the influence of channel estimation errors on AN. These issues constitute vital dimensions in the domain of AN and deserve significant attention from researchers and practitioners alike.

B. Channel Correlation

1) Challenge

The presence of correlation between the legitimate channel and the wiretap channel may introduce a reduction in the effectiveness of AN. This correlation is particularly pronounced in scenarios where the locations of Bob and Eve are in close proximity. When such correlation exists, it becomes imperative to develop strategies to compensate for the performance degradation that arises from this issue.

2) Current Status

One approach to mitigating the impact of correlation-based performance loss is to implement a correlation-based power allocation scheme, as proposed in [229], specifically tailored to situations where transmitter-side correlation is prevalent. Additionally, in cases characterized by high reception correlation, an AN-aided beamforming scheme was introduced in [230]. The findings of these studies confirm that channel correlation does indeed diminish the efficacy of AN. However, this adverse effect can be partially mitigated by allocating higher power to AN.

3) Future Direction

It is worth mentioning that the degree of channel correlation is highly contingent on the relative positions of Bob and Eve. This dependency is especially pronounced when LoS paths dominate the overall channel as opposed to non-light-of-sight (nLoS) paths. Consequently, the modeling of channel correlation can be substantially enhanced by incorporating positioning algorithms designed to accurately determine the locations of Eve [231]–[233]. Such positioning algorithms play a crucial role in optimizing AN strategies by providing more precise information about the spatial relationship between Bob and Eve, thus enabling more effective countermeasures against the negative impact of channel correlation.

C. Adversarial Scheme

1) Challenge

As mentioned before, the evaluation of secrecy performance in most research papers has primarily revolved around metrics like secrecy capacity or secrecy rate, which effectively gauge the security of information transmission by measuring the gap in channel qualities between Bob and Eve. In this conventional framework, the AN is typically treated as an interference source that degrades signal quality by reducing the equivalent SINR. However, it is important to recognize that Eve may employ various countermeasures to mitigate the detrimental effects of AN. When Eve's strategies allow for the neutralization of AN, it becomes necessary to adapt the evaluation metrics accordingly.

2) Current Status

As shown in Fig. 15, the adversarial scheme adopted by Eve is to project the received signal to minimize the jamming effect caused by AN.

Specifically, the ZF-aided artificial noise elimination (ANE) method, as presented in [234], offers a solution for Eve to mitigate the impact of AN. With the CSI of Alice-Bob link, Eve is capable of mitigating the influence of AN by multiplying the project matrix

$$\mathbf{W}= \mathbf{H}(\mathbf{G}\mathbf{G})^{-1}\mathbf{G}^{H} \tag{104}$$

at the left side of received signal, which proves particularly effective when Eve has more antennas than Alice, i.e., $N_e \geqslant N_a$. In [235], theoretical analysis is derived to characterize the secrecy rate of the AN scheme even with the adversarial scheme.

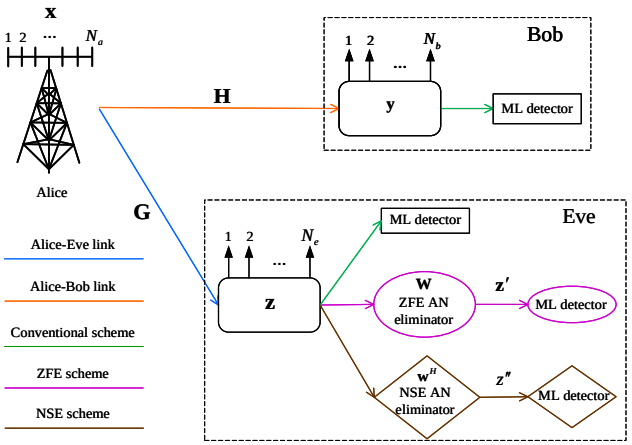

Fig. 15. Adversarial Model of AN.

Simulation results from this work revealed that increasing AN power has little effect on increasing secrecy rate when the number of antennas at Eve exceeds that of Alice.

Moreover, the null-space elimination, outlined in [236], also use the CSI of Alice-Bob link to assist Eve to achieve ANE. Compared to [234], the work in [236] reduces the hardware requirements of Eve to $N_e \geqslant N_a - N_b + 1$ and provides better performance for ANE by solving

$$\max_{\mathbf{w}} \frac{\left\|\mathbf{w}^H \mathbf{G}\mathbf{p}\right\|}{\mathbf{w}^H \mathbf{w}} \tag{105a}$$

$$\text{s.t. } \mathbf{w}^H \mathbf{G}\mathbf{V} = \mathbf{0}. \tag{105b}$$

With the development of the adversarial model, it can be found that in theory Eve can mitigate the interference of AN at the cost of higher hardware requirements. However, in practice, it is difficult for Eve to cooperate with Alice and Bob to obtain their CSI.

Against this background, the authors of [237] proposed the hyperplane clustering algorithm to achieve ANE without the legitimate CSI. The basic principle is to use numerous AN-mixed received signals to extract signal features, which provides superior anti-AN performance in comparison to conventional techniques such as multiple signal classification.

Additionally, also with multiple AN-mixed received signals, Ref. [238] demonstrated that machine-learning-based ANE algorithms are effective for Eve under the constraint of

$$M > N_a - N_b, \tag{106}$$

where M denotes the number of received signals. Furthermore, the authors of [239] also defined the artificial noise to signal ratio (ANSR) as a metric to quantify the effectiveness of ANE without the legitimate CSI, i.e.,

$$\text{ANSR} = \left\|\mathbf{w}^H \mathbf{G}\mathbf{V}\right\|^2 / \left\|\mathbf{w}^H \mathbf{G}\mathbf{p}\right\|^2. \tag{107}$$

3) Future Direction

It is worth mentioning that the countermeasures discussed above typically require Eve to commit more resources and incur higher computational complexity than Bob. These additional resources might encompass a greater number of RF chains and higher computational complexity. This observation implies that the deployment of AN as a security mechanism effectively coerces Eve into increasing hardware and computational requirements in her attempts to undermine the security of the communication.

Given these considerations, there is a compelling need to develop more robust evaluation standards that factor in the interplay between AN and specific countermeasures employed by Eve. Such standards should facilitate a comprehensive and accurate assessment of the secrecy enhancement provided by AN in diverse scenarios, accounting for the evolving landscape of secure communication protocols.

D. Practical Optimization Algorithms

1) Challenge

A fair number of AN optimization strategies tended to maximize the secrecy capacity or secrecy rate so as to enhance the overall secrecy performance. However, these approaches often rely on the availability of Eve's CSI, which is not always feasible in practice. Note that the instantaneous CSI of Eve may be challenging to obtain, except two main scenarios: i) Eve is active, allowing the BS to monitor her behavior and obtain its CSI, or ii) the CSI of a passive Eve can be obtained by exploiting the power leakage from her local oscillator through the received RF front end of RF receiver [240], [241]. The same assumption aligns with similar considerations in the field of PLS, as seen in [180], [196].

2) Current Status

An example of utilizing Eve's instantaneous CSI is presented in [242], where a multi-antenna Alice aims to transmit a confidential message to a single-antenna IR while transferring wireless energy to multiple multi-antenna ERs. Assuming imperfect instantaneous CSI of all channels at the transmitter, the covariances of confidential information and AN were jointly optimized to maximize the secrecy rate at the IR with the constraint that each ER receives a prescribed amount of wireless energy. Similarly, the authors of [243] considered an AN-aided wireless powered backscatter communication system in which an FD Alice transmits multi-sinewave signals to power backscatter devices.

However, compared to the instantaneous CSI scenarios, a more operational assumption is that Alice only obtains the statistical CSI of Eve, which may occur when the location of Eve can be confirmed [244], [245]. In such cases, AN can still provide better performance than the case without any knowledge CSI of Eve, although it may not achieve the same level of performance as when instantaneous CSI is available. This difference in performance is observed in terms of secrecy rate [246] and energy efficiency [247]. In addition, some other technologies, such as antenna grouping [248] and cooperative jamming [249], can be compatible with this scenario. For instance, researchers in [250] studied the AN-aided distributed antenna systems with statistical CSI for all channels by maximizing the ESR under a per-antenna power constraint.

3) Future Direction

While the aforementioned approaches are challenging to implement without knowledge of Eve's CSI, they often come with high computational complexity and deviate from the original intention of AN (to provide secure communication with low complexity). Therefore, practical AN optimization algorithms with low computational complexity and high jamming intensity are desired. Achieving this may involve developing novel quantization standards for situations where Eve's CSI is unavailable and pursuing closed-form solutions for AN design. These efforts could bridge the gap between theoretical developments and practical implementation of AN.

E. Wider Usage Scenarios and Technological Combination

1) Future Direction

The commercialization of the 5G mobile communications has brought forth new application scenarios that demand both communication and sensing capabilities, leading to the consensus on the ISAC in future wireless networks. In the long term, ISAC not only requires the provision of sensing services such as localization and imaging based on the acquired sensing information but also demands a more reliable transmission by utilizing the information in turn to enhance robust security and communication performance for the integration of architectures and waveforms. In this context, AN, with its unique ability to artificially generate interference, holds significant potential for ISAC applications.

Simultaneously, the 6G era is expected to introduce space-air-ground integrated network to provide global coverage, necessitating support for a diverse array of emerging applications in high-mobility and hostile environments. Conventional AN schemes, often used in slow fading channels [251], may encounter performance degradation due to significant Doppler shifts. This issue can be addressed by integrating AN with a novel 2D modulation techniques, such as orthogonal time frequency space [252], tailored for high-mobility use cases in future communication systems.

Furthermore, due to its flexible strategies and excellent performance, the AN finds application across a wide range of scenarios and can be combined with various technologies, including but not limited to interference channel [253], [254], broadcast channel [255], multi-casting [256], [257], vehicle communications [258], cognitive wireless sensor networks [259], large-scale spectrum sharing networks [260], layered PLS [261], IA-based networks [262], time-reversal-based transmission [263], adaptive scheme [264], secure state estimation [265], antenna selection [266], space-time line code [267], [268], stacked intelligent metasurfaces [269], [270], fluid antenna systems [271]–[273], cell-free MIMO [274]–[276], and reconfiguring wireless environments [277]–[280], etc.

VI. Conclusions

In this paper, we introduced the emerging concept of AN and its evolution, along with generic system models and technical backgrounds. Furthermore, a comprehensive survey of the current state of research on various AN-enabled scenarios and AN-combined technologies was provided. Finally, we discussed the most significant research issues and challenges to tackle.

References

[1] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 347-376, 1st Quart. 2017.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent Advances, and future trends," *Proc. IEEE.*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[3] H. Zimmermann, "OSI reference model - The ISO model of architecture for open systems interconnection," *IEEE Trans. Commun.*, vol. 28, no. 4, pp. 425-432, Apr. 1980.

[4] M. B. Yassein, M. Q. Shatnawi, and D. Al-zoubi, "Application layer protocols for the Internet of Things: A survey," in *Proc. Int. Conf. Eng. MIS (ICEMIS)*, Agadir, Morocco, Sep. 2016, pp. 1-4.

[5] C. Huang and H. Kung, "A synchronization infrastructure for multicast multimedia at the presentation layer," *IEEE Trans. Consum. Electron.*, vol. 43, no. 3, pp. 370-380, Aug. 1997.

[6] M. Polese *et al.*, "A survey on recent advances in transport layer protocols," *IEEE Commun. Surv. Tut.*, vol. 21, no. 4, pp. 3584-3608, Aug. 2019.

[7] R. Jurdak, C. Lopes, and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks," *IEEE Commun. Surv. Tut.*, vol. 6, no. 1, pp. 2-16, Apr. 2004.

[8] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Communications Magazine.*, vol. 44, no. 4, pp. 115-121, Apr. 2006.

[9] Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550-1573, 3rd Quart. 2014.

[10] X. Chen, D. W. K. Ng, W. H. Gerstacker and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1027-1053, 2nd Quart. 2017.

[11] Y. Gao *et al.*, "Modeling and practise of satellite communication systems using physical layer security: A survey," in *Proc. 2017 IEEE Int. Conf. Comput. Sci. Eng. (CSE)*, Guangzhou, China, Jul. 2017, pp. 829-832.

[12] Y. Wu, *et. al.*, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679-695, Apr. 2018.

[13] M. Obeed, A. M. Salhab, M. S. Alouini, and S. A. Zummo, "Survey on physical layer security in optical wireless communication systems," in *Proc. 7th Int. Conf. Commun. Netw. (ComNet)*, Hammamet, Tunisia, Nov. 2018, pp. 1-5.

[14] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1773-1828, 2nd Quart. 2019.

[15] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1878-1911, 2nd Quart. 2019.

[16] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2734-2771, 3rd Quart. 2019.

[17] J. D. Vega Sánchez, L. Urquiza-Aguiar, and M. C. Paredes Paredes, "Physical layer security for 5G wireless networks: A comprehensive survey," in *Proc. 3rd Cyber Secur. Netw. Conf. (CSNet)*, Quito, Ecuador, Oct. 2019, pp. 122-129.

[18] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33-52, Jan. 2020.

[19] M. A. Arfaoui *et al.*, "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1887-1908, 3rd Quart. 2020.

[20] P. Rojas, S. Alahmadi, and M. Bayoumi, "Physical layer security for IoT communications - A survey," in *Proc. 7th World Forum Internet Things (WF-IoT)*, New Orleans, LA, USA, Jun. 2021, pp. 95-100.

[21] J. Wang *et al.*, "Physical layer security for UAV communications: A comprehensive survey," *China Commun.*, vol. 19, no. 9, pp. 77-115, Sep. 2022.

[22] G. Jang, B. You, and H. Jung, "A survey on physical layer security schemes in satellite networks," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, Jeju Island, Korea, Republic of, Oct. 2022, pp. 1213-1215.

[23] R. Dhakal and L. N. Kandel, "A survey of physical layer-aided UAV security," in *Proc. 2023 Integr. Commun. Navigation Surveillance Conf. (ICNS)*, Herndon, VA, USA, Apr. 2023, pp. 1-8.

[24] R. Kaur *et al.*, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 172-199, Jan. 2024.

[25] C. Kolias, G. Kambourakis, and S. Gritzalis, "Attacks and countermeasures on 802.16: Analysis and assessment," *IEEE Commun. Surv. Tut.*, vol. 15, no. 1, pp. 487-514, Feb. 2013.

[26] K. A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Commun. Surv. Tut.*, vol. 18, no. 1, pp. 577-601, 1st Quart. 2016.

[27] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[28] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd Veh. Technol. Conf. (VTC-Fall)*, Dallas, TX, USA, Sep. 2005, pp. 1906-1910.

[29] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[30] T. M. Hoang, T. Q. Duong, N. S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174-177, Apr. 2017.

[31] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *2013 IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2013, pp. 160-173.

[32] Z. Wang, M. Xiao, M. Skoglund, and H. V. Poor, "Secure degrees of freedom of wireless X networks using artificial noise alignment," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2632-2646, Jul. 2015.

[33] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1470-1482, Jun. 2017.

[34] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7036-7050, Sep. 2016.

[35] C. Song, "Leakage rate analysis for artificial noise assisted massive MIMO with non-coherent passive eavesdropper in block-fading," *IEEE Trans. Wirel. Commun.*, vol. 18, no. 4, pp. 2111-2124, Apr. 2019.

[36] H. Chen, X. Tao, N. Li, and X. Li, "Secrecy performance of the artificial noise assisted broadcast channel with confidential messages and external eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May. 2016, pp. 1-6.

[37] S. H. Lai, P. H. Lin, S. C. Lin, and H. J. Su, "On optimal artificial-noise assisted secure beamforming for the multiple-input multiple-output fading eavesdropper channel," in *Proc. IEEE Wirel. Commun. Netw. Conf. (WCNC)*, Paris, France, Apr. 2012, pp. 513-517.

[38] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728-1740, Sep. 2013.

[39] T. Y. Liu, Y. C. Chen, and Y. W. Peter Hong, "Artificial noise design for discriminatory channel estimation in wireless MIMO systems," in *Proc. IEEE Glob. Commun. Conf.*, Austin, TX, USA, Dec. 2014, pp. 3032-3037.

[40] M. Ahmed and L. Bai, "Secrecy capacity of artificial noise aided secure communication in MIMO Rician channels," *IEEE Access*, vol. 6, pp. 7921-7929, Feb. 2018.

[41] Y. Gu, Z. Wu, Z. Yin, and X. Zhang, "The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in MIMO system," *IEEE Access*, vol. 7, pp. 58353-58360, Mar. 2019.

[42] S. Yun, J. M. Kang, I. M. Kim, and J. Ha, "Deep artificial noise: Deep learning-based precoding optimization for artificial noise scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3465-3469, Mar. 2020.

[43] T. Akitaya, S. Asano, and T. Saba, "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 807-812.

[44] A. D. Harper and X. Ma, "MIMO wireless secure communication using data-carrying artificial noise," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 12, pp. 8051-8062, Dec. 2016.

[45] S. Yun, S. Im, I. M. Kim, and J. Ha, "On the secrecy rate and optimal power allocation for artificial noise assisted MIMOME channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3098-3113, Apr. 2018.

[46] H. Niu, X. Lei, Y. Xiao, Y. Li, and W. Xiang, "Performance analysis and optimization of secure generalized spatial modulation," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4451-4460, Jul. 2020.

[47] A. Li *et al.*, "A tutorial on interference exploitation via symbol-level precoding: Overview, state-of-the-art and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 796-839, Mar. 2020.

[48] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Sig. Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016.

[49] M. R. Khandaker, C. Masouros, and K.-K. Wong, "Constructive interference based secure precoding: A new dimension in physical layer security," *IEEE Trans. Inf. Forensics and Security*, vol. 13, no. 9, pp. 2256–2268, Sept. 2018.

[50] M. R. Khandaker, C. Masouros, K.-K. Wong, and S. Timotheou, "Secure SWIPT by exploiting constructive interference and artificial noise," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1326–1340, Feb. 2018.

[51] H. Niu, X. Lei, Y. Xiao, D. Liu, Y. Li, and H. Zhang, "Power minimization in artificial noise aided generalized spatial modulation," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 961-965, May 2020.

[52] S. Liu, Y. Hong, and E. Viterbo, "Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 8, pp. 4193-4203, Aug. 2015.

[53] N. Yang, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise with optimal power allocation in multi-input single-output wiretap channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 2184-2190.

[54] G. Shi, Y. Li, W. Cheng, X. Gao, and W. Zhang, "An artificial-noise-based approach for the secrecy rate maximization of MISO VLC wiretap channel with multi-Eves," *IEEE Access*, vol. 9, pp. 651-659, 2021.

[55] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and artificial noise design for cognitive MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6753-6758, Aug. 2016,

[56] H. Yu and J. Joung, "Design of the power and dimension of artificial noise for secure communication systems," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4001-4010, Jun. 2021.

[57] W. Mei, Z. Chen, and J. Fang, "Sum secrecy rate optimization for MIMOME wiretap channel with artificial noise and D2D underlay communication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1-7.

[58] J. Zhu, R. Schober, and V. K. Bhargava, "Secrecy analysis of multi-cell massive MIMO systems with RCI precoding and artificial noise transmission," in *Proc. 6th Int. Symp. Commun. Control Signal Process. (ISCCSP)*, Athens, Greece, May 2014, pp. 101-104.

[59] G. Li, P. Wang, T. Yang, and H. Che, "Secrecy sum-rate enhancement for NOMA-VLC system with pseudo user," *IEEE Commun. Lett.*, vol. 27, no. 1, pp. 243-247, Jan. 2023.

[60] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931-2943, May 2014.

[61] X. Zhou, M. R. McKay, B. Maham, and A. Hjϕrungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302-304, Mar. 2011.

[62] Y. Zhu, Y. Zhou, S. Patel, X. Chen, L. Pang, and Z. Xue, "Artificial Noise Generated in MIMO Scenario: Optimal Power Design," *IEEE Signal Process. Lett.*, vol. 20, no. 10, pp. 964-967, Oct. 2013.

[63] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *Proc. 3rd Int. Conf. Signal Process. Commun. Syst.*, Omaha, NE, USA, Sep. 2009, pp. 1-5.

[64] T. X. Zheng *et al.*, "Multi-Antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347-4362, Nov. 2015.

[65] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 971-975, May 2020.

[66] N. Li, X. Tao, and J. Xu, "Artificial noise assisted communication in the multiuser downlink: Optimal power allocation," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 295-298, Feb. 2015.

[67] S. H. Chae and W. Choi, "Optimal power allocation for artificial noise in a Poisson interference field," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1671-1674, Aug. 2016.

[68] T. X. Zheng and H. M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812-8817, Oct. 2016.

[69] H. Qin *et al.*, "Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1-5.

[70] N. Romero Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71-74, Feb. 2012.

[71] S. H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479-3493, Jul. 2014.

[72] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

[73] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination inwireless downlink," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Dallas, TX, USA, Mar. 2010, pp. 2562-2565.

[74] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202-1216, Mar. 2011.

[75] F. Wu, L. L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544-1547, Sep. 2015.

[76] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483-1486, Jul. 2013.

[77] H. Liu and X. J. Li, "Data-Driven Privacy-Enhancement for Cyber-Physical Systems: A Joint-Design Method of Controller and Artificial Noise," *IEEE Trans. Control Netw. Syst.*, vol. 12, no. 1, pp. 713-722, Mar. 2025.

[78] Ö. Cepheli, G. Dartmann, G. K. Kurt, and G. Ascheid, "A joint optimization scheme for artificial noise and transmit filter for half and full duplex wireless cyber physical systems," *IEEE Trans. Sustain. Comput.*, vol. 3, no. 2, pp. 126-136, Jul. 2018.

[79] P. Chen *et al.*,"Artificial-noise-aided energy-efficient secure beamforming for multi-eavesdroppers in cognitive radio networks," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3801-3812, Sep. 2020.

[80] M. Khojastehnia and S. Loyka, "Comments on "Precoding and artificial noise design for cognitive MIMOME wiretap channels"," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2917-2921, Mar. 2021.

[81] Y. He, J. Evans, and S. Dey, "Secrecy rate maximization for cooperative overlay cognitive radio networks with artificial noise," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 1663-1668.

[82] Y. Wu, X. Chen, and X. Chen, "Secure beamforming for cognitive radio networks with artificial noise," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, Oct. 2015, pp. 1-5.

[83] Y. Jiang, Y. Zou, J. Ouyang, and J. Zhu, "Secrecy energy efficiency optimization for artificial noise aided physical-layer security in OFDM-based cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11858-11872, Dec. 2018.

[84] S. Yan, Y. Shang, X. Zhang, D. Li, and X. Li, "An artificial noise scheme for secure communication in heterogeneous D2D and cellular networks," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Montreal, QC, Canada, Sep. 2016, pp. 1-5.

[85] X. Kang, X. Ji, K. Huang, and Z. Zhong, "Secure D2D communication underlying cellular networks: Artificial noise assisted," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Montreal, QC, Canada, Sep. 2016, pp. 1-5.

[86] G. Jang, D. Kim, I. H. Lee, and H. Jung, "Cooperative beamforming with artificial noise injection for physical-layer security," *IEEE Access*, vol. 11, pp. 22553-22573, Mar. 2023.

[87] R. Ruby *et al.*,"Enhancing secrecy performance of cooperative NOMA-nased IoT networks via multiantenna-aided artificial noise," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5108-5127, Apr. 2022.

[88] Y. Ju, Y. Zhu, H. M. Wang, Q. Pei, and H. Zheng, "Artificial noise hopping: A practical secure transmission technique with experimental analysis for millimeter wave systems," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5121-5132, Dec. 2020.

[89] S. Wang *et al.*, "Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems," *IEEE Access*, vol. 7, pp. 28597-28606, Feb. 2019.

[90] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmWave MISO systems with partial channel knowledge," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1729-1733, Nov. 2017.

[91] Y. Ju *et al.*, "Secrecy throughput maximization for millimeter wave systems with artificial noise," in *Proc. IEEE 27th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Valencia, Spain, Sep. 2016, pp. 1-6.

[92] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmission with artificial noise in millimeter wave systems," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Doha, Qatar, Apr. 2016, pp. 1-6.

[93] W. Mei, B. Fu, L. Li, Z. Chen, and C. Huang, "Artificial-noise aided transmit design for multi-user MISO systems with service integration and energy harvesting," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Kuala Lumpur, May. 2016, pp. 219-225.

[94] W. Mei, Z. Chen, and C. Huang, "Robust artificial-noise aided transmit design for multi-user MISO systems with integrated services," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Shanghai, China, Mar. 2016, pp. 3856-3860.

[95] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, "On artificial-noise-aided transmit design for multiuser MISO systems with integrated services," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8179-8195, Sep. 2017.

[96] M. Yang *et al.*, "Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11394-11398, Dec. 2017.

[97] L. Sun, R. Wang, Z. Tang, and V. C. M. Leung, "Artificial-noise-aided nonlinear secure transmission for multiuser multi-antenna systems with finite-Rate feedback," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2274-2293, Mar. 2019.

[98] L. Sun, L. Cao, Z. Tang, and Y. Feng, "Artificial-noise-aided secure multi-user multi-antenna transmission with quantized CSIT: A comprehensive design and analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3734-3748, Jun. 2020.

[99] E. Choi *et al.*, "Joint precoding and artificial noise design for MU-MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1564-1578, Mar. 2023.

[100] I. Bang, S. M. Kim, and D. K. Sung, "Artificial noise-aided user scheduling for optimal secrecy multiuser diversity," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 528-531, Mar. 2017.

[101] I. Bang, S. M. Kim, and D. K. Sung, "Artificial noise-aided user scheduling from the perspective of secrecy outage probability," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7816-7820, Aug. 2018.

[102] Y. Y. Zhang, J. K. Zhang, and H. Y. Yu, "Physically securing energy-based massive MIMO MAC via joint alignment of multi-user constellations and artificial noise," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 829-844, Apr. 2018.

[103] M. F. Marzban, A. El Shafie, N. Al-Dhahir, and R. Hamila, "Security-enhanced SC-FDMA transmissions using temporal artificial-noise and secret key aided schemes," *IEEE Access*, vol. 7, pp. 14807-14824, Jan. 2019.

[104] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487-490, May 2013.

[105] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1617-1628, Oct. 2014.

[106] B. Li, M. Zhang, Y. Rong, and Z. Han, "Artificial noise-aided secure relay communication with unknown channel knowledge of eavesdropper," *IEEE Trans. Wireless. Commun.*, vol. 20, no. 5, pp. 3168-3179, May 2021.

[107] D. Tubail, M. El-Absi, S. S. Ikki, W. Mesbah, and T. Kaiser, "Artificial noise-based physical-layer security in interference alignment multipair two-way relaying networks," *IEEE Access*, vol. 6, pp. 19073-19085, Mar. 2018.

[108] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless. Commun.*, vol. 13, no. 4, pp. 2189-2203, Apr. 2014.

[109] Y. Liu, Liang Li, and M. Pesavento, "Enhancing physical layer security in untrusted relay networks with artificial noise: A symbol error rate based approach," in *Proc. IEEE 8th SAM*, A Coruna, Jun. 2014, pp. 261-264.

[110] J. Yang *et al.*, "Joint secure AF relaying and artificial noise optimization: A penalized difference-of-convex programming framework," *IEEE Access*, vol. 4, pp. 10076-10095, 2016.

[111] D. Goeckel *et al.*, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067-2076, Dec. 2011.

[112] M. Lin, J. Ge, Y. Yang, and Y. Ji, "Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 380-383, Feb. 2014.

[113] Y. Yang, Q. Li, W. K. Ma, J. Ge, and M. Lin, "Optimal joint cooperative beamforming and artificial noise design for secrecy rate maximization in AF relay networks," in *Proc. IEEE 14th Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Darmstadt, Germany, Jun. 2013, pp. 360-364.

[114] Q. Li *et al.*, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206-220, Jan. 2015.

[115] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Artificial-noise-aided secure MIMO full-duplex relay channels with fixed-power transmissions," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1591-1594, Aug. 2016.

[116] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless. Commun.*, vol. 15, no. 11, pp. 7444-7456, Nov. 2016.

[117] Y. Feng, Z. Yang, and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Singapore, Dec. 2017, pp. 1-6.

[118] B. Zheng et al., "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426-1440, Jul. 2018.

[119] S. Jia, J. Zhang, H. Zhao, Y. Lou, and Y. Xu, "Relay selection for improved physical layer security in cognitive relay networks using artificial noise," *IEEE Access*, vol. 6, pp. 64836-64846, Oct. 2018.

[120] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930-3941, May 2017.

[121] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "User and relay selection with artificial noise to enhance physical layer security," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10906-10920, Nov. 2018.

[122] B. Li, Z. Fei, and H. Chen, "Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay networks," *IEEE Access*, vol. 4, pp. 7921-7929, Nov. 2016.

[123] Q. Li and L. Yang, "Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 10, pp. 2628-2638, Oct. 2018.

[124] R. Xu, X. Da, H. Hu, Y. Liang, and L. Ni, "Power and time slot allocation method for secured satellite transmission based on weighted fractional data carrying artificial noise," *IEEE Access*, vol. 6, pp. 65043-65054, Oct. 2018.

[125] W. Lu, T. Liang, K. An, and H. Yang, "Secure beamforming and artificial noise algorithms in cognitive satellite-terrestrial networks with multiple eavesdroppers," *IEEE Access*, vol. 6, pp. 65760-65771, Oct. 2018.

[126] W. Mei, Z. Chen, and J. Fang, "Artificial noise aided energy efficiency optimization in MIMOME system with SWIPT," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1795-1798, Aug. 2017.

[127] A. El Shafie, K. Tourki, and N. Al Dhahir, "An artificial-noise-aided hybrid TS/PS scheme for OFDM-based SWIPT systems," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 632-635, Mar. 2017.

[128] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918-931, Apr. 2018.

[129] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087-1098, Feb. 2018.

[130] Y. Lu, K. Xiong, P. Fan, Z. Zhong, and K. B. Letaief, "Coordinated beamforming with artificial noise for secure SWIPT under non-linear EH model: Centralized and distributed designs," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1544-1563, Jul. 2018.

[131] Z. Chu et al., "Robust design for MISO SWIPT system with artificial noise and cooperative jamming," in *Proc. IEEE Globecom*, Singapore, Dec. 2017, pp. 1-6.

[132] Y. Ma, T. Lv, H. Liu, T. Li, J. Zeng, and G. Pan, "Secrecy outage analysis of CR-SWIPT networks with artificial noise and spatially random secondary terminals," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 931-945, Jun. 2022.

[133] W. Gao, C. Han, and Z. Chen, "Receiver artificial noise aided terahertz secure communications with eavesdropper in close proximity," in *Proc. IEEE Globecom*, Taipei, Taiwan, Jan. 2020, pp. 1-6.

[134] W. Gao, C. Han, and Z. Chen, "DNN-powered SIC-free receiver artificial noise aided terahertz secure communications with randomly distributed eavesdroppers," *IEEE Trans. Wireless. Commun.*, vol. 21, no. 1, pp. 563-576, Jan. 2022.

[135] A. Li, W. Zhang, and S. Dou, "UAV-enabled secure data dissemination via artificial noise: Joint trajectory and communication optimization," *IEEE Access*, vol. 8, pp. 102348-102356, May 2020.

[136] M. T. Mamaghani, and Y. Hong, "Joint trajectory and power allocation design for secure artificial noise aided UAV communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2850-2855, Mar. 2021.

[137] Y. Li, H. Zhang, and K. Long, "Joint resource, trajectory, and artificial noise optimization in secure driven 3-D UAVs with NOMA and imperfect CSI," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3363-3377, Nov. 2021.

[138] M. A. Arfaoui, H. Zaid, Z. Rezki, A. Ghrayeb, A. Chaaban, and M. S. Alouini, "Artificial noise-based beamforming for the MISO VLC wiretap channel," *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 2866-2879, Apr. 2019.

[139] T. V. Pham and A. T. Pham, "Energy efficient artificial noise-aided precoding designs for secured visible light communication systems," *IEEE Trans. Wireless. Commun.*, vol. 20, no. 1, pp. 653-666, Jan. 2021.

[140] T. V. Pham, T. Hayashi, and A. T. Pham, "Artificial-noise-aided precoding design for multi-user visible light communication channels," *IEEE Access*, vol. 7, pp. 3767-3777, Dec. 2018.

[141] X. Liu, Z. Chen, Y. Wang, F. Zhou, and S. Ma, "Robust artificial noise-aided beamforming for a secure MISO-NOMA visible light communication system," *China Commun.*, vol. 17, no. 11, pp. 42-53, Nov. 2020.

[142] F. Yang, K. Zhang, Y. Zhai, J. Quan, and Y. Dong, "Artificial noise design in time domain for indoor SISO DCO-OFDM VLC wiretap systems," *J. Light. Technol.*, vol. 39, no. 20, pp. 6450-6458, Oct. 2021.

[143] D. Luo, Z. Ye, B. Si, and J. Zhu, "Secure transmit beamforming for radar-communication system without eavesdropper CSI," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9794-9804, Sep. 2022.

[144] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Trans. Wireless. Commun.*, vol. 20, no. 1, pp. 83-95, Jan. 2021.

[145] N. Su, F. Liu, Z. Wei, Y. F. Liu, and C. Masouros, "Secure dual-functional radar-communication transmission: Exploiting interference for resilience against target eavesdropping," *IEEE Trans. Wireless. Commun.*, vol. 21, no. 9, pp. 7238-7252, Sep. 2022.

[146] J. Chu, R. Liu, M. Li, Y. Liu, and Q. Liu, "Joint Secure Transmit Beamforming Designs for Integrated Sensing and Communication Systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 4778-4791, Apr. 2023.

[147] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proc. IEEE Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2011, pp. 651-655.

[148] J. Choi, J. Joung, and Y. -S. Cho, "Artificial-noise-aided space-time line code for enhancing physical layer security of multiuser MIMO downlink transmission," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1289-1300, Mar. 2022.

[149] S. Jain and R. Bose, "Secure cooperative transmission in rateless-coded environment using TAS and artificial noise," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12416-12421, Dec. 2019.

[150] H. Bai, L. Jin, and M. Yi, "Artificial noise aided polar codes for physical layer security," *China Commun.*, vol. 14, no. 12, pp. 15-24, Dec. 2017.

[151] R. Soltani, B. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert single-hop communication in a wireless network with distributed artificial noise generation," in *Proc. IEEE 52nd Allerton Conf.*, Monticello, IL, USA, Oct. 2014, pp. 1078-1085.

[152] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless. Commun.*, vol. 17, no. 11, pp. 7252-7267, Nov. 2018.

[153] W. He et al., "Optimal transmission probabilities of information and artificial noise in covert communications," in *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 2865-2869, Dec. 2022.

[154] Y. Jiang, L. Wang, and H. H. Chen, "Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2980-2992, Mar. 2020.

[155] S. Feng, X. Lu, S. Sun, and D. Niyato, "Mean-field artificial noise assistance and uplink power control in covert IoT systems," *IEEE Trans. Wireless. Commun.*, vol. 21, no. 9, pp. 7358-7373, Sep. 2022.

[156] J. Chen *et al.*, "A survey on directional modulation: Opportunities, challenges, recent advances, implementations, and future trends," *IEEE Internet Things J.*, early access, 2025, doi: 10.1109/JIOT.2025.3574824.

[157] Y. Ding and V. Fusco, "A far-field pattern separation approach for the synthesis of directional modulation transmitter arrays," in *Proc. 31st URSI Gen. Assem. Sci. Symp.*, Beijing, China, Aug. 2014, pp. 1-4.

[158] Y. Ding and V. Fusco, "Vector representation of directional modulation transmitters," in *Proc. 8th Eur. Conf. Antennas Propag.*, The Hague, Netherlands, Apr. 2014, pp. 367-371.

[159] Y. Ding and V. Fusco, "Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters," *IEEE Antennas Wirel. Propag. Lett.*, vol. 14, pp. 1330-1333, Feb. 2015.

[160] H. Yu, S. Wan, W. Cai, L. Xu, X. Zhou, J. Wang, Y. Wu, F. Shu, J. Wang, and J. Wang, "GPI-based secrecy rate maximization beamforming scheme for wireless transmission with AN-aided directional modulation," *IEEE Access*, vol. 6, pp. 12044-12051, Mar. 2018.

[161] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614-6623, Oct. 2016.

[162] F. Shu, W. Zhu, X. Zhou, J. Li, and J. Lu, "Robust secure transmission of using main-lobe-integration-based leakage beamforming in directional modulation MU-MIMO systems," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3775-3785, Nov. 2018.

[163] J. Chen, Y. Xiao, K. Liu, Y. Zhong, X. Lei, and M. Xiao, "Physical layer security for near-field communications via directional modulation," *IEEE Trans. Veh. Technol.*, vol. 73, no. 8, pp. 12242-12246, Aug. 2024.

[164] C. Song, M. Zhao, W. Guo, C. Shi, H. Zhao, and S. Shao, "Artificial noise shielded frequency-hopping systems: Transceiver design and performance analysis," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1286-1289, Jun. 2021.

[165] C. Song, H. Zhao, L. Qin, R. Wen, and S. Shao, "Analysis and optimization of transceiver IQ imbalances in artificial noise shielded FH communication," *IEEE Trans. Signal Process.*, vol. 70, pp. 2798-2813, 2022.

[166] C. Song, W. Guo, H. Zhao, and S. Shao, "Artificial noise sheltered FH broadcasting with frequency mismatch: Secrecy analysis and power allocation," *IEEE Trans. Broadcast.*, vol. 68, no. 1, pp. 279-285, Mar. 2022.

[167] S. Yun, I. M. Kim, and J. Ha, "Artificial noise scheme for correlated MISO wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9323-9327, Sep. 2019.

[168] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2096-2099, Nov. 2013.

[169] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18-21, Jan. 2015.

[170] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771-1783, May 2015.

[171] D. Hu, P. Mu, W. Zhang, and W. Wang, "Minimization of secrecy outage probability with artificial-noise-aided beamforming for MISO wiretap channels," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 401-404, Feb. 2020.

[172] B. Wang, P. Mu, and Z. Li, "Artificial-noise-aided beamforming design in the MISOME wiretap channel under the secrecy outage probability constraint," *IEEE Trans. Wireless. Commun.*, vol. 16, no. 11, pp. 7207-7220, Nov. 2017.

[173] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 1875-1889, Aug. 2018.

[174] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170-2181, Apr. 2016.

[175] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless. Commun.*, vol. 14, no. 1, pp. 94-106, Jan. 2015.

[176] Q. Li and W. K. Ma, "A robust artificial noise aided transmit design for MISO secrecy," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Prague, Czech Republic, May 2011, pp. 3436-3439.

[177] Q. Li, W. K. Ma, and A. M. C. So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. IEEE Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2011, pp. 207-211.

[178] L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving physical layer security for MISO systems via using artificial noise," in *Proc. IEEE Globecom*, San Diego, CA, USA, Dec. 2015, pp. 1-6.

[179] Z. Li, P. Mu, B. Wang, and X. Hu, "Optimal semiadaptive transmission with artificial-noise-aided beamforming in MISO wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7021-7035, Sep. 2016.

[180] Q. Li and W. K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-Eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704-2717, May 2013.

[181] W. Xu, B. Li, L. Tao, and W. Xiang, "Artificial noise assisted secure transmission for uplink of massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6750-6762, July 2021.

[182] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless. Commun.*, vol. 15, no. 3, pp. 2245-2261, Mar. 2016.

[183] 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 J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 802-816, Apr. 2018.

[184] A. Qu, X. Zhang, K. An, G. Zheng, and S. Chatzinotas, "Secure transmission in massive MIMO system with specular component-based beamforming and artificial noise over Ricean fading channel," *IEEE Wireless Commun. Lett.*, vol. 10, no. 11, pp. 2479-2483, Nov. 2021.

[185] M. Zeng, N. P. Nguyen, O. A. Dobre, and H. V. Poor, "Securing downlink massive MIMO-NOMA networks with artificial noise," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 685-699, Jun. 2019.

[186] Z. Cao et al., "Artificial noise aided secure communications for cooperative NOMA networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 946-963, Jun. 2022.

[187] C. Gong, X. Yue, Z. Zhang, X. Wang, and X. Dai, "Enhancing physical layer security with artificial noise in large-scale NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2349-2361, Mar. 2021.

[188] Y. Han, N. Li, Y. Liu, T. Zhang, and X. Tao, "Artificial noise aided secure NOMA communications in STAR-RIS networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1191-1195, Jun. 2022.

[189] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700-6705, Jul. 2018.

[190] M. F. Marzban, R. Chabaan, N. Al-Dhahir, and A. El Shafie, "Securing OFDM-based wireless links using temporal artificial-noise injection," in *Proc. 15th IEEE Annu. CCNC*, Las Vegas, NV, USA, Jan. 2018, pp. 1-6.

[191] H. Qin et al., "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717-2729, Jun. 2013.

[192] H. Qin, X. Chen, X. Zhong, F. He, M. Zhao, and J. Wang, "Joint power allocation and artificial noise design for multiuser wiretap OFDM channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Budapest, Hungary, Jun. 2013, pp. 2193-2198.

[193] D. Cheng, Z. Gao, F. Liu, and X. Liao, "A general time-domain artificial noise design for OFDM AF relay systems," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Shenzhen, China, Nov. 2015, pp. 1-6.

[194] A. E. Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871-3886, May 2017.

[195] Ö. Cepheli and G. K. Kurt, "Efficient PHY layer security in MIMO-OFDM: Spatiotemporal selective artificial noise," in *Proc. IEEE 14th Int. Symp. WoWMoM*, Madrid, Spain, Jun. 2013, pp. 1-6.

[196] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless. Commun.*, vol. 15, no. 4, pp. 3085-3096, Apr. 2016.

[197] A. El Shafie, M. F. Marzban, R. Chabaan, and N. Al-Dhahir, "An artificial-noise-aided secure scheme for hybrid parallel PLC/wireless OFDM systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1-6.

[198] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Artificial noise-aided MIMO physical layer authentication with imperfect CSI," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2173-2185, Jan. 2021.

[199] X. Wu, Z. Yang, C. Ling, and X. G. Xia, "Artificial-noise-aided message authentication codes with information-theoretic security," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 6, pp. 1278-1290, Jun. 2016.

[200] X. Wu, Z. Yang, C. Ling, and X. G. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless. Commun.*, vol. 15, no. 10, pp. 6611-6625, Oct. 2016.

[201] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 377-380, Aug. 2014.

[202] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778-782, Jun. 2020.

[203] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7851-7866, Dec. 2020.

[204] S. Fang, G. Chen, Z. Abdullah, and Y. Li, "Intelligent omni surface-assisted secure MIMO communication networks with artificial noise," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1231-1235, Jun. 2022.

[205] B. Li, W. Wu, Y. Li, and W. Zhao, "Intelligent reflecting surface and artificial-noise-assisted secure transmission of MEC system," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11477-11488, Jul. 2022.

[206] H. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 27, pp. 1300-1304, Jul. 2020.

[207] H. Niu, X. Lei, Y. Xiao, M. Xiao, and S. Mumtaz, "On the efficient design of RIS-assisted secure MISO transmission," *IEEE Wireless Commun. Lett.*, vol. 11, no. 8, pp. 1664-1668, Aug. 2022.

[208] Y. Yang and B. Jiao, "Artificial-noise strategy for single-antenna systems over multi-path fading channels," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Dubrovnik, Croatia, Aug. 2015, pp. 96-101.

[209] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless. Commun.*, vol. 17, no. 9, pp. 6190-6204, Sep. 2018.

[210] H. He and P. Ren, "Joint artificial noise and repetition coding for secure wireless communications in TDD systems," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1700-1703, Dec. 2019.

[211] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577-9581, Oct. 2017.

[212] W. Guo, L. Lin, H. Zhao, S. Shao, and Y. Tang, "Reference-free artificial noise waveform design and cancellation for secure transmission," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 10149-10154, Sep. 2022.

[213] Z. Gao, H. Hu, D. Cheng, J. Xu, and X. Sun, "Physical layer security based on artificial noise and spatial modulation," in *Proc. 8th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Yangzhou, China, Oct. 2016, pp. 1-5.

[214] X. Yu, Y. Hu, Q. Pan, X. Dang, N. Li, and M. H. Shan, "Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect CSI," *IEEE Access*, vol. 6, pp. 41060-41067, Jul. 2018.

[215] Y. Wang, T. Zhang, W. Yang, J. Guo, Y. Liu, and X. Shang, "Secure transmission for differential quadrature spatial modulation with artificial noise," *IEEE Access*, vol. 7, pp. 7641-7650, Dec. 2019.

[216] W. Yu et al., "Security enhancing spatial modulation using antenna selection and artificial noise cancellation," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Honolulu, HI, USA, Feb. 2019, pp. 105-109.

[217] P. Yang, X. Qiu, and F. Mu, "Artificial noise-aided secure generalized spatial modulation for multiuser transmission," *IEEE Commun. Lett.*, vol. 24, no. 11, pp. 2416-2420, Nov. 2020.

[218] T. Y. Liu, S. C. Lin, T. H. Chang, and Y. W. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 4782-4787.

[219] T. Y. Liu, S. C. Lin, and Y. W. P. Hong, "On the role of artificial noise in training and data transmission for secret communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 3, pp. 516-531, Mar. 2017.

[220] F. U. Din and F. Labeau, "Artificial noise assisted in-band full-duplex secure channel estimation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6800-6813, Jul. 2021.

[221] Y. L. Liang, Y. S. Wang, T. H. Chang, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea (South), Jun. 2009, pp. 2351-2355.

[222] X. Zhang, X. Zhou, M. R. McKay, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Florence, Italy, Jul. 2014, pp. 3968-3972.

[223] S. C. Lin, T. H. Chang, Y. L. Liang, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless. Commun.*, vol. 10, no. 3, pp. 901-915, Mar. 2011.

[224] J. Bai, T. Dong, Q. Zhang, S. Wang, and N. Li, "Coordinated beamforming and artificial noise in the downlink secure multi-cell MIMO systems under imperfect CSI," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 1023-1026, Jul. 2020.

[225] H. He, P. Ren, Q. Du, and H. Lin, "Joint feedback and artificial noise design for secure communications over fading channels without eavesdropper's CSI," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11414-11418, Dec. 2017.

[226] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-noise-aided secure transmission scheme with limited training and feedback overhead," *IEEE Trans. Wireless. Commun.*, vol. 16, no. 1, pp. 193-205, Jan. 2017.

[227] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless. Commun.*, vol. 14, no. 5, pp. 2742-2754, May 2015.

[228] Z. Tang, L. Sun, X. Tian, D. Niyato, and Y. Zhang, "Artificial-noise-aided coordinated secure transmission design in multi-cell multi-antenna networks with limited feedback," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1750-1765, Feb. 2022.

[229] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless. Commun.*, vol. 15, no. 12, pp. 8286-8297, Dec. 2016.

[230] J. Wang, S. Han, S. Xu, and J. Li, "SNR-outage-based robust artificial noise-aided beamforming for correlated MISO wiretap channels under Gaussian channel uncertainties," *IEEE Syst. J.*, vol. 17, no. 1, pp. 1569-1580, Mar. 2023.

[231] T. Ma, Y. Xiao, X. Lei, L. Zhang, Y. Niu, and G. K. Karagiannidis, "Reconfigurable intelligent surface-assisted localization: Technologies, challenges, and the road ahead," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1430-1451, Jul. 2023.

[232] T. Wu et al., "Exploit high-dimensional RIS information to localization: What is the impact of faulty element?," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 10, pp. 2803-2819, Oct. 2024.

[233] T. Ma, Y. Xiao, X. Lei, W. Xiong, and Y. Ding, "Indoor localization with reconfigurable intelligent surface," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 161-165, Jan. 2021.

[234] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited: When Eve has more antennas than Alice," in *Proc. Int. Conf. Signal Process. Commun. (SPCOM)*, Bangalore, India, Jul. 2014, pp. 1-5.

[235] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901-3911, Jul. 2015.

[236] H. Niu, Y. Xiao, X. Lei, and M. Xiao, "Artificial noise elimination: From the perspective of eavesdroppers," *IEEE Trans. Commun.*, vol. 70, no. 7, pp. 4745-4754, Jul. 2022.

[237] L. Liu, J. Liang, and K. Huang, "Eavesdropping against artificial noise: Hyperplane clustering," in *Proc. IEEE 3rd Int. Conf. Inf. Sci. Technol. (ICIST)*, Yangzhou, China, Feb. 2013, pp. 1571-1575.

[238] H. Niu, Y. Xiao, X. Lei, G. Wang, M. Xiao, and S. Mumtaz, "When the CSI from Alice to Bob is unavailable: What can Eve do to eliminate the artificial noise?," in *Proc. IEEE 96th Veh. Technol. Conf. (VTC2022-Fall)*, London, United Kingdom, Sep. 2022, pp. 1-5.

[239] H. Niu, X. Lei, G. Wu, G. Wang, C. Yuen, and F. Adachi, "Artificial noise elimination without the transmitter-receiver link CSI," *IEEE Trans. Veh. Technol.*, vol. 73, no. 9, pp. 13206-13218, Sep. 2024.

[240] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[241] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 2809-2812.

[242] Q. Li, W. K. Ma, and A. M. C. So, "Robust artificial noise-aided transmit optimization for achieving secrecy and energy harvesting," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Florence, Italy, Jul. 2014, pp. 1596-1600.

[243] P. Wang, Z. Yan, N. Wang, and K. Zeng, "Resource allocation optimization for secure multidevice wirelessly powered backscatter

communication with artificial noise," *IEEE Trans. Wireless. Commun.*, vol. 21, no. 9, pp. 7794-7809, Sep. 2022.

[244] W. Wang, X. Chen, L. You, X. Yi, and X. Gao, "Artificial noise assisted secure massive MIMO transmission exploiting statistical CSI," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2386-2389, Dec. 2019.

[245] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1-5.

[246] A. Zappone, P. -H. Lin, and E. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J.Sel. Top. Signal Process.*, vol. 10, no. 8, pp. 1462-1477, Dec. 2016.

[247] H. M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285-6298, Dec. 2015.

[248] H. Son and S. Park, "Antenna grouping-based blind artificial noise for TDD secure transmission," *IEEE Access*, vol. 9, pp. 124348-124359, Aug. 2021.

[249] S. R. Aghdam and T. M. Duman, "Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate," *IEEE Trans. Wireless. Commun.*, vol. 16, no. 6, pp. 3913-3923, Jun. 2017.

[250] H. M. Wang, C. Wang, D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050-4064, Aug. 2016.

[251] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170-2181, Jun 2013.

[252] W. Yuan et al., "New delay Doppler communication paradigm in 6G era: A survey of orthogonal time frequency space (OTFS)," *China Commun.*, vol. 20, no. 6, pp. 1-25, Jun. 2023.

[253] A. Özcelikkale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2234-2238, Dec. 2015.

[254] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885-887, Oct. 2010.

[255] H. Chen, X. Tao, N. Li, and X. Li, "Secrecy performance of the artificial noise assisted broadcast channel with confidential messages and external eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1-6.

[256] B. Wang and P. Mu, "Artificial noise-aided secure multicasting design under secrecy outage constraint," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5401-5414, Dec. 2017.

[257] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1568-1571, Aug. 2013.

[258] C. Wang, Z. Li, X. G. Xia, J. Shi, J. Si, and Y. Zou, "Physical layer security enhancement using artificial noise in cellular vehicle-to-everything (C-V2X) networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15253-15268, Dec. 2020.

[259] A. Araujo, J. Blesa, E. Romero, and O. Nieto-Taladriz, "Artificial noise scheme to ensure secure communications in CWSN," in *Proc. 8th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Limassol, Cyprus, Aug. 2012, pp. 1023-1027.

[260] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116-2129, May 2016.

[261] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Artificial-noise-aided optimal beamforming in layered physical layer security," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 72-75, Jan. 2019.

[262] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Secure transmission in interference alignment (IA)-based networks with artificial noise," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, Nanjing, China, May 2016, pp. 1-5.

[263] Q. Xu, P. Ren, Q. Du, and L. Sun, "Security-aware waveform and artificial noise design for time-reversal-based transmission," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5486-5490, Jun. 2018.

[264] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, "Three artificial-noise-aided secure transmission schemes in wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3669-3673, Apr. 2018.

[265] A. S. Leong, A. Redder, D. E. Quevedo, and S. Dey, "On the use of artificial noise for secure state estimation in the presence of eavesdroppers," in *Proc. Eur. Control Conf. (ECC)*, Limassol, Cyprus, Jun. 2018, pp. 325-330.

[266] Y. Zhong, Y. Xiao, and H. Niu, "Transmit antenna selection and artificial noise design for secure STBC-SM transmission," in *Proc. IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Helsinki, Finland, Jun. 2022, pp. 1-6.

[267] J. Joung and C. Yuen, "Space-time line code hopping for physical-layer secure communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 7720-7729, Aug. 2024.

[268] Y. Pang, X. Lei, Y. Xiao, and H. Niu, "Reconfigurable intelligent surface assisted space-time line code for SIMO transmission," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 3069-3073, Dec. 2022.

[269] H. Niu, X. Lei, J. An, L. Zhang, and C. Yuen, "On the efficient design of stacked intelligent metasurfaces for secure SISO transmission," *IEEE Trans. Inf. Forensics Secur.*, vol. 20, pp. 60-70, Nov. 2024.

[270] H. Niu, J. An, L. Zhang, X. Lei, and C. Yuen, "Enhancing physical layer security for SISO systems using stacked intelligent metasurfaces," in *Proc. 2024 IEEE VTS Asia Pacific Wireless Commun. Symp. (APWCS)*, Singapore, Aug. 2024, pp. 1-5.

[271] J. Zheng et al., "Unlocking FAS-RIS security analysis with block-correlation model," *IEEE Wireless Commun. Lett.*, early access, 2025, doi: 10.1109/LWC.2025.3561763.

[272] S. Yang et al., "Towards intelligent antenna positioning: Leveraging DRL for FAS-aided ISAC systems," *IEEE Internet Things J.*, early access, 2025, doi: 10.1109/JIOT.2025.3576235.

[273] T. Wu, et al., "Fluid antenna systems enabling 6G: Principles, applications, and research directions," arXiv: 2412.03839[eess.SP], Dec. 2024.

[274] E. Shi et al., "Joint AP-UE association and precoding for SIM-aided cell-free massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 24, no. 6, pp. 5352-5367, Jun. 2025.

[275] E. Shi, J. Zhang, Y. Zhu, J. An, C. Yuen, and B. Ai, "Uplink performance of stacked intelligent metasurface-enhanced cell-free massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 24, no. 5, 3731-3746, May 2025.

[276] E. Shi et al., "RIS-aided cell-free massive MIMO systems for 6G: Fundamentals, system design, and applications," *Proc. IEEE*, vol. 112, no. 4, pp. 331-364, Apr. 2024.

[277] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1196-1217, May. 2023.

[278] Xu J et al., "Reconfiguring wireless environments via intelligent surfaces for 6G: Reflection, modulation, and security," *Sci. China Inf. Sci.*, vol. 66, no. 3, pp. 130304, Nov. 2023.

[279] H. Niu, Y. Xiao, X. Lei, L. Dan, W. Xiang, and C. Yuen, "Reconfigurable intelligent surface-assisted passive beamforming attack," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 8236-8247, Aug. 2024.

[280] L. Zhang, X. Lei, T. Ma, H. Niu, and C. Yuen, "Joint User Localization, Channel Estimation, and Pilot Optimization for RIS-ISAC," *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 19302-19316, Dec. 2024.