CONTRIBUTED PAPER

Physical Layer Covert Communication in B5G Wireless Networks—Its Research, Applications, and Challenges

This article provides an extensive overview of the basic theories and several strategies in physical layer covert communications.

By Yu'e Jiang, *Member IEEE*, Liangmin Wang, *Member IEEE*, Hsiao-Hwa Chen, *Fellow IEEE*, and Xuemin Shen, *Fellow IEEE*

ABSTRACT | Physical layer covert communication is a crucial secure communication technology that enables a transmitter to convey information covertly to a recipient without being detected by adversaries. Unlike typical cryptography and physical layer security systems that concentrate on protecting the sent signal content, covert communications seek to conceal the existence of legitimate transmission. Thus, with beyond fifth-generation (B5G) wireless communications, covert communications can operate in tandem or as a supplement to conventional security techniques. We provide an extensive overview of the basic theories and several strategies in physical layer covert communications in this article. In particular, we go into great detail about the basic theories of physical layer covert communications, such as channel models, codes, secret keys, and covertness metrics, as well as various covert schemes in progressively more complicated scenarios, such as covert communications in single-antenna and multiantenna three-node systems and covert communications in jammer- and relay-aided systems. In addition, we identify the challenges and future directions for research on covert communications in B5G wireless networks.

KEYWORDS | Communication security; covert communications; jammer-/relay-aided communications; multiantenna.

Manuscript received 21 August 2022; revised 1 June 2023 and 21 December 2023; accepted 2 February 2024. Date of publication 21 February 2024; date of current version 4 March 2024. This work was supported in part by the National Natural Science Foundation of China under Grant U1764263; in part by the Key Project on Anhui Provincial Natural Science Study by Colleges and Universities under Grant KJ2020A0497; and in part by the Taiwan Ministry of Science and Technologies under Grant 109-2221-E-006-175-MY3, Grant 109-2221-E-006-182-MY3, and Grant 112-2221-E-006-127. *(Corresponding authors: Hsiao-Hwa Chen; Liangmin Wang.)*

Yu'e Jiang is with the University Key Laboratory of Intelligent Perception and Computing of Anhui Province, Anqing Normal University, Anqing 246011, China (e-mail: jiang2012118@163.com).

Liangmin Wang is with the School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China (e-mail: liangmin@seu.edu.cn).

Hsiao-Hwa Chen is with the Department of Engineering Science, National Cheng Kung University, Taiwan 70101, Taiwan (e-mail: hshwchen@ieee.org).

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@uwaterloo.ca).

Digital Object Identifier 10.1109/JPROC.2024.3364256

NOMENCLATURE

5G/B5G/6G	Fifth generation/beyond 5G/sixth generation.
PLS	Physical layer security.
SRL	Square-root law.
CSI/CDI	Channel state information/channel distribution information.
FD/HD	Full-duplex/half-duplex.
BS	Base station.
PSD	Power spectral density.
UWB	Ultrawideband.
LPD	Low probability of detection.

IoT	Internet of Things.
AWGN	Additive white Gaussian noise.
AN	Artificial noise.
UAV	Unmanned aerial vehicle.
IRS	Intelligent reflecting surface.
mmWave/THz	Millimeter wave/terahertz.
FA/MD	False alarm/missed detection.
DMC	Discrete memoryless channel.
MAC	Multiple-access channel.
BSC	Binary symmetric channel.
PPM/MLC	Pulse-position modulation/multilevel coding.
KL/NP	Kullback–Leibler/Neyman–Pearson.
MISO/MIMO	Multiple-input single-output/ multiple-input multiple-output.
SIMO	Single-input multiple-output.
SNR	Signal-to-noise ratio.
SI	Self-interference.
TCIPC	Truncated channel inversion power control.
ZF	Zero-forcing.
NOMA	Nonorthogonal multiple access.
ST	Secondary transmitter.
TCI	Truncated channel inversion.
p.p.p.	Poisson point process.
AF	Amplify-and-forward.
NE	Nash equilibrium.
MRT	Maximum-ratio transmission.
SWIPT/HOR	Simultaneous wireless information and power transfer/harvest-and-opportunistically-relay.
MC/FC	Markov chain/fusion center.
PDE	Probability of detection error.
ACR	Average covert rate.
SDR	Semidefinite relaxation.
GAN	Generative adversarial network.
DRL	Deep reinforcement learning.
QKD	Quantum key distribution.
D2D	Device-to-device.

I. INTRODUCTION

A. Background

While the 5G wireless communication networks are being implemented globally, it is anticipated that these networks will not be sufficient by 2030 and beyond [1], [2], [3], [4]. With new paradigm shifts such as integrated space–air–ground communication networks, full-spectrum exploration, extremely heterogeneous networks, and network security, B5G or the 6G will spearhead a comprehensive wave of the digital revolution in the economy and society [5], [6], [7], [8]. To meet the need for ubiquitous and massive wireless connectivity, a large-scale heterogeneous network architecture that incorporates satellites, UAVs, and other devices will be investigated. A broader spectrum range, encompassing sub-6 GHz, mmWave, and THz, will be explored in order to offer an ultrahigh data rate. Furthermore, B5G will stimulate creative smart applications powered by machine learning (ML) and artificial intelligence. Not to mention, B5G needs robust or endogenous network security for both the physical and network layers in order to establish trust in a variety of services, such as entertainment, telemedicine, and autonomous driving.

While conventional cryptography can be employed to increase wireless communications security, adversaries with ever-increasing computing power remain a threat to its integrity [9], [10]. Traditional upper layer security cryptography systems (such as application layer cryptography) can be supplemented by PLS. On one hand, traditional security techniques outlined above concentrate on safeguarding the information content that is delivered, leaving the transmission's existence vulnerable to detection by adversaries. On the other hand, the primary goal of physical layer covert communication is to prevent eavesdroppers from hearing/deciphering the information that is received, with the help of natural characteristics of wireless channels, such as noise and interference [11], [12], [13], [14]. There are many instances where users try to communicate without being detected by others. To prevent an enemy from attacking after learning of a transmission, for instance, a side in a military combat action may want to communicate information surreptitiously [15]. In a dynamic spectrum access network, a secondary user attempting to communicate without being detected by the primary user is another example [16]. Sending information in a way that makes it invisible to its enemies might, therefore, be the better course of action.

Thankfully, physical layer covert communications make it possible for a transmitter to securely and covertly communicate with a recipient without being detected by adversaries [17], [18]. The scaling law for physical layer covert communications over AWGN channels was discovered in [17], a landmark study by Bash et al. More specifically, the SRL states that the maximum amount of information bits that may be reliably and covertly conveyed is equal to the square root of the block length n. For a number of metrics [18] and channels [16], [19], [20], [21], [22], [23], this scaling law has been improved and characterized. Specifically, the first tight capacity bound for DMCs was provided by Bloch [16] and Wang et al. [19]. In addition, a number of significant technical results were established, which either generalize or expand on previous works, such as improving upon [17] in terms of secret-key length. There has also been discussion of codes and secret keys for covert communications at the physical layer [16], [20], [24], [25]. Wang and Bloch [24] provided the first code with efficient key and verifiable guarantees. Keyless communications were set up for MACs [20] and DMCs [16], [25]. Section II provides details on other contributions made in [16], [17], [18], [19], [20], [21], [22], [23], [25], and [24]. Nevertheless, when $n \to \infty$, the covert rate is zero, meaning that $\lim_{n\to\infty}(O((n)^{1/2})/n) = 0$. Encouraged by these foundational studies [16], [17], [18],

[19], [20], [23], additional investigations revealed that a positive covert rate (explained in Section III) could be produced by the adversary's ambiguity regarding wiretap channel noise [26], covert signal transmit time [27], and CSI [28]. Subsequently, in combination with different practical considerations, it was discovered that the covertness requirement can also be met, and even the covert rate can even be increased by using ANs or jamming signals from jammers [15], randomly located friendly nodes [29], Poisson distributed interferers [30], greedy relays and FD relays [31], [32], or FD receivers [33], [34] (see more discussions in Sections IV–VI).

Given its capacity to conceal wireless communications, physical layer covert communication has the potential to serve as the first line of protection against malicious attacks. At the same time, it may be used as an additional security mechanism in conjunction with or in addition to existing security measures [34], [35], [36], [37], [38]. Some study on physical layer covert communication in B5G networks has recently been undertaken [39], [40], [41]. For instance, Tatar Mamaghani and Hong [39] focused on the construction of an energy-efficient multi-UAV wireless communication system for covert data dissemination in the B5G IoT network operating at THz bands. Physical layer covert transmissions in 6G wireless networks using numerous essential technologies, including reconfigurable intelligent surface (RIS), rate-splitting multiple access, and NOMA, were investigated [40]. Yang et al. [41] addressed the topic of covert communication in cellular-enabled UAV networks, which is envisioned as a network paradigm in B5G wireless networks. In this regard, physical layer covert communications are predicted to be a significant security solution to fulfill the ever-increasing requirement for robust security in B5G or 6G wireless networks while also leaving numerous security and performance improvement difficulties as challenges. The possibilities and problems of physical layer covert communication in B5G wireless networks will be examined in the Motivation subsection, and more will be covered in Section VII.

B. Physical Layer Covert Communications

Covertness and communication performance are two key concerns that need to be balanced in the context of physical layer covert communications [17]. To do the following analysis, consider a simple covert communication network depicted in Fig. 1 without losing generality. Its primary goal is to make it possible for a sender (Alice) to securely communicate data to a legitimate user (Bob) all the while ensuring that the communication itself is hidden from detection by an adversary (Willie). From the adversary's (Willie's) point of view, covertness ought to be quantified in order to determine how the statistics of the observations vary when communication is present vs absent. Conversely, from the standpoint of the transmitter (Alice), we must tackle the problems of enhancing the main link's communication performance

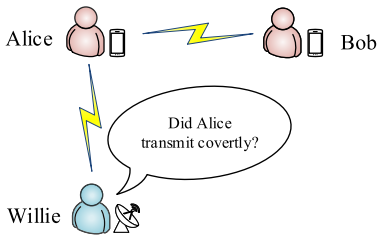

Fig. 1. *Illustration of physical layer covert communications, where Alice, the transmitter, wishes to send signals to Bob, the receiver, in a covert manner so that Alice is not discovered by Willie, the adversary.*

(the Alice-to-Bob channel) while maintaining the necessary levels of covertness.

In order to determine if Alice transmits, Willie typically uses a statistical hypothesis testing on its received signals [17]. The measure of covertness is the adversary's error detection probability; several metrics can be applied to particular application scenarios, as discussed in Section II-D [17], [18], [38]. The total variation distance between the channel output distributions created with and without communication between Alice and Bob can be used to quantify covertness for an optimal detector at Willie. From Alice's point of view, the design of Alice's transmit information, including the coding structure and transmit power, will constrain Willie's detection performance since the total variation represents a lower constraint on the error of all hypothesis tests that Willie can utilize. However, as further discussed in Section II, Alice's coding method to achieve covert capacity is typically connected to the block length n. As previously said [17], the maximum amount of trustworthy and covert bits via n channel usage is approximately $(n)^{1/2}$ bits. Because of this, performance analysis is made more challenging by the covertness constraint. Alice's coding scheme must be carefully designed to address a tradeoff between communication performance and the requirement for covertness, such that Alice can reliably and covertly transmit data to Bob with capacity-achieving performance.

C. Physical Layer Covert Communications Versus Other Security Techniques

The field of covert communication has its roots in early hidden information transmission technologies, which shares a long history with steganography where a network protocol must be used as a carrier when creating a covert communication channel. For example, information can be hidden in software binary codes or images [42], inserted into training sequences, cyclic prefixes, or a corrupted constellation of Wi-Fi signals [43], [44], [45]. Traditional steganography requires embedding cover signals, which are typically found in text, into innocent content.

Spread spectrum techniques are an alternate covert communication scheme on the physical layer that has been examined in [46]. The goal of spread spectrum

Table 1 Physical Layer Covert Communications Versus Traditional Security Schemes

Types	Physical layer	Covertness	Information-theoretic	Focuse	Typical characteristics
Conventional cryptography [9, 10]	–	–	–	Protect the content of transmitted signals	There is a risk that adversaries with strong computers could break it.
Physical layer security [11–14]	✓	–	✓	Protect the content of transmitted signals	By using the randomness of wireless media, it seeks to increase the rate difference between legitimate and eavesdropping channels.
Steganography [42–45]	–	✓	–	Hide the transmitted covert information	It uses an agreed network protocol as a carrier and inserts covert messages into seemingly innocent content.
Spread spectrum techniques [46]	✓	–	✓	Reduce PSD of transmit signal with low visibility	It expands signal spectrum to improve the robustness of communications.
Physical layer covert communications [19, 23, 35, 47]	✓	✓	✓	Send information covertly without being discovered by adversaries	Two issues should be addressed jointly, i.e., covertness and communication performance requirements.

"Physical layer" column: ✓denotes the techniques were examined from the perspective of the physical layer; otherwise, it is shown as –.
"Covertness" column: ✓denotes the approaches can be used to send signals covertly, and the achieved covertness has been theoretically verified; otherwise denoted as –.
"Information-theoretic" column: ✓denotes the schemes were studied from an information-theoretic perspective; otherwise denoted as –.

techniques is to partially conceal transmitted signals by lowering the PSD of transmit signals with low visibility. One way to think of the UWB signal as a covert option is that it can be transmitted considerably below the noise level of an interceptor. However, as noted in the works of [17], the underlying notions of covert communications and feasible covertness have not been thoroughly explored in a systematic way until quite recently. Table 1 compares various similar strategies for covert communications at the physical layer. As was previously said, PLS and conventional cryptography prioritize signal content protection over signal covertness, which may not meet the needs of the transmitted signal. While both spread spectrum and steganography have their uses in concealing signal transmissions, both have their limitations. For example, spread spectrum techniques cannot be theoretically demonstrated to achieve covertness [38], and steganography typically requires a network protocol as a carrier.

On the other hand, from an information-theoretic standpoint, the research of physical layer covert communications should address two fundamental issues: covertness and communication performance requirements. The literature has a number of tutorial works on covert communications at the physical layer. This survey notes that the term "covert communications" will be used synonymously to refer to the following concepts: LPD [17], [19], [35], stealthy [23], [47], [48], [49], [50], undetectable [26], [51], [52], or covert wireless communications [30], [35], [36], [53]. This is because all of those terms have a similar meaning when it comes to covert communications.

D. Motivations

Physical layer covert communications will face both opportunities and challenges with the rapid advancement of B5G networks and the impending new paradigm shifts, new network architectures, massive device deployments with diverse characteristics, and the integration of various new technologies [5], [39], [40], [41], [53].

In particular, the following factors primarily highlight the opportunities. To meet the requirements for covertness, physical layer covert communications generally take advantage of opponents' uncertainty. Examples of such strategies include artificial interference, distance information, channel fading coefficients, coding design, and more [24], [29], [30], [54]. To meet the requirements for covertness in B5G wireless networks, a higher degree of freedom can be explored for designing uncertainty factors against eavesdroppers. The actual placement of equipment or nodes, the introduction of new devices, or the use of novel technology can all accomplish these goals.

To forward the covert signals, for instance, a UAV equipped with an IRS acts as a relay [55]. As of right now, 6G wireless networks are needed in order to facilitate 5G systems' improved latency, higher energy efficiency, ultramassive machine-to-machine connections, faster data speeds, and greater user diversity. In the framework of covert communications, a multitude of solutions will be discovered to fulfill the requirements of both performance and covertness in B5G wireless networks. To increase the transmission rate, thousands of antennas or extremely massive antenna arrays could be installed at the transceivers. Higher data speeds can be supported by high-frequency spectrum, such as THz and mmWave bands, which can offer an enormous accessible bandwidth [56], [57]. Covert communications, as a secure communication technology, have drawn a lot of attention with the rapid development of B5G wireless communications. These applications include covert communications in near-field communications, ML-based covert communications, and quantum-enhanced covert communications [58], [59], [60].

Potential challenges will also surface if more thorough research is done on covert communications in B5G wireless networks. Covert communication systems in complex B5G networks, such as massive nodes, multilink coexistence in ultradense networks, high network scalability, and THz wireless systems, may make network modeling more

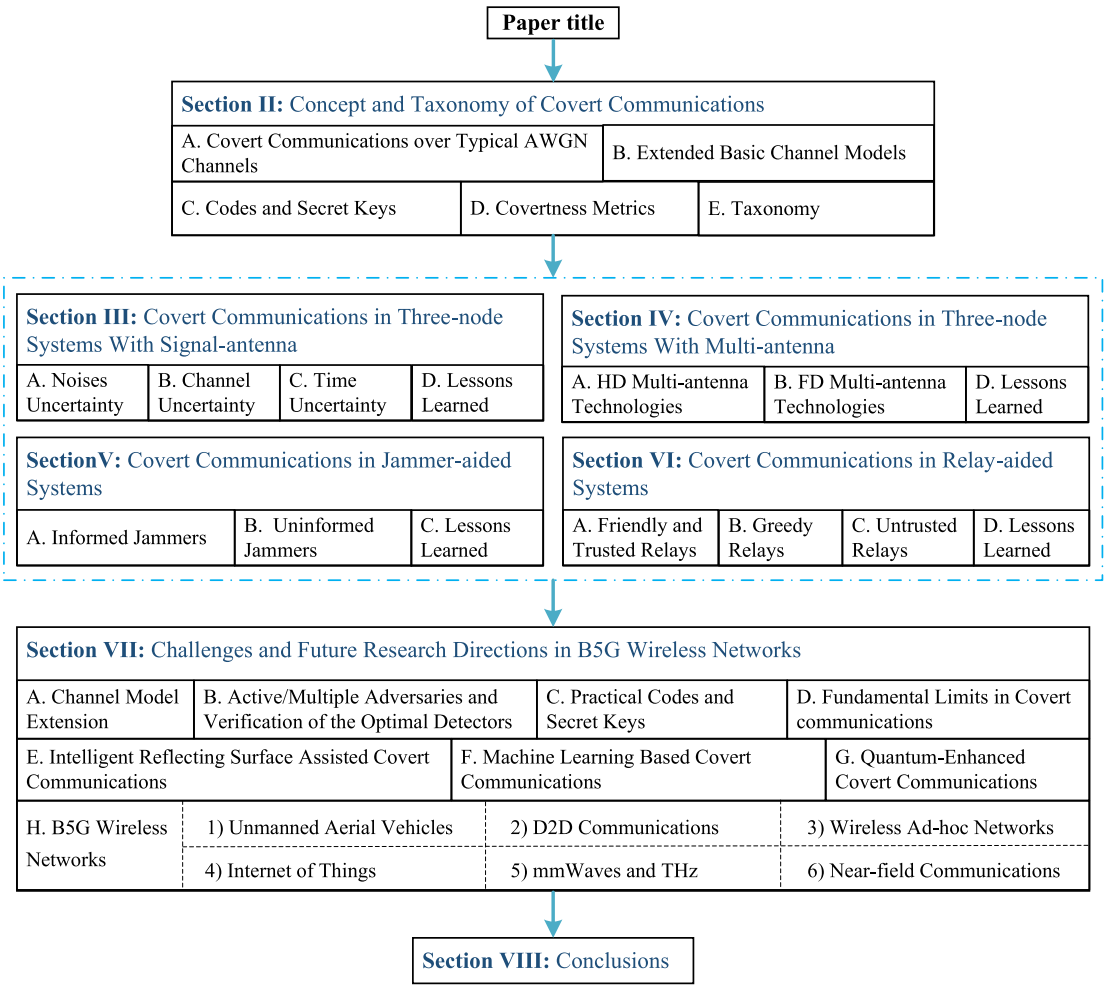

Fig. 2. ***Structural diagram of this survey.***

challenging because it can be difficult to directly apply traditional channel models to new architectures, such as the mmWave/THz channel [53] and new air interface [5]. To balance the covertness and communication data rate, sophisticated interference management and resource coordination are required, which poses new challenges for the optimization and analysis of overall covert performance. As a result of technological advancements, opponents' detection abilities, such as those of active adversaries [61] and multiple colluding adversaries [62], continue to advance, creating new challenges for the development of covert communication schemes.

However, due to the rapid advancement in physical layer covert communication research in recent years, some important up-to-date works are missing in the currently available surveys [35], [47], [63]. Only a small number of pertinent references are covered by the existing surveys, and the majority of them are specialized to certain networks or systems, such as UAV-assisted networks [64] and IoT systems [36]. Second, in contrast to previous surveys [35], [63], we offer a taxonomy that tracks the increasing intricacy of application scenarios in order to evaluate the current covert schemes and extract the knowledge that will facilitate further research on B5G wireless networks. We hope that this will enable users to understand how to use network resources in covert communication scheme designs for various application scenarios in an efficient manner. Finally, and perhaps most importantly, we list several unresolved difficulties and research challenges related to covert communications at the physical layer in B5G wireless networks. The important features of this survey and those that already exist are listed in Table 2.

In conclusion, a review of the most recent findings in physical layer covert communications is required. More than 200 generally pertinent papers and books are included in this survey. In addition, it points out unresolved problems and research obstacles related to the application of covert communications in B5G networks.

E. Salient Features of This Article

In order to highlight research objectives and problems for covert communications in B5G wireless networks, we intend to make a thorough assessment of the most recent research efforts on physical layer covert communications in this study. This survey article's structural diagram is shown in Fig. 2, and Nomenclature provides a list of the

Table 2 Important Features of This Survey on Physical Layer Covert Communications and Those That Already Exist

Authors	Year	Contributions
Che *et al.* [47]	2014	A review on reliable, deniable, and hidden communications.
Bash *et al.* [35]	2015	Basic limits of covert communications by hiding information in noise backgrounds.
Liu *et al.* [36]	2018	Covert transmissions in the IoT networks using interference to hide confidential information.
Yan *et al.* [63]	2019	Summarize the key features of low detection probability communications.
Jiang *et al.* [64]	2021	Focus on the issues of covert communications in UAV-assisted networks, e.g., typical applications and covert schemes.
This survey	2024	A comprehensive survey on the theories and techniques of covert communications emerging in recent years, to identify its applications and challenges in B5G wireless networks.

abbreviations used throughout this article for convenient cross-referencing. The following is a list of this article's main features.

1) The concept of covert communications in AWGN channels provides a theoretical basis for covert schemes design in B5G wireless networks, including the setting of codes and secret keys, the definitions of covertness metrics, and the fundamental limits of covert communications, as detailed in Section II. Based on these important concepts, we can go ahead to conduct the performance evaluation for more generalized use cases, including covert communications over other basic channel models.
2) Following the gradual complexity of application scenarios, we present a taxonomy for the existing research on covert communications, i.e., covert communications in three-node systems with single antenna (see discussion in Section III), in three-node systems with multiantenna (detailed in Section IV), in jammer-aided systems (more discussion in Section V), and in relay-aided systems (detailed in Section VI). Based on this taxonomy, the covert schemes and their performance are analyzed and discussed, and their advantages and challenges arising from the gradual complexity of application scenarios are revealed, which sheds light on the design of covert schemes in B5G wireless communications.
3) More research challenges and open issues for physical layer covert communications in B5G wireless networks are identified in Section VII. Specifically, they include channel model extension, active/multiple adversaries, verification of the optimal detectors, practical codes and secret keys design, fundamental limits in covert communications, IRS-assisted covert communications, machine-learning-based covert communications, quantum-enhanced covert communications, and the covert communications in B5G wireless networks, including UAVs, mmWaves, THz, and near-field communications.

II. CONCEPTS AND TAXONOMY OF COVERT COMMUNICATIONS

The method of covert communications over a typical discrete-time AWGN channel, along with its extension and key components, will be covered in this section. In addition, the taxonomy utilized in this work will be presented as well.

A. Covert Communications Over Typical AWGN Channels

Let us take the discrete-time AWGN channel model from the seminal work in [17] as an example to analyze the processes of covert communications. As illustrated in Fig. 3, a single-antenna three-node communication system consists of a transmitter (Alice), a legitimate receiver (Bob), and an adversary (Willie). Alice attempts to reliably communicate with Bob over an AWGN channel while keeping the communication undetectable for Willie who is observing over another AWGN channel. In this model, Willie is assumed to be a passive eavesdropper, and it does not intend to jam the legitimate link between Alice and Bob.

The first theorem in [17] was proven using the whole codebook that Alice and Bob secretly share. Their further discussions revealed that a public codebook can be utilized when Alice and Bob share $O((n)^{1/2}\log n)$ covert bits. In this case, we assume that Alice and Bob use a public codebook C_0 and that they also share a secret key S, which they keep hidden from Willie. Let Λ be a binary variable that represents Alice's current state. The input blocks of M bits are encoded to a n-bit codeword with a rate of $R = M/n$ bits/symbol if $\Lambda = 1$ and with the aid of S.

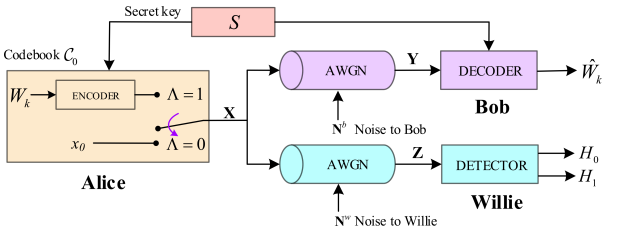

Fig. 3. *Structural diagram of covert communications over a discrete-time AWGN channel. When Alice's transmission status satisfies $\Lambda = 1$ with a codebook $\mathcal{C}_0$ and a secret key S, the message W_k is encoded into X. If $\Lambda = 0$, Alice is not sending covert messages, and it always transmits x_0, here set so that $x_0 = 0$. N^b and N^w are noises observed at Bob and Willie. With the observed vector Y, Bob estimates Alice's message as $\hat{W}_k$. Based on the observed vector Z, Willie employs a statistical hypothesis test to determine whether Alice transmits the message H_1 or not H_0.*

The message W_k is encoded into $X = (X_1, X_2, \ldots, X_n)$, as illustrated in Fig. 3.

The received vector at Bob is denoted as $Y = (Y_1, Y_2, \ldots, Y_n)$, and each symbol is equal to $Y_i = X_i + N_i^b$, $i \in (1, 2, \ldots, n)$, where $N^b = [N_1^b, N_2^b, \ldots, N_n^b]$ is a noise vector of the AWGN channel from Alice to Bob. Similarly, the received vector at Willie is $Z = (Z_1, Z_2, \ldots, Z_n)$, and each symbol is equal to $Z_i = X_i + N_i^w$, where $N^w = [N_1^w, N_2^w, \ldots, N_n^w]$ is the noise vector of the AWGN channel between Alice and Willie.

If $\Lambda = 0$, Alice has no covert message to transmit, and hence, here, we set $x_0 = 0$. Each received symbol is equal to $Y_i = N_i^b$ at Bob and $Z_i = N_i^w$ at Willie. Moreover, both N_i^b and N_i^w are independent identically distributed (i.i.d.) random variables, i.e., $N_i^b \sim \mathcal{N}(0, \sigma_b^2)$ and $N_i^w \sim \mathcal{N}(0, \sigma_w^2)$.

In order to determine Alice's transmission state, Willie runs a statistical hypothesis test on its received vector of n channel observations $\mathbf{Z}$. The null hypothesis H_0 denotes that Alice does not transmit and its corresponding probability distribution of the adversary's channel observations is $\mathbb{P}_0$. H_1 is an alternative hypothesis, in which Alice is sending the message, and the probability distribution of Willie's channel observation is $\mathbb{P}_1$. Assume that Willie has an equal prior probability for H_0 and H_1, i.e., $\mathbb{P}(H_0) = \mathbb{P}(H_1) = 0.5$. More discussion is detailed in Section II-D. In the process of Willie's statistical test, there are two types of errors, i.e., FA and MD. When Alice is not transmitting, while Willie rejects H_0, the probability is denoted as $\mathbb{P}_{\text{FA}}$ (or α). Otherwise, when Alice is transmitting, the probability that Willie accepts H_0 is $\mathbb{P}_{\text{MD}}$ (or β). Combined with Fact 1 in [17], $\alpha + \beta = 1 - \mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$ is used to measure the covertness, where $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$ is the total variation distance between $\mathbb{P}_0$ and $\mathbb{P}_1$. Thus, Alice can limit Willie's detection performance by upper bounding the total variation distance, i.e., $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \leq \epsilon$.

In addition to the covertness requirements that should be guaranteed, covert communications also need to ensure that Bob can correctly decode the information sent by Alice. Based on the received vector $\mathbf{Y}$, Bob will decode and estimate message W_k transmitted by Alice as $\hat{W}_k$. Here, the probability of Bob's detection error is calculated by averaging over C_0, that is, $P_e^b = \mathbb{E}_{\mathcal{C}_0}[\mathbb{P}(\hat{W}_k \neq W_k)]$. As proved in [17], if Alice knows a lower bound of Willie's channel noise, with the covertness constraint $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \leq \epsilon$, P_e^b decays exponentially to zero as n increases and Bob obtains $O((n)^{1/2})$ covert bits in n channel uses. Conversely, if Alice attempts to transmit $\omega((n)^{1/2})$ covert bits over n channel resource units, then, as $n \to \infty$, either Willie detects her message with an arbitrarily low error probability or Bob cannot decode her message reliably.

In summary, the following procedures can be used to assess and quantify the previously mentioned covert communication between Alice and Bob.

1) *Key and codebook:* Before transmission, Alice and Bob share a secret key S, and a public codebook C_0 is utilized. Using the shared secret key S, the covert message W_k is encoded into $\mathbf{X} = Enc_{\mathcal{C}_0}(\cdot)$ if Alice's current status is $\Lambda = 1$. This is done while making sure that Willie is unaware of it. Alice then sends out the secret signal vector X.
2) *Willie's detection rule:* Based on the observation vector $\mathbf{Z}$, Willie performs a statistical hypothesis test to determine the transmission state of Alice. The probability of Willie's error detection is adopted to measure the covertness.
3) *Bob's detection and covert performance:* Based on the received vector $\mathbf{Y}$, Bob will decode and estimate the transmitted message as $\hat{W}_k$. To ensure that the probability of Bob's error detection decays exponentially to zero and the probability of Willie's error detection meets the covertness requirement, the number of bits that can be transmitted to Bob is used to quantify the performance of covert communications.

According to Bash et al. [17], SRL governs covert communication across discrete AWGN channels, that is, the number of reliable and covert message bits over n channel uses scales as much as $(n)^{1/2}$. The precise constant before $(n)^{1/2}$, which functions as a covert capacity, has subsequently been characterized for various channels: DMCs and AWGN channels [16], [18], [19], MACs [20], classical-quantum channels [65], and noncoherent fast Rayleigh-fading wireless channel [66]. In particular, Bloch [16] and Wang et al. [19] characterized the first tight capacity bound for DMCs. Subsequently, Tahmasbi and Bloch [18] investigated the first- and second-order asymptotic behaviors of covert communications for three different covertness metrics over binary-input DMCs. Please refer to Section II-B for additional information regarding covert communications over DMCs. It was demonstrated that an amplitude-constrained input distribution, which has a finite number of mass points, including the one at zero, may be used to attain the covert capacity in a noncoherent fast Rayleigh-fading wireless channel [66]. Furthermore, it suggested that the input distribution might be best with two mass points at fixed places. $(2)^{1/2}\theta_m^2$ was obtained as a straightforward bound for covert capacity; the definition of θ_m is given in [16, Th. III.1].

Performance analysis is more challenging because, for the covertness requirement, the block length n is typically connected to the ideal input distribution to attain capacity [16], [19], [66]. For DMC channels, for instance, the input distribution that must be employed to reach capacity is a sparse distribution, where the covert symbols are used for a fraction of $1/(n)^{1/2}$ when they are transmitted. Gaussian or Binary phase shift keying signaling with an average power diminishing as $O(1/n)$ is the best coding strategy for AWGN channels. Therefore, it is essential for optimality to encode information in the phase of modulation symbols along with a proper power [66]. In order to simplify the performance analysis and demonstrate other aspects, such as the adversary's uncertainty from an uninformed jammer,

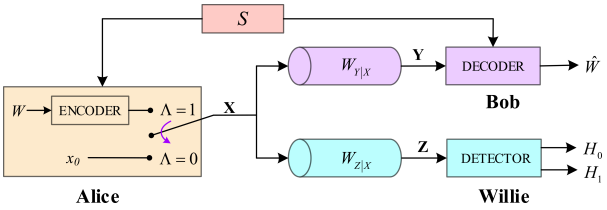

Fig. 4. *Structural diagram of covert communications over DMCs. When Alice's transmission status is $\Lambda = 0$, an innocent symbol x_0 is sent. If $\Lambda = 1$, the message W is encoded as a vector X with a secret key S. Let $W_{Y|X}$ and $W_{Z|X}$ denote the transition probabilities of Alice-to-Bob and Alice-to-Willie channels, respectively. Based on the obtained vector Y, Bob estimates W as $\hat{W}$. Using the observation of Z, Wille employs a hypothesis test to decide whether Alice transmits the message (H_1) or not (H_0).*

transmit time [27], and a greedy relay [32], some subsequent studies utilize random Gaussian codebooks and set the adversary as a radiometer.

Sections III–VI and the accompanying tables will cover the specifics of the covert performance. As previously mentioned, the process of covert communications involves a number of important components, including the definition of the channel model, the establishment of codes and secret keys, and the assessment of covertness. In the content that follows, we shall examine the related extension cases.

B. Extended Basic Channel Models

Numerous studies on covert communications have been conducted, extending discrete-time AWGN channels to various channel types. Several popular basic channel model types, including DMCs, discrete-time MACs, discrete-time broadcast channels, and continuous-time AWGN channels, will be examined in this section.

1) DMCs: Aspects such as coding techniques, error exponent characterization, and fundamental restrictions of covert communications over DMCs have been studied [16], [19], [21], [23]. Particularly, the works in [16] by Bloch, [19] by Wang et al., and [21] by Tahmasbi et al. offered some interesting insights on covert communication, such as the DMC model derived from [16], as detailed in Fig. 4.

Revisiting the issue of covert communications from a resolvability standpoint, Bloch [16] established a number of technical conclusions that build upon and broaden earlier research. First, a technological improvement on the coding scheme in [17] demonstrated that it is feasible to transmit on the order of $(n)^{1/2}$ reliable and covert bits over n channel uses with on the scale of $(n)^{1/2}\log n$ shared secret bits. Second, when Bob's channel is superior to Willie's channel, a different coding technique was devised that does not require a secret key and simply requires Alice and Bob to share on the order of $(n)^{1/2}$ bits. Third, Theorems 3 and 4 and Corollary 3 in [16] provided explicit formulas for the optimal asymptotic scaling of the message and key size for covert and secrecy communications over DMC and AWGN channels. Tahmasbi et al. [21] defined and proved a characterization of error exponent (which contains the lower and upper bounds) for covert communications over binary-input DMCs, solving the technical challenges that arise from "low-weight" of codewords.

Different from [23], where Willie's channel is "noisier" than Bob's channel, in [19], Bob and Willie observe the same channel outputs but with an available secret key, whereas the objective of Willie is to judge whether the transmitter is ON or OFF (it always transmits 0). Then, Wang et al. refined the scaling result of Bash et al. [17] to establish an optimal asymptotic throughput for covert communications over DMC and AWGN channels in different situations. Detailed formulas on L (for its definition please refer to [19, eq. (7)]) were derived as an indicator to characterize the maximum amount of information that can be transmitted over any DMC under the LPD constraint. For example, it was proven that if input symbol 0 is redundant, L can be infinity. A simple value of $L = (2\mathbf{var}_{Q_0}(\log(Q_0(Y)/Q^*(Y))))^{1/2}$ was derived for DMC under given condition, where $\mathbf{var}_{Q_0}(\cdot)$ denotes the variance of Y with the distribution Q_0, and Q^* is the capacity-achieving output distribution. More results about L for a broad class of DMC and AWGN channels can be found in [19].

2) Discrete-Time MACs: In this model, two legitimate transmitters, Alice 1 and Alice 2, attempt to establish a legitimate communication link with Bob over a discrete-time memoryless MAC, while they do not want Willie, who is observing through another MAC link, to know their communication statuses, as illustrated in Fig. 5. Bloch et al. extended or updated beyond (i.e., part of the converse proof presents more challenges) the achievability and converse techniques that they developed in [16], [19], and [21] to MACs [20], [67].

In [20], a major technical challenge in the converse proof is addressed, capturing the interplay between the weights of two codewords from transmitters. It is proven that there exists a coding scheme to ensure that Alice 1

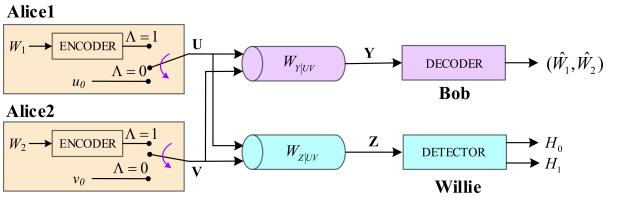

Fig. 5. *Structural diagram for covert communications in discrete-time memoryless MACs. If $\Lambda = 0$, innocent symbols u_0 and v_0 are sent by Alice 1 and Alice 2; otherwise, the messages W_1 and W_2 are encoded into vectors U and V, respectively. Let $W_{Y|UV}$ and $W_{Z|UV}$ denote the transition probabilities of the channels from Alice 1 and Alice 2 to Bob and Willie, respectively. Based on the obtained vector Y, Bob estimates message pair (W_1, W_2) as $(\widehat{W_1}, \widehat{W_2})$. Willie performs a statistical test on his noisy observation Z to determine whether the message pair is transmitted H_1 or not H_0.*

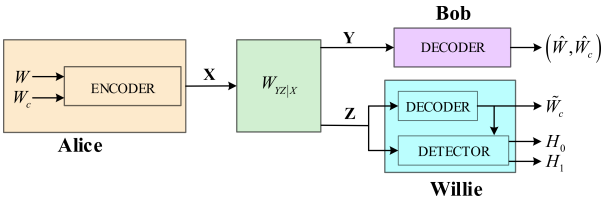

Fig. 6. ***Structural diagram for covert communications over broadcast channels. Alice tries to transmit a common message W_c to Bob and Willie, while a covert message W is available to Bob only. Alice encodes message pair (W, W_c) to X. Bob and Willie obtain Y and Z over the channel $W_{YZ|X}$, respectively. Bob decodes the message pair as $(\hat{W}, \widehat{W_c})$. Willie decodes W_c as $\widetilde{W_c}$ and performs a statistical test to decide whether the covert message has been transmitted (H_1) or not (H_0).***

and Alice 2 covertly and reliably transmit on the order of $(n)^{1/2}$ bits per n channel resources without using a secret key when Bob's channel is "better" than Willie's channel. Moreover, the optimality of the scaling along with the preconstants was established, characterizing the covert capacity region. Arumugam and Bloch [67] extended the work of Arumugam and Bloch [20] to more general scenarios with K transmitters, where each transmitter may use its own shared key with Bob. The covert capacity region of K-user binary-input MAC (for the detail formulas, please refer to [67, Th. 1]) was characterized and provided the achievability and converse proofs. It is shown that each transmitter can covertly and reliably transmit on the order of $(n)^{1/2}$ bits per n channel used. In addition, there are no active constraints on the sum rate.

3) Discrete-Time Broadcast Channels: Let us consider another scenario, in which Alice transmits common signals simultaneously to Bob and Willie over a binary-input discrete memoryless broadcast channel, while covert messages are only available to Bob, as illustrated in Fig. 6. The work reported in [68] addressed the issue of how to hide covert information with the help of an innocent codebook. It found a close relationship between the rate of the codebook and the number of available covert bits. Specifically, when the rate is high enough and close to the channel capacity, an upper bound in the number of covert bits can be obtained. Moreover, the codes for covert and innocent signals were designed jointly in this model. Kibloff et al. [69] considered degraded broadcast channels, in which common messages were predesigned, and total variation distance was adopted to measure the covertness. It characterized the asymptotic performance for this particular class of degraded broadcast models. The work in [70] extended the model to more broadcast scenarios (i.e., channels are not necessarily degraded, less noisy, or more reliable), and time-division strategies were proven to achieve optimal covert performance.

4) Continuous-Time AWGN Channels: In a continuous-time AWGN channel model with a bandwidth constraint of B Hz, if Alice uses an optimal band-limited pulse shape $\mathrm{sinc}(2Bt)$ and extracts information from the channel at a sampling rate of $2B$ samples/s, all conclusions from the discrete-time AWGN models can be applied directly to the continuous-time channel models [71]. Subsequently, covert communication over a continuous-time channel was studied with different constraints. Taking the model in [72] as an example, a spectral mask was applied to curb excessive radiation beyond bandwidth B at Bob. Alice was proven to be able to send $O((BT)^{1/2})$ bits covertly and reliably with a fixed T. When the bandwidth B is infinity or the maximum time T becomes sufficiently large, the covert communications could obtain a positive rate [73].

The issues associated with covert communications over basic channel models are covered in this subsection, and Table 3 compares and summarizes the features and findings of the previously discussed covert communication techniques. The previously presented studies have resulted in a comparatively comprehensive description of the fundamental limits for covert communication across several channel models, together with the presentation of the associated coding schemes and error exponents. These efforts establish a strong basis for the subsequent exploration of more intricate situations, such as the influence of network dynamics, fading, and interference from other nodes.

C. Codes and Secret Keys

Two essential challenges in the characterization of covert communications are code designs and secret key issues, which are discussed as follows.

1) Code Designs: To maintain the required covertness in a covert communication system, Alice typically uses "lightweight" codewords, meaning that their weights are no greater than $O((n)^{1/2})$ [23]. For example, Bob receives a n-bit long sequence from Alice via a BSC, while Willie observes via a different BSC (p_w). If Alice uses binary codes to construct "heavy-weight" codewords [e.g., $w((n)^{1/2})$], Willie can easily count the number of nonzero symbols to derive the status of Alice. If Alice selects codebooks carefully with a "light-weight" codewords [e.g., $O((n)^{1/2})$], Willie's observed value is $np_w + O((n)^{1/2})$ (i.e., the value is about the same as noise level), which may be viewed as noise. In addition, conventional linear codes are unable to meet the requirements for being "lightweight." While a number of works [19], [23], [48], [74] have attempted to introduce nonlinearity through random or stochastic techniques, they are not easily implementable in real-world scenarios or decipherable by the recipient. A nonlinear code that combines a graph-based nonlinear code with a serial concatenation of a linear code was proposed, but without proved guarantees, for covert communications via BSCs [75].

A number of practical codes have recently been proposed for covert communications that either reach or approach the information-theoretic limits with low complexity [24], [76], [77], [78], [80]. Their models, coding schemes, and contributions are compiled in Table 4.

Table 3 Covert Communications Over Basic Channel Models

Time	Channel	Warden	Codes	Keys	Infinite	Characteristics	Conclusions
D	AWGN [17]	G	✓	✓	✓/×	Reveal the scaling law for physical layer covert communications over AWGN channels.	Alice and Bob share $O(\sqrt{n}\log n)$ secret bits to transmit $O(\sqrt{n})$ bits reliably over n channel resource units.
	DMCs/ AWGN [16]	G	✓	✓/×	×	Revisit the problem of covert communications from a resolvability perspective.	Show a series of technical results that generalize and extend prior work [17], e.g., coding schemes, asymptotic scalings of message, and key size.
	DMCs/ AWGNs [19]	G	✓	✓	×	Put Willie in the same position as Bob, requiring a shared secret key, and relative entropy is used as the covertness metric.	Derive a series of optimal asymptotic throughput in different situations, e.g., $L=\sqrt{2\mathbf{var}_{Q_0}(\log(Q_0(Y)/Q^*(Y)))}$ for DMC under given condition.
	Binary-input DMCs [21]	G	✓	✓	✓	Solve the technical challenges that arise from the requirements of covertness and "low-weight" of codewords.	The error exponent and its corresponding upper and lower bounds are derived.
	BSCs [23]	G	✓	–	✓/×	Willie's BSC noise is much larger than Bob's BSC noise.	An arbitrarily small probability of detection is possible without a secret key in this model.
	MACs (two senders) [20]	G	✓	–	✓	Address a technical challenge that is to capture the interplay between the weights of two codewords from transmitters.	Two transmitters can transmit on the order of $\sqrt{n}$ reliable and covert bits per n channel uses, and the pre-constants of the scaling are established.
	MACs (K senders) [67]	G	✓	✓	✓	K transmitters attempt to send covert messages reliably to a legitimate user with its own shared secret key.	Reveal the covert capacity region of K-user binary-input MAC without active constraints on sum-rate.
	Broadcast [68]	G	✓	–	✓	Address the issues of hiding covert signals with the help of an innocent codebook.	When the rate of innocent signals is high enough, a limited number of covert bits can be transmitted.
	Degraded broadcast [69]	G	✓	–	✓/×	The common messages are predesigned and a total variation distance is adopted.	Characterize the asymptotic performance of covert communications for this particular class of degraded broadcast models.
	Broadcast [70]	G	✓	✓	✓	Broadcast channels does not have to be degraded, less noisy, or more reliable.	Time-division strategies is proven to achieve optimal covert performance.
C	AWGN [71]	G	✓	✓	✓	An optimal band-limited pulse shape and extraction rate are adopted.	All the conclusions made for discrete-time AWGN channel models can be applied directly to continuous-time channel models.
	AWGN [72]	G	✓	✓	✓	A spectral mask is applied to curb excessive out-of-band radiation at Bob.	Alice is able to send $O(\sqrt{BT})$ bits covertly and reliably with a fixed T.
	AWGN [73]	G	–	✓	✓	The bandwidth is infinity or the maximum time is sufficiently long.	The covert communications could obtain a positive rate.

D: Discrete-time; C: Continuous-time; G: Warden used a general detector.
✓means the option was considered or discussed explicitly; – means the option was not considered or discussed explicitly; × means the block length was finite.

A concatenated coding scheme for covert communication via BSCs and binary input DMCs was given in [76]. Its computational complexity grows polynomially with the block length n. The system consists of an outer Reed–Solomon and an inner random code of modest length. For covert communications across DMC channels, a more established inner code (PPM) and a random outer code were developed in [77]. It is proven that covertness can be partially ensured through modulation by using the PPM with a single noninnocent symbol in a block of $O((n)^{1/2})$ symbols. Furthermore, we can take advantage of low-complexity binary codes, such as polar codes [79], which provide both channel capacity and channel resolvability through the use of MLC. Bloch et al. subsequently made a number of contributions to the explicit coding scheme design for covert communications along with giving proven guarantees, in combination with PPM, MLC, polar codes, and channel resolvability codes [24], [78], [80]. Kadampot et al. [78] developed an ideal low-complexity coding scheme that uses PPM and MLC to accomplish covert communications across binary-input DMCs while adhering to information-theoretic bounds. The channel at a particular level in the suggested MLC-PPM scheme is independent of both the total number of levels and the codeword length for a suitable decoder. The binary phase shift keying modulation or Gaussian random codebooks are used to accomplish the covert capacity for AWGN channels; hence, the sparse modulation approach for DMCs [78] cannot be directly applied to AWGN channels. Kadampot et al. [80] suggested a low-complexity modified PPM and MLC coding technique that helps to resolve the conflict between sparse and diffuse signals. In addition, Wang and Bloch [24] improve the works in [78] and [80], which presents explicit details for operation at limited block length and is the first code with provable guarantees and efficiency with regard to key usage.

Table 4 Practical Coding Designs for Covert Communications

Authors	Channel model	Code schemes	Conclusions
Zhang *et al.* [76]	BSCs and binary-input DMCs	Combined with an outer Reed-Solomon and a light-weight inner random code	Computational complexity is polynomial with block length n.
Bloch *et al.* [77]	DMCs	Combined with a structured inner code (PPM) and a random outer code	It is demonstrated that covertness can be partially ensured by modulation using the PPM with a single non-innocent symbol in a block of $O(\sqrt{n})$ symbols.
Kadampot *et al.* [78]	Binary-input DMCs	Combined with PPM and MLC	For an appropriate decoder, the channel at a given level is independent of the total number of levels and the codeword length.
Kadampot *et al.* [80]	AWGN channels	Combined with modified PPM and MLC	The designed codes with low complexity can achieve covert capacity, and the work contributes to reconciling the tension between diffuse and sparse signals.
Wang and Bloch [24]	BSCs	Combined with polar codes and invertible extractors	The work offered the first code with provable guarantees and efficiency with respect to key usage.

2) Secret Keys: As previously mentioned, secret keys are typically used to establish covert communications. Alice, the transmitter, and Bob, the receiver, share these keys, but Willie, the warden, is kept in the dark. We shall use the following three perspectives to discuss the concept of secret keys.

Do covert communications require shared secret keys? The work in [23] studied covert transmissions over a special BSC model. Specifically, if Willie observes a noisier channel than Bob, i.e., $p_w > p_b$, Alice could transmit signals covertly to Bob without any shared secret key, so named keyless covert communications. Later, keyless covert communication was generalized to DMCs [16], [81] and MACs [20]. Specifically, Bloch [16] and Arumugam and Bloch [20] made a precise definition of "Bob's channel is better than Willie's channel" and proved that under the definition, it is possible to transmit on the order of $(n)^{1/2}$ reliable and covert bits over n channel uses without a secret key. It was proven in [82] that shared randomness extracted from the state effectively takes the place of the external secret key in other models. The authors further proved that it requires only a secret key at a negligible rate to bootstrap the communication, and the shared randomness can be obtained from the CSI [25]. However, when the prerequisite that the receiver channel should be better than the warden's channel cannot be satisfied, a shared secret key between the legitimate users is usually required to realize covert communications [17].

What is the length of the shared secret key for covert communications? Many references usually assume that a shared secret key between Alice and Bob is available, without paying attention to its length, e.g., simply set it long enough without a specific limit, or as long as the message is communicated [19], [28], [74], [83]. It was stated that $O((n)^{1/2}\log n)$ key bits should be required for covert communications over AWGN channels. These results were revisited in [16], and an alternative coding scheme was designed to support covert communications over DMCs with a secret key at an order of $O((n)^{1/2})$ bits. In addition, the optimal asymptotic scaling of the key size was identified and extended to Gaussian channels.

How to generate a secret key covertly? Tahmasbi and Bloch [61] addressed the issues of how to generate a secret key covertly. In the considered scenarios, secret keys were generated with the help of a public authenticated channel between Alice and Bob, which the adversary (Willie) does not know. Willie applied a hypothesis test to measure the covertness of the secret key generation process. Since the generation of the secret key between Alice and Bob was done before the covert communications, we should not extend the discussions further in this survey, and the detailed process can be referred to in [61] and [84].

D. Covertness Metrics

Let us take a three-node (e.g., Alice–Bob–Willie) communication system as an example. Willie aims to know whether Alice transmits covert signals. $\mathbb{P}_1$ is the probability distribution function of n observations when covert signals are transmitted; otherwise, the corresponding probability distribution function is denoted as $\mathbb{P}_0$. As shown in [17], additional information about the likelihood of Alice's transmission helps Willie, and the SRL still holds. Specifically, suppose that Willie knows that Alice does not transmit with probability $\pi_0 = \mathbb{P}(H_0)$, otherwise with probability $\pi_1 = \mathbb{P}(H_1)$. The error probability of Willie's hypothesis $\mathbb{P}_e^w$ can be calculated as $\mathbb{P}_e^w \geq \min\{\pi_0, \pi_1\} - \max\{\pi_0, \pi_1\}\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$. Thus, the values of π_0 and π_1 are usually ignored (e.g., either set to $\pi_0 = \pi_1$ or ignored) to simplify the calculation. In summary, the following three types of metrics are commonly used to measure covertness.

1) When the values of π_0 and π_1 are ignored, for the optimal test, the total variation distance $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$ between $\mathbb{P}_0$ and $\mathbb{P}_1$ can be used to measure the covertness, i.e.,

$$\mathcal{V}_T\left(\mathbb{P}_0, \mathbb{P}_1\right) \leq \epsilon. \tag{1}$$

2) Applying Pinsker's inequality on $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$, we can obtain the relative entropy $\mathcal{D}(\mathbb{P}_0 \| \mathbb{P}_1)$, i.e.,

$$\mathcal{V}_T\left(\mathbb{P}_0, \mathbb{P}_1\right) \leq \sqrt{\frac{1}{2}\mathcal{D}\left(\mathbb{P}_0 \| \mathbb{P}_1\right)} \tag{2}$$

$$\mathcal{D}\left(\mathbb{P}_0 \| \mathbb{P}_1\right) = \int_{\mathcal{K}} p_0\left(k\right) \ln \frac{p_0\left(k\right)}{p_1\left(k\right)} dk \tag{3}$$

where $\mathcal{K}$ is the support of $p_1(k)$. The covertness will be measured by $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1) \leq \epsilon$, also named KL divergence.

3) Specific probability values of FA and MD should be calculated first and then summed up to obtain $\pi_0\mathbb{P}_{\text{FA}} + \pi_1\mathbb{P}_{\text{MD}} = \pi_0\alpha + \pi_1\beta \geq 1 - \epsilon$.

According to Tahmasbi and Bloch [18], under the three covertness metrics, total variation distance, relative entropy, and the probability of MD for a fixed probability of FA, the first- and second-order asymptotic features of covert communications across binary-input DMCs were examined. Remark 2 examined their various practical meanings. The metrics of variational distance and the probability of FA are likely more appropriate because they have a direct relationship to the adversary's detection process, as demonstrated in Theorem 1. Moreover, there is no restriction on the adversary's operating location on its receiver operation characteristic curve when variational distance is employed as a covertness metric. Therefore, it can be said that from an operational standpoint, variational distance may be a metric more pertinent to the performance of the adversary's detector. The variational distance will be the correct value when equal prior probabilities are assumed ($\pi_0 = \pi_1 = 0.5$), and this value corresponds to the adversary's minimum PDE [17]. The variational distance metric is typically cumbersome for products of probability measures, as noted in [17]. For example, it applied Pinsker's inequality and relative entropy to obtain $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \leq (\epsilon f(n)/\sigma_w^2)$, where Willie is unsure of $f(n) = o(1)$ or $f(n) = w(1/(n)^{1/2})$ with σ_w^2. Given that the variational distance can be loosely represented by the relative entropy and that Pinsker's inequality is not tight, Wang and Bloch [22] accomplished a number of technical feats, including proving the converse proof and employing the variational distance as the covertness metric. Remark 2 contains additional discussion on this topic.

Relative entropy has gained popularity as a covertness metric despite its limits (as explained in [18] and [22]) because of its practical analytical and mathematical qualities [16], [19], [20], [38], [67]. Wang et al. [19] assessed the fundamental bounds of covert communications over DMCs and AWGN channels using $\mathcal{D}(\mathbb{P}_1\|\mathbb{P}_0)$ as the covertness constraint. Several secret key methods for covert communications over DMCs, MACs, and K-user MACs were examined in [16], [20], and [67], respectively, under the same covertness constraint. A more nuanced viewpoint on the optimality of Gaussian signaling for covert communications over AWGN channels at finite length with two forms of relative entropy as the covertness metrics was provided by the work in [38]. An upper bound on $\mathcal{D}(\mathbb{P}_1\|\mathbb{P}_0)$ for Gaussian signals is a tighter constraint on covertness than the same upper bound on $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1)$ because of $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1) \leq \mathcal{D}(\mathbb{P}_1\|\mathbb{P}_0)$. This was demonstrated in [38].

As explained in Sections III–VI, the third metric is also frequently employed in some real-world situations where it is possible to compute the probabilities of FA and MD directly. Furthermore, several studies have used the likelihood of MD for a fixed FA to assess covertness [17], [23]. In particular, an adversary may fix the FA probability $\mathbb{P}_{\text{FA}}$ and apply the NP criteria to attain the lowest $\mathbb{P}_{\text{MD}}$ for a given $\mathbb{P}_{\text{FA}}$ by adopting a practical detector. Lately, there has been a lot of interest in the literature on the effect of unequal prior probabilities (i.e., $\pi_0 \neq \pi_1$) on covertness performance [85]. According to Shahzad et al. [85], selecting a previous transmission probability of 0.5 is not necessarily the optimal option when it comes to attaining optimal covertness performance.

E. Taxonomy

Ever since Bash et al. [17] released his groundbreaking work, physical layer covert communication has attracted a considerable amount of research efforts. Based on the analysis presented in Motivation, it is evident that as the network structure gets more complicated, more strategies, such as the introduction of new devices and the use of new technologies, can be employed to combat adversaries. With novel network topologies, new applications, and enabling technologies, 6G intends to provide ubiquitous data sensing and flexible information sharing across diverse nodes, which may present both opportunities and problems for covert communication system designs. This article aims to provide an overview of the methods used in current complicated network designs to establish covert communications. It then delves into relevant solutions and lessons learned to enable the development of covert schemes in B5G wireless networks.

Let us introduce a taxonomy for covert communications in typical scenarios. Specifically, in terms of the increasing complexity of application scenarios, we can classify these typical scenarios into four categories, i.e., covert communications in three-node systems with a single antenna, covert communications in three-node systems with multi-antenna, covert communications in jammer-aided systems, and covert communications in relay-aided systems.

1) In a three-node system, i.e., a covert transmitter, a covert receiver, and an eavesdropper, each node is configured with a single antenna. Given that this kind of system architecture serves as the foundation for the network, analyzing and summarizing its possible covert performance enhancement solutions will enable us to more effectively handle any complex structural changes, such as the addition of new nodes, enabled by new technologies and new applications. Moreover, the eavesdropper's uncertainty about the associated parameters is normally used to ensure the covertness requirement, even to improve the covert performance. Therefore, we can analyze the covert communications in three-node systems with a single antenna, where the eavesdropper is uncertain about the parameters of the relevant noises, channels, and transmission time (i.e., Section III).

2) For covert communications in three-node setups, multiple antennas add an extra degree of flexibility. It is possible to counter and even cope with more powerful adversaries by configuring multiple antennas at the legitimate party. Furthermore, B5G wireless networks have been envisaged to be equipped with numerous massive and even ultramassive antennas placed at different nodes. The analysis of the three-node multiantenna covert communication schemes will help the in-depth research of B5G wireless network security with ultramassive MIMO. Based on the operation mode of multiple antennas, we can classify the three-node systems with multiantenna into the following two categories, i.e., HD multiantenna schemes (see Section IV-A) and FD multiantenna schemes (see Section IV-B).
3) Jammers have greater freedom to produce AN, deal with the wardens who wish to identify the presence of target communication, and prevent SI of FD receivers than three-node systems using multiple antennas. Jammer-aided covert communication is one of the most important network components, and the target covert link (e.g., Alice–Bob) is usually hidden among multiple nodes. However, an important research direction is how to fully utilize other nodes in the network (any node other than the adversary and target transceiver) as jammers for efficient resource management and interference coordination to enhance the covert performance, particularly in B5G networks where large numbers of devices coexist. We can divide them into two groups: informed jammers (see Section V-A) and uninformed jammers (see Section V-B), depending on whether the jammer(s) and legitimate nodes are sufficiently coordinated.
4) Relays have attracted a lot of attention since they can be purposefully designed to implement covert communication. B5G is anticipated to improve connectivity in traditional coverage areas and for space–air–ground applications. Relay-aided architecture, in which the relay may be a number of devices, such as IRSs and UAVs, also becomes one of the most important network architectures with a significant increase in coverage and network heterogeneity. We may divide relays into three groups according to the functions they perform: trusted and reliable relays (see Section VI-A), greedy relays (see Section VI-B), and untrusted relays (see Section VI-C).

III. COVERT COMMUNICATIONS IN THREE-NODE SYSTEMS WITH SINGLE-ANTENNA

The SRL in the context of covert communications specifies that, in the system models, the maximum number of covert bits that may be communicated via n channel resource units is $O((n)^{1/2})$. As $n \to \infty$, the covert rate does indeed become zero, that is, $\lim_{n\to\infty}(O((n)^{1/2})/n) = 0$. Numerous research attempts were spurred by the question of how to break the fundamental limits of SRL in three-node systems (a covert transmitter Alice, a covert receiver Bob, and an adversary Willie) using a single antenna. It has been discovered that the performance of covert communications can be enhanced by the warden's uncertainty about all associated variables (i.e., background noise, wiretap channel, and sending time). Therefore, in this section, we will go over and provide an overview of their particular implementations.

A. Noise Uncertainty

The adversary Willie conducts statistical tests in the presence of background noise in a three-node system with a single antenna to ascertain whether Alice and Bob have established covert communication.

When employing a radiometer and being uncertain of the background noise, wardens can attain a positive covert rate, as shown in [26]. $\hat{\Gamma}_d \in [(1/\rho)\Gamma_d, \rho\Gamma_d]$ represents the warden's uncertainty about background noise, and it is derived from [86]. In this model, Γ_d represents the true noise level, and ρ describes the uncertainty; for example, $\rho = 1$ indicates that Willie is fully aware of the background noise. With the noise uncertainty at Willie, it was determined that a reliable detection of Alice's signal transmission was not possible. At Willie, there is an SNR wall because the estimated level and real power are not in agreement. Therefore, even if it gathers an infinite amount of samples, Willie is unable to discover Alice when SNR at Bob is less than $\rho - 1/\rho$ [26], [86].

In practical applications, background noise can be far more complex, and a number of variables, including thermal noise, shooting noise, quantization errors, imperfect filters, and so on, can have an impact on its value. It is typically challenging to model the uncertainties of noise brought on by variations in temperature, ambient conditions, and calibration errors. Consequently, He et al. [87] conducted more research on the mathematical modeling of noise uncertainty in covert communications.

The studies conducted in [87] examined two types of noise uncertainty models: bounded and unbounded cases. In the former case, a log-uniform distribution of σ_w^2 was employed to characterize the model [88]. The actual power σ_w^2 is uniformly distributed within a finite interval around a nominal value $\bar{\sigma}_w^2$. Since a finite range cannot be applied directly to the unbounded uncertainty model, the log-normal distribution of σ_w^2 was assumed in this model [89], [90], [91], and the difference between σ_w^2 and $\bar{\sigma}_w^2$ following a normal distribution was employed. The covert performance was analyzed using the Bayesian statistic and outage-based covertness metrics, which were based on the two models mentioned above. The result showed that it was possible to achieve a positive covert rate, meaning that $O(n)$ covert bits could be transmitted over n channel resource units.

As a result, in more complex application scenarios, a thorough examination of the modeling technique under

multifactor fusion and the sources of noise uncertainty are required. It has been possible to break the SRL by making use of the warden's uncertainty regarding background noise in addition to or instead of channel and broadcast time uncertainty.

B. Channel Uncertainty

In [48], covert communications over compound BSCs were discussed. Channel noises at receiver Bob and adversary Willie were supposed to follow uniform distributions over a range of values although the exact values are unknown to any of the three persons involved (transmitters Alice, Bob, and Willie). A positive rate is feasible because Alice has an extra resource to conceal her transmission due to Willie's uncertainty about the channel specifications. Utilizing all receivers' uncertainty on the CSI, covert communications over block fading channels were examined [54]. The channel coefficient in this work between transmitter Alice (a) and receiver k was given as follows: $h_{ak} = \hat{h}_{ak} + \tilde{h}_{ak}$, where the known and uncertain parts of h_{ak} are denoted, respectively, by $\hat{h}_{ak}$ and $\tilde{h}_{ak}$ [92], [93]. Either the adversary Willie (w) or the receiver Bob (b) is indicated by the subscript k. It was demonstrated that the warden's uncertainties about CSI could present opportunities to carry out covert transmission.

Both the adversary's optimum threshold and the exact rates that can be attained have been evaluated. Similarly, Hu et al. [94] used reverse channel power control, which prevented both adversary Willie and receiver Bob from accurately estimating noise using CSI feedback. Increasing the noise uncertainty at the warden and the receiver at the same time may not continually enhance the effective covert rate even though the adversary's uncertainties might be exploited to meet the requirements for covertness. Shahzad and Zhou [95] examined two scenarios for covert communications over quasi-static block fading channels: the ideal CSI and just CDI. The findings demonstrated that in the large detection error regime, the warden does not benefit from the quality of CSI to enhance its detection performance. Unlike [48], [54], [94], and [95], different perspectives on the advantages of channel uncertainties were explored to demonstrate that channel statistics that are unknown to the warden can aid Alice in covert communication [28], assuming that Alice and Bob have a shared secret key that is long enough and Alice has causal or noncausal knowledge of the channel states.

For the receiver Bob and the adversary Willie, channels are modeled as i.i.d. uncertain variables over different channel resources. The covert rate was proven to be zero if Alice did not know the CSI, while the covert rate was larger than zero with noncausal CSI at the transmitter. It also derived the lower bounds on the rate of the secret key that is needed to achieve covert capacity. Ta and Kim [96] examined the combined effects of noise and channel uncertainty on the covert performance over a Rayleigh fading channel. In order to examine the influence on covert capacity, the threshold values for received SNR and noise uncertainty were determined. To further reveal the effects on covertness requirements, the two aforementioned elements were examined, and it was shown that the channel's influence increased in the presence of noise uncertainty.

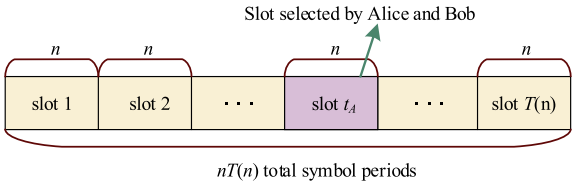

Fig. 7. *Total number of symbol durations is denoted as nT(n), where n is the number of symbol durations in each slot and T(n) indicates the number of slots in the duration. The legitimate users select slot t_A to transmit covert signals.*

C. Time Uncertainty

It is also possible to achieve covert communication with a positive rate when the adversary is uncertain of the transmission period. To be more precise, let us look at a real-world scenario in which the adversary Willie was unaware of a prearranged sending time that only transmitter Alice and receiver Bob knew, such as a particular time on a given date. In contrast to [71] and [17], Bash et al. [27] examined a slotted AWGN channel.

Let the total number of transmit slots available be $T(n)$. In contrast to the previous methods, the number of symbol durations in each slot, n, is much smaller than the total possible transmit time $nT(n)$; for example, it is only a few seconds over the duration of a day, as shown in Fig. 7. In order to carry out their covert communications, Alice and Bob chose one slot t_A, making sure to conceal their selection from their adversary. With the aid of $\log(T(n))$ bits that are shared between legitimate users prior to the transmission, it was determined that $O\{\min[(n \log T(n))^{1/2}, n]\}$ bits may be covertly and reliably transmitted.

D. Lessons Learned

Table 5 illustrates the properties of covert communications using single-antenna nodes in three-node scenarios, which is summarized in this section. The scenarios were divided into four categories: noise uncertainty, channel uncertainty, noise and channel uncertainty, and time uncertainty, depending on the eavesdropper's uncertainty regarding the parameters that were associated with each scenario. The following lessons can be learned from the above discussions.

1) Under certain limitations, such as the warden being considered to be a power detector [26], [87], the warden's uncertainty about the associated parameters does help to achieve covert transmission with a positive rate. Meanwhile, the legitimate party's uncertainty about these parameters may also impair its covert performance. The performance of covert

Table 5 Covert Communications in Three-Node Systems With Single Antenna

Types	Channel	Time	Warden	Codes	Keys	Infinite	Characteristics	Conclusions
Noise	AWGN [26]	D	P	✓	✓	✓/×	Warden was uncertain about background noise level. The covertness metric was $\alpha+\beta$ as its minimum value.	Willie's noise uncertainty is introduced to achieve a positive covert rate, i.e., $O(n)$ bits can be covertly transmitted.
	AWGN [87]	D	P	–	–	✓	Bounded and unbounded noise uncertainty models were used.	The achievable rates with the constraint of Bayesian statistics/outage-based covertness were analyzed.
Channel	BSCs [48]	D	G	✓	–	✓/×	The exact value of channel noise was unknown, and the covertness was measured as relative entropy.	A random coding scheme was used to ensure that Alice can send signals covertly and reliably.
	Fading [54]	D	OP	–	–	✓	All receivers experience uncertainties on the CSI. The covertness was measured by the average value of $\alpha+\beta$.	It illustrated how the covert performance is affected by the channel uncertainty and the exact achievable rates were quantified.
	Fading [94]	D	P	–	–	✓	Reverse channel power control was adopted. The minimum $\alpha+\beta$ was the covertness metric.	Increasing the noise uncertainty at warden and receiver may not improve effective covert rate.
	Fading [95]	D	G	✓	✓	✓	Two warden's cases were considered, i.e., perfect CSI and CDI only. The minimum $\alpha+\beta$ was the covertness metric.	Warden's channel knowledge does not play an important role in the scenarios with a large detection error regime.
	DMC, AWGN [28]	D	G	✓	✓	✓	Causal or non-causal information of the channel state was considered. Relative entropy was the covertness metric.	A positive rate was available with non-causal CSI at Alice; otherwise it was zero. The lower bounds on the rate of secret key were derived.
Noise and channel	Fading [96]	D	P	–	–	✓	Imperfect estimation of channel gain and noise power were considered. The minimum $\alpha+\beta$ was the covertness metric.	The influence of channel uncertainty was proven to be greater if noise uncertainty existed.
Time	AWGN [27]	D	G	✓	–	✓	The slot selected by Alice and Bob was secret to Willie. $\alpha+\beta$ was the covertness metric.	$O\{\min[\sqrt{n\log T(n)}, n]\}$ covert bits can be transmitted with the help of $\log(T(n))$ shared secret bits.

Types: Different types of uncertainties used in the reference.
D: Discrete-time; C: Continuous-time.
G: Warden uses a general detector; P: Warden uses a power detector; OP: Power detector is verified as the optimal detector.
✓means the option is considered or discussed explicitly; – means the option is not considered or discussed explicitly; × means the block length is finite.

communications with an infinite block length was examined in the majority of the aforementioned studies.

2) As suggested in [97], the covert rate might not rise when an adversary's detector permits access across codeword slots, even if it lacks the knowledge of its channel statistics. Then, using more auxiliary nodes (such as jammers or relays) or adding more antennas to reliable nodes could be a useful way to enhance covert performance.

These uncertainty factors need to be managed carefully in complicated network systems, but if they can be controlled well, that can help increase covert performance. Therefore, an intriguing study area for physical layer covert communications in B5G wireless networks is how to proactively add controllable uncertainty factors through efficient techniques.

IV. COVERT COMMUNICATIONS IN THREE-NODE SYSTEMS WITH MULTIANTENNA

In addition, to overcome bandwidth constraints and improve overall throughput, multiple-antenna systems have been commonly utilized in wireless communications (including covert communications) [14], [98], [99]. We will concentrate on covert communications in multiantenna three-node systems in this section. Specifically, there are two primary ways that multiantenna technology has been applied to covert communications: HD and FD systems. Be aware that, unless otherwise noted, the nodes in this survey operate in HD mode.

A. HD Multiantenna Technologies

The origins of the research on covert communications via MIMO channels against adversaries with multiple antennas may be found in the early LPD works in [100], where various CSI assumptions were used to determine the average transmit power needed to meet LPD requirements. The conclusions reached had nothing to do with the SRL directly because the authors did not concentrate on the asymptotic performance analysis.

Several attempts have been made to investigate the covert communication problem in HD multiantenna settings after these foundation works in [16], [17], [19], [22], [101], [102], and [103]. In [101], covert communications via a MISO channel with multiple antennas equipped at the transmitter were examined. By beamforming with its multiantenna, the transmitter can achieve a positive rate when it can obtain the perfect CSI of an adversary's associated link. The adversary is implicitly

modeled in its derivation as a power detector. Then, in the event that the transmitter had imperfect adversarial CSI, the beamforming vector and transmit power were simultaneously optimized to maximize the covert rate. The findings indicate that the covert rate will decrease as a result of the CSI estimation error. Reducing the transmission power or carefully designing the beamforming vector could be useful ways to enhance covert performance.

The fundament limits of covert communications over MIMO AWGN were studied in [102] and its conference paper [103]. In the considered scenario, an HD multiantenna transmitter Alice aims to transmit covert signals to Bob with an HD multiantenna against an adversary Willie with an HD multiantenna. KL was used as the covertness metric. A variety of settings were examined, including the transmitter's knowledge of the adversary's CSI, the presence of a shared secret codebook, the number of transmit antennas, and covert capacity (positive/zero). Table 1 [102] contains the specific findings and presumptions. The scaling of the maximum number of covert bits, for instance, is $L = (2N)^{1/2}\lambda_b/\delta_b^2\hat{\lambda}_w$ when Bob's channel is well-conditioned (the eigenvalues are independent and roughly identical), where N is the channel uses, λ_b and δ_b^2 are the eigenvalues and received noises of Bob's channel, respectively, and $\hat{\lambda_w}$ is a bounded factor of Willie's channel. Theorems 1–5 in [102], along with the corollary for each, contain all of the specific expressions.

It was demonstrated that, under certain circumstances, a positive covert capacity can be attained in a massive MIMO system, where the number of transmit antennas increases. The variational distance is a statistic that is operationally relevant to the adversary's detector's performance, as mentioned in Section II-D. Wang and Bloch [22] examined covert communications using MIMO AWGN channels, employing the total variational distance as the metric for covertness. This article assumed that the null space of Bob and Willie's channel matrices is trivial and revisited the model of [102] and [103]. In addition, the authors examined covert communications over compound MIMO-AWGN channels without implicitly placing restrictions on the adversary's operations. Several significant conclusions were drawn. For instance, they developed a comprehensive description of the covert capacity using the variational distance as the covertness metric, i.e., $C = \delta_w^2(2\text{tr}(\Lambda_b^4(\Lambda_w^{-1}))^4)^{1/2}/\delta_b^2$, where δ_w^2, δ_b^2, Λ_w, and Λ_b have received noises and decomposition parameters of Willie's and Bob's channels, respectively. $\text{tr}(\cdot)$ is the trace of a matrix. For more information, see Theorem 1 in [22]. In addition, the characterization of the covert capacity was expanded to include a class of channels where Willie's channel matrix is only known up to a rank and a spectral norm restriction, while Bob's channel matrix is known.

B. FD Multiantenna Technologies

Numerous studies have investigated the performance of covert communications with FD multiantennas at a receiver due to the structural diversity of various networks and the benefits of FD technologies. While SI between a transmitter and its own receiver is a major obstacle to the successful implementation of FD techniques, FD technologies enable simultaneous transmission and reception at the same frequency [104]. A variety of domains, including propagation domain suppression, analog cancellation, and digital cancellation, have seen the application of SI cancellation approaches studied in recent years [105]. It is feasible to effectively carry out the FD communications by using these SI cancellation techniques to cancel the SI to a low enough level. PLS research areas have seen a great deal of study on FD technologies in particular [106]. Consequently, there has been a lot of interest in using FD technologies for covert communications, particularly in the construction of different covert transmission systems in SIMO models using FD multiple-antenna receivers.

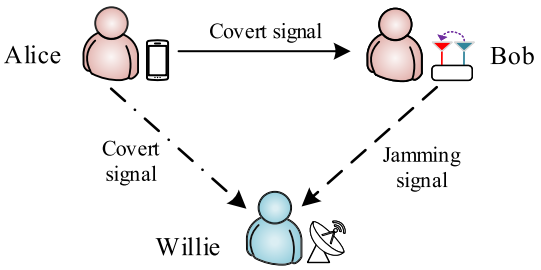

Fig. 8. *Example of a typical SIMO covert communication scenario, where Bob, using a two-antenna FD receiver, receives a covert transmission from Alice, using a single-antenna HD transmitter, against an adversary using a single-antenna HD receiver. In order to communicate covertly, Bob also sends Willie ANs to confuse him.*

In contrast to [85] (as illustrated in Fig. 8), Xu et al. [107] examined a more realistic FD scenario in which Willie, the warden, only has access to knowledge of CDI. Random AN from an FD transmitter was found to be able to enhance performance with an indefinite block length. Together, the optimal powers for Alice and AN are designed in order to reduce the likelihood of an outage at Bob. If CDI is the only one obtained at Willie, then analysis and numerical findings demonstrated that there exists an optimal AN power to reduce the outage performance.

Wang et al. [108] discussed how to use the CSI in the main link to further improve the capability of covert schemes. More precisely, it comprises transmission time selection and power control techniques, both putting forward to take advantage of the CSI for covert performance improvement. The former technique only transmits signals when the network quality improves; otherwise, it terminates communication. The transmit power was modified in the latter technique in response to the channel coefficient changing. Numerous experimental findings and analyses revealed that the power control method performs better when the conditions for covertness and the SI residual

factor are strict; otherwise, the transmission time selection technique performs better.

Typically, pilot signals are sent to estimate the channel, or feedback is received from a receiver to get CSI. These procedures face the danger of disclosing the transmitter's position information before covert communications, though. For this reason, channel inversion power control (CIPC) at Alice was suggested in [37]. Moreover, requirements for covertness were met by using a different AN from FD Bob. In particular, Alice modifies the power and phase of each channel resource that she sends to Bob, allowing the receiver to decode these signals without the main link CSI being aware of it. Using this strategy could aid in keeping Alice's existence a secret from warden Willie. Two CIPC schemes, conventional CIPC and truncated CIPC, were used. While truncated CIPC could only carry out signal transmission when the quality of the main link is higher than a predetermined value, conventional CIPC carried out covert communications without taking the main link's quality into account. The truncated CIPC scheme outperforms the regular CIPC scheme. It was deduced that there is an optimal value of the maximum transmit power of AN at Bob to maximize effective covert throughput. The work in [109] concentrated on achieving covert communication using an FD multiantenna receiver (Bob's antennae can have two or more). In this study, one of the remaining antennas was chosen to emit AN with variable power, and the best antenna was chosen to receive covert signals from Alice. It was demonstrated through research on the maximum effective covert rate that the capacity of covert communications grows with the number of antennas.

Shu et al. [34] examined covert techniques with two FD antennas at Bob under the assumption of a finite block length, i.e., delay-constrained, in contrast to [33], [37], [85], [107], [108], and [109], which made the assumption of an indefinite block length. Even when AN was delivered with a fixed power, covert communications could be formed successfully because Willie was unable to gather all available information. Furthermore, the ideal AN transmit power was determined for both locally and globally optimized transmit power scenarios. It was determined that improving covert capacity benefits from a larger AN power. In both fast and slow fading scenarios, Zheng et al. [110] investigated covert communication techniques across noncoherent Rayleigh fading channels.

It is possible to design the AN in the first two scenarios to produce a positive covert rate, either by using a fixed power or changing power from the FD receiver. Covert communications were also established recently with the aid of AN from an FD receiver in [111]. In the meantime, the tradeoff between the requirements for covertness and the rate of covert communication was investigated using the nondominated sorting genetic algorithm. In [112], the robust joint power and position optimization were examined, and the receiver's ideal location was determined. Chen et al. [113] discussed the issues of using covert communications to frustrate eavesdroppers who may be located in unknown locations. An FD antenna on the receiver was intended to broadcast AN. The monotonicity of the covert outage probability was used to determine the optimal location for the eavesdropper. The outcomes demonstrated that by maximizing the ratio of transmit power to AN power, the maximum connection probability could be achieved. The optimum transmission rate was found using the bisection method, which was also employed to improve connection throughput while maintaining covertness.

C. Lessons Learned

Table 6 shows the attributes and efficacy of covert communications using HD and FD multiantennas. The following is a summary of the lessons learned from the relevant research works.

1) The majority of the aforementioned references, particularly in the context of fading channel communication, ignored code and/or key settings while modeling the adversary as a power detector to enable covert communication.
2) More attention has been paid to covert communication under infinite block length constraints, either by taking computational complexity into account or by following the SRL. However, a lot of application scenarios (such as automated factories, smart meters, and connected cars) call for the transmission of short data packets (such as roughly 100 channel resource units), which must meet strict latency requirements. In other words, more discussion about covert communication with limited block duration is required.
3) Establishing covert communications is facilitated by multiple antennas configured on the legitimate parties (i.e., a covert transmitter or receiver). Covert communication using FD multiantenna receivers has drawn more attention as a result of the benefits of increased AN design freedom and the relaxing of limitations on the hardware implementation of FD multiantennas (e.g., increasingly sophisticated SI cancellation technique).

Covert transmission strategies against attackers with multiple antennas in B5G wireless networks still require more research. Furthermore, it is imperative to optimize the covert transmission rate with respect to several characteristics, such as transmit power, secret codebook size, and space–time diversity. There are still unanswered questions in the literature that is now accessible on the adoption of a more realistic residual SI model for multiple-antenna FD nodes, particularly for an MIMO or even a massive MIMO system, and the analysis of its impact on covert performance.

V. COVERT COMMUNICATIONS IN JAMMER-AIDED SYSTEMS

Even though Willie utilizes a general detector, adding a jammer to the Alice–Bob–Willie scenario can help obtain

Table 6 Covert Communications in Three-Node Systems With Multiantenna

Types	Channel	Time	Warden	Codes	Keys	Infinite	Covert schemes	Conclusions
HD	AWGN [101]	D	G	–	–	✓	Relative entropy was used to measure covertness. Error model and a second-order cone programming problem were established for analysis.	A positive covert rate was obtained with perfect CSI; otherwise beamforming vector and transmit power were designed jointly to maximize communication rate.
	AWGN [102]	D	G	✓	✓/–	✓	Establish covert communications with the help of secret codebooks or known CSI of warden. Relative entropy was the covertness metric.	Maximum covert coding rate was derived under different parameter settings, e.g., the number of transmit antennas and warden's CSI. In massive MIMO scenarios, conditions were examined in order to attain a non-zero concealed capacity.
	AWGN [22]	D	G	✓	✓	✓	Consideration was given to a conservative number of secret keys and limited restrictions on the warden's activities. The variational distance serves as the covertness metric.	It provided an in-depth analysis of the covert capacity and expanded it to include a group of channels. A greater number of covert bits results from using the variational distance as the covertness metric.
FD	Fading [33, 85]	D	P	✓	✓	✓	AN with varying power from the receiver was designed. Detection error probability with general prior probabilities was used to measure covertness.	Transmission of AN helps to achieve covertness but its transmit power needs to be set carefully. An equal prior transmission probability may not be an optimal choice.
	Fading [108]	D	OP	–	✓	✓	Time selection and power control schemes were proposed. $\pi_0\alpha + \pi_1\beta$ measures the covertness.	When several constraints were strict, power control strategy may offer a better covert performance, e.g., effective transmission rate, receive power at Bob.
	Fading [37]	D	P	–	–	✓	CIPC was adopted at Alice and AN with varying power from Bob was used. $\pi_0\alpha+\pi_1\beta$ was the covertness metric.	There is an optimal maximum power of AN to improve covert throughput in truncated CIPC scheme, which outperforms conventional CIPC scheme.
	Fading [109]	D	P	–	–	✓	The best antenna was used to receive signals, and one of the remaining antennas transmits AN with varying power. $\alpha+\beta$ was the covertness metric.	The maximum effective covert rate was studied, showing that the number of antennas increases the capacity of covert communications.
	Fading [107]	D	P	–	–	✓	AN with varying power from an FD receiver could improve performance. $\alpha + \beta$ was the covertness metric.	There is an optimal AN power to minimize outage performance when only CDI is obtained at Willie.
	AWGN [34]	D	OP	–	–	×	AN with a fixed transmit power was transmitted to multi-antenna Bob. Relative entropy was the covertness metric.	AN with a fixed power improves covert communications with delay constraints. A higher maximum power of AN is beneficial for enhancing covert throughput.
	Fading [110]	D	P	✓	✓	✓	AN schemes with both constant and variable power from the receiver were developed. $\alpha+\beta$ was the covertness metric.	In both fast and slow fading channels, the proposed scheme was designed to obtain a positive covert rate.
	AWGN [111]	D	P	–	–	✓	AN with varying power from a receiver was designed. The covertness metric was $\alpha + \beta$.	Results provided a set of solutions with trade-off between covert communication rate and covertness requirement.
	Fading [112]	D	P	–	–	✓	AN and warden's uncertainty about the receiver's position were used. Covertness was measured by a minimum value of $\alpha + \beta$.	To optimize effective covert throughput, robust joint power and position optimization were taken into consideration, and the optimal receiver position was shown.
	Fading [113]	D	P	–	–	✓	One of receiver's FD antennas was designed to transmit AN. Covert outage probability was defined to measure covertness.	To ensure covertness and provide an optimal transmission rate and throughput, a bisection approach was employed.

D: Discrete-time; C: Continuous-time;
G: Warden used a general detector; P: Warden used a power detector; OP: Power detector was verified as the optimal detector.
✓means the option was considered or discussed explicitly; – means the option was not considered or discussed explicitly; × means the block length was finite.

a good covert rate. The additional nodes to the initial three-node system for covert communications are primarily referred to as jammers in this section. Fig. 9 depicts a typical jammer-aided situation with four distinct types of nodes, a transmitter named Alice, a receiver named Bob, an adversary named Willie, and a jammer, that could potentially meet the requirement for covertness. As in [97], Alice and Bob want to establish covert communica-

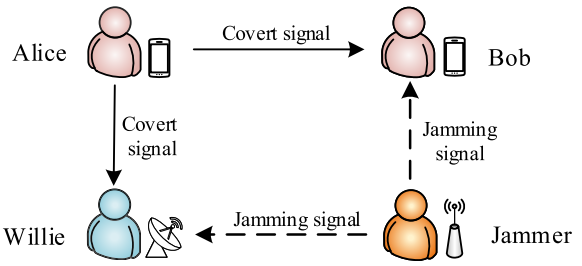

Fig. 9. *Four different types of nodes make up a jammer-aided covert communication scenario: a jammer, an adversary named Willie, an intended receiver named Bob, and a transmitter named Alice. Alice tries to transmit Bob covert signals, while Willie is present using the jammer's jamming signals.*

tions without being discovered by Willie, who is thought to be a general receiver. Jammers can be classified into two categories: informed jammers and uninformed jammers. These categories will be explored based on whether there is adequate coordination between jammers and legitimate users.

A. Informed Jammers

An informed jammer operates by having knowledge about Alice's transmission time and signal structure. A discrete-time AWGN channel was created between the nodes in the informed jammer-aided scenario that Sobers et al. [114] described. In a comparable setup to the one illustrated in Fig. 9, Alice and Bob shared a codebook that was created by Alice independently selecting symbols from Gaussian distributions at Alice. The jammer reduces the strength of its Gaussian noise until Alice completes her signal transmission before increasing it once further when she begins to transmit a codeword.

Ma et al. [115] examined covert communications using one public receiver, one covert receiver, and a multi-antenna transmitter against a general adversary. The purpose of the robust beamformer, ZF beamformer, and covert beamformer was to optimize the covert rate at the adversary with imperfect or perfect CSI, respectively. A weak user was used as a cover to assist the strong user in downlink NOMA systems [116]. A public user using TCIPC was utilized as a cover in [117]. It has been demonstrated that boosting the cover's maximum transmit power will increase the effective covert throughput. Tao et al. [118] used an energy-harvesting jammer to study covert communications. It was proposed that in order to maximize performance, there should be a time-switching factor and optimum transmit power at the receiver or the energy supplier. In overlay cognitive radio networks [119], the AN was sent by another carefully chosen ST in addition to the covert ST pair. Three different user-jammer scheduling schemes, rate-oriented, link-oriented, and fairness-oriented secondary user scheduling, were used to examine the covert rate and the fairness performance.

From the aforementioned research efforts, it is clear that a key factor in jammer-assisted covert communications is the coordination between transmitters and various jammer types (such as intentionally introduced nodes or already-existing nodes in the network). The next part summarizes uninformed jammer-aided schemes that have a higher degree of design freedom and require less coordination than informed jammer-aided covert communications.

B. Uninformed Jammers

There are two categories of covert schemes with uninformed jammers: a single jammer and multiple jammers. Sobers et al. [15] examined how well uninformed jammer-aided covert communications can deceive a warden using a general detector. The power detector was confirmed to be the warden's preferred strategy there. A pair of channel models, AWGN and block fading channels, were developed in order to investigate the covert performance in more detail. It was assumed that Alice, the transmitter, and Bob, the receiver, should share a long enough secret key. An uninformed jammer emits Gaussian noise in the AWGN channels, i.e., Case 1, at a power level that is intended to fluctuate randomly in each slot of n symbols. In order to facilitate Alice's covert transmission, Willie's background noise assessment was uncertain due to the dynamic transmission power of the jammer. It was demonstrated that Alice could send n symbols at a constant power. In the meantime, Bob could receive $O(n)$ bits with guaranteed covertness and decoding requirements, and Willie used an optimal detector.

Furthermore, the authors deduced that the optimum detector ought to assess the acquired power against a predetermined threshold. Two examples were explored in a block fading channel with M_b blocks. The same conclusions as those in AWGN channels might be made when the fading block length is $M_b = 1$ or Case 2. That is, the optimal detector at Willie should compare the obtained power with a threshold, and a positive covert rate could be obtained between Alice and Bob. In the event that $M_b > 1$, or in Case 3, a power detector would no longer be optimal; nonetheless, Alice might still carry out covert communication by utilizing certain strategies, even in the event that Willie utilizes an optimal detector. Table 7 provides a summary of the findings.

In [120], dynamic variations in background noise and their effect on covert capacity were examined in a block fading channel using a model akin to that employed in [15] and [114]. Let us assume that for every codeword of length n, the fading signal varies independently for $f(n)$ times. Two types of variation were assumed: fast fading across several blocks $f(n) = cn$ with a constant c and slow fading equal to a constant value C. It was noted that Alice did not benefit from very slow or fast fading. Willie might assess the current channel environment if the dynamic range was too low [97]. Willie was able to average the changes and set a limit on the covert capacity if the dynamic range

Table 7 Uninformed Jammer-Aided Covert Communication Scheme With a Single Adversary

Case	Channel model	Jamming signal	A power detector is optimal for Willie?
1	AWGN channels in all links	Variable power	Yes
2	Block fading channel with $M_b = 1$ in jammer-to-Willie link	Constant power	Yes
3	Block fading channel with $M_b > 1$ in jammer-to-Willie link	Constant power	No

changed too fast. This clarifies why it is appropriate to use the intermediate rate of change assumption provided in [15] in order to prevent the adversary from acquiring channel estimations that are sufficiently accurate. A function of $f(n)$ was used to determine the number of covert bits broadcast against two distinct types of wardens: power detectors and general detectors.

The optimum power adaption for covert communications with an uninformed jammer was recently examined in [121]. Particularly, in the following scenarios, namely, an AWGN or a Rayleigh fading jammer-to-adversary channel, the power adaptation via the TCI scheme [122] was proposed to combine with different covertness requirements (e.g., the average and instantaneous values of $\alpha+\beta$). It was demonstrated that in some circumstances, TCI is ideal, i.e., to maximize the likelihood that the recipient can dependably decode the covert signal.

In [123], the impact of a multiantenna at a jammer on covert communications was examined. Bob was equipped with a multiantenna when a single-antenna warden was present. The related AN techniques for the jammer were developed to optimize Bob's SNR with $\alpha + \beta \geq 1 - \epsilon$ as the covertness metric, depending on whether the jammer is aware of the CSI of an eavesdropper. The jammer's best course of action is to employ all of its power and beamforming in one direction while adhering to the restriction that it transmits isotropically to all directions or to the legitimate receiver's null space when its CSI is known. Li et al. [124] examined covert communications over continuous-time channel models, while a jammer was present. An alternative strategy was taken into consideration in [124], where the adversary uses an interference cancellation detector, because the performance of the investigated continuous-time systems cannot be immediately extended from the prior results of discrete-time systems. A continuous-time channel with an asymptotic bandwidth of W can transmit $O(WT)$ reliable and covert bits in T seconds. Depending on whether or not the transmitter and jammer are believed to be in frame synchronization, the amount of covert bits was determined in various circumstances. The evaluation of the covert performance at a transmitter/warden with various uncertain CDI restrictions was conducted in [125]. The maximum covert rate, or Alice's available covert transmission rate with a minimal covertness metric of $\alpha + \beta$, was examined under several scenarios, such as two potential adversary assumptions and three alternative CDI characterizations. Note that you should refer to [125] for these particular definitions.

Interference nodes [29], [30], [126] could also be thought of as generalized jammers in more intricate wireless networks. In [29], since each of them was modeled as a p.p.p., jammers (friendly nodes) were inserted to introduce uncertainty at a warden. Transmitter Alice's time and the other friendly nodes' transmissions were not in synchronization. In order to confuse the warden, the node that was nearest to the adversary was chosen to transmit ANs. It was demonstrated that Alice could send $O(\min\{n, m_f^{\gamma/2}\})$ bit to Bob in n channel resources in a reliable and covert manner, where γ represented the path-loss exponent and m_f was the density of friendly nodes. Alice could transmit $O\{\min(n, m_f^{\gamma/2}(n)^{1/2}/N_w^{\gamma})\}$ covert bits with $\gamma > 2$ when there were N_w collaborating adversaries uniformly and randomly located in the network, whereas $O\{\min(n, m_f(n)^{1/2}/N_w^2 \log^2 N_w)$ covert bits with $\gamma = 2$. The locations of the friendly nodes are unknown to the warden, but he is aware of the channel statistics.

The study in [30] introduced the uncertainty of aggregate received interferences from all devices that were also distributed according to a homogenous PPP because it can be challenging to choose the closest friendly node. All received ambient signals were described by an uncertain shot noise process [127], taking into account both nonfading and fading channels. Some intriguing results were found, such as the possibility that performance may be enhanced by an increase in the number of interferers or by boosting transmit power at each friendly node, while these variables had little effect on the regions with few interferences. Several jammers that meet a predetermined threshold are constructed and used to broadcast jamming signals in [126]. The outcomes demonstrated that the proposed methods' covert throughput performs better than traditional single-jammer schemes.

ZivariFard et al. [128] investigated covert communications in the presence of a cooperative jammer that does not require access to infinite local randomness, in contrast to earlier findings in the literature mentioned above [15], [115], [117], [120]. Instead of the i.i.d. sequence found in [15] and [121], the jammer transmits a nonindependent and identically distributed coded sequence in the models under consideration. For three comparable models, where the jammer coordinates with Alice using a secret key, and where there is no direct communication or coordination between the jammer and Alice, the inner and outer bounds of the covert capacity region were determined. It helped to uncover the basic interaction between the rates of secret key, local randomness, and covert communication.

Table 8 Covert Communications in Jammer-Aided Systems

Types	Channel	Time	Warden	Codes	Keys	Infinite	Covert schemes	Conclusions
Single informed	Fading [115]	D	G	–	–	✓	A public receiver and beamformer were used to ensure covertness, which is measured by the relative entropy.	To maximize the covert rate with perfect or imperfect adversary CSI, three types of beamformers were designed.
	Fading [116]	D	P	–	–	✓	A weak user in NOMA was a cover, and $\alpha+\beta$ was used.	Maximum covert rate was related to the maximum transmit power of the cover.
	Fading [117]	D	OP	–	–	✓	A public user was used as a cover, and minimum value of $\alpha+\beta$ was adopted.	Increasing the maximum transmit power of the cover will lead to a larger effective covert throughput.
	Fading [118]	D	OP	–	–	✓	Energy harvesting jammer was used. Minimum $\alpha+\beta$ was used to measure covertness.	An optimal transmit power existed at the receiver and the time switching factor was used to maximize effective covert rate.
Multiple informed	Fading [119]	D	P	–	–	✓	Another carefully selected ST was used to transmit AN. Minimum $\alpha+\beta$ was used to measure covertness.	Covert rate and fairness performance were studied in three schemes, i.e., rate-oriented, link-oriented, and fairness-oriented secondary user scheduling.
Single uninformed	Fading, AWGN [15]	D	OP	✓	✓	–	Jamming signals with varying power or fading channel. $\alpha+\beta$ was used to measure covertness.	Covert bits were quantified in three proposed cases. The number of covert bits is $O(n)$ in Cases 1 and 2, while it is $O(\sqrt{n})$ in Case 3.
	Fading [120]	D	G/P	✓	–	✓	Channel mobility or time-varying jamming signal was considered, and $\alpha+\beta$ was used.	Covert throughput with the variation of background noise was derived, including the upper and lower bounds for corresponding construction schemes.
	AWGN, fading [121]	D	OP	✓	–	✓	Jamming signals were used to ensure covertness requirements, which were measured by average and instantaneous values of $\alpha+\beta$.	Optimal power adaptation schemes were used to minimize average outage probability under different covertness constraints and channel models.
	AWGN [123]	D	P	✓	✓	✓	AN schemes were designed and $\alpha+\beta$ was used.	AN scheme to maximize Bob's SNR was related to warden's CSI.
	AWGN [124]	C	G	✓	✓	–	Jamming signals and $\alpha+\beta$ were used. Frame synchronization between Alice and jammer was considered.	Interference cancellation detector is optimal for adversary and $O(WT)$ covert and reliable bits can be transmitted.
	Fading [125]	D	P	✓	–	✓	Jamming signals and/or uncertain CDI were considered, and minimum value of $\alpha+\beta$ was used.	Alice's available covert rate was analyzed for different situations, e.g., three types of CDI characterizations and two assumptions for adversary.
Multiple uninformed	AWGN [29]	D	G	✓	✓	✓	The closest node to Willie was selected to send AN. Relative entropy metric was used to measure covertness.	The number of covert bits was $O\{\min(n, m_f^{\gamma/2}\sqrt{n}/N_w^{\gamma})\}$ with $\gamma > 2$, while the value was $O\{\min(n, m_f\sqrt{n}/N_w^2 \log^2 N_w)$ with $\gamma = 2$.
	Non-/fading [30]	D	P	✓	✓	✓	Ambient interferences, average value, and outage probability of $\alpha+\beta$ were used.	Covert throughput could be improved with an increasing density of jammer's transmit power under strict constraints.
	Fading [126]	D	P	–	–	✓	Jammers that satisfy a certain threshold and minimum value of $\alpha+\beta$ were used.	Maximal covert throughput was improved significantly as the number of helpers increased.

D: Discrete-time; C: Continuous-time.
G: Warden used a general detector; P: Warden used a power detector; OP: Power detector was verified as the optimal detector.
✓means the option was considered or discussed explicitly; – means the option was not considered or discussed explicitly.

C. Lessons Learned

The strategies to employ jammers to improve covertness performance are outlined in this section. The features and efficacy of covert communications facilitated by jammers have been examined from the following perspectives: informed jammers (both single and multiple) and uninformed jammers (single and multiple), as illustrated in Table 8. Specifically, the following lessons can be learned.

1) The majority of the aforementioned references examined covert strategies in discrete-time scenarios in which the block length was infinite. More research is still needed to fully understand the properties and effectiveness of the other various models (such as continuous-time, finite block length, or other channel fading factors) in jammer-aided covert communications.
2) The power detector is the optimal for the model under consideration, as shown in [15]; many later works [117], [118] followed this finding. In situations that are more complicated or distinct, the adversary's detection strategy is unknown, and the best detection strategy has not been demonstrated. The majority of the aforementioned research efforts

continue to use the premise that the adversary is a power detector, hence simplifying analysis and emphasizing the influence of additional characteristics on covert performance, such as jammer density in [30].

3) The designs of transmit signals, jamming schemes, coding schemes, and the adversary's knowledge of the related CSI are the primary aspects of covert performance evaluation.

Future study in this area should be directed in a number of ways, particularly with regard to covert communications on B5G wireless networks. For instance, there is a lack in the literature on the combined design of covert and jamming signals to maximize covert performance, including coding scheme design, transmit power allocation, and spatial distribution. There will be new link modeling, complex interference coordination management, covert performance optimization challenges, and so on as a result of the complex deployment of various jammers in the network, such as drones, IRS, and equipment using ultra-high frequency; for a more thorough discussion, refer to Section VII.

VI. COVERT COMMUNICATIONS IN RELAY-AIDED SYSTEMS

Relay technologies are useful for increasing network coverage, boosting throughput in wireless communications, and optimizing energy efficiency, specifically, when diverse PLS schemes have been employed [129], [130]. Kumar Arumugam, Bloch, and Wang [131] expanded the method developed in [16], [19], [20], and [70] to relay channels, where two noncolluding wardens monitored communication between the transmitter and the relay across two DMCs. The optimal asymptotic scaling of the message and key bits has been identified, and this establishes the theoretical basis for further research with less restrictive conditions, such as using Gaussian codebooks, having a default encoding method, or having an adversary that is a power detector. Three types of research exist for relay-assisted covert communications under these lax restrictions: untrusted relays, greedy relays, and friendly and trusted relays. In this section, we will go over them in more detail.

A. Friendly and Trusted Relays

Fig. 10 shows covert communications using a relay. Alice uses a trusted and friendly relay to transfer her messages to Bob in a covert manner. The relay functions as both a cooperative, friendly jammer that transmits AN when needed and an intermediary node that forwards information from Alice [132]. The relay serves as a cooperative aid and sends AN with a uniformly fluctuating power level when Alice is not sending covert signals. However, the relay may use the AF protocol to broadcast the amplified signal whose transmit power has the same distribution as the AN when Alice sends covert signals.

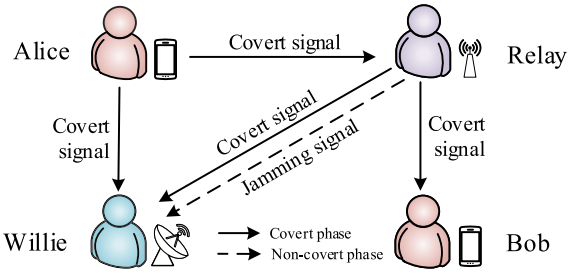

Fig. 10. *Covert communications with the help of a relay with its dual roles, i.e., a cooperative jammer and an AF relay node. As the role of a cooperative jammer, the relay transmits the jamming signal in [132] while forwarding the received noise in [31] in the noncovert transmission phase. As the role of an AF relay, the transmitter Alice tries to communicate with Bob covertly in the presence of an adversary Willie in the covert transmission phase.*

The relay is an FD node in this study, and it is assumed that SI is insignificant. Let us assume that an adversary adopts a power detector. It is possible to determine the optimal settings for error probability and detection threshold in order to enhance performance. Furthermore, Alice's transmit power was adjusted to maximize the covert rate while staying within the relay's maximum transmit power limitations. The outcomes demonstrated that obtaining a favorable covert rate is aided by the relay with dual roles. Upon completion of the covert transmission, the relay functions as a cooperative jammer [31], rather than producing AN as in [132]. It may also amplify and forward received noise. In addition, the gain was changed to maintain the same transmit power as during covert transmission. We used channel uncertainty between the relay and Willie to make Willie less effective at detecting signals [194]. Numerical results showed that with the aid of a relay and channel uncertainty, Alice could covertly communicate $O(n)$ bits to Bob.

In [133], covert communications in a one-way relay scenario with an active warden were examined. The FD relay employed the AF protocol to send information in two phases: Phase 1: the relay transmits jamming signals to confuse the warden (Willie) while simultaneously receiving the covert signals from Alice; Phase 2: the signals are boosted by the relay and sent to Bob. A noncooperative game including Alice and Willie's behaviors was modeled, and it had a stable NE. Covert transmission over n channel resource units is possible for $O(n)$ bits. The performance of covert communications was studied by Gao et al. [134], who presented two relay selection schemes, superior-link selection and random selection, taking into account various friendly relays in the systems. The outcomes demonstrated that a higher maximum covert rate was provided by the superior-link relay selection techniques. Sun et al. [135] examined the covert communication performance of relays in HD, FD, and combined HD/FD modes, quantifying the effects of relay transmission power and mode selection.

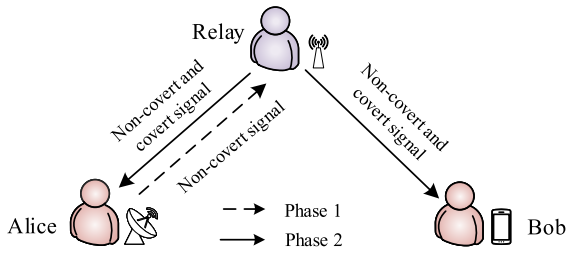

Fig. 11. *Greedy relay attempts, while relaying signals from Alice, to covertly and opportunistically send its own signals to Bob. There are two stages taken into consideration: in Phase 1, Alice sends the noncovert signal to the relay; in Phase 2, the relay transfers Alice's noncovert signal and sends Bob its own covert signal.*

B. Greedy Relays

As illustrated in Fig. 11, there are application scenarios in which a greedy relay tries to transmit its source signals to Bob while covertly transmitting its own signals. A one-way relay scenario was examined in [32], where Alice served as a warden of covert transmission due to the relay's unauthorized usage of forwarding resources that were intended for noncovert signals. Phase 1 of the procedure began when Alice attempted to send its own signal, that is, a noncovert signal, to the relay. Subsequently, the relay transmitted its own covert signals while amplifying and forwarding the noncovert signal. For the relay, two covert schemes, rate-control and power-control schemes, were put forward. Based on the analysis's numerical results, the relay's available covert rate rose with its forwarding capabilities (i.e., maximum transmit power and so on), and it should convey noncovert signals to conceal its own private information.

Wireless energy harvesting and information transmission techniques were applied to the proposed one-way relay network [136] in order to address energy-limit issues. Specifically, Hu et al. [137] employed a self-sustaining relay, in which a relay obtained data while concurrently harvesting energy from the source Alice. There were two stages to the information transfer in this study from Alice to Bob. Alice sends energy and noncovert signals to the relay during Phase 1. Using the power that was harvested from the source node in Phase 1, the relay sends Bob its own covert signal while relaying Alice's noncovert signal.

In addition, two energy harvesting strategies, power splitting and time switching, were proposed. It was shown that in some cases, the maximum effective covert rates in the two systems differed, but the source's lowest error probability remained the same and was solely dependent on energy conversion efficiency. SWIPT was used in [138] to implement HOR as an FD relay. In addition, MC was employed to examine the remaining energy of the relay. It was demonstrated that the suggested HOR model could improve covert performance by controlling the leftover energy or optimum detection threshold. Using multiantenna relays, Lv et al. [139] investigated covert communications. There were two relay beamforming systems designed: random and MRT. The outcomes demonstrated that compared to the random beamforming system, the MRT beamforming technique delivers a greater covert rate. Su et al. [140] examined relay selection in covert communications. The chosen relay attempted, using the forward data as a cover, to send its own message. By increasing the source transmission rate, the relay selection strategy was able to obtain a lower PDE (with a minimum value of $\pi_0\alpha + \pi_1\beta$) and a higher ACR.

C. Untrusted Relays

Relays can also be used in certain scenarios to forward information, but by decoding the information from a PLS perspective, they may not be trusted [141]. Forouzesh et al. [142] studied a one-way relay scenario that includes one multiantenna source, Alice, and several other nodes (with single antenna), such as receiver Bob, untrusted AF relay, and warden Willie. This was done in light of the crucial role that untrusted relays play in heterogeneous networks and IoT networks. This study addressed two security issues: secure transmission of Alice's signals without the untrusted relay decoding them and covert communication across the Alice-relay-Bob link without being detected by the warden.

Two transmission phases of jamming signals from Alice and Bob were used to address the aforementioned two problems. In particular, Alice used MRT beamforming techniques to send covert messages to the relay [143]. In the meantime, Bob injected jamming signals into the Alice-to-relay link in order to combat Willie's interception and prevent the unreliable relay from decoding. In the second phase, Alice transmits jamming signals to confuse Willie and accomplish covert transmission over the relay-to-Bob link, while the untrusted relay amplifies and forwards the data Alice received in the first phase. In order to meet covertness requirements in two phases and achieve an optimal secrecy rate, various power allocation techniques were tested in this work. For the performance analysis, a successive convex approximation method [144] was used to solve the nonconvex problems after a transformation. It should be noted that the results have been expanded to include more general networks, which might include Alice that has multiple antennas and other nodes with a single antenna. In [142], there are numerous wardens named Willies in addition to the legitimate receiver Bob and multiple noncolluding untrusted AF relays. To specifically address the two security vulnerabilities described earlier, one relay was chosen from the multiple relays to battle wardens in two scenarios, meaning that all Willies operate either independently or collaboratively. There is a tradeoff between covert communications and secure transmission when more relays are added since covertness performance suffers as the security rate rises.

Table 9 Covert Communications in Relay-Aided Systems

Types	Channel	Time	Warden	Relay	Codes	Keys	Infinite	Covert schemes	Conclusions
Friendly and trusted relays	DMC [131]	D	G	HD	✓	✓	✓	Two non-colluding wardens observed communications from transmitter and relay, and covertness metric was relative entropy.	Optimal asymptotic scaling of message and key bits was identified.
	Fading [132]	D	P	FD	–	–	✓	AN was sent in non-covert phase. The minimum value of $\alpha + \beta$ was used as the covertness metric.	Relay helped to obtain a positive covert throughput, and the maximum covert rate was analyzed.
	Fading [31]	D	OP	FD	–	✓	✓	Received noise was used as a cover. The minimum value of $\alpha + \beta$ was used.	Alice could transmit $O(n)$ bits covertly to Bob with the help of a relay and channel uncertainty.
	Fading [133]	D	OP	FD	✓	✓	✓	Covert transmissions were established in two phases. $\alpha+\beta$ was used as a metric.	NE was stable and $O(n)$ covert bits could be transmitted.
	Fading [134]	D	P	HD	–	–	✓	Random relay selection and superior-link relay selection were proposed. The covertness metric was $\alpha + \beta$.	Superior-link relay selection scheme obtained a better maximum covert rate.
	Fading [135]	D	OP	HD/FD	–	–	×	HD, FD, and joint modes for relays were studied. Relative entropy was used.	The effect of mode selection and relay power control on the maximum covert rate was studied.
Greedy relays	Fading [32]	D	P	HD	–	–	✓	Rate and power-control schemes were applied to relays. Minimum $\alpha + \beta$ was the covertness metric.	Non-covert signals should be used by relays and effective covert rate increases with its forwarding ability.
	Fading [137]	D	OP	HD	✓	✓	✓	Two energy harvesting strategies were used for relays. Minimum $\alpha + \beta$ was used.	For the two schemes, costs of achieving covertness were the same, while maximum effective covert rates were different.
	Fading [138]	D	OP	HD	–	–	✓	HOR model was proposed and MC theory was applied. Minimum $\alpha + \beta$ was adopted.	Covert performance (i.e., transmission outage probability) was enhanced via managing residual energy or detection threshold.
	Fading [139]	D	P	HD	–	–	✓	Two beamforming schemes (i.e., random and MRT) were designed. Minimum $\alpha + \beta$ was adopted.	MRT beamforming scheme offered a higher covert rate than random beamforming scheme.
	Fading [140]	D	P	HD	–	–	✓	Forward signals were used as a cover. Minimum $\pi_0\alpha+\pi_1\beta$ was adopted.	Relay selection scheme obtained a lower PDE and a higher ACR with an increasing source's transmit rate.
Untrusted relays	AWGN [142]	D	OP	HD	✓	–	✓	Jamming signals were designed jointly. Minimum $\alpha + \beta$ was used.	A trade-off between covert communications and secure transmissions could be achieved.

D: Discrete-time; C: Continuous-time; HD: Relay worked in half-duplex mode; FD: Relay worked in full-duplex mode.
G: Warden was a general detector; P: Warden was a power detector; OP: Power detector was verified as an optimal detector.
✓means the option was considered or discussed explicitly; – means the option was not considered or discussed explicitly;× means the block length was finite.

D. Lessons Learned

This section provided an overview of covert relay systems, in which relays can fulfill various relay-related forwarding and/or communication requirements by taking on multiple roles. As indicated in Table 9, we examined the features and efficacy of the various strategies with regard to greedy relays, untrusted relays, and friendly and untrusted relays. The following are the key lessons learned from the relevant research endeavors.

1) In order to meet the requirement of covertness, friendly and trusted relays were typically designed to send AN at the appropriate moment. There is still a need to investigate more covert scenarios under various constraints, such as relay scenarios with requirements for covertness in two-hop or multihop connections and relay scenarios in hybrid HD/FD mode with a finite block length.
2) Greedy relays were often used to transmit signals covertly in order to carry out their own covert transmissions. More research should be done on the tradeoff between security performance and covert requirements.
3) When there are untrusted relays present, PLS analysis must be done to assess the threat that these relays provide to forwarding signals, and the transmission of signals must be sufficiently covert to fend off external wardens. Hence, in untrusted relay scenarios with varying restrictions, a tradeoff between PLS and covert communications is a crucial issue for further investigation.

4) It is anticipated that covert communications will enable relays to be used in more realistic application scenarios. One-way relays can be expanded to two-way relays in certain application scenarios. More research on multirelay and its selection algorithms is needed for covert communications.

In order to achieve its goal of connecting everything, B5G can employ a wider range of communication nodes, including multihop nodes, cars, UAVs, IRSs, and more, as relays. These nodes will be covered in greater detail in Section VII. More in-depth research on covert communications in B5G wireless networks can be aided by the aforementioned research subjects and lessons discovered on relay-aided covert communications.

VII. CHALLENGES AND NEW RESEARCH DIRECTIONS

Though a significant amount of research efforts have been made in covert communications, much work needs to be done before covert communications can be easily integrated into future wireless communications. Here, we would like to outline the challenges and suggest a few fresh lines of research for further in-depth study in the context of B5G wireless networks.

A. Channel Model Extension

1) Continuous-Time Scenarios: The majority of research on covert communications has been conducted in discrete-time scenarios, and it was typically expected that the findings would apply to continuous-time scenarios as well. Subsequent studies, however, showed that this theory is not solid. For instance, it is very difficult to obtain exact symbol synchronization or perfect pulse shapes in real-world applications. Therefore, in both continuous- and discrete-time contexts, the quantization process lacks research on a few crucial topics related to covert communications.

More attention has recently been focused on covert communications in continuous-time scenarios [71], [72], [73], [124]. The majority of published works examined covert communications over AWGN channels in point-to-point scenarios subject to a number of restrictions, including an infinity bandwidth [73], an ideal spectral mask constraint [72], and a perfect band-limited pulse shape [71]. For example, in [124], the continuous-time scenarios with jammers were taken into consideration. The subjects discussed above shed light on the difficulties of covert communications in continuous-time environments. Future studies should focus on covert communications in a variety of other continuous-time scenarios, such as those including relay nodes, multiantenna nodes, and more intricate network arrangements. Finding improved carrier pulse waveforms that could outperform commonly utilized raised cosine pulses is another approach. Schemes intended for imperfect symbol synchronization are also necessary.

2) Imperfect CSIs: Research on channel estimate is well recognized to be difficult, particularly in covert communication networks where a very high-security requirement exists. Extra caution should be used when designing covert schemes, where the possible eavesdroppers and the covert transmitter have varying levels of knowledge about the CSI of relevant links [108]. CIPC is typically utilized to satisfy the covert requirement in order to alleviate the problem that a legitimate receiver cannot gain the CSI via pilots from a covert transmitter [37], [94], [145]. However, in order to facilitate covert communications, this CIPC needs channel reciprocity. In the context of covert wireless communications, Xu et al. [146] examined channel estimation techniques with pilots. It was demonstrated that in the settings under consideration, the adversary's detection ability might be weakened by using both an optimal amount of channel resources and an equal transmit power for information and pilot signals. Therefore, another area that needs more in-depth study is channel estimation design in the context of covert wireless communications for various application scenarios.

In many covert methods, the CSI of an eavesdropping link is traditionally considered to be fully known in order to assist the analysis. It is challenging for a covert transmitter to get the ideal CSI of the eavesdropping link, though, because the eavesdropper is typically a passive, unresponsive, or unwilling node. In some less ideal receiver conditions with inadequate CSI, the true expressions of channel coefficients must be defined as the total of the two components, that is, the estimation value and the estimation errors. This is in contrast to certain research that employed CDI in place of CSI [54]. The covert performance at the transmitter/warden with various unclear CDI restrictions was examined by Forouzesh et al. [125]. One of the areas of future research will be how to define the CSI's estimating errors while balancing practicality and accuracy.

3) Different Fading Characteristics: Distinct fading characteristics are introduced due to the varying nature of a real application environment (e.g., mountains, forests, and oceans) and the movement of nodes. This places distinct constraints on the establishment of covert channel models. Wireless channels often exhibit two types of fading characteristics: small-scale fading and large-scale fading. Shadowing fading with a log-normal distribution and distance-dependent path loss are examples of large-scale fading. The primary causes of small-scale fading are the Doppler effect (sometimes referred to as fast fading or slow fading) or multipath propagation (also known as frequency selective fading or flat fading). The majority of previous research on covert communications focused on flat Rayleigh fading models and/or distance-dependent path loss, leaving out more complex fading models, such as Rician, Nakagami-m, or frequency selective fading models, which should be included in future studies.

B. Active/Multiple Adversaries and Verification of the Optimal Detectors

1) Active Adversaries: The majority of earlier research on covert communications had the implicit assumption that adversaries are static and passive. The difficulties in maintaining covert communications in the face of various active eavesdroppers, such as those who flip covert bits maliciously [84], [147], send jamming signals [41], [133], change their location dynamically, or use multiple antennas [148], have only been noted in a very small number of works. It is necessary to develop and study the corresponding methods in order to counter these active wardens. According to Zhang et al. [84], in order to meet the requirements for covertness, a shared secret key must be added even in cases when the adversary has a better channel than the legitimate recipient. In contrast to passive wardens, active wardens as described in [41] and [133] degraded covert performance. To increase covert capacity, cooperative jamming or relay was used. Nevertheless, even in a noisy environment or with the assistance of friendly jammers, it was discovered that covert communications cannot be established against an active warden that applies a trend test to determine the transmission of covert signals [148]. As a result, there are still a lot of unanswered concerns about active eavesdroppers that merit further investigation, such as the number of active strategies that a warden can employ, the extent of their potential benefits, and the best ways to create a covert strategy to counteract various active wardens.

2) Multiple Adversaries: The literature examined covert communications when there were several eavesdroppers present. Based on their degree of collaboration, the eavesdroppers are often divided into two categories: noncolluding [149], [150] and colluding [29], [62], [142], [151]. A preservation zone was introduced around every warden node by the efforts in [149]. Several attackers were depicted as independent, uniformly distributed nodes inside a disk area surrounding a receiver in [150]. Typically, it was believed that these adversaries were i.i.d. On the other hand, multiple adversaries might cooperate to improve their detecting capabilities. The majority of earlier works placed numerous limits on these wardens in an effort to lessen the burden of analysis. For instance, Soltani et al. [29] assumed that every warden was placed uniformly and independently within a unit square. In [142] and [151], the observations of various wardens were taken to be noncorrelative, and an FC that integrates all the wardens' data was defined to determine the presence or absence of covert signals. A multivariate Gaussian probability distribution function was recently employed in [62] to describe the correlation between observations made by various wardens in a scenario where the block duration was finite. Consequently, there are still a lot of application scenarios that need to be further studied given the correlation of the observations made by various wardens. For instance, Ma et al. [62] investigated covert communications in a similar setting using relays, jammers, or multiantenna nodes. Furthermore, it is currently unclear how to describe the joint probability distribution of aggregated data in the case of an indefinite block length.

3) Verification of the Optimal Detector: The adversary in many instances involving covert communication was typically considered to be a radiometer or power detector [26], [30]. Power detectors were found to be the optimal detectors in a limited number of scenarios (e.g., Alice–Bob–Willie-jammer model [31], [114]). While more application scenarios are still worth investigating, numerous efforts have set the groundwork for covert communications over some classic channel types against general adversaries [16], [19], [20]. Furthermore, there is still a problem with verifying the optimal detector that an attacker uses in different scenarios.

C. Practical Codes and Secret Keys

1) Practical Codes: The findings from numerous earlier studies indicate that normal linear codes lack the qualities of "low-weight" codes, so they cannot be employed directly in covert communications [23]. Random or stochastic encoding was utilized in several covert communication techniques to satisfy the nonlinearity criteria [19], [23], [48], [74]. Practical applications are hampered by the random or stochastic encoding systems' poor computational efficiency and high decoding complexity. In fact, relevant codes that are simple to decode are not random codes. A few studies made an effort to create workable coding schemes, such as by combining linear and nonlinear codes into concatenated codes [75], [76], [77], [80]. Wang and Bloch recently provided the first code with efficiency and proven guarantees for key usage [24]. However, there are still a lot of topics that require more investigation. For instance, rather than being created for the general scenario, most current coding schemes are created for particular models or applications. Rigid proof is missing for a few of the suggested moderate-density concatenated codes. Applications may find codes with lower decoding complexity more appealing. Thus, further in-depth investigation and discussion are necessary when it comes to investigating more useful, verifiable, and effective codes for covert communication.

2) Secret Keys: Three subproblems, namely, whether a shared secret key is required, how long should the shared secret key be, and how to generate a secret key, were partially addressed in the context of secret keys for covert communications. Additional research efforts should focus on the implementation details of shared secret keys, such as general requirements for keyless covert communications [25], [82] and optimization of the length needed for shared secret keys [16], [28]. Some concepts still need to be validated and put into practice. More specifically, when the current preconditions for keyless covert communication (i.e., a receiver has a better link than a

watcher's) are not met, can we purposefully insert helpers or friendly nodes in covert transmission? Furthermore, by using a randomized processing scheme for its sent signals, a transmitter may be able to shorten or possibly do away with the shared secret key altogether. Recent research, for instance, [128], examined covert communication in the presence of a cooperative jammer; the findings demonstrate the interaction of local randomness, secret rate, and covert communication rate. More specifically, in certain scenarios, only a rate-limited shared secret key between the transmitter and the receiver is required.

D. Fundamental Limits in Covert Communications

The SRL that governs physical layer covert communications over AWGN channels was demonstrated by Bash et al. [17], therefore illuminating the fundamental limit of covert communications. To be more precise, the scaling number of reliable and covert bits cannot be greater than $(n)^{1/2}$ for every n channel used. For AWGN channels and DMCs [16], [18], [19], [21], MACs [67], MIMO [102], [103], classical-quantum [65], [172], and so on, the precise characterizations for the scaling constant have been refined [16], [18], [19], [21]. Numerous subsequent studies have focused on figuring out when the SRL does not apply, e.g., when the adversary is unsure about the channel [48], [54], [94], [95], the background noise [26], [87], or the transmit time [27].

Many works [32], [132], [134] tend to restrict the adversary's detection capabilities and so lessen the analytical complexity when studying covert performance in more complicated application settings. One such method is to set the adversary up as a power detector. Many covert performance optimization problems are changed into optimization problems with power as a variable because an adversary is a power detector. As a result, the potential encoding and keys in the scheme are either ignored or simplified, for example, because the default key is sufficiently long or the encoding schemes and keys are implicit. The literature has identified a number of findings on covert communications based on an infinite block length n, which was obtained from a limit when n approaches infinity [52]. Research efforts have been drawn to the corresponding covert performance in scenarios with a finite block length [152], [153], [154]; nevertheless, further investigation is still needed to fully understand the tradeoff between coding schemes and finite block length in complex network environments.

E. IRS-Assisted Covert Communications

While reflecting the received signals, an IRS, or IRS, can be utilized to suppress or cancel unwanted signals and amplify desired signals in the legitimate links [39], [155]. Without the need for specialized additional signal processing, smart reflection is achieved by proactively modifying the IRS elements' phase shift vectors and amplitudes under software control. Thus, by controllable intelligent signal reflection, the IRS can assist in creating a suitable covert communications environment. Using the IRS to improve covert communications was proposed in [156]. To improve covert performance, a joint design of the IRS reflection coefficients and transmit power was suggested [157], [158], [159]. Kong et al. [160] jointly took into account IRS reflection coefficients, transmit power, and transmission probability in order to maximize the attainable rate. In the meanwhile, the work was expanded to include various applications, such as NOMA systems [162] and IoT networks [161]. Specifically, the IRS works using several covert strategies, such as multiple antennas [163], [164], [165]. We think that the developing IRS technology will provide many new approaches to develop covert communication strategies in the future. Prospective directions for future investigation encompass the scaling laws of IRS-assisted covert capacity and the many forms of IRSs (e.g., mobile IRSs and fixed IRSs) supporting covert schemes.

The IRS adds operational and design complexity while also providing opportunities for covert communications. A low-complexity two-stage technique was developed in [157] and [159] to strike a compromise between computational complexity and covert performance. The first stage of the algorithm involves IRS beamforming, while the second stage involves transmit power allocation of the covert signal. In [158] and [160], a 1-D search technique was used to solve a joint optimization problem with several parameters (such as transmit power, IRS's reflection matrix, and transmission probability).

In [163], a sequential rank-one constraint relaxation algorithm was presented to solve an alternating optimization algorithm with a convex subproblem. The covert performance optimization problem was solved in other specific applications by combining various techniques, such as alternating optimization and SDR [162], S-lemma, alternate iteration [161], Gaussian randomization techniques, SDR, alternative optimization algorithm [165], penalty dual decomposition, and successive convex approximation [164]. The computational complexity of optimization processes or iterations rapidly rises with the complexity of application scenarios. An appropriate tradeoff between complexity and covert performance still has to be investigated, despite the fact that current works have made some attempts to lower the optimization complexity of IRS-based covert communications in specific scenarios.

F. Jammer-Assisted Covert Communications

The covert communications in the previously indicated scenarios are compared and summarized in Table 10. The use of covert communications in three-node setups with a single antenna typically depends passively on the warden's uncertainty regarding the related parameters. Then, in three-node settings, multiantennas add a higher degree of freedom for covert communications; for example, receivers' FD antennas can be utilized to send AN. To examine the corresponding covert performance in more

complex MIMO circumstances, such as more powerful wardens, further research is still required. In order to prevent SI issues brought on by FD receivers, jammers offer a greater degree of freedom in the design of AN, which is compatible with other technologies, such as multiantenna jammers.

More work is necessary, nevertheless, to quantitatively analyze coordinated or joint interferences amongst multiple jammers. Relaying's effect on covert messages depends on how friendly or trustworthy, or greedy or untrustworthy, it is within the network. In particular, friendly relays can help to enhance covert performance. A greedy relay operates under the supervision of resource-providing nodes to carry out its own covert transmission. Signals can be forwarded via the untrusted relay, but other nodes are still needed to provide the covertness criterion. With its high degree of interoperability with various technologies and adjustable intelligent signal reflection, the IRS provides more options for improving covert communication performance.

G. ML-Based Covert Communications

ML-enabled solutions can boost communication performance in B5G wireless networks by taking advantage of more opportunities due to their ability to learn in unpredictable and dynamic environments. A tradeoff between the transmission performance of legitimate users and the covertness requirement (i.e., the characterization of the detection performance of adversaries) is always present in the context of physical layer covert communications. A single-objective optimization problem with constraints, such as the optimization of cover communication rate under the constraint of the eavesdropper's error detection probability, was the focus of the majority of earlier publications that revolutionized the study of covert systems. However, most traditional methods can hardly solve the performance optimization problem with intense interactions between the eavesdropper and the legitimate users when the systems have adversaries capable of dynamically adjusting their detection parameters (e.g., detection thresholds or detector types), especially in the case of insufficient prior conditions.

A technique for creating generative models with deep learning techniques is the GAN. A GAN typically comprises two models: a discriminator model and a generator model. In order to generate new samples, the generator model attempts to mimic the features of actual samples. When attempting to differentiate the created samples from the real ones, the discriminator can often be a binary classifier. In a covert communication game, adversaries and legitimate users compete with one another to attain NE. This process in GAN is compatible with those of the two models. To create a transmit power allocation method for covert signals, for instance, a legitimate user can be viewed as a generator module, and the discriminator can be used as an adversary to determine whether the covert signal is present [166]. The two models (adversaries and legitimate users) in GAN-based covert communications are alternately trained in a competitive way to arrive at a close to optimum power allocation solution. A hybrid GAN-based trajectory and power performance optimization approach with fast convergence and near-optimal results was presented by Li et al. [58]. Therefore, future research should focus on GAN-based covert performance optimization issues in a wider range of application contexts and with varying limitations.

In addition, a recent study trend in artificial intelligence applications is DRL. It is a dynamic programming approach that learns optimal solutions under changing conditions and adjusts to the environment. DRL has been widely employed as an efficient technique in the field of wireless communications to handle a variety of issues, including resource allocation, wireless caching, multiple access, data rate regulation, and so forth [167], [168], [169]. Many issues, including cyber–physical attacks and interference management in communications, can be represented as games. Existing DRLs have been applied to these games to tackle various issues, including determining NEs when information is inadequate [170]. Then, it is anticipated that DRL-based covert communications will also be a significant study area in the future based on the features of performance optimization in covert communications, i.e., the game between legitimate users and eavesdroppers in an imperfect information network.

H. Quantum-Enhanced Covert Communications

Numerous fundamental laws of nature are governed by quantum mechanics. Quantum information theory is required to analyze the limits of a communication system, and it led to the invention of covert communications via lossy thermal noise boson channels [171]. Bash et al. [172] defined the upper bound on the amount of data that may be covertly and reliably transferred across a lossy thermal-noise bosonic channel. Arrazola and Scarani [173] extended covert communications to the quantum domain, where they came to the conclusion that covert QKD is also feasible in a scenario in which the adversary has complete control over the channel. Liu et al. [174] investigated and demonstrated the possibility of covert communications over metropolitan distances by experiment. Arrazola and Amiri [175] examined how covert communication techniques can be used to accomplish secure secret key expansion. Using carefully designed protocols, Bash et al. [172], Arrazola and Scarani [173], Liu [174], and Arrazola and Amiri [175] guaranteed covertness and led to the conclusion that covert QKD needs more secret bits than it can generate. Tahmasbi and Bloch suggested in [176] an uncoordinated protocol based on the use of "sparse signaling" for quantum state distribution to achieve covertness in contrast to [172], [173], [174], and [175]. They suggested a partial coordination protocol based on PPM and MLC to prolong the secret key in order to lessen

Table 10 Comparison of Covert Communication Schemes in Different Scenarios

Scenarios	Types	Measures & covert schemes	Typical characteristics
Three-node scenarios with single-antenna	Noise uncertainty	Quantify Warden's uncertainty about noise to ensure covertness requirement.	A positive covert rate was obtained, while the estimation of noise uncertainty was a key factor.
	Channel uncertainty	Exploiting warden's uncertainty in wiretap channel to ensure covertness requirement.	Warden's uncertainty on associated channel facilitates the establishment of covert communications, but receiver's uncertainty may hinder performance.
	Noise and channel uncertainty	Warden's joint uncertainty about noise and channel was used to ensure covertness requirement.	Influence of channel uncertainty was proven to be greater if noise uncertainty exists.
	Time uncertainty	Slot selected for covert signal transmission was designed to be secret to warden.	A total number of available transmit slots may have some impact on covert performance.
Three-node scenarios with multi-antenna	HD	Coding schemes, a known CSI of warden, or careful design beamforming can be exploited to satisfy the covertness requirement.	Multi-antenna has the potential to increase covert rate, while the number of covert bits is decided jointly with different parameters, e.g., beamforming vector, or space-time diversity.
	FD	To guarantee the required covertness, receiver equipped with FD multiple antennae simultaneously sent AN in addition to receiving covert signals.	Covert performance can be improved by setting the parameters of AN, e.g., the number of transmit antennas, maximum transmit power, varying/fixed transmit power for infinite/finite block length, and so on.
Jammer-aided scenarios	Single informed jammer	Use a jammer or other network users (e.g., a general receiver, a weak user in NOMA) as a cover to ensure covertness requirement.	Synchronization between transmitter and jammer is a key factor. Other techniques, e.g., beamformer using multi-antenna at transmitter, can be used jointly to improve performance.
	Multiple informed jammers	Other multiple friendly nodes in networks can be used as covers (jammers) to ensure covertness requirements.	Performance can be improved by adjusting a joint user-jammer scheduling scheme under different performance requirements.
	Single uninformed jammer	Jammer sent a jamming signal with different configurations, e.g., time-varying AN, channel mobility, and multi-antenna, to ensure covertness requirement.	Jammer has a higher design freedom and can be combined with more AN schemes. Jamming and covert signals are relatively independent.
	Multiple uninformed jammers	Ambient interferences or jamming signals were used to ensure covertness requirements.	Under strict constraints, increasing jammer density or transmit power helped to improve covert performance.
Relay-aided scenarios	Friendly and trusted relays	As a covert re-transmitter, it takes forwarding non-covert signal as a cover.	Relays helped ensure covert communications, and specific performance analysis needs to consider several factors, i.e., relay selection, HD/FD, etc..
	Greedy relays	Working as an adversary to decode forward signal, while covertness requirement is satisfied by other techniques.	Relay can realize its own covert transmission under supervision of an energy provider or the primary user with its forward signal as a cover.
	Untrusted relays	Working as an adversary to decode forward signal, while covertness requirement was satisfied by other techniques.	Relays cannot be used to satisfy covertness requirements, and system should work jointly with other techniques, e.g., multi-antennas, and full-duplex.
Covert communications with IRS	IRS assisted	Strengthen desired signals in legitimate links and suppress undesired signals by reflecting received signals.	A favorable covert communications environment can be established with IRS via controllable intelligent signal reflection.

the complexity of the process [177]. To demonstrate the presence of positive covert throughputs for a variety of bosonic channel parameters, a new bound was introduced. The protocol performance showed that it is possible to expand a covert secret key utilizing both a quantum channel under precisely defined control of an adversary and a publicly authenticated classical channel.

In the meantime, quantum-secure covert communication via bosonic channels was the main focus of Gagatsos et al. [59] and Bullock et al. [178]. In addition, they deduced an expression for the quantum-secure covert capacity in the bosonic channels with and without entanglement support, as well as the maximum mean photon number. The basic scaling rule in covert communications was discovered to change from $O((n)^{1/2})$ to $O((n)^{1/2}\log n)$ with entanglement help. Di Candia et al. [179] combined covert communications in microwave regimes with backscattering concepts to propose a new paradigm for secure quantum communications.

Quantum-enhanced covert sensing conceals the probe light in a noisy environment, much like covert communications. An entanglement-enhanced covert sensing protocol was proposed and experimentally implemented by Hao et al. [180], which opened the door for quantum-enhanced secure sensing, communications, and its information processing. They are both significant applications in the B5G wireless networks and merit much more in-depth research even though the tasks of covert communications and sensing have different goals (i.e., covert communication is evaluated by the number of bits that can be covertly transmitted, while covert sensing concerns the precision of parameter estimation).

I. B5G Wireless Networks

1) Unmanned Aerial Vehicles: Numerous B5G applications, including environmental inspection, surveillance, emergency communications, and more, have proposed the usage of UAVs. UAV-enabled communications offer several advantages over conventional wireless communications, including low operating costs, flexible geographic locations, line-of-sight connectivity, and high mobility. Owing to the peculiarities of wireless channels, adversaries may pose a variety of security concerns to UAVs. An adversary might also readily utilize UAVs to threaten legitimate communication channels.

In order to safeguard UAV-enabled wireless transmission from different perspectives, researchers have studied covert communications. Various schemes have been developed, including ways to conceal the UAV receiver [181], [182], [183], [184], [185]; joint optimization of UAV trajectory and other resource utilization [186], [187]; D2D underlaid UAV networks [188]; and UAV relays [189]. UAVs were used as friendly nodes, that is, covert transmitters, receivers, or relays, in covert communications during the aforementioned research projects.

UAVs may still be employed by illegal organizations in certain circumstances [190], or they may be utilized by law enforcement agencies to find illegal covert connections [191]. Furthermore, joint optimization of the trajectory, propulsion, and thrust powers for UAV-on-UAV covert video tracking and surveillance services was investigated in [192]. A multiple-antenna transmitter used relay-transmitted AN and MRT in [193] to create confusion among adversaries. To increase covert throughput, the block length and transmit power of the transmitter and relay should be designed jointly.

While research on covert communications via UAV-enabled networks has been conducted, it is important to note that these efforts are relatively new, having only begun in very recent years. For instance, there are no covert communications in dynamic and heterogeneous networks assisted by UAVs. Another example is the collaborative design of many factors, such as UAV trajectory, altitude, node scheduling, and associated node transmit powers, to maximize covert performance in diverse application circumstances.

2) D2D Communications: In the literature, some efforts were devoted to covert communications in D2D-enabled wireless networks. In [194], we suggested implementing covert communications via D2D networks, wherein cellular and noncovert signals may be conveyed, with performance being enhanced through the use of cooperative NOMA and successive interference cancellation. In addition, we investigated two D2D covert schemes at an FD BS using various multiantenna configurations, where AN was employed to meet the requirements for covertness [195]. We recently proposed a covert communication technique for D2D underlaying cellular networks enabled by wireless energy harvesting. The scheme leverages power beacons to broadcast jamming signals during idle time intervals in order to confuse random adversaries [196]. For D2D information exchange, Wan et al. [197] and Shi et al. [198], [199] concentrated on covert communications. In [200], D2D covert strategies were examined. To safeguard legitimate users from wardens, a guard area was established.

The intricate relationships between various links, such as D2D links and in-band cellular links, make it challenging to carry out covert communications in many D2D application scenarios, despite some basic research studies having been done in the literature. An important area of research is the coordination between resource allocation, interference coordination, and covertness requirements. A lot of recently developed new technologies, including relay and FD technology, can also be used for D2D covert communications. The majority of research so far has concentrated on covert communications in single-tier cellular networks; further investigation is required to determine the best way to apply these findings to multitier or heterogeneous cellular networks.

3) Wireless Ad Hoc Networks: With the aid of other devices and the infrastructure, such as BSs or access points, communication links are created between a source device and a destination device in wireless ad hoc networks. While the low security and restricted bandwidth, that is, vulnerability to adversarial monitoring, may impede the effective implementations of this type of network, it also overcomes the geographical constraints of traditional networks and permits flexible node placement [201], [202]. The work in [203] expanded the findings to a multihop network and made some first attempts to study a two-hop covert communication system in AWGN channels. Sheikholeslami et al. [204] examined multihop covert communications through intermediary relays when there were numerous wardens collaborating. Within a unit area, the legitimate and warden nodes were distributed based on a p.p.p. in [149]. Im and Lee [205] examined the impact of node mobility on covert performance.

Nevertheless, more research is needed to determine how to quantify covert performance or expand the models to additional settings if we loosen the ideal assumptions made in the aforementioned study. For instance, in many situations, the latency resulting from multiple hops is not insignificant; therefore, improving overall performance under various limitations on latency tolerance and covertness requirements is an intriguing area of research.

4) IoT: Wearable technology and smart cities are only two examples of how IoT technologies have penetrated many facets of our lives. Sensitive and private data, including real-time location data and electronic health information, are being generated by a growing number of wireless IoT devices. IoT system security and privacy have grown significantly across a range of applications. Despite several study attempts on secure communications in the IoT from the standpoint of PLS [206], only very few studies took covert communications, especially in IoT networks, into

consideration. For instance, Liu et al. [36] used aggregated interference as a cover; Liu et al. [53] proposed covert schemes in THz-band AWGN scenarios; Hu et al. [94] considered covert transmissions without CSI knowledge; Wang et al. [207] used improper Gaussian signaling for the covert transmitter; Feng et al. [208] sent AN by in-band FD IoT gateways; and Wang et al. [209] proposed covert communications based on improper Gaussian signaling.

The topic of covert communications in the context of IoT networks requires further investigation. Certain strict latency requirements are highlighted in many IoT application situations, and delay-constrained covert communications can be extended to IoT networks. Many IoT devices are low-power nodes; some even experience issues with battery charging for lifetime extension. The integration of wireless power transfer technologies with covert communications in IoT networks is one potential area of future research in this field. Moreover, covert communication strategies ought to be developed for a sizable IoT network encompassing a wide area.

5) mmWaves and THz: Interest in higher frequency bands, such as mmWave and THz, has increased due to the growing demand for larger bandwidths in B5G wireless networks. THz and mmWave communications are attractive for covert transmissions due to their extremely directed nature. Cotton et al. [210] proposed a conceptual framework for covert mmWave communications. In [211], a dual-beam mmWave transmitter simultaneously broadcasts the intended signal to the destination and a jamming signal to deteriorate the warden's link performance. This constitutes a covert mmWave communication system. A hybrid precoder was designed in [212], which examined covert mmWave communications with an FD receiver.

A hybrid beamforming system for covert multicast mmWave communications was developed in [213]. A covert multiuser beam training method was proposed by Zhang et al. [214] for a multiple-user covert mmWave communication scenario with a friendly jammer. They also offered a joint design of beam training and data transmission for a covert mmWave communication system [215]. To improve the performance of covert mmWave communications, a beamforming technique based on a random frequency diversity array was studied in [216]. Bai et al. [56] examined the corresponding covert performance and suggested a metric to quantify the intrinsic sparsity of the mmWave large MIMO channels in the spatial domain. Recently, research in [53] found that covert communication based on reflection or diffusion scattering is feasible even though line-of-sight communications in a THz-band IoT network can be easily detected by a warden. Mamaghani and Hong [39] investigated energy-efficient multi-UAV covert transmission strategy for aerial IRS-enabled THz covert communications in B5G IoT systems. [57] devised a distance-adaptive absorption peak modulation for THz covert communications.

Only recently has research on covert communications in the mmWave/THz frequencies begun. It is inevitable that these initiatives will be crucial to the development of the upcoming 6G wireless networks, and they need a much more thorough investigation. In the future, research may concentrate on practical mmWave/THz channel modeling and how it can be integrated with other methods or platforms, such as massive MIMO, IRS, UAVs, and IoT.

6) Near-Field Communications: Numerous near-field (Fresnel) applications are part of 6G wireless communications. A comprehensive review of the prospects and challenges for future 6G systems operating in the near-field region was given by Zhang et al. [217]. The contrasts between near-field and far-field communications were examined by Liu et al. [218] from four different perspectives: beamforming, channel modeling, performance analysis, and applications. The study conducted in [60] examined the salient features of near-field radiation, utilizing a spherical waveform propagation model for its wireless power transmission applications. The feasibility and possibilities of beam focusing in near-field communications were examined in [219] in order to support high-rate multiuser downlink MIMO systems. The foundations, difficulties, opportunities, and future directions of near-field MIMO communications for 6G wireless networks were examined in the works in [220]. From a PLS standpoint, Zhang et al. [221] presented a near-field secure transmission architecture.

As far as we are aware, not enough studies have been done on physical layer covert communications in near-field communications context. Due to its significant role in 6G wireless networks and unique characteristics (beamforming, channeling, and so on), physical layer covert communications in the near-field domain will be one of the areas of research that needs more investigation.

VIII. CONCLUSION

This article identified research directions and problems for covert communications in B5G wireless networks while offering an in-depth review of the fundamental theories and implementation strategies of covert communications. First, the main ideas in covert communications were introduced, using a typical discrete-time AWGN channel as an example. These key ideas have been thoroughly explored and include channel models, codes and secret keys, and covertness measurements. Moreover, scenarios for applications with progressively higher levels of complexity were taken into consideration. A taxonomy of covert communications, specifically for single-antenna and multiantenna three-node systems, as well as systems assisted by jammers and relays, was presented. The main issues about the covert schemes in various contexts were addressed based on the taxonomy. Particular lessons learned are noted at the end of each section. In conclusion, we enumerated the various obstacles and future research directions related to covert communications in B5G wireless networks. ■

REFERENCES

[1] D. Je, J. Jung, and S. Choi, "Toward 6G security: Technology trends, threats, and solutions," *IEEE Commun. Standards Mag.*, vol. 5, no. 3, pp. 64–71, Sep. 2021.

[2] M. A. Khan et al., "Swarm of UAVs for network management in 6G: A technical review," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 1, pp. 741–761, Mar. 2023.

[3] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland and F. Tufvesson, "6G wireless systems: Vision, requirements, challenges, insights, and opportunities," *Proc. IEEE*, vol. 109, no. 7, pp. 1166–1199, Jul. 2021.

[4] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020.

[5] X. You et al., "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, Jan. 2021, Art. no. 110301.

[6] Y. Li, Y. Yu, W. Susilo, Z. Hong, and M. Guizani, "Security and privacy for edge intelligence in 5G and beyond networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 63–69, Apr. 2021.

[7] X. Shen, J. Gao, W. Wu, M. Li, C. Zhou, and W. Zhuang, "Holistic network virtualization and pervasive network intelligence for 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 1–30, 1st Quart., 2022.

[8] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6G network edge: A survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1095–1127, 2nd Quart., 2023.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[10] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[12] 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.

[13] 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 Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[14] Y. Liu, H.-H. Chen, L. Wang, and W. Meng, "Artificial noisy MIMO systems under correlated scattering Rayleigh fading—A physical layer security approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2121–2132, Jun. 2020.

[15] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

[16] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[17] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[18] M. Tahmasbi and M. R. Bloch, "First- and second-order asymptotics in covert communication," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2190–2212, Apr. 2019.

[19] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[20] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2229–2233.

[21] M. Tahmasbi, M. R. Bloch, and V. Y. F. Tan, "Error exponent for covert communications over discrete memoryless channels," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2017, pp. 304–308.

[22] S.-Y. Wang and M. R. Bloch, "Covert MIMO communications under variational distance constraint," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4605–4620, 2021.

[23] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2945–2949.

[24] S.-Y. Wang and M. R. Bloch, "Explicit design of provably covert channel codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 190–195.

[25] H. Zivarifard, M. R. Bloch, and A. Nosratinia, "Keyless covert communication via channel state information," *IEEE Trans. Inf. Theory*, vol. 68, no. 8, pp. 5440–5474, Aug. 2022.

[26] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[27] B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversary's ignorance of transmission time," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8394–8405, Dec. 2016.

[28] S.-H. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2310–2319, Sep. 2018.

[29] 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.

[30] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a Poisson field of interferers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6005–6017, Sep. 2018.

[31] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 317–320, Feb. 2019.

[32] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jul. 2018.

[33] J. Hu, K. Shahzad, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert communications with a full-duplex receiver over wireless fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2018, pp. 1–6.

[34] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 813–816, Jun. 2019.

[35] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

[36] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: Hiding information in interference," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 46–52, Dec. 2018.

[37] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert wireless communications with channel inversion power control in Rayleigh fading," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12135–12149, Dec. 2019.

[38] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3542–3553, Jul. 2019.

[39] M. Tatar Mamaghani and Y. Hong, "Aerial intelligent reflecting surface-enabled terahertz covert communications in beyond-5G Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 19012–19033, Oct. 2022.

[40] L. Yang et al., "Covert transmission and secrecy analysis of RS-RIS-NOMA-aided 6G wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 10659–10670, Aug. 2023.

[41] B. Yang, T. Taleb, G. Chen, and S. Shen, "Covert communication for cellular and X2U-enabled UAV networks with active and passive wardens," *IEEE Netw.*, vol. 36, no. 1, pp. 166–173, Jan. 2022.

[42] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[43] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Sep. 2015, pp. 209–217.

[44] S. Grabski and K. Szczypiorski, "Steganography in OFDM symbols of fast IEEE 802.11n networks," in *Proc. IEEE Secur. Privacy Workshops*, May 2013, pp. 158–164.

[45] S. D'Oro, F. Restuccia, and T. Melodia, "Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2019, pp. 1585–1593.

[46] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York, NY, USA: McGraw-Hill, 5555.

[47] P. H. Che, S. Kadhe, M. Bakshi, C. Chan, S. Jaggi, and A. Sprintson, "Reliable, deniable and hidable communication: A quick survey," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014, pp. 227–231.

[48] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable deniable communication with channel uncertainty," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014, pp. 30–34.

[49] S. Kadhe, S. Jaggi, M. Bakshi, and A. Sprintson, "Reliable, deniable, and hidable communication over multipath networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 611–615.

[50] P.-H. Lin, C. R. Janda, and E. A. Jorswieck, "Stealthy secret key generation," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Nov. 2017, pp. 492–496.

[51] S. Lee, R. J. Baxley, J. B. McMahon, and R. S. Frazier, "Achieving positive rate with undetectable communication over MIMO Rayleigh channels," in *Proc. IEEE 8th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Jun. 2014, pp. 257–260.

[52] S. Lee and R. J. Baxley, "Achieving positive rate with undetectable communication over AWGN and Rayleigh channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 780–785.

[53] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: From AWGN channel to THz band," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3378–3388, Apr. 2020.

[54] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *Proc. IEEE 85th Veh. Technol. Conf.*, Jun. 2017, pp. 1–5.

[55] Y. Qian, C. Yang, Z. Mei, X. Zhou, L. Shi, and J. Li, "On joint optimization of trajectory and phase shift for IRS-UAV assisted covert communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 12873–12883, Oct. 2023, doi: 10.1109/TVT.2023.3271461.

[56] L. Bai, J. Xu, and L. Zhou, "Covert communication for spatially sparse mmWave massive MIMO channels," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1615–1630, Mar. 2023.

[57] W. Gao, Y. Chen, C. Han, and Z. Chen, "Distance-adaptive absorption peak modulation (DA-APM) for terahertz covert communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3,

pp. 2064–2077, Mar. 2021.
[58] Z. Li, X. Liao, J. Shi, L. Li, and P. Xiao, "MD-GAN-based UAV trajectory and power optimization for cognitive covert communications," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10187–10199, Jun. 2022.
[59] C. N. Gagatsos, M. S. Bullock, and B. A. Bash, "Covert capacity of bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 555–567, Aug. 2020.
[60] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M. F. Imani, and Y. C. Eldar, "Near-field wireless power transfer for 6G Internet of Everything mobile networks: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 60, no. 3, pp. 12–18, Mar. 2022.
[61] M. Tahmasbi and M. R. Bloch, "Covert secret key generation with an active warden," *IEEE Trans. Inf.Forensics Security*, vol. 15, pp. 1026–1039, 2020.
[62] R. Ma, W. Yang, L. Tao, X. Lu, Z. Xiang, and J. Liu, "Covert communications with randomly distributed wardens in the finite blocklength regime," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 533–544, Jan. 2022.
[63] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 19–25, Oct. 2019.
[64] X. Jiang et al., "Covert communication in UAV-assisted air-ground networks," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 190–197, Aug. 2021.
[65] L. Wang, "Optimal throughput for covert communication over a classical-quantum channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2016, pp. 364–368.
[66] M. Tahmasbi, A. Savard, and M. R. Bloch, "Covert capacity of non-coherent Rayleigh-fading channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 1979–2005, Apr. 2020.
[67] K. S. K. Arumugam and M. R. Bloch, "Covert communication over a K-user multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 7020–7044, Nov. 2019.
[68] K. S. Kumar Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2787–2801, Oct. 2019.
[69] D. Kibloff, S. M. Perlaza, and L. Wang, "Embedding covert information on a given broadcast code," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jan. 2019, pp. 2169–2173.
[70] V. Y. F. Tan and S.-H. Lee, "Time-division is optimal for covert communication over some broadcast channels," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1377–1389, May 2019.
[71] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 448–452.
[72] Q. E. Zhang, M. R. Bloch, M. Bakshi, and S. Jaggi, "Undetectable radios: Covert communication under spectral mask constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 992–996.
[73] L. Wang, "On covert communication over infinite-bandwidth Gaussian channels," in *Proc. IEEE 19th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2018, pp. 1–5.
[74] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable, deniable and hidable communication," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2014, pp. 1–10.
[75] M. Lamarca and D. Matas, "A non-linear channel code for covert communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–7.
[76] Q. Zhang, M. Bakshi, and S. Jaggi, "Covert communication with polynomial computational complexity," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1354–1384, Mar. 2020.
[77] M. R. Bloch and S. Guha, "Optimal covert communications using pulse-position modulation," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 2825–2829.
[78] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, "Multilevel-coded pulse-position modulation for covert communications over binary-input discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6001–6023, Oct. 2020.
[79] G. Frèche, M. R. Bloch, and M. Barret, "Polar codes for covert communications over asynchronous discrete memoryless channels," in *Proc. 51st Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2017, pp. 1–3.
[80] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, "Codes for covert communication over additive white Gaussian noise channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 977–981.
[81] K. S. K. Arumugam and M. R. Bloch, "Keyless asynchronous covert communication," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2016, pp. 191–195.
[82] H. ZivariFard, M. Bloch, and A. Nosratinia, "Keyless covert communication in the presence of non-causal channel state information," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Aug. 2019, pp. 1–5.
[83] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.
[84] Q. E. Zhang, M. Bakshi, and S. Jaggi, "Covert communication over adversarially jammed channels," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.
[85] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.
[86] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.
[87] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, Apr. 2017.
[88] Y. Zeng, Y.-C. Liang, A. T. Hoang, and E. C. Y. Peh, "Reliability of spectrum sensing under noise and interference uncertainty," in *Proc. IEEE Int. Conf. Commun. Workshops*, Jun. 2009, pp. 1–5.
[89] A. Sonnenschein and P. M. Fishman, "Radiometric detection of spread-spectrum signals in noise of uncertain power," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 28, no. 3, pp. 654–660, Jul. 1992.
[90] W. Jouini, "Energy detection limits under log-normal approximated noise uncertainty," *IEEE Signal Process. Lett.*, vol. 18, no. 7, pp. 423–426, Jul. 2011.
[91] M. A. Hammouda and J. W. Wallace, "Noise uncertainty in cognitive radio sensing: Analytical modeling and detection performance," in *Proc. Int. ITG Workshop Smart Antennas (WSA)*, Mar. 2012, pp. 287–293.
[92] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.
[93] A. Vakili, M. Sharif, and B. Hassibi, "The effect of channel estimation error on the throughput of broadcast channels," in *Proc. IEEE Int. Conf. Acoust. Speed Signal Process.*, May 2006, pp. 29–32.
[94] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communications without channel state information at receiver in IoT systems," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11103–11114, Nov. 2020.
[95] K. Shahzad and X. Zhou, "Covert wireless communications under quasi-static fading with channel uncertainty," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1104–1116, 2021.
[96] H. Q. Ta and S. W. Kim, "Covert communication under channel uncertainty and noise uncertainty," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[97] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 236–239, Feb. 2016.
[98] 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. 1–15, Jan. 2015.
[99] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, Apr. 2020.
[100] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[101] X. Peng, J. Wang, S. Xiao, and W. Tang, "Strategies in covert communication with imperfect channel state information," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.
[102] A. Bendary, A. Abdelaziz, and C. E. Koksal, "Achieving positive covert capacity over MIMO AWGN channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 149–162, Mar. 2021.
[103] A. Abdelaziz and C. E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 1–9.
[104] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.
[105] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex bidirectional MIMO: Achievable rates under limited dynamic range," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3702–3713, Jul. 2012.
[106] W. Afifi, M. J. Abdel-Rahman, M. Krunz, and A. B. MacKenzie, "Full-duplex or half-duplex: A Bayesian game for wireless networks with heterogeneous self-interference cancellation capabilities," *IEEE Trans. Mobile Comput.*, vol. 17, no. 5, pp. 1076–1089, May 2018.
[107] T. Xu, L. Xu, X. Liu, and Z. Lu, "Covert communication with a full-duplex receiver based on channel distribution information," in *Proc. 12th Int. Symp. Antennas, Propag. EM Theory (ISAPE)*, Dec. 2018, pp. 1–4.
[108] J. Wang, Y. Li, W. Tang, X. Li, and S. Li, "Channel state information based optimal strategy for covert communication," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2019, pp. 1–6.
[109] L. Yang, W. Yang, S. Xu, L. Tang, and Z. He, "Achieving covert wireless communications using a full-duplex multi-antenna receiver," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, 2019, pp. 912–916.
[110] M. Zheng, A. Hamilton, and C. Ling, "Covert communications with a full-duplex receiver in non-coherent Rayleigh fading," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1882–1895, Mar. 2021.
[111] Y. Zhao, Z. Li, D. Wang, and N. Cheng, "Tradeoffs in covert wireless communication with a controllable full-duplex receiver," *China Commun.*, vol. 19, no. 5, pp. 87–101, May 2022.
[112] R. Xu, L. Guan, Y. Zhao, Z. Li, and D. Wang, "Robust power and position optimization for the full-duplex receiver in covert communication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.
[113] X. Chen et al., "Multi-antenna covert communication via full-duplex jamming against a warden with uncertain locations," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 5467–5480, Aug. 2021.
[114] T. V. Sobers, B. A. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert communication with the help of an uninformed jammer achieves positive rate,"

in *Proc. 49th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 625–629.
[115] S. Ma et al., "Robust beamforming design for covert communications," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3026–3038, 2021.
[116] L. Tao, W. Yang, S. Yan, D. Wu, X. Guan, and D. Chen, "Covert communication in downlink NOMA systems with random transmit power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 2000–2004, Nov. 2020.
[117] M. Wang, W. Yang, X. Lu, C. Hu, B. Liu, and X. Lv, "Channel inversion power control aided covert communications in uplink NOMA systems," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 871–875, Apr. 2022.
[118] L. Tao, W. Yang, X. Lu, M. Wang, and Y. Song, "Achieving covert communication in uplink NOMA systems via energy harvesting jammer," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 3785–3789, Dec. 2021.
[119] R. Chen, Z. Li, J. Shi, L. Yang, and J. Hu, "Achieving covert communication in overlay cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15113–15126, Dec. 2020.
[120] D. Goeckel, A. Sheikholeslami, T. Sobers, B. A. Bash, O. Towsley, and S. Guha, "Covert communications in a dynamic interference environment," in *Proc. IEEE 19th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2018, pp. 1–5.
[121] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3463–3473, May 2020.
[122] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4454–4469, Aug. 2014.
[123] O. Shmuel, A. Cohen, and O. Gurewitz, "Multi-antenna jamming in covert communication," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4644–4658, Jul. 2021.
[124] K. Li, T. V. Sobers, D. Towsley, and D. Goeckel, "Covert communication in continuous-time systems in the presence of a jammer," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 4883–4897, Jul. 2022.
[125] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Robust power allocation in covert communication: Imperfect CDI," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5789–5802, Jun. 2021.
[126] T. Zheng, Z. Yang, C. Wang, Z. Li, J. Yuan, and X. Guan, "Wireless covert communications aided by distributed cooperative jamming over slow fading channels," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7026–7039, Nov. 2021.
[127] S. B. Lowen and M. C. Teich, "Power-law shot noise," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1302–1318, Nov. 1990.
[128] H. ZivariFard, M. R. Bloch, and A. Nosratinia, "Covert communication in the presence of an uninformed, informed, and coordinated jammer," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, Jun./Jul. 2022, pp. 306–311.
[129] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.
[130] M. Chraiti, A. Ghrayeb, C. Assi, and M. O. Hasna, "On the achievable secrecy diversity of cooperative networks with untrusted relays," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 39–53, Jan. 2018.
[131] K. S. Kumar Arumugam, M. R. Bloch, and L. Wang, "Covert communication over a physically degraded relay channel with non-colluding wardens," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 766–770.
[132] K. Shahzad, "Relaying via cooperative jamming in covert wireless communications," in *Proc. 12th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2018, pp. 1–6.
[133] J. Wang, Y. Sun, W. Tang, X. Li, and S. Li, "Power threshold game for covert communication in relay networks with an active warden," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2019, pp. 1–6.
[134] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6313–6323, Apr. 2021.
[135] R. Sun, B. Yang, S. Ma, Y. Shen, and X. Jiang, "Covert rate maximization in wireless full-duplex relaying systems with power control," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6198–6212, Sep. 2021.
[136] H. Chen, Y. Li, J. L. Rebelatto, B. F. Ucha-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, Apr. 2015.
[137] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4089–4102, Aug. 2019.
[138] Y. Li, R. Zhao, Y. Deng, F. Shu, Z. Nie, and A. H. Aghvami, "Harvest-and-Opportunistically-relay: Analyses on transmission outage and covertness," *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 7779–7795, Dec. 2020.
[139] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 760–773, 2022.
[140] Y. Su, H. Sun, Z. Zhang, Z. Lian, Z. Xie, and Y. Wang, "Covert communication with relay selection," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 421–425, Feb. 2021.
[141] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure beamforming for full-duplex MIMO two-way untrusted relay systems," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3775–3790, 2020.
[142] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737–3749, Jun. 2020.
[143] T. K. Y. Lo, "Maximum ratio transmission," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct. 1999.
[144] Y. Yang, M. Pesavento, S. Chatzinotas, and B. Ottersten, "Successive convex approximation algorithms for sparse signal estimation with nonconvex regularizations," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 6, pp. 1286–1302, Dec. 2018.
[145] R. Ma, X. Yang, G. Pan, X. Guan, Y. Zhang, and W. Yang, "Covert communications with channel inversion power control in the finite blocklength regime," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 835–839, Apr. 2021.
[146] T. Xu, L. Sun, S. Yan, J. Hu, and F. Shu, "Pilot-based channel estimation design in covert wireless communication," 2019, *arXiv:1908.00226*.
[147] Q. Zhang, M. Bakshi, and S. Jaggi, "Covert communication over adversarially jammed channels," *IEEE Trans. Inf. Theory*, vol. 67, no. 9, pp. 6096–6121, Sep. 2021.
[148] Z. Liu, S. Li, Y. Zeng, and J. Ma, "Covert wireless communications in the presence of an active adversary," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.
[149] K.-H. Cho, S.-H. Lee, and V. Y. F. Tan, "Throughput scaling of covert communication over wireless adhoc networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 2164–2168.
[150] T.-X. Zheng, H.-M. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1974–1987, Mar. 2019.
[151] A. Arghavani, A. Ahlén, A. Teixeira, and S. Dey, "A game-theoretic approach to covert communications in the presence of multiple colluding wardens," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–7.
[152] B. Che, C. Gao, R. Ma, X. Zheng, and W. Yang, "Covert wireless communication in multichannel systems," *IEEE Wireless Commun. Lett.*, vol. 11, no. 9, pp. 1790–1794, Sep. 2022.
[153] Y. Lin, L. Jin, K. Huang, X. Sun, and F. Wang, "Multiantenna joint covert communication system with finite blocklength," *IEEE Syst. J.*, vol. 17, no. 1, pp. 1170–1180, Mar. 2023.
[154] C. Wang, Z. Li, H. Zhang, D. W. K. Ng, and N. Al-Dhahir, "Achieving covertness and security in broadcast channels with finite blocklength," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7624–7640, Sep. 2022.
[155] H. Du, J. Kang, D. Niyato, J. Zhang, and D. I. Kim, "Reconfigurable intelligent surface-aided joint radar and covert communications: Fundamentals, optimization, and challenges," *IEEE Veh. Technol. Mag.*, vol. 17, no. 3, pp. 54–64, Sep. 2022.
[156] X. Lu, E. Hossain, T. Shafique, S. Feng, H. Jiang, and D. Niyato, "Intelligent reflecting surface enabled covert communications in wireless networks," *IEEE Netw.*, vol. 34, no. 5, pp. 148–155, Sep./Oct. 2020.
[157] X. Zhou, S. Yan, Q. Wu, F. Shu, and D. W. K. Ng, "Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 532–547, Jan. 2022.
[158] C. Wu, S. Yan, X. Zhou, R. Chen, and J. Sun, "Intelligent reflecting surface (IRS)-aided covert communication with warden's statistical CSI," *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1449–1453, Jul. 2021.
[159] X. Zhou, S. Yan, Q. Wu, F. Shu, and D. W. K. Ng, "Joint transmit power and reflection beamforming design for IRS-aided covert communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.
[160] J. Kong, F. T. Dagefus, J. Choi, and P. Spasojevic, "Intelligent reflecting surface assisted covert communication with transmission probability optimization," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1825–1829, Aug. 2021.
[161] S. Ma et al., "Covert beamforming design for intelligent-reflecting-surface-assisted IoT networks," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5489–5501, Apr. 2022.
[162] L. Lv, Q. Wu, Z. Li, Z. Ding, N. Al-Dhahir, and J. Chen, "Covert communication in intelligent reflecting surface-assisted NOMA systems: Design, analysis, and optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1735–1750, Mar. 2022.
[163] X. Chen, T.-X. Zheng, L. Dong, M. Lin, and J. Yuan, "Enhancing MIMO covert communications via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 11, no. 1, pp. 33–37, Jan. 2022.
[164] C. Wang, Z. Li, J. Shi, and D. W. K. Ng, "Intelligent reflecting surface-assisted multi-antenna covert communications: Joint active and passive beamforming optimization," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3984–4000, Jun. 2021.
[165] J. Si et al., "Covert transmission assisted by intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394–5408, Aug. 2021.
[166] X. Liao, J. Si, J. Shi, Z. Li, and H. Ding, "Generative adversarial network assisted power allocation for cooperative cognitive covert communication system," *IEEE Commun. Lett.*, vol. 24, no. 7, pp. 1463–1467, Jul. 2020.
[167] R. Ding, Y. Xu, F. Gao, and X. Shen, "Trajectory design and access control for air–ground coordinated communications system with

multiagent deep reinforcement learning," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5785–5798, Apr. 2022.
[168] K. Yu, H. Zhou, Z. Tang, X. Shen, and F. Hou, "Deep reinforcement learning-based RAN slicing for UL/DL decoupled cellular V2X," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3523–3535, May 2022.
[169] L. Lei, Y. Tan, K. Zheng, S. Liu, K. Zhang, and X. Shen, "Deep reinforcement learning for autonomous Internet of Things: Model, applications and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1722–1760, 3rd Quart., 2020.
[170] N. C. Luong et al., "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3133–3174, 4th Quart., 2019.
[171] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. New York, NY, USA: Cambridge Univ. Press, 2010.
[172] B. A. Bash et al., "Quantum-secure covert communication on bosonic channels," *Nature Commun.*, vol. 6, no. 1, p. 8626, Oct. 2015.
[173] J. M. Arrazola and V. Scarani, "Covert quantum communication," *Phys. Rev. Lett.*, vol. 117, no. 25, Dec. 2016, Art. no. 250503.
[174] Y. Liu, J. M. Arrazola, W. Z. Liu, and I. William, "Experimental covert communication over metropolitan distances," in *Proc. Int. Conf. Quantum Cryptogr.*, Sep. 2017, pp. 1–3.
[175] J. M. Arrazola and R. Amiri, "Secret-key expansion from covert communication," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 2, Feb. 2018, Art. no. 022325.
[176] M. Tahmasbi and M. R. Bloch, "Framework for covert and secret key expansion over classical-quantum channels," *Phys. Rev. A, Gen. Phys.*, vol. 99, no. 5, May 2019, Art. no. 052329.
[177] M. Tahmasbi and M. R. Bloch, "Toward undetectable quantum key distribution over bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 585–598, Aug. 2020.
[178] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 471–482, Mar. 2020.
[179] R. Di Candia, H. Yiğitler, G. S. Paraoanu, and R. Jäntti, "Two-way covert quantum communication in the microwave regime," *PRX Quantum*, vol. 2, no. 2, May 2021, Art. no. 020316.
[180] S. Hao et al., "Demonstration of entanglement-enhanced covert sensing," *Phys. Rev. Lett.*, vol. 129, no. 1, Jun. 2022, Art. no. 010501.
[181] S. Yan, S. V. Hanly, I. B. Collings, and D. L. Goeckel, "Hiding unmanned aerial vehicles for wireless transmissions by covert communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[182] X. Zhou, S. Yan, F. Shu, R. Chen, and J. Li, "Covert wireless data collection based on unmanned aerial vehicles," in *Proc. IEEE Global Commun. Workshops*, Dec. 2019, pp. 1–6.
[183] X. Zhou, S. Yan, F. Shu, R. Chen, and J. Li, "UAV-enabled covert wireless data collection," *IEEE J.Sel. Areas Commun.*, vol. 39, no. 11, pp. 3348–3362, Nov. 2021.
[184] X. Chen, N. Zhang, J. Tang, M. Liu, N. Zhao, and D. Niyato, "UAV-aided covert communication with a multi-antenna jammer," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11619–11631, Nov. 2021.
[185] D. Wang, Z. Zheng, G. He, P. Qi, Y. Zhao, and Z. Li, "Resource allocation for covert wireless transmission in UAV communication networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 01–06.
[186] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, "Joint optimization of a UAV's trajectory and transmit power for covert communications," *IEEE Trans. Signal Process.*, vol. 67, no. 16, pp. 4276–4290, Aug. 2019.
[187] X. Jiang, Z. Yang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Resource allocation and trajectory optimization for UAV-enabled multi-user covert communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1989–1994, Feb. 2021.
[188] B. Yang, T. Taleb, Y. Fan, and S. Shen, "Mode selection and cooperative jamming for covert communication in D2D underlaid UAV networks," *IEEE Netw.*, vol. 35, no. 2, pp. 104–111, Mar. 2021.
[189] R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang, and A. Nallanathan, "UAV relay assisted cooperative jamming for covert communications over Rician fading," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7936–7941, Jul. 2022.
[190] J. Hu, Y. Wu, R. Chen, F. Shu, and J. Wang, "Optimal detection of UAV's transmission with beam sweeping in covert wireless networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1080–1085, Jan. 2020.
[191] H.-M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 389–401, Jan. 2020.
[192] S. Hu, W. Ni, X. Wang, A. Jamalipour, and D. Ta, "Joint optimization of trajectory, propulsion, and thrust powers for covert UAV-on-UAV video tracking and surveillance," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1959–1972, 2021.
[193] X. Chen, M. Sheng, N. Zhao, W. Xu, and D. Niyato, "UAV-relayed covert communication towards a flying warden," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7659–7672, Nov. 2021.
[194] Y. Jiang, L. Wang, H. Zhao, and H.-H. Chen, "Covert communications in D2D underlaying cellular networks with power domain NOMA," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3717–3728, Sep. 2020.
[195] 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.
[196] Y. Jiang, L. Wang, and H.-H. Chen, "Covert communications with randomly distributed adversaries in wireless energy harvesting enabled D2D underlaying cellular networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5401–5415, 2023.
[197] C. Wan, D. Wu, M. Wang, X. Shi, and X. Guan, "Covert communication with power uncertainty for D2D content sharing," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2019, pp. 1–6.
[198] X. Shi, D. Wu, C. Yue, C. Wan, and X. Guan, "Resource allocation for covert communication in D2D content sharing: A matching game approach," *IEEE Access*, vol. 7, pp. 72835–72849, 2019.
[199] X. Shi, D. Wu, C. Wan, M. Wang, and Y. Zhang, "Trust evaluation and covert communication-based secure content delivery for D2D networks: A hierarchical matching approach," *IEEE Access*, vol. 7, pp. 134838–134853, 2019.
[200] H. Rao, M. Wu, J. Wang, W. Tang, S. Xiao, and S. Li, "D2D covert communications with safety area," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2331–2341, Jun. 2021.
[201] S. Weber, J. G. Andrews, and N. Jindal, "The effect of fading, channel inversion, and threshold scheduling onAd HocNetworks," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4127–4149, Nov. 2007.
[202] B. Yang, Y. Shen, X. Jiang, and T. Taleb, "Generalized cooperative multicast in mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2631–2643, Mar. 2018.
[203] H. Wu, X. Liao, Y. Dang, Y. Shen, and X. Jiang, "Limits of covert communication on two-hop AWGN channels," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2017, pp. 42–47.
[204] A. Sheikholeslami, M. Ghaderi, D. Towsley, B. A. Bash, S. Guha, and D. Goeckel, "Multi-hop routing in covert wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3656–3669, Jun. 2018.
[205] H.-S. Im and S.-H. Lee, "Mobility-assisted covert communication over wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1768–1781, 2021.
[206] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
[207] D. Wang, P. Qi, N. Zhang, J. Si, Z. Li, and N. Al-Dhahir, "Covert wireless communication with spectrum mask in Internet of Things networks," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8402–8415, Dec. 2021.
[208] 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.
[209] D. Wang, Q. Fu, J. Si, N. Zhang, and Z. Li, "Improper Gaussian signaling based covert wireless communication in IoT networks," in *Proc. IEEE Global Commun. Conf.*, May 2021, pp. 1–6.
[210] S. L. Cotton, W. G. Scanlon, and B. K. Madahar, "Millimeter-wave soldier-to-soldier communications for covert battlefield operations," *IEEE Commun. Mag.*, vol. 47, no. 10, pp. 72–81, Oct. 2009.
[211] M. V. Jamali and H. Mahdavifar, "Covert millimeter-wave communication: Design strategies and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 3691–3704, Jun. 2022.
[212] C. Wang, Z. Li, and D. W. K. Ng, "Covert rate optimization of millimeter wave full-duplex communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 2844–2861, May 2022.
[213] W. Ci, C. Qi, G. Y. Li, and S. Mao, "Hybrid beamforming design for covert multicast mmWave massive MIMO communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.
[214] J. Zhang et al., "Joint beam training and data transmission design for covert millimeter-wave communication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2232–2245, 2021.
[215] J. Zhang, M. Li, M.-J. Zhao, X. Ji, and W. Xu, "Multi-user beam training and transmission design for covert millimeter-wave communication," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1528–1543, 2022.
[216] R. Ma, W. Yang, J. Hu, and X. Lu, "Covert mmWave communication when the warden locates in the beam direction," *IEEE Wireless Commun. Lett.*, vol. 11, no. 12, pp. 2595–2599, Dec. 2022.
[217] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, and Y. C. Eldar, "6G wireless communications: From far-field beam steering to near-field beam focusing," *IEEE Commun. Mag.*, vol. 61, no. 4, pp. 72–77, Apr. 2023.
[218] Y. Liu, J. Xu, Z. Wang, X. Mu, and L. Hanzo, "Near-field communications: What will be different?" 2023, *arXiv:2303.04003*.
[219] H. Zhang et al., "Beam focusing for near-field multiuser MIMO communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7476–7490, Sep. 2022.
[220] M. Cui, Z. Wu, Y. Lu, X. Wei, and L. Dai, "Near-field MIMO communications for 6G: Fundamentals, challenges, potentials, and future directions," *IEEE Commun. Mag.*, vol. 61, no. 1, pp. 40–46, Jan. 2023.
[221] Z. Zhang, Y. Liu, Z. Wang, X. Mu, and J. Chen, "Physical layer security in near-field communications," 2023, *arXiv:2302.04189*.

ABOUT THE AUTHORS

Yu'e Jiang (Member, IEEE) received the M.Sc. degree in communication and information systems from Nanjing University of Science and Technology, Nanjing, China, in April 2012, and the Ph.D. degree in computer application technology from Jiangsu University, Zhenjiang, China, in September 2021.

She is currently an Associate Professor with the School of Computer Science and Information Engineering, Anqing Normal University, Anqing, China. Her research interests include physical layer covert communications, device-to-device (D2D) communications, and physical layer security.

Liangmin Wang (Member, IEEE) received the B.Sc. degree in computational mathematics from Jilin University, Changchun, China, in 1999, and the Ph.D. degree from Xidian University, Xi'an, China, in 2007.

He is currently a Distinguished Professor with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. He has published over 90 technical papers in premium international journals and conferences, including IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (TIFS), IEEE/ACM TRANSACTIONS ON NETWORKING (TON), IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS (TPDS), IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING (TKDE), and IEEE International Conference on Computer Communications (INFOCOM). His research interests include data security and privacy.

Dr. Wang has served as a TPC Member of many IEEE conferences, such as IEEE International Conference on Communications (ICC), IEEE International Conference on High Performance Computing and Communications (HPCC), and IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). He is a member of the Association for Computing Machinery (ACM) and a Senior Member of China Computer Federation (CCF). He has been honored as a "Wan-Jiang Scholar" of Anhui Province since November 2013. He is also an Associate Editor of *Security and Communication Networks* journal.

Hsiao-Hwa Chen (Fellow, IEEE) received the B.Sc. and M.Sc. degrees from Zhejiang University, Hangzhou, China, in 1982 and 1985, respectively, and the Ph.D. degree from the University of Oulu, Oulu, Finland, in 1991.

He is currently a Distinguished Professor with the Department of Engineering Science, National Cheng Kung University, Taiwan, Taiwan. He has authored or coauthored over 500 technical papers in major international journals and conferences, six books, and more than ten book chapters in the areas of communications.

Dr. Chen was an elected Member-at-Large of IEEE Communications Society (ComSoc) from 2015 to 2016. He is a Fellow of the Institution of Engineering and Technology (IET). He was a recipient of the 2021 Best Paper Award in IEEE SYSTEMS JOURNAL and the IEEE 2016 Jack Neubauer Memorial Award. He has served as the TPC Chair of IEEE Global Communications Conference (Globecom) 2019. He has served as the Editor-in-Chief of IEEE WIRELESS COMMUNICATIONS from 2012 to 2015. He is the Founding Editor-in-Chief of *Security and Communication Networks* journal (Wiley).

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990.

He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on network resource management, wireless network security, the Internet of Things, 5G and beyond, and vehicular networks.

Dr. Shen is a registered Professional Engineer of Ontario, Canada; an Engineering Institute of Canada Fellow; a Canadian Academy of Engineering Fellow; a Royal Society of Canada Fellow; a Chinese Academy of Engineering Foreign Member; and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He received the West Lake Friendship Award from Zhejiang Province in 2023; the President's Excellence in Research from the University of Waterloo in 2022; the Canadian Award for Telecommunications Research from the Canadian Society of Information Theory (CSIT) in 2021; the R.A. Fessenden Award from the IEEE Canada in 2019; the Award of Merit from the Federation of Chinese Canadian Professionals (Ontario) in 2019; the James Evans Avant Garde Award from the IEEE Vehicular Technology Society in 2018; the Joseph LoCicero Award and the Education Award from the IEEE Communications Society (ComSoc) in 2015 and 2017, respectively; and the Technical Recognition Awards from the Wireless Communications Technical Committee in 2019 and the AHSN Technical Committee in 2013. He received the Excellent Graduate Supervision Award from the University of Waterloo in 2006 and the Premier's Research Excellence Award (PREA) from the Province of Ontario, Canada, in 2003. He serves/has served as the General Chair of the 6G Global Conference 2023 and Association for Computing Machinery (ACM) Mobihoc 2015; the Technical Program Committee Chair/Co-Chair of IEEE Global Communications Conference (Globecom) 2024, 2016, and 2007; the IEEE Infocom 2014; and IEEE Conference on Vehicular Technology (VTC) 2010 Fall, and the Chair of the IEEE ComSoc Technical Committee on Wireless Communications. He was the President of IEEE ComSoc, the Vice-President for Technical and Educational Activities, the Vice-President of Publications, a Member-at-Large on the Board of Governors, the Chair of the Distinguished Lecturer Selection Committee, and a member of the IEEE Fellow Selection Committee of ComSoc. He has served as the Editor-in-Chief of IEEE INTERNET OF THINGS JOURNAL, *IEEE Network*, and *Peer-to-Peer Networking and Applications* (PPNA).