Covert Communications: A Comprehensive Survey

Xinying Chen, Jianping An, *Member, IEEE,* Zehui Xiong, *Senior Member, IEEE,* Chengwen Xing, *Member, IEEE,* Nan Zhao, *Senior Member, IEEE,* F. Richard Yu, *Fellow, IEEE,* and Arumugam Nallanathan, *Fellow, IEEE,*

***Abstract*—Information security has always been a critical issue in wireless networks. Apart from other secure techniques, covert communication emerges as a potential solution to security for wireless networks owing to its high-security level. In covert communication networks, the transmitter hides the transmitted signals into environmental or artificial noise by introducing randomness to avoid detection at the warden. By eliminating the existence of transmitted signals at the warden, information security can be preserved more solidly than other secure transmission techniques, i.e., without noticing the existence. Due to the promising security protection, covert communication has been successfully utilized in tremendous wireless communication scenarios. However, fundamental challenges in its practical implementation still exist, e.g., the effectiveness of randomness utilization, the low signal-to-interference-plus-noise ratio at legitimate users, *etc*. In this survey, we demonstrate a comprehensive review concentrating on the applications, solutions, and future challenges of covert communications. Specifically, the covert principle and research categories are first introduced. Then, the applications in the networks with different topologies and the effective covert techniques in the existing literature are reviewed. We also discuss the potential implementation of covert communications in future networks and the open challenges.**

***Index Terms*—Covert communication, information hiding, low probability of detection, physical layer security, square root law.**

I. Introduction

With the boosting of terminal devices in the fifth generation (5G) and the upcoming sixth generation (6G) wireless communications, the modern society is getting more and more reliant on information transmission [1]–[3]. Besides the convenience of wireless communications, information security related problems are also critical and cannot be ignored [4]–[6]. The research focusing on transmission security has never stopped. It even becomes more critical with the coming of Internet of things (IoT) era [7], [8], where the transmitted data contain more individual information, e.g., the data related to user health. Previously, the information security protection either relied on the steganography [9] or the physical layer security (PLS) [10], [11], i.e., the message encryption in the application layer or the transmission techniques in the physical layer. For the message encryption, a more complicated username and password can be created, or a more complex encryption protocol can be established to secure the user privacy. On the PLS side, it utilizes the inherent properties of wireless channels together with coding or signal processing to provide security protection [12]–[15]. These techniques can efficiently utilize radio resources to realize higher transmission throughput while guaranteeing information security [16]. Many physical-layer resources can be jointly optimized to secure the privacy of user information, which is preferred for the reliable transmission with the low-complexity cost of PLS [17]. Thus, plenty of literature is conducted to improve the secure transmission in PLS to guarantee the security while offering outstanding transmission performance, e.g., sufficient high secrecy rate. These PLS methods can utilize power allocation, beamforming, and polarization to realize the secure transmission [18]. Nevertheless, the steganography and PLS can only hide the information in a chaotic order to prevent the eavesdroppers from decoding the legitimate information in the received signals [19]. However, they cannot stop the malicious eavesdroppers from improving their decoding techniques to acquire the transmitted contents, including the distributed computing to tackle the password or the advanced channel state information (CSI) estimation [20], [21]. Under such conditions, the transmission security cannot be guaranteed once the eavesdroppers improve their decoding ability.

Recently, milestone research conducted by Bash *et al.* has shed light on the secure transmission solutions, which focus on the capacity of covert communications [22]. The covert communication hides the very existence of transmission from the detection of wardens, which can provide a higher level of security to transmitters [23]. By hiding the transmitted signals from being detected by wardens, the transmitters can well guarantee their information security. This is because the wardens will not try to decode the content in the signals if they are not aware of the transmission. The wardens will assume that the "signals" are merely the environmental noise, and will not exploit resources to tackle them. By leveraging the concept of covert communications into wireless transmission, the user information can be hidden into "noise", which includes the environmental or artificial noise, to prevent the privacy leakage. Combined with other techniques, such as non-orthogonal multiple access (NOMA) or Turbo encoding, covert communications can further help to improve the wireless security while guaranteeing the transmission performance [24], [25].

The transmitted signals can be "hidden" successfully from wardens by leveraging several conventional techniques to

X. Chen and N. Zhao are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian, 116024, China (email: cxy@mail.dlut.edu.cn, zhaonan@dlut.edu.cn).

Jianping An and Chengwen Xing are with the School of Information and Electronics, Beijing Institute of Technologies, Beijing 100081, China (e-mail: an@bit.edu.cn, xingchengwen@gmail.com).

Zehui Xiong is with the Information Systems Technology and Design Pillar, Singapore University of Technology and Design, Singapore 487372 (e-mail: zehui_xiong@sutd.edu.sg).

F. Richard Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: richard.yu@carleton.ca).

A.Nallanathan is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: a.nallanathan@qmul.ac.uk).

(*Corresponding Author: Nan Zhao*)

realize the covert transmission [26]. First, the channel path loss and the environmental noise are utilized in [27]–[29] to introduce confusion and mislead the wardens, who may feel confused about deciding whether the transmitter carries out a transmission. The small-scale fading results in the randomness in channel coefficients, which will lead to the random variation of the received signals at the wardens [30]. Zheng *et al.* demonstrated in [31] that by taking the advantage of multi-path small-scale channel fading, we can realize that 1) introduce the randomness to the detection of wardens, and 2) precode the multi-antenna transmitting matrix to realize the maximum ratio transmission (MRT) [32]. In [33], Ta *et al.* analyzed the influence of the channel and noise uncertainty on the detection of Willie, where the covert throughput was derived while considering the channel and fading uncertainty. In addition, the power variation at the transmitter, jammer, or relay is utilized in [34]–[36] to guarantee that the received signal power varies randomly, which will result in the uncertainty at the warden on the decision whether the transmitter is sending the information or not. By controlling the power of transmitted signals, the securely transmitted signals can be buried into the environmental noise or the artificial noise, which is usually vibrating constantly to avoid being detected [37]. The introduction of interference or noise can emphasize the total amount of uncertainty, which includes the environmental interference from other users and the artificial noise, and thus the system can tolerate stronger transmitted signals [38]–[40]. Meanwhile, Gaussian-related signaling can be also leveraged to confuse the detection at the warden [41]–[43]. Different from utilizing the channel fading and the transmit power variation, the changing of the transmitter's location can be also utilized to further enhance the stealth of covert communications. Zhou *et al.* alleviated the location variation in [44] to deceive the transmission from the transmitter. Although the location randomness can be utilized to alter the received signal power and confuse the warden about the existence of the transmission, it has a stricter limitation, i.e., the location variation between two time slots is constrained by the maximum allowed velocity. Moreover, the random selection mode such as digital modulation can be leveraged via modulating the transmitted signals to realize the covert communication [45]–[48]. Various uncertainty techniques for covert communications are summarized in Table I.

Thus, covert communications can fulfill the common observations that it can be deployed to tackle the security problem fundamentally. By hiding the transmission into the environmental or artificial noise, the covert communications can improve the secrecy of communications to a much deeper level [63], [111], [112]. The typical benefits of covert communications can be summarized as follows.

- *Simple deployment and low computational complexity:* The typical covert communication utilizes the uncertainty introduced from fundamental wireless transmission factors, e.g., transmit power [95], channel fading coefficients [69], location variation, *etc*. These factors can be designed by essential wireless equipment, which are easy to configure and deploy. Without highly depending on mathematical solutions, such as the big data prediction or the machine learning based solutions, covert communications can be realized with only the basic equipment.
- *Active security protection:* Covert communications can hide the transmitted signals proactively. By actively designing the transmission strategies, e.g., the format of transmit power or the distribution of artificial noise, the sensitive signals can be hidden into the noise to avoid being detected by wardens rather than preventing cracking after being received by eavesdroppers. Each transmission metric, such as transmit power, wireless channels, and distribution of friendly jammers [96], can be carefully designed to improve the performance of covert communications.
- *Comprehensive security protection:* By utilizing covert communications, secure information can be covertly transmitted without being detected by malicious wardens. The transmitted signals are buried into the environmental noise, which varies constantly and randomly, and can confuse the wardens during the detection. To hide the stealthy signals into noise without being noticed, the transmit power tends to be low, limiting the transmission range. For long-range covert communications, relays can be deployed to enlarge the coverage [113]. Therefore, covert communications can prevent malicious wardens from detecting the secure transmission, and comprehensive protection can be provided.
- *Extension from existing techniques:* The deployment of covert communications is expected to provide full protection for information transmission by preventing its existence from being detected. No existence indicates no observation, and then no crack. In addition, combined with other existing secure transmission techniques, such as PLS or encryption, the user security can be comprehensively guaranteed. Accordingly, the information leakage can be greatly reduced.

Although the covert communication serves as a secure transmission technique similar to PLS and encryption, it is essentially different from these two techniques [114]. By embedding the transmitted signals into noise, covert communications can achieve a higher probability of stealth without being cracked by technological progress at detectors [115]. Compared with the PLS that aims at achieving a lower eavesdropping rate, the covert communication does not even allow the user security under the risk of being "noticed", which can dramatically increase the security level [116]. Covert communications also differ from the encryption, which alters the appearance of private information into another version of context [117], [118]. The cryptographic contexts are mainly presented in the random order of information, which makes no sense if the eavesdropper does not know the secret key. Thus, the secure information protection can be achieved by encryption. Without worrying about the secret keys obtained by eavesdroppers, covert communications can provide better stealth for confidential information. Furthermore, these aforementioned three fundamental secure transmission techniques can be combined to obtain a higher level of covertness. We

TABLE I
SUMMARY OF THE UNCERTAINTY INTRODUCED IN THE RESEARCH ON COVERT COMMUNICATIONS

	Uncertainty Techniques		References
Uncertainty Solution	Rayleigh Fading		[27], [28], [31], [35], [38], [49]–[86]
	Transmit Power	Alice	[34], [40], [47], [58], [73], [87]–[93]
		Jammer	[35], [37], [39], [40], [94]–[98]
		Relay	[36], [61], [82], [90], [92]
	Gaussian Signaling		[35], [39], [41]–[43], [57], [63], [71], [76], [79], [94], [96], [98]–[104]
	Location Variation		[31], [44], [65], [89], [105]–[107]
	Random Mode Selection		[45]–[48], [53], [55], [62], [64], [94], [108]–[110]

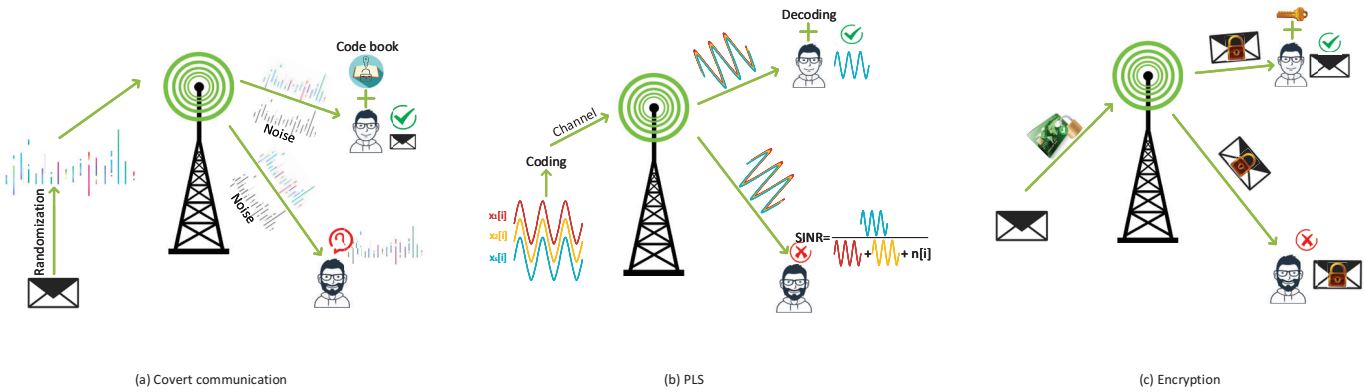

Fig. 1. Comparision of covert communication with PLS and encription.

present the main features of these three secure transmission techniques in Fig. 1. Such differences among covert communications and the other two techniques provoke the necessity and importance of providing a comprehensive research review of covert communication networks. The transmitter in Fig. 1(a) utilizes the randomization techniques of covert communication to introduce uncertainty to confuse the detection at the warden. In Fig. 1(b), the transmitter exploits the physical characteristics of channels or with the help of artificial noise to realize the communication security via minimizing the signal-to-interference-plus-noise ratio (SINR) at the eavesdroppers. With the encryption leveraged in Fig. 1(c), the legitimate user can decode the secure information via its secret key, while the eavesdropper cannot crack the encrypted messages. Therefore, this survey aims at illustrating the elementary concepts of physical principles, the technical solutions, the typical applications, and the performance analysis of covert communication related networks.

Although a few surveys aim to illustrate the covert channels [119]–[122], the covert communications is not well surveyed in the existing literature. A covert channel in computer network protocols is used to transfer information between two parties in a hidden or covert way. Such channels can be created by exploiting the vulnerabilities in the network protocol or by manipulating the transmission system in a way that was not originally intended. Covert communication, on the other hand, refers to a communication system that intends to hide its transmitted signal into the environmental noise or artificial uncertainties to avoid the transmission behavior being detected by the warden, and thus achieving the private transmission without being noticed. Therefore, our survey provides a detailed introduction and tutorial on the fundamental knowledge of covert communications. In addition, we also demonstrate a comprehensive review of extensive schemes and applications in covert networks. The rest of this paper is organized as follows. In Section II, we present the fundamental covert communication model and narrate the differences compared to the conventional security solutions. Three typical research categories of covert communications are listed in Section III to demonstrate the fundamental methods for covert communications and elaborate the differences in each category. Section IV demonstrates possible application scenarios of covert communications in different networks. In Section V, the effective covert communication techniques are reviewed and discussed comprehensively, which include the most recent techniques to introduce uncertainties and guarantee the covertness. In Section VI, we discuss the potential emerging and future applications and scenarios of covert communications. Finally, the future issues and open challenges are pointed out in VII. The major topics of this paper are illustrated in Fig. 2, and a list of all the abbreviations in this survey is presented in Table II.

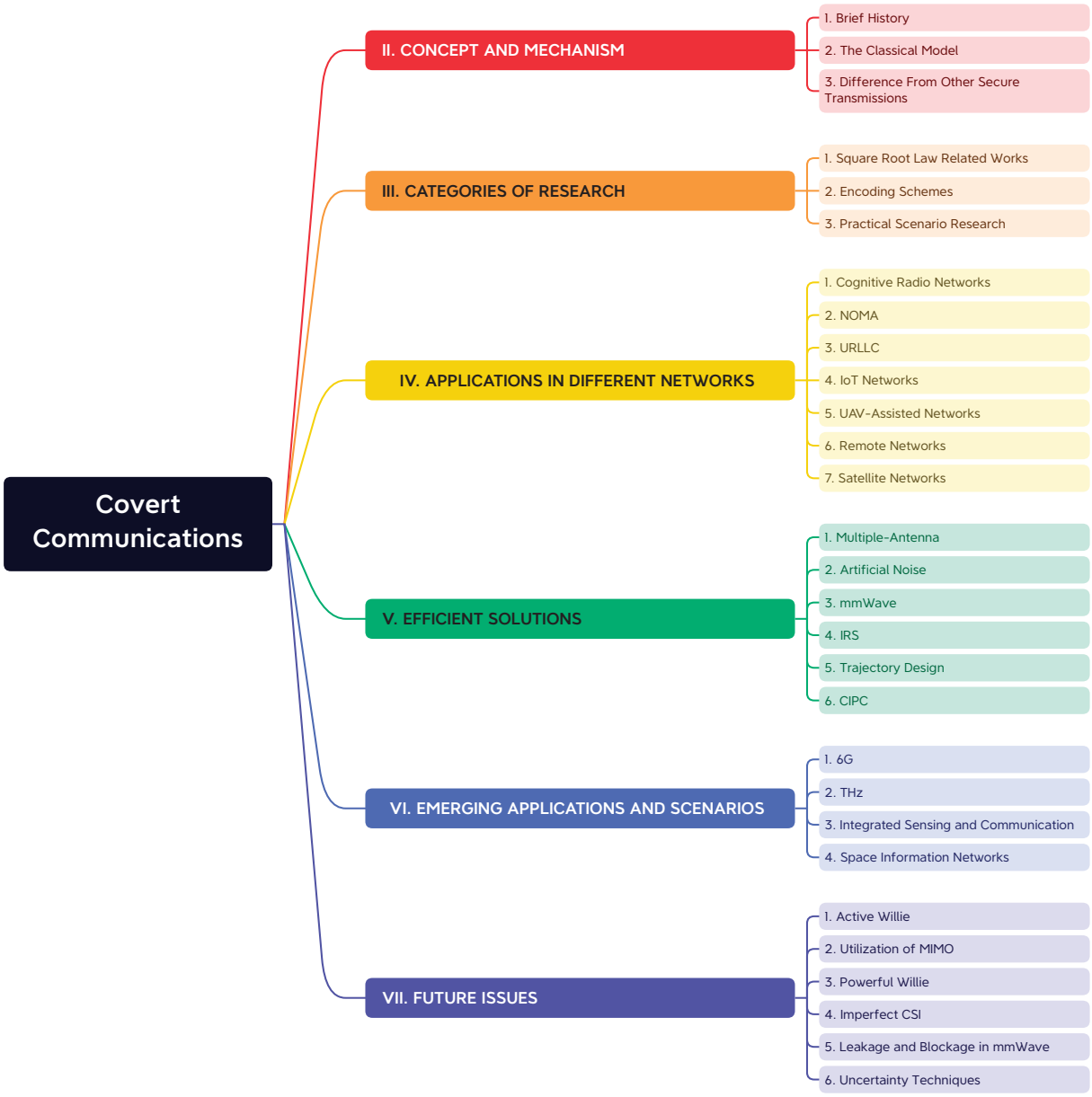

Fig. 2. Outline and roadmap of this survey for covert communications.

II. Concept and Mechanism of Covert Communications

In this section, the developing history of covert communications is first introduced. Then, we demonstrate and discuss the basic metrics and primary considerations of the three-user covert communication model to illustrate the sketchy concept briefly. Furthermore, different strategies to guarantee the security are discussed and compared.

A. Brief History of Covert Communications

Various techniques and schemes have been developed to improve the security protection in covert communications, which can be also referred to as information hiding. In different research areas, the security topology has different elements. The well-known basic covert communication model is the prisoner problem, which is first mentioned by Simmons in 1983 [123]. As illustrated in Fig. 3, the typical covert communication prisoner problem can be described as that Alice is prisoned and would like to communicate with Bob to discuss her escape. However, there exists a warden Willie, who keeps monitoring the environmental signal to prevent Alice from planning to escape. The escaping plan of Alice will be terminated once the warden has any reasonable suspicion about her transmission. The warden doesn't care about the content of the transmission, and any correct detection will cause an extreme trouble for Alice. Thus, Alice should secretly communicate with Bob, expecting Willie not to notice. The

TABLE II
LIST OF ABBREVIATIONS

Abbreviation	Full form
3D	Three-Dimensional
5G/6G	Fifth Generation/Sixth Generation
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BS	Base Station
CAS/DAS	Centralized/Distributed Antenna System
CDI	Channel Distribution Information
CDMA	Code Division Multiple Access
CIPC	Channel Inverse Power Control
CR	Cognitive Radio
CSI	Channel State Information
D2D	Device-to-Device
FA	False alarm
FD/HD	Full-duplex/Half-Duplex
GAN-PA	Generative Adversarial Network Based Power Allocation
IoT	Internet of Things
IRS	Intelligent Reflecting Surface
LoS	Line-of-Sight
LPD	Low Probability Detection
MD	Miss Detection
MIMO	Multiple Input Multiple Output
MISO	Multiple-Input Single-Output
mmWave	Millimeter Wave
MRT	Maximum Ratio Transmission
NLoS	Non-Line-of-Sight
NOMA	Non-orthogonal Multiple Access
PLS	Physical Layer Security
RF	Radio Frequency
SC	Superposition Coding
SIC	Successive Interference Cancellation
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SRL	Squre Root Law
THz	Terahertz
UAV	Unmanned Aerial Vehicle
URLLC	Ultra-Reliable Low-Latency Communication

competition between Alice and Willie can be described from both of their aspects. For Alice, she would like to hide her transmission from being detected by Willie. For Willie, he aims at sensing whether Alice has sent any information or not, which is a binary detection problem.

Before the covert communication, also known as low probability of detection (LPD), emerged in the first international workshop of "Information Hiding" at Cambridge of UK in 1996 [124], the spread spectrum was widely utilized to hide the information into noise to prevent the secure message from being found in the early of 20-th century. The spread spectrum technique expands the transmitted signal from its required bandwidth B_r to a much wider bandwidth B_w, where $B_r \ll B_w$, to spread the power spectral density of the transmitted signal lower than the environmental noise to achieve information hiding. Even though the spread spectrum has developed rapidly and provided covertness during World War II, its fundamental performance limitations have not been

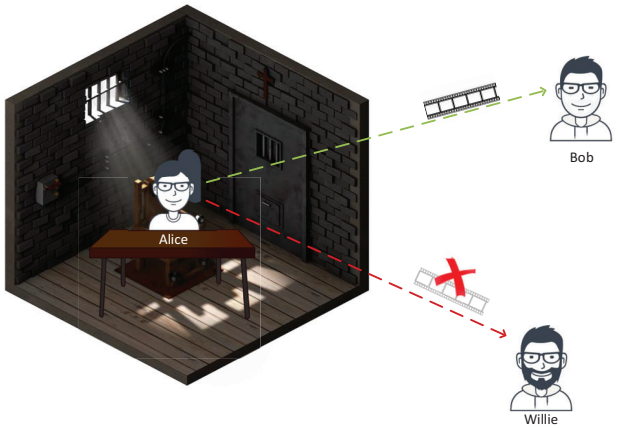

Fig. 3. Typical model of covert communications.

analyzed. Without the performance limitation evaluation, we cannot quantify the performance of covertness provided by the spectrum spreading, e.g., the detection probability for a system and the maximum covert transmitted data within a specific risk probability are not clear. Accordingly, the emergence of covert communication shed light on the information hiding research, especially the square root law (SRL) presented by Bash *et al.* [22].

B. Classical Alice-Bob-Willie Model

The typical model of covert communication can be classified into two stages, which are the transmission at Alice and the detection at Willie, as shown in Fig. 3. On one hand, Alice transmits her stealthy message $x[i]$ with the probability of π_1 to avoid the detection of Willie and tries to improve her transmission performance. With the other π_0 probability, Alice keeps quiet. Practically, researchers assume that $\pi_1 = \pi_0 = 0.5$ to reduce the detection probability at Willie [31], [64]. On the other hand, Willie tries his best to correctly detect whether Alice is transmitting or not.

Assume that the environmental noise can be described as $n[i]$. According to the possible conditions that Alice may transmit or not, the observations of Willie can be described in two hypotheses as

$$\begin{aligned} \mathcal{H}_0 &: y_w[i] = n[i], \\ \mathcal{H}_1 &: y_w[i] = x[i] + n[i], \end{aligned} \tag{1}$$

where $\mathcal{H}_0$ indicates that Alice is keeping silent, while $\mathcal{H}_1$ represents that Alice is transmitting. In typical covert communications, Willie makes decisions whether Alice is transmitting $\mathcal{D}_1$ or keeping silence $\mathcal{D}_0$ based on his averaged receiving signal power $\bar{P}_w$, which can be expressed as

$$\bar{P}_w = \frac{1}{n}\sum_{i=1}^{n} |y_w[i]|^2 \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma, \tag{2}$$

where n is the channel uses of Alice to transmit her secret message and Γ denotes the preset power threshold at Willie. The summation term in (2) represents that Willie makes his decision based on the averaged received signal power of his n observations. Willie considers that Alice is transmitting $\mathcal{D}_1$

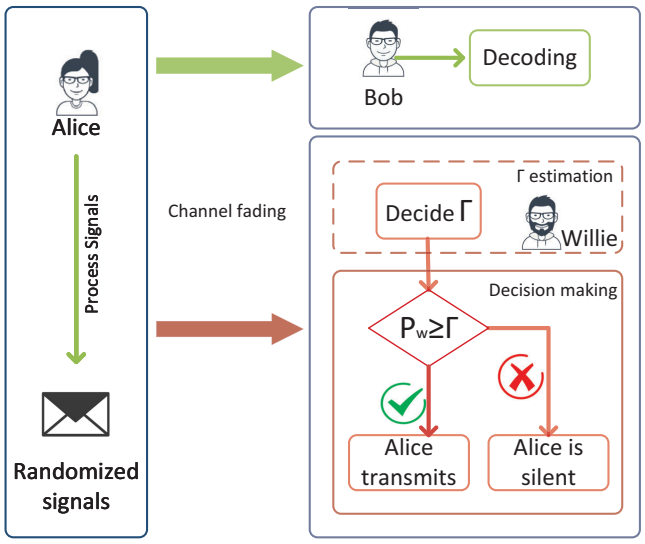

Fig. 4. The process of covert communication.

when $\bar{P}_w \geq \Gamma$ and believes that Alice is keeping silence $\mathcal{D}_0$ when $\bar{P}_w \leq \Gamma$. Therefore, the preset power threshold is critical, and severely impacts Willie's detection accuracy. The detailed structure of covert communication is shown in Fig. 4.

There are two possible mistakes that Willie may make, which are namely the false alarm (FA) and miss detection (MD). The probability of Willie to make an FA mistake $\alpha = Pr\{\mathcal{D}_1|\mathcal{H}_0\}$ can be described as Willie thinks that Alice is transmitting while Alice is keeping quiet. The probability of Willie to make an MD mistake $\beta = Pr\{\mathcal{D}_0|\mathcal{H}_1\}$ indicates that Willie believes that Alice is quiet while she is transmitting her secret message. The purpose of Willie is to minimize the total error probability $\alpha + \beta$ by properly setting the power detection threshold Γ.

Referred to [22], the error detection probability for the optimal test at Willie can be described as

$$\begin{aligned} \alpha + \beta &= 1 - \mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \\ &\geq 1 - \sqrt{\frac{1}{2}\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)}, \end{aligned} \tag{3}$$

where $\mathbb{P}_0$ is defined as the probability distribution of Willie's observations when Alice is transmitting, and $\mathbb{P}_1$ represents the probability distribution of Willie's observations when Alice keeps silent. $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$ is the total variation distance of $\mathbb{P}_0$ and $\mathbb{P}_1$. By applying the Pinsker's inequality, i.e., $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \leq \sqrt{\frac{1}{2}\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)}$, (3) can be derived. $\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)$ is the relative entropy between $\mathbb{P}_0$ and $\mathbb{P}_1$.

The optimal detection can be obtained when the detection threshold Γ is set to its optimal value, where the optimal power detection threshold Γ^* can be derived when

$$\frac{\mathbb{P}_1}{\mathbb{P}_0} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} 1. \tag{4}$$

Then, the optimal power detection threshold Γ^* can be derived from the combination of (2), (3) and (4) [22].

Owing to the unawareness between Alice and Willie, covert communication can be conducted. The unawareness is mutual between Willie and Alice, i.e., Willie does not know when Alice will transmit or the real-time CSI, and neither does Alice know the detection threshold set by Willie or his CSI. However, Alice needs to guarantee that the total detection error probability at Willie exceeds $1 - \epsilon$, i.e., $\alpha + \beta \geq 1 - \epsilon$. Therefore, the typical assumption of covert communications at Alice is that Willie sets his detection threshold with the optimal value Γ^*, which can guarantee an even higher covertness when Willie does not set his detection threshold to Γ^*.

Based on the optimal detection at Willie, Alice can jointly optimize her parameters, e.g., transmit power, transmission rate, or precoding vector, to achieve better performance.

C. Differences from Other Security Techniques

We mainly compare the differences of covert communications with the PLS, cryptography and spread spectrum as follows, which has been concluded in Table III.

TABLE III
DIFFERENCES BETWEEN THE SECURITY TECHNIQUES

	PLS	**Encryption**	**Covert Communication**
Purpose	Reduce SINR at eavesdroppers	Hide the transmitted signal	Prevent crack
Strategies	Jamming; Channel fading; Channel coding;	Convert to an unreadable format without the key	Uncertainty introduction
Layer	Physical layer	Application layer	Physical layer

1) Physical Layer Security: In general, the PLS can be achieved by jointly utilizing the characteristics of wireless channels, e.g., the fading, via signaling or channel coding in the physical layer rather than the upper layer. Different from covert communications, the PLS mainly prevents eavesdroppers from decoding the secure data rather than obtaining them. One of the advantages of PLS is that it does not need the super computational ability for legitimate users. The primary purpose of PLS is to reduce the SINR at the eavesdroppers while guaranteeing the transmission performance at the legitimate receivers. However, in a PLS system, the design of precoding vectors or beamforming matrices usually assumes that the CSI of eavesdroppers is available at the transmitter. This is impractical even though plenty of research has focused on the CSI estimation. In addition, the improvement of decoding ability at eavesdroppers can also threaten the PLS.

2) Cryptography: For cryptography, the transmitted data are converted to an unreadable or meaningless format, and can only be decrypted by a specific key, which includes public/private key decryption or harsh-function decryption. The public/private key system can verify the identity of users,

while the hash functions can transfer the message to a group of other unbreakable formats of data. The primary purpose of cryptography is to protect the content of transmitted message, and the eavesdroppers cannot interpret the content of encrypted message. However, significant threats will be posted on the cryptographic technique when the quantum computing or other supercomputing techniques are further developed and applied by eavesdroppers. Therefore, the encrypted message is still at the risk of being found.

3) Spread Spectrum Communication: This is another technique similar to covert communications, which can protect the transmission behavior rather than hiding the content of transmitted signal. It consumes more frequency resource to realize the information hiding. Specifically, the spread spectrum communication utilizes a much wider bandwidth B_w than the required one B_r, i.e., $B_w \gg B_r$, to spread the secret message into the environmental noise. Literatures have proved that the spread spectrum can provide security for wireless communications [125]–[127]. However, there are no detailed analytical results about it, e.g., the amount of secure information, the probability of detection, and the error detection probability. Even though the spread spectrum has been well applied in military during the earlier 20-th century, the lack of a solid theoretical performance limit still results in the loss of security.

III. Categories of Covert Communication Research

The core concept of covert communications is to hide the transmitted information from being detected by the warden [128]. Since the milestone result proposed by Bash *et al.* illustrated the performance limits in [22], the covert communication related research has bloomed. Then, the followed covert communication related research mainly focus on three categories, which are the theoretical performance limits, encoding schemes, and practical scenarios. The theoretical research on performance limits mainly aims at deriving the information amount that can be covertly transmitted to the receiver with a specific low detection probability at the information theory level. The second branch focuses on achieving the information limits with their proposed encoding schemes and derives the required secret-key length. For the third category, the researchers aim at applying covert communications to practical scenarios with the assistance of other techniques to improve the performance of covert communications. In this section, we discuss these three research aspects in detail and provide a review of literature to demonstrate each category.

A. Square Root Law Related Works

The breakthrough conducted by Bash *et al.* demonstrated the SRL for a covert communication network with additive white Gaussian noise (AWGN) [22], which illuminates the performance limits of covert communications. In this scenario, a typical covert communication model is considered, including a transmitter Alice, a receiver Bob, and a warden Willie. Specifically, Bash *et al.* investigated the square root limits in an AWGN channel model with the power variance $\sigma_b^2 > 0$ at the receiver Bob and $\sigma_w^2 > 0$ at Willie under two conditions when the noise power is known and unknown, respectively. They assumed that the available channels used by Alice to communicate with Bob are n and the shared secret is sufficient. Considering that the total observed power at Willie is $\sigma_w^2 n$ when Alice is keeping silent, the total received power over n channel uses will increase and cause suspiciousness when Alice performs her transmission. Bash *et al.* has theoretically proved that Alice can reliably transmit $o(\sqrt{n})$ bits when the decoding error probability is extremely low, where $o(f(n))$ represents the upper bound. ϵ represents any arbitrary small error detection probability at Willie to guarantee that $\alpha+\beta \geq 1-\epsilon$ when σ_w^2 is unknown at Alice. They further proved if Alice knows the lower bound of σ_w^2, the information amount that she can transmit is $\mathcal{O}(\sqrt{n})$ within n channel uses and with an arbitrary small ϵ satisfying $\alpha+\beta \geq 1-\epsilon$, where $\mathcal{O}(f(n))$ represents the asymptotic upper bound. In addition, an insightful conclusion was drawn, which indicates that when $n \to \infty$, the transmitted signal per channel equals to 0, i.e., $\lim_{n\to\infty} \frac{\mathcal{O}(\sqrt{n})}{n} \to 0$.

After the initial work mentioned above, plenty of research related to covert limits is further conducted [97], [129]–[135]. For example, Bash *et al.* in [134] further investigated the SRL in a more practical assumption that the warden does not know the exact transmission time slot. It has been proved that the transmission of Alice will occur a high probability of being detected by the warden if she transmits more than $\mathcal{O}(\min\{n\log T(n)^{\frac{1}{2}}, n\})$ bits within $T(n)$ time slots in n channel uses. Based on the same system model in [134], Goeckel *et al.* in [135] derived the information limits that can be transmitted covertly when the warden has no pre-knowledge of the environmental noise. They proved that under the synchronous condition Alice cannot reliably transmit more than $\omega(\sqrt{n\log T(n)})$ bits within one of the $T(n)$ time slots, where $\omega f(n)$ represents the asymptotic lower bound. On the condition that Willie is not aware of the asynchronous information when is the codeword boundaries of Alice's transmission, they also proved that Alice still cannot transmit more than $\omega(\sqrt{n\log T(n)})$ bits of information with n channel uses and a constant transmit power. The results mentioned above also limit the condition when Alice selects several of the $T(n)$ slots to transmit. Different from the assumption that the warden has the complete channel statistical knowledge in [22], Sobers *et al.* in [97] proved that the transmitter can transmit $\mathcal{O}(n)$ bits covertly and accurately in n channel uses to the receiver with the help of a friendly jammer without being detected by Willie under both the optimal and non-optimal conditions. The results in [97] were derived with all the constraints on the detector of Willie removed, including the statistical model of channels, the length of the codeword n, the distribution of Alice's codeword, the jamming distribution, the possible transmission time of Alice, and the distance from Alice.

All of the research mentioned above is based on the AWGN channel assumption. For other channels, Bullock *et al.* in [136] explored the fundamental limits of covert communication over Bosonic channels and classical-quantum channels [137]. They derived the SRL of the single-mode bosonic lossy thermal

channel model, which applies to the covert communication in the quantum scenarios of optical environment, radio-frequency (RF) channels, and microwave. The detailed expression of SRL in bosonic channels was demonstrated with the assumption of Willie being quantum-limited. Then, Sheikholes *et al.* in [137] proved that the SRL can be achieved in a memoryless classical-quantum channels.

B. Encoding Schemes for Covert Communications

After the pioneering SRL research in [22], many works are performed to establish the coding schemes or the shared secret-key length between Alice and Bob [138]–[142]. They mainly aim at realizing the SRL in practical scenarios by designing suitable encoding schemes [143]–[148]. In [138], Wang *et al.* agreed that the SRL can hold among lots of discrete memoryless channels. They derived the expression of scaling constant for the maximum transmitted information under the assumptions which include: 1) Willie has the same observations of channel information; 2) the shared key between Alice and Bob is adequately long. In addition, Alice sends the "off" symbol once she turns off. Following the same assumption of the alphabet involving an "off" symbol, Cho and Loe in [149] studied the covert communication under discrete memoryless interference channels for K user pairs. They proved that the optimal scheme is the point-to-point related scheme that treats the interference as noise. In addition, they also analyzed the minimum required length of the secret key in each user pair, which turns out to be 0. Prior works have agreed that $\mathcal{O}(\sqrt{n})$ bits of information can be covertly transmitted with n channel uses only on the condition of the exponential computational complexity. Zhang *et al.* in [150] proposed a coding scheme that can guarantee the covert capacity while maintaining the computational complexity polynomially related to the channel uses n. They applied the systematic Reed-Solomon code to eliminate the dependence of the coding content, which can post uncertainty at Willie as well. Yu *et al.* studied the maximum channel coding rate of infinite-blocklength covert communications in [151]. They applied the Gaussian randomization coding scheme to achieve a more convenient analysis of the total variation distance. The maximal and average error probabilities were derived for the random coding scheme with input constraints. In addition, they also compared the derived achievable bounds and the current results. In [152], Xu *et al.*, different from other works, proposed a scheme utilizing a non-zero mean Gaussian sequence, where they modulated the mean with a stealthy binary bit. The covert and transmission performance were both analyzed based on the proposed scheme.

C. Practical Scenarios With Different Types of Willies

The typical applications of covert communication can be characterized into three categories based on the modes of wardens, i.e., single Willie, multiple Willies, and active Willie. Many schemes have been proposed to guarantee the stealth in covert communications against different obstacles posted on Alice under each mode, which is summarized as in Table IV.

TABLE IV
DIFFERENCES BETWEEN SECURITY TECHNIQUES

Types of Willie	Reference	Challenges
Single Willie	[44], [57], [59], [68], [73]	Basic detection
Multiple Willies	[31], [62], [62], [70], [70], [76], [84], [89], [99], [103], [153], [154]	Joint detection
Active Willie	[75], [155]–[158]	Improved detection through Willie's mobility

Single Willie: In most of the typical covert communication models, there exist a transmitter, a legitimate receiver, and a passive malicious warden [59]. When there is only one warden, we can utilize different techniques to confuse Willie from finding out the transmission. In particular, the techniques can leverage the small-scale channel fading or exploit transmit power variation. These solutions can introduce uncertainty to the received signals at the warden. Zhou *et al.* in [44] considered the unmanned aerial vehicle (UAV) trajectory design of covert communication with the location estimation errors, which can bring uncertainty to the covert communication. The small-scale path-loss randomness was leveraged in [68], [159] by Chen *et al.* to confuse the single warden from successfully detecting the transmission of Alice. Then, Chen *et al.* further investigated the single warden covert communication within the finite-blocklength regime in [57], [160], which is practical in IoT-related networks. The transmitted samples of the signal were assumed to follow the complex Gaussian distribution by Shahzad *et al.* in [73], which can deceive Willie about the covert communication.

Multiple Willies: When multiple wardens can combine their observation results and make the conclusion accordingly, the error detection probability will reduce sharply [99], [153], [154]. This poses significant threats to the covert communications. Soltani *et al.* in [89] considered the covert communication under the scenarios of both the single warden and multiple collaborating wardens. With the assistance of friendly nodes to generate jamming to disrupt Willies, Alice can guarantee the covertness of transmission. Then, the strategy to leverage multiple relays in long-distance covert communications against multiple Willies with fixed locations was proposed by Sheikholeslami *et al.* in [103]. The covert communication concerning multiple Willies with unfixed locations was studied in [31] by Zheng *et al.*, where the locations of Willies follow a uniform distribution. They investigated the influence of multi-antenna Alice under both the centralized antenna system (CAS) and distributed antenna system (DAS). Following the abovementioned work, Chen *et al.* further considered the covert communication with multiple wardens in the UAV-aided LPD in [84], [161], where the cooperative wardens are distributed with binomial point process locations. Recently, Ma *et al.* in [76] expanded the multi-warden covert communication

network into the regime of finite blocklength, where the random distribution of wardens follows the Poisson point process. In [70] and [62], long-distance covert communications were discussed. To guarantee the communication performance, long-distance transmission requires higher transmit power, which poses a higher risk of being detected. As mentioned, multiple Willies can cooperate with each other to jointly make the detection results of Alice's transmission. Forouzesh *et al.* in [70] utilized relays to conquer the obstacle of long-distance covert communications, where they also prevented the untrusted relays from decoding the source information. In [62], Rao *et al.* further examined the covert communication against the detection of multiple wardens with the help of a dynamic relay selection scheme.

Active Willie: In most existing research, the malicious Willie is assumed to stay at a fixed location, which underestimates its detection ability. Actually, Willie can alter his detection location accordingly during his observations [75], [155]. During the detection of an active Willie, he can adjust his decision rules or change his detection locations. In [156], Forozesh *et al.* considered the covert communication in a more practical scenario when the estimated location of Willie is imperfect at Alice. In addition, they equipped multiple antennas at a friendly jammer to provide a higher covert transmission rate by beamforming towards the legitimate receiver in a null space to eliminate the interference. They also improved the transmission performance by leveraging a 3-dimensional (3D) beamforming antenna array. Liu *et al.* in [157] found that Alice cannot hide her transmission from an active Willie if she does not know his prior knowledge, where Willie can dynamically change his detection location according to the trend of detection results. In addition, Alice can randomize her scheduling of transmission, where the transmission probability should be lower than a threshold, to realize the covert communication against an active Willie. Tahmasbi and Bloch in [158] proposed a dynamic protocol that allows Alice and Bob to exchange a secret key, which is unavailable to the active warden, to achieve the covert communication.

IV. Applications of Covert Communications

By smartly hiding the stealthy transmitted signal into noise, the confidential signal can be covertly transmitted to the intended receiver while keeping the malicious warden from detecting their existence. The theoretical square root limit in AWGN channels has been well demonstrated and proved in [22], which broke the ice of covert communication research. In this section, we provide a comprehensive review for major applications of covert communications in different kinds of networks, which are listed in Table V. Typical applications of covert communication include cognitive radio (CR), NOMA, ultra-reliable and low-latency communications (URLLC), IoT networks, UAV-assisted networks, remote networks, and satellite networks, the brief structure of which is illustrated in Fig. 5

A. Covert Communications in CR

CR is developing as a key technique to improve the cooperative spectrum efficiency. In CR networks, the radio resource

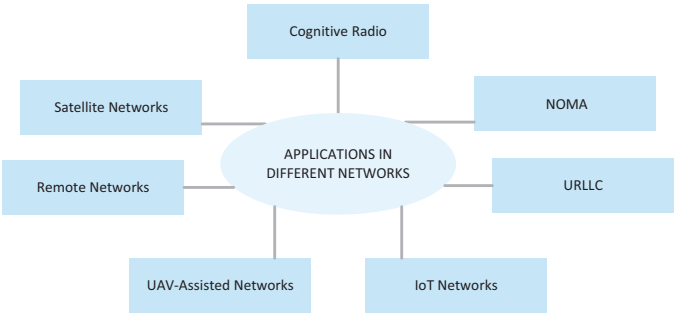

Fig. 5. Applications of covert communications in different kinds of networks.

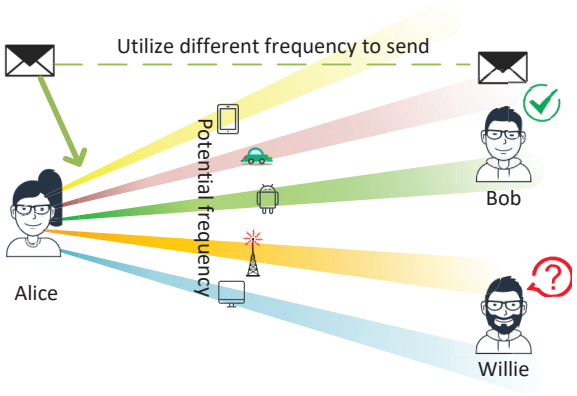

Fig. 6. Covert communication in CR networks.

is dynamically programmed to utilize the optimal or most available spectrum to avoid interference among users, which can be simply concerned with dynamic spectrum management to solve the shortage of spectrum resource in future networks [175]. However, owing to its dynamic characteristics and structures, malicious eavesdroppers may have the possibilities to attack, which is also caused by the access availability of multiple devices. By applying covert communication to CR networks, we can guarantee both the information stealth and spectrum efficiency simultaneously [105]. The basic CR covert network is demonstrated in Fig. 6.

Liao *et al.* in [61] proposed a novel generative adversarial network-based power allocation (GAN-PA) scheme to protect the covert communication in a CR network. In the GAN model, one generator simultaneously transmits real and fake samples to misguide the warden from detecting the actual samples from the fake ones. They considered a secondary transmitter assisted CR covert network, where the greedy relay may use the spectrum resource to transfer its illegal message to the receiver. A warden is deployed to detect whether the relay transfers the legal message received from the transmitter or transmit his own illegal message. They utilized the game theory to analyze and optimize the transmission rate of all channels at the receiver and the detection error probability at the warden. Their proposed GAN-PA scheme can obtain the near-optimal power allocation solution with rapid convergence. Following similar scenarios, Chen *et al.* in [49] investigated

TABLE V
PRACTICAL COVERT COMMUNICATION APPLICATIONS IN DIFFERENT NETWORKS

Network	Advantages	References	Main Contributions
CR	Spectrum efficienty improvement	[49]	Improve covertness under rate-oriented, link-oriented, and fairness-oriented relay schedules.
		[61]	Utilize game theory to prevent the greedy relay from transfering illegal messages.
		[101]	Cognitive jammer provides more efficient jamming.
		[162]	Interwave covert cognitive networks are investigated.
NOMA	Higher security and frequency efficiency	[51]	Provide more secure D2D covert communication with the help of other users.
		[52]	Utilize CIPC to hide covert signals into common users for higher covertness.
		[54]	Utilize energy harvesting to improve the battery life for longer covert communication.
		[163]	Consider the channel estimation errors in covert NOMA networks.
URLLC	Low latency and high reliability of covert communications	[109]	Random channel selection in short-package covert communications.
		[164], [165]	Utilize channel randomness in covert URLLC networks to avoid detection.
		[102]	Randomize the transmit power in short-package covert communications.
IoT Networks	More security for IoT networks	[66], [166]	Utilize power control to provide covert communication in IoT networks.
		[108]	Long-distance covert communication in IoT networks.
		[107], [167]	Investigate IoT covert communication under different channel models.
		[168]	Build a hardware platform for covert IoT networks.
UAV Networks	Stealth in air-to-ground communications	[57], [84], [88], [91]	UAV works as different roles in covert communications.
		[169]	Utilize beam sweeping to detect suspicious UAV transmission.
		[106]	UAV trajectory design in covert communications.
Remote Networks	Covertness for long-range networks	[36], [71], [92], [170]	Single relay is considered in different remote networks.
		[28]	Greedy relay detection is proposed.
		[27], [55]	Selection strategy is investigated in multi-relay covert networks.
		[171]	Multi-hop relays are considered.
Satellite Networks	Covertness for satellite communications	[172]	Apply NOMA to covert satellite communications.
		[173], [174]	Utilize polar code in covert satellite communications.

the covert communication in CR networks, with multiple secondary transmitters considered. Three scheduling schemes were proposed, i.e., rate-oriented, link-oriented, and fairness-oriented secondary user schedulings. Two of the secondary transmitters were selected to forward the covert message to the secondary receiver, while avoiding being detected by the warden, as a relay and a jammer, respectively. Three transmission strategies were derived based on the maximization of the covert transmission rate, the received signal-to-noise ratio (SNR), and the fairness while maintaining the error detection probability at Willie. Different from the aforementioned relay-assisted model, Xiong *et al.* investigated a cognitive jammer in covert communication networks in [101], which can sense the environment to perceive the transmission of Alice, and then decide its jamming strategy. Among the n blocks in which Alice transmits, the jammer observes the first m blocks, and then transmits the jamming signals during the rest $n-m$ blocks based on observing the silence of Alice, or keeping silence otherwise. With the help of a cognitive jammer, they maximized the covert transmission rate while keeping the error detection probability above its constraint. In [162], the interwave cognitive radio was investigated by Xu *et al.*, where the blocklength of spectrum sensing and data transmission were studied and optimized to maximize the effective throughput.

B. Covert Communications in NOMA

NOMA, as a potential technique for future networks, enables more users to utilize the same spectrum resource, which can significantly improve the spectrum efficiency. Taking the power-domain NOMA as an example, the base station (BS) combines and transmits the information of multiple users together in the same frequency band with the superposition coding (SC), and then the users can receive and subtract their own signals via successive interference cancellation (SIC). In NOMA, the transmitter assigns higher transmit power to the weaker users, i.e., the users with poorer channel conditions. Since each user has the access to other high-power users' information, the users with worse channel conditions are at risk of information leakage. Thus, information security is critical for NOMA networks. Different from the PLS, applying covert communication to NOMA networks can realize the most fundamental protection, i.e., hiding the very existence of transmitted signals from detection [34], [90]. The covert NOMA network can be demeonstrated in Fig. 7.

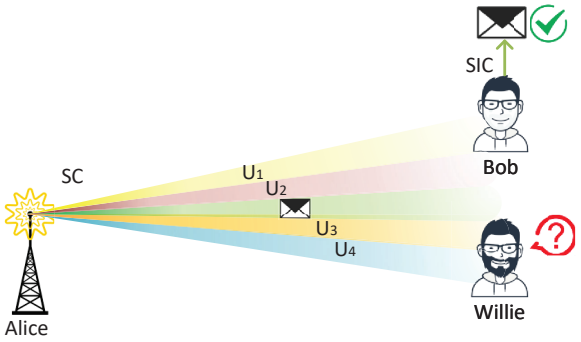

Fig. 7. Utilization of NOMA in covert networks.

Tao *et al.* in [54] considered the covert communication in a downlink NOMA system realized by randomizing the transmit power. In this letter, Alice performs the covert communication in a NOMA network with two legitimate users, where a weak user covers for the stronger user. On the consideration of battery life, they leveraged an energy harvesting jammer to assist the covert communication. There are two phases in the scheme [54], namely the energy harvesting phase and the information transmission phase. The jamming signal and weak public message are transmitted during the whole information transmission phase, while the covert signal is transmitted occasionally. They optimized the transmit power of covert signal to maximize the covert transmission rate while constraining the minimum detection error probability and connection outage probabilities. The covert communication in NOMA networks was also investigated in [52], where Wang *et al.* adopted the channel inversion power control (CIPC) to achieve the covertness. In this system, the public users and Bob cooperate together to deceive the warden from detecting the transmission of Alice. Alice transmits to Bob and a public user according to NOMA with the probability of 0.5 while sending message only to the public user when she keeps silent. Meanwhile, the public user sends the artificial noise with the truncated CIPC to confuse Willie and help Alice with the covert communication. The device-to-device (D2D) covert communication in NOMA systems was studied by Jiang *et al.* in [51]. The D2D communication is vulnerable to malicious attacks owing to the battery limitation, where the security can be improved with the covert transaction. In this paper, they utilized the non-covert D2D user as well as the BS as friendly jammers to assist the covert communication conducted by D2D devices. The D2D transmitter covertly transmits to the D2D receiver with the help of channel fading, which follows complex Gaussian distribution. The average transmission data rate over a D2D link was maximized by optimizing the covert transmit power while the error detection probability was kept under its constraint. In [171], Mallikarachchi *et al.* investigated the multiple relays in a multi-hop UAV network, where the transmission method was presented to achieve the covert communication under some specific constraints. Zhang *et al.* investigated the covert transmission in NOMA networks with channel estimation errors considered in [163].

C. Covert Communications in URLLC

To achieve better transmission performance and reduce the communication latency, URLLC is proposed to achieve the ultra-reliable and low-latency performance for 5G networks, where the short-packet transmission is important to realize the URLLC requirements. To guarantee the reliability and reduce the latency, the information should be transmitted via short packets. However, its security is still a critical problem once regarding to wireless communications, which can be solved by leveraging covert communication into finite-blocklength networks [42]. Different from the conventional infinite-blocklength communications, Shannon theory does not hold in finite-blocklength networks, which is of extreme importance for 5G networks. In the merits of transmission performance and covertness, both the decoding error probability and the information leakage probability need to be considered [56].

In [109], Xu *et al.* investigated the typical Alice-Bob-Willie covert communication model in a finite-blocklength network, where the channel selection is randomized. The relative entropy at Willie and the decoding error probability at Bob were analyzed under the condition of finite blocklength in this letter. Under the constraint of the error detection probability at Willie, the error decoding probability at Bob is minimized via properly adjusting the probability of channel uses. Then, Ma *et al.* investigated the power control scheme in [164] to provide the covert communication in a finite-blocklength regime. This letter studied the covert communication in the short-packet regime with both the conventional and the trunked CIPC schemes. In the CIPC system, the transmit power at Alice was inversely proportional to the channel coefficients between herself and Bob. The truncated scheme indicated that Alice will not transmit any signal unless the coefficients of channel gain exceed the preset value. With these two schemes, the finite-blocklength efficient covert throughput can be maximized under the constraint that the detection error probability at Willie is larger than the threshold via adjusting the power control parameter. In addition, the deployment of UAV Alice was designed in a time-intolerant covert communication network in [165]. In this paper, Zhou *et al.* analyzed the hovering location of UAV Alice to derive the optimal location to result in a higher detection error probability at Willie and provide sufficient effective throughput. With the optimal derived transmitting location of UAV, the transmit power and the hovering altitude are also optimized within the above-mentioned constraints. Yan *et al.* in [102] also discussed the covert communication in a finite-blocklength wireless network with either fixed or randomized transmit power. They discussed the impact of blocklength on both the detection at Willie and the transmission at Alice, and then derived the optimal value. With the monotonicity analysis of the detection threshold and the transmitted information amount with respect to the blocklength, they concluded that the optimal blocklength should achieve its maximum to obtain the maximal transmitted information.

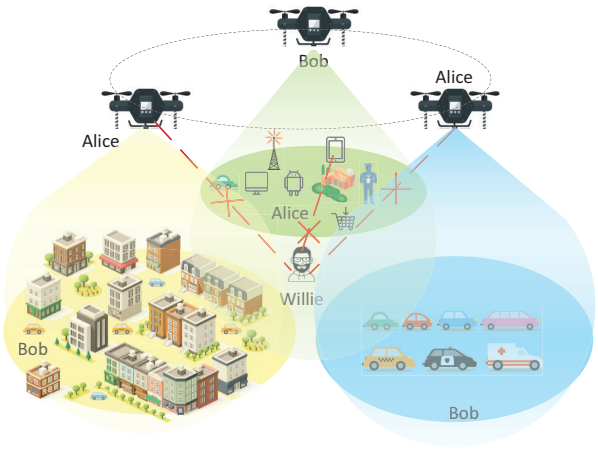

Fig. 8. Application of covert communication in IoT networks.

D. Covert Communications in IoT Networks

IoT emerges as a revolution of the next-generation mobile networks, where ubiquitous devices can be connected within the same network. These everyone-related devices can transmit a rush of private information, including monitoring videos, user trajectory information, personal health data, *etc*. However, wireless communications always undergo the risk of being eavesdropped and privacy leakage. Many techniques have been exploited to handle the information leakage, including PLS and encryption. Moreover, the covert communication can be also leveraged to realize the information security in IoT networks as shown in Fig. 8, owing to its advantage of information hiding. The devices in IoT networks are usually of small size and with low-battery supplements, which leads to the incapability of complex coding [74]. Thus, the application of covert communications in IoT networks should not require high computational abilities [112], [176].

Wang *et al.* in [166] utilized the improper Gaussian signaling in a covert IoT network to improve the covert transmission rate. In this paper, an IoT node wishes to covertly transmit to Bob with the help of a spectrum shelter formed by the BS and its related receiver. They proved that the covert transmission rate can be improved by utilizing the improper Gaussian signaling and interference together compared to only exploiting the proper Gaussian signaling. In [66], Hu *et al.* investigated the IoT covert communication network with the CSI unawareness at Bob. The CIPC scheme was adopted to guarantee the constant signal power at Bob without the requirement of knowing the CSI between himself and Alice. They derived the optimal power control parameter to maximize the covert transmission capacity while maintaining the total error detection probability higher than its requirement. In addition, they also proved that increasing noise uncertainty at both Bob and Willie cannot improve the covert performance. Gao *et al.* in [108] considered the IoT covert communication in a long-distance scenario. Different from the conventional long-range wireless relay-assisted communication considering only one relay, multiple relays were deployed and selected in this IoT network. They compared the covert wireless IoT communication under the random relay selection scheme and the superior-link selection scheme. They proved that the superior-link selection scheme can provide higher covert capacity under the same constraint compared with the random relay selection scheme. Most of the existing covert communication schemes are conducted under the AWGN channel, while Sodagari studied the covert communication in IoT networks under the Nakagami fading in [167]. Liu *et al.* in [107] considered the covert IoT communication under terahertz (THz). They utilized a specular reflection surface to assist the covert communication in IoT networks. Apart from the theoretical research, Shelley *et al.* conducted the covert communication against a hardware trojan in [168], where they performed the experiments at the hardware platform. The results showed that the malicious hardware trojan emission can be detected by wisely observing and detecting at the legal warden due to the low transmit power of other IoT devices.

E. Covert Communications in UAV-Assisted Networks

UAVs can be leveraged to achieve the flexibility of network configuration owing to the high mobility and easy deployment. In addition, the utilization of UAVs in wireless communication can benefit the transmission performance from the high probability of line-of-sight (LoS) channels in air-to-ground links. Although the LoS channels can improve the communication performance, it is also vulnerable to the attacks by malicious eavesdroppers because of the open-access characteristic of wireless signals. Different from the conventional security solutions, covert communication can be adopted to secure the UAV-related transmission effectively. Based on the functions of UAVs, the UAV-related communication can be divided into four categories, i.e., UAV as an Alice, a Bob, a Willie, and a jammer [78], which are summarized in Table VI.

TABLE VI
ROLES OF UAV IN COVERT NETWORKS

Role of UAV	Reference	Benefits
Alice	[88], [106], [169]	LoS channels
Bob	[57], [84]	LoS channels
Willie	[57]	Mobility
Jammer	[91]	LoS Channels; Mobility;

Yan *et al.* in [88] investigated the covert communication in a network with UAV as Alice. In this paper, the UAV Alice wants to transmit secret signals to a ground Bob, and tries to avoid being detected by Willie. They analyzed the impacts of the flying location of Alice based on the transmission to Bob and the covertness towards Willie in six scenarios. They proved that although the nearest possible transmission location can bring a high transmission rate, it is not always the optimal location concerning the covertness protection. In [169], the strategy of detecting a suspicious UAV's transmission via beam sweeping was proposed by Hu *et*

al.. They divided the suspicious aerial area into several sectors and utilized the beamforming gain to improve the detection accuracy. They derived the optimal number of detection sectors to minimize the error detection probability. For a UAV as Alice in the covert communication for data collection, Jiang *et al.* in [106] designed the trajectory and resource allocation strategy for the UAV in a multi-user network. They jointly designed the time allocation, trajectory, and transmit power of each user to maximize the average covert transmission rate while guaranteeing that the error detection probability at the warden is larger than a constraint. Different from the works discussed above, Chen *et al.* in [84] investigated the UAV-assisted covert communication when the UAV works as a receiver. By leveraging its mobility, the UAV Bob can adjust its hovering location to achieve better transmission performance. They derived the optimal hovering location of Bob together with other resource allocation strategies to maximize the covert transmission rate while keeping the error detection probability higher than its constraint. Liang *et al.* in [91] studied the scenario when the UAV works as a jammer, and the UAV jammer can be easily deployed to disturb the detection at the warden. With the assistance of UAV jammer, they analyzed the covert communication performance under both AWGN and Nakagami-m fading. The mobility of UAV can be also leveraged to serve as a malicious Willie or a relay. Chen *et al.* in [57] investigated the scenario where both Willie and the relay are UAVs. The covert communication is under a worst case, where the UAV Willie can change his detection locations, and the communication range is so long that it requires the help of a relay. Under this worst situation, they proposed a scheme to realize the covert communication with the covertness and transmission performance requirements.

F. Covert Communications in Remote Networks

Without doubt, wireless communication can bring great convenience to everyone's daily life. However, the quality of wireless communication can be influenced or reduced by channel fading, which becomes more severe in the long-range transmission. Although the transmission range can be extended by increasing the transmit power, it will also on the other hand introduce severe security risks [171]. Thus, relays can be deployed to improve the transmission performance [82], [177]. In addition, the security of relay-assisted networks can be further guaranteed with the help of covert communication [178], [179], as shown in Fig. 9.

In [71], Wang *et al.* performed the covert communication in a long-distance network assisted by a relay via exploring the channel uncertainty. They assumed that the channel coefficients follow the Rayleigh fading, and the transmitted signal follows the complex Gaussian distribution. The channel uncertainty is considered at both Bob and Willie. With the help of the relay, it was proved that Alice can transmit $\mathcal{O}(n)$ bits with n channel uses. Sun *et al.* in [36] investigated the relay-assisted covert communication under both full-duplex (FD) and half-duplex (HD) modes. They proved that by jointly switching the relaying modes between FD and HD and optimizing the transmit power, the covert communication can obtain a better

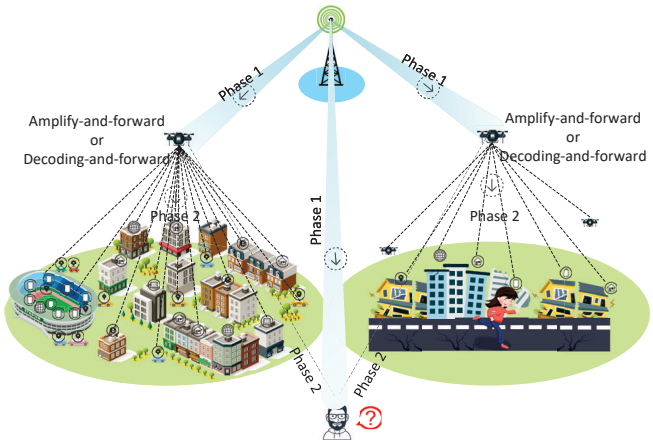

Fig. 9. Fundamental model of covert communications in remote networks.

performance regarding to the covert transmission rate. To further improve the communication performance, Lv *et al.* in [92] leveraged a multi-antenna relay to increase the covert transmission rate. Two beamforming-related schemes were proposed, namely the maximum ratio transmission (MRT) scheme and the random beamforming scheme, which are distinguished by whether the CSI between the relay and Bob is available. They proved that the MRT scheme can achieve a higher covert transmission rate under the same error detection probability constraint compared with the random beamforming scheme. Malicious relays can be also used to assist the long-range transmission, which was studied in [28] by Hu *et al.*. The relay is greedy and tries to transmit its own message together with the relayed message from the source using the public resource. They proposed two schemes, i.e., the rate-control and the power-control, to achieve the illegal covert communication detection. The rate-control scheme was proved to achieve a higher effective covert transmission rate. In [27], Wang *et al.* investigated the covert communication in a longer range, which requires multiple relays to multi-hop the message. In this paper, the scheme was proposed to realize the covert communication via several terrestrial nodes against the detection of a UAV warden. The UAV can jointly detect the covert transmission since the relays adopt the decode-and-forward mode. This poses severe risks to be detected by the legitimate warden. They designed the transmit power, the coding rate, and the hopping number to maximize the secrecy throughput while constraining the joint error detection probability at Willie. When there are more available relays, the covert communication can be even optimized via selecting the relay with the optimal CSI. Sun *et al.* in [55] designed a relay selection scheme by utilizing the optimal relay. The proposed scheme is effective to decrease the error detection probability, and the average covert transmission rate can be also increased under the same covertness constraint. In [170], Hu *et al.* jointly optimized the transmit power of Alice and the UAV relay, and the hovering height of UAV, to maximize the covert throughput while keeping the error detection probability of Willie higher than the maximum allowed constraint.

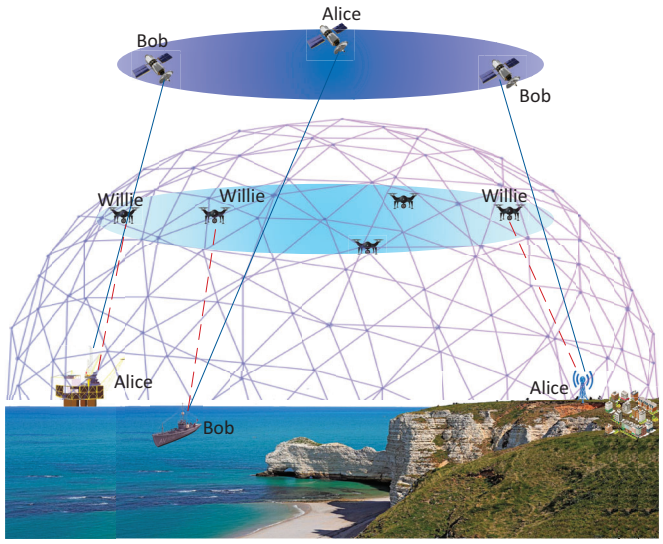

Fig. 10. Application of covert communication in satellite networks.

G. Covert Communications in Satellite Networks

To realize a more extensive range of wireless communication without being limited by geographical blocks, satellite becomes a premier choice owing to its advanced capability [180]. Satellite communication has gained plenty of attention because of its state-of-the-art characteristics, i.e., long communication range, high reliability, and multiple access. Satellite communication can provide an extremely wider coverage. In addition, it also provides highly reliable links, which will not be affected by the BS destruction in geological disasters. Moreover, the satellite communication can be achieved with low cost for broadcast and multiple access to receive at different locations. Although the satellite communication can leverage many techniques to secure the transmitted information, there still exists a high risk of being eavesdropped, owing to the open characteristics of wireless broadcast and wide coverage. As shown in Fig. 10, applying covert communication to satellite networks can prevent Willie from detecting the transmission of Alice, and further avoid information leakage. However, how to achieve covertness while guaranteeing the quality of transmission is still challenging.

Kang *et al.* in [172] compared the covertness performance in three typical NOMA schemes. One terrestrial Alice among multiple public users transmits the uplink information to the satellite Bob while avoiding the detection of a UAV Willie in this paper. The covert message is transmitted under the cover of public information, both of which are superposed via three satellite-related NOMA schemes, such as sparse code multiple access, multi-user shared access, and pattern division multiple access. In [173], Chen *et al.* utilized the polar code to solve the synchronization problem of low-SNR scenario in a multi-carrier intelligent covert satellite communication. In addition, Wu *et al.* further adopted the polar code aided frequency offset estimation scheme to solve the spectrum limitation in [174]. Based on the proposed schemes, they analyzed the covert outage probability and achievable transmission performance for covert satellite communication.

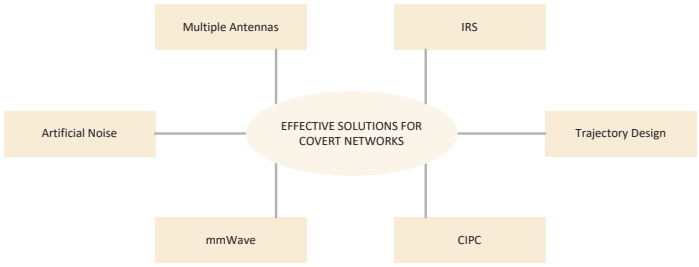

Fig. 11. Potential solutions for covert communications networks.

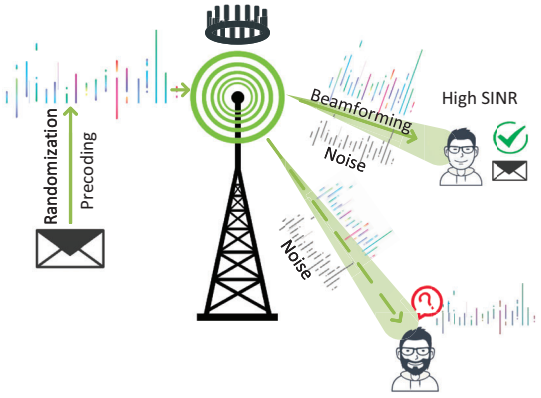

Fig. 12. Utilization of multiple antennas in covert communication networks.

V. Solutions for Covert Communication Networks

Wireless security can be well realized by introducing covert communication, especially for the air-to-ground communications, where the LoS channels can benefit the malicious eavesdroppers. Therefore, the methodologies to guarantee the covertness are essential to be investigated. In this section, we provide a review on several typical techniques that have been utilized to introduce uncertainty at Willie to achieve covertness, which is summarized in Table VII. These potential covert solutions include multiple antennas, artificial noise (AN), millimeter wave (mmWave), intelligent reflecting surface (IRS), trajectory design, and CIPC, a brief summary of which is shown in Fig. 11.

A. Multiple Antennas

The application of multiple antennas in wireless communication can bring many advantages, which include expanding the coverage, increasing the channel capacity, boosting the user connections, increasing the reliability, *etc*. As shown in Fig. 12, with more antennas equipped at the transmitter, the received SNR can be increased significantly [60], [196]–[198]. Furthermore, applying MRT by the transmitter can boost the SNR at the targeted receiver more than other malicious users. However, the warden can also leverage this technique to decrease the risk of being detected at Alice.

Multiple antennas were applied at Alice by Forouzesh *et al.* in [80] to help improve the performance of covert

TABLE VII
EFFECTIVE RANDOMNESS SOLUTIONS FOR COVERT COMMUNICATION NETWORKS

Effective Solutions	References	Main Characteristics
Multiple antennas	[31], [80], [181]	MRT to achieve high SINR at Bob.
	[58], [156]	Null space jamming to reduce interference at legitimate receivers.
	[182]	Utilize MIMO to obtain a non-zero covert capacity over n AWGN channels.
	[183], [184]	Randomly select the optimal antenna to receive signals.
	[185]	Covert communication under composite fading and shadowing channels.
Artificial noise	[72], [101]	Jam the warden to avoid being detected.
	[53]	Intelligently select jammer with smaller channel gains regarding to Bob.
	[186]	Post severe risk on Bob to derive a more secure covertness scheme.
	[187]	The optimal AN and signal transmission probability is analyzed.
mmWave	[100]	Optimal mmWave beam pair selection to improve effective throughput.
	[87]	Adopt beam sweeping to improve covert performance.
	[188]	Assist covert communication with the jamming of full-duplex Bob.
IRS	[35]	Jointly adopt active and passive beamforming at IRS to provide a better transmission.
	[67], [104], [189]	Improve the covert performance via IRS configuration.
	[190]	Configure IRS with Willie unaware of CSI and noise information.
	[191]	Propose an energy-efficient IRS-aided covert scheme.
Trajectory	[65]	A UAV works as a transmitter to provide covert communication through her mobility.
	[98]	A UAV data collector is investigated in a covert communication network.
	[192]	A legitimate UAV monitoring covert network is investigated.
	[193]	Adopt the geometric method to optimize UAV's trajectory.
CIPC	[164], [194]	CIPC is adopted at the transmitter to maintain the received power at receiver.
	[195]	Utilize CIPC at the jammer to improve the performance of covertness with the threshold parameter.

communication networks, where the MRT beamforming was adopted to increase the achievable rate while maintaining the covertness. The MRT was also leveraged by Zheng *et al.* in [31], where the performance of CAS and DAS were compared. In addition, Forouzesh *et al.* in [156] adopted multiple antennas at Alice to leverage the null space together with the 3D beamforming to improve the transmission performance. They employed multiple antennas at the jammer to introduce interference at the warden while putting the legitimate receiver in the null space. In [58], multiple antennas were equipped at both the jammer and Bob by Shmuel *et al.*. The jamming power is randomized, and it utilizes the beamforming to maximize the transmission rate of Alice at Bob. In addition, they also leveraged the multiple receiving antennas at Bob to cooperate with the jammer to maximize the receiving SINR. Multiple-input multiple-output (MIMO) was utilized by Bendary *et al.* in [182] to provide a non-zero covert capacity over n AWGN channels, which can satisfy the condition that either the transmit antennas scale up fast or the transmitter performs the null space on Willie. In [181], Yu *et al.* investigated the beamforming of multiple-input single-output (MISO) channels in covert communications. They proved that the optimal signaling under the complex Gaussian channel is the symmetric complex Gaussian distribution. They also discussed the optimal translation with different CSI knowledge at the transmitter. Yang *et al.* utilized multiple antennas at the receiver and the relay in [183] and [184], respectively. In [183], the legitimate Bob was assumed to select the best antenna to receive the covert information and utilize the remaining ones to jam Willie. Results were investigated under the cases of Willie knowing or not knowing the CSI between him and Bob. In [184], multiple antennas were assumed to be equipped at the relay, and it selected its optimal antenna to receive signals from Alice while utilizing the rest to jam Willie during the first phase. During the second phase, the relay was assumed to utilize its multiple antennas to perform zero-forcing towards Bob to jam Willie. Different from other covert communication research, Du *et al.* investigated the multi-antenna covert communication under the composite fading and shadowing models in [185]. However, the applications of multi-antenna MRT in covert communications usually require perfect CSI, which on the other hand may increase the design complexity of the network.

B. Artificial Noise

Similar to the noise uncertainty, channel uncertainty and relay assistance, artificial noise can be leveraged as one of the promising techniques to confuse the detection at Willie, as shown in Fig. 13. The uncertainty brought by the jammer can be introduced from the random transmit power or even

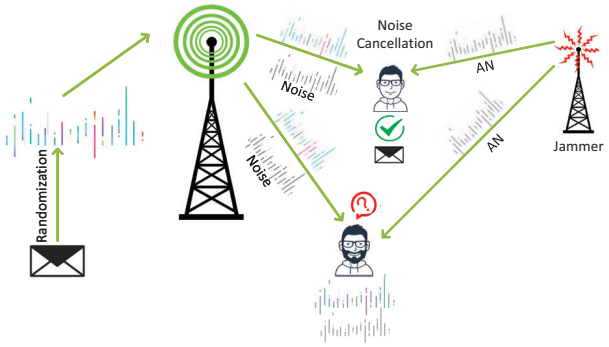

Fig. 13. Application of AN in covert communication networks.

from a full-duplex receiver either with fixed or random power. The introduced jamming signal can work together with the environmental noise and other uncertain factors to degrade the received signals at the warden effectively [199].

Huang *et al.* utilized a friendly jammer in [72] to covertly transmit to K users via mutually orthogonal frequency access, where the jamming sequence of each user follows a complex Gaussian distribution. In [101], Xiong *et al.* studied the covert communication with the assistance of a cognitive jammer. The jammer senses Alice's transmission of the first m slots, and jams with complex Gaussian signalling during the rest $m+1$ slots if it detects her transmission. The results show that the proposed cognitive covert jamming scheme can improve the data transmission rate and reduce the possibility of detection. Different from the typical jammer-assisted covert communication, Zheng *et al.* in [53] proposed a scheme that can intelligently select jammers regarding their CSI to achieve a better performance in both covertness and throughput. To confuse the detection at the warden as well as reducing the interference at Bob, they selected the potential jammers with smaller channel gains between themselves and the receiver. With the uncertainty brought by the locations and the number of jammers, the detection at Willie can be severely influenced. On the other hand, the jamming can be also leveraged by malicious users to disrupt the transmission among legitimate users. Zhang *et al.* in [186] studied the covert communication when the channels are jammed by an adversarial user. To overcome this challenge, they proposed to increase the size of shared key to guarantee the reliability of covert communication. In [200], Zhao *et al.* utilized a full-duplex Bob to interfere the detection of Willie. They inviestigated the tradeoff between communication and eavesdropping links, where the covert transmission was optimized via properly selecting the variation range of Bob's jamming power. He *et al.* analyzed and derived the optimal transmission probability of both Alice and the jammer in [187]. Nevertheless, by applying artificial jamming to introduce randomness, the impact of jamming signals on legitimate users cannot be ignored, especially when the it cannot be well eliminated. In addition, the energy efficiency of jamming signals should be also taken into consideration.

C. mmWave

mmWave can utilize beamforming to overcome the severe path loss and enormously increase the transmission rate of covert communication. Nevertheless, the mmWave resource has not been well used, which can enable a higher transmission rate of mmWave-related communications. The mmWave has strong directions, which can provide inherent security for covert communication and make it more difficult for Willie to detect [50].

In [100], Zhang *et al.* first designed a mmWave covert communication scheme, where the directional nature of mmWave can help to protect the security of covert communication. In this paper, Alice and Bob utilize a beam training method to establish the directional link between them and pick up the optimal beam pair for data transmission. They also designed a scheme to jointly optimize the beam training overhead to maximize the effective throughput. In addition, Zhang *et al.* optimized the covert transmission rate of UAV-assisted mmWave communication via beam sweeping in [87]. With the directional characteristic of mmWave, the transmission of Alice can be better secured. They considered the transmission of Alice without the location information of both Bob and Willie, and Alice utilizes the beam sweeping to improve the covert communication performance. In [188], Wang *et al.* considered the covert communication with a full-duplex Bob, where the receiver can emit the jamming signal to assist the covert communication. They analyzed both the scenarios of single data stream and multiple data streams, and the performance can be improved accordingly. To make a summary, the highly directional mmWave can provide better transmission performance, which on the other hand also requires a more precise design to achieve the expected effects. In addition, mmWave is vulnerable to the jamming interference. Thus, preventing malicious jamming is also critical in mmWave based covert communication networks.

D. IRS

IRS can be designed to realize a desirable direction of the received signals at the target users via optimizing its reflection matrix, as shown in Fig. 14. Compared with the typical covert communication model, adopting IRS can further benefit from the uncertainty brought by channel fading [77], [79], [201]. Thus, IRS can be introduced into covert communication networks to improve the covert transmission performance at the legitimate receiver via reconfiguring the wireless channels from Alice [83], [202]–[205].

In [189], Lu *et al.* listed four typical IRS-enhanced covert communication systems, i.e., with RF harvesting, blockage, interference, and active attack. Then, they further analyzed a case of how to configure the IRS to maximize the transmission performance while keeping the covertness. Wu *et al.* in [67] discussed a practical IRS-assisted covert scenario when the CSI of warden is unavailable at the transmitter. They jointly designed the transmit power at Alice and the reflection phase as well as the amplitude of IRS to minimize the outage probability at Bob. In [104], Zhou *et al.* studied a short-packet scheme of IRS-aided covert communications, where

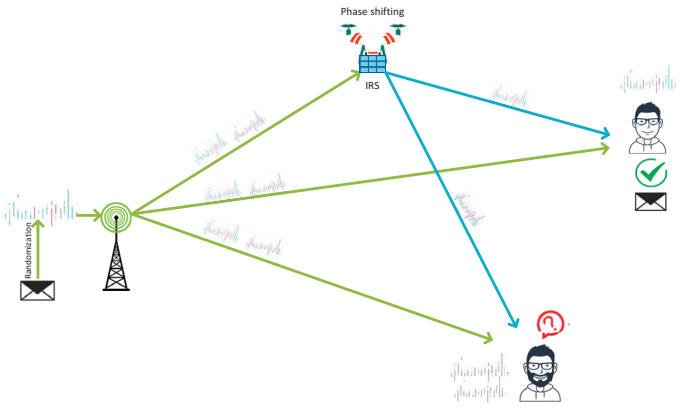

Fig. 14. Adopting IRS in covert communication networks to achieve better performance.

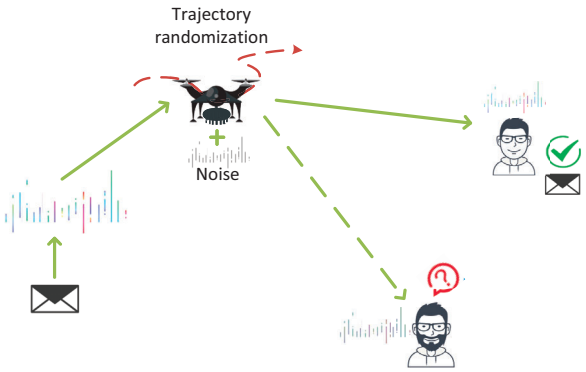

Fig. 15. Uncertainty introduced by a random trajectory of UAV Alice in covert communication networks.

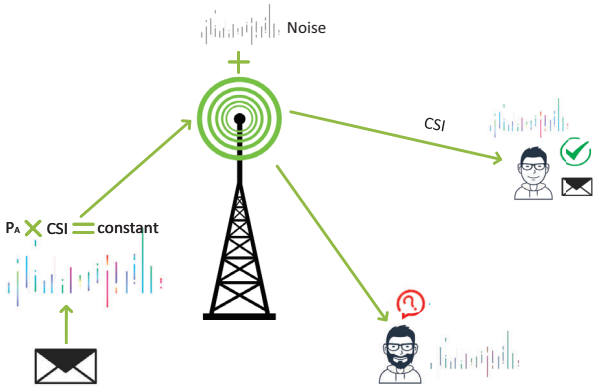

Fig. 16. Randomness introduced by CIPC in covert communication networks.

the uncertainty is caused by the transmitted complex Gaussian signal from Alice. Wang *et al.* in [35] investigated the IRS-assisted covert communications under both active and passive beamforming patterns. In this paper, the direct link between Alice and Bob is blocked, where an IRS is adopted to relay the covert communication to Bob, which works as a full-duplex jammer to disturb the detection of Willie. The active beamforming at Alice and the passive beamforming at IRS are jointly optimized to provide a better transmission performance while maintaining the correct detection probability of Willie under a specific constraint. In [190], Zou *et al.* studied the covert communication network with the uncertainty at Willie about the CSI between Alice-IRS and IRS-Willie, and Willie is also unaware of his noise power. They analyzed the detection of Willie under a practical scenario to realize the stealth of covert communication. Different from most existing literature, Li *et al.* investigated an energy-efficient IRS-aided covert communication in [191], where the IRS is mounted on a UAV to improve its coverage. However, there exist some difficulties for IRS-aided covert communications. The phase shift matrix design of IRS highly relies on the estimated CSI, which may lead to a worse performance without proper design. In addition, the introduction of IRS can also lead to higher path loss. Therefore, a trade-off between the channel design and the signal decay should be carefully considered.

E. Trajectory Design

UAV has attracted tremendous academic attentions owing to its high mobility, easy configuration, and excellent channel conditions. One of the most typical techniques for UAV communications to introduce uncertainty is leveraging the random channel fading. Further combining the mobility of UAV with channel fading, the uncertainty introduced at the warden can be greatly improved, as shown in Fig. 15, which helps to greatly improve the covertness for Alice.

In [65], Jiang *et al.* discussed the application of UAVs in covert communications, where they discussed the categories of UAV's functions in detail. Then, they proposed an effective scheme in which the UAV works as a transmitter and utilizes her mobility to covertly transmit to multiple ground users while maximizing the data capacity. Zhou *et al.* considered the uplink covert transmission from a terrestrial user in [98], where the uncertainty introduced to wardens is caused by the channel fading. Specifically, the trajectory of UAV is optimized to achieve a higher data rate while maintaining the covertness. In [192], Hu *et al.* considered the legitimate UAV monitoring in covert communication. They optimized the propulsion and thrust power, together with the trajectory to achieve a better monitoring performance. Rao *et al.* utilized a geometric method to optimize the trajectory of UAV covert networks in [193]. Thus, location randomness is an interesting design especially in UAV-related covert communication networks. However, the design assumption should be practical, since the speed of UAV is limited, which limits its location variation range.

F. CIPC

CIPC indicates that the transmitter varies its transmit power to maintain the received power of signals as a specific constant at its target user. By utilizing CIPC, the received signal's power at Bob can be designed to remain constant, but the received power at Willie will vary according to the channel fading. This can be leveraged to introduce additional uncertainty to Willie while maintaining the transmission performance at the legitimate user, as shown in Fig. 16.

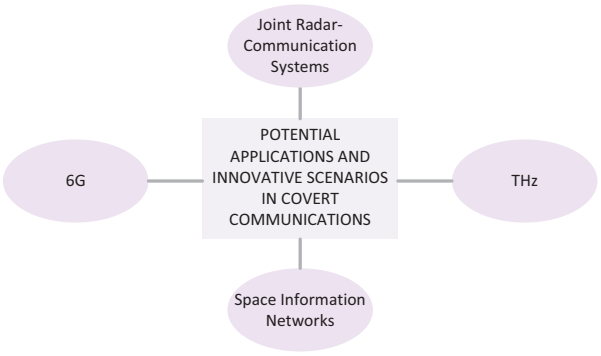

Fig. 17. Emerging applications and scenarios of covert communications.

In [194], Hu *et al.* leveraged the Rayleigh fading into CIPC at the transmitter to achieve a guaranteed communication performance while introducing uncertainty to the warden. Alice randomizes her transmit power inversely according to the channel coefficient between herself and Bob to confuse the detection at Willie. In addition, the receiver emits the full-duplex jamming signal with random power, which allows Alice to guarantee the security with higher transmit power. According to the time intolerant system, Ma *et al.* in [164] studied the CIPC-assisted covert communication. Apart from the impact of Rayleigh fading of CIPC, Alice also adopts the Gaussian signaling to import uncertainty at Willie. The optimal detection threshold at Willie is derived, and the maximal effective covert throughput is also demonstrated. In [195], [206], Wang *et al.* investigated the covert communication with a CIPC jammer, which employs the CIPC to avert the channel estimation pilot as well as bringing uncertainty to the detection of warden. They proved that the performance of covertness can be improved with the preset threshold parameter of CIPC. Zoran *et al.* proposed an near-ideal covertness scheme of NOMA networks in [207] by utilizing CIPC. Nevertheless, the most critical requirement in CIPC is channel estimation. Without reliable estimation of CSI, the power control at the transmitter will be difficult to achieve.

VI. Emerging Applications and Scenarios

With the rapid development of wireless techniques, covert communications need to further improve the methodologies to introduce uncertainty and adapt to the security requirement in the emerging applications and scenarios, especially to fight against the increasing computational ability of wardens. In this section, we discuss and elaborate the potential applications and possible scenarios for covert communications, the brief summary of which is demonstrated in Fig. 17.

A. 6G

Mobile devices enable everyone to access the Internet everywhere, anytime, and with anyone. Specifically, the convenience of wireless communications allows people to imagine the Internet to be much faster, more accessible, and even more diverse. The motivation of 6G is to provide a higher transmission rate, less time delay, and more comprehensive wireless coverage [208], [209]. It proposes the concept of space-air-ground-sea seamless coverage, where the information of human society will become available anywhere, and thus the security becomes a more critical factor [210]. In addition, the ubiquitous connections in 6G require more complicated communication protocols, which have extremely high complexity and face great challenges to guarantee the transmission security. By leveraging covert communications, the user security can be further guaranteed, and the basic scenario can be described in Fig. 18. In [94], Ma *et al.* studied the covert communication of hybrid devices for 6G wireless communications with both active and passive modes. They explored the inherent uncertainty of active links to realize the covertness with the help of passive backscattering sensors, which work as interferers. However, the 6G-related covert communication still requires further research. More effort should be paid to utilize the ubiquitous devices and new techniques to achieve covert communications, which should be emphasized in the future.

B. THz

TeraHertz (THz) is defined as the electromagnetic wave with the frequency range from 0.3 THz to 3 THz, which largely broads the band of wireless communications by exploring more available frequency resource [211]. Due to the directional characteristics and narrower beams, THz is considered to be more secure than the conventional low-frequency communications. Although THz, as a high-frequency communication, has the drawback of severe channel fading caused by spreading and scattering, it can avoid detection outside the beam sectors [212]. There have been a few THz-related studies, but the channel model of THz is still not fully investigated. In [213], Gao *et al.* proposed a distance-adaptive absorption peak modulation covert communication scheme to utilize the frequency-dependent molecular absorption. They first formulated the fundamental THz covert communication metrics and then analyzed the covert performance of the proposed scheme. However, the highly directional characteristic also poses a significant threat to the transmission between Alice and Bob, which is easy to be blocked once the malicious user blocks the direct LoS links. Liu *et al.* in [107] proposed to utilize non-line-of-sight (NLoS) to migrate the fixed transmission path to an unpredictable one to hide the information transmission and avoid being terminated. They proposed to utilize a specular reflection component to scatter the covert signal. However, the existing THz-related covert communication research is still limited, and many fundamental concepts have not been well established. For example, the elemental channel models and transmission characteristics of THz communication still need to be developed. In addition, techniques to introduce more uncertainty at Willie still need to be developed.

C. Integrated Sensing and Communication

Frequency resource is becoming increasingly scarce with the development of requirements for wireless devices. Combining sensing and communication can currently share the overlapped bands, which may result in interference to both of these two

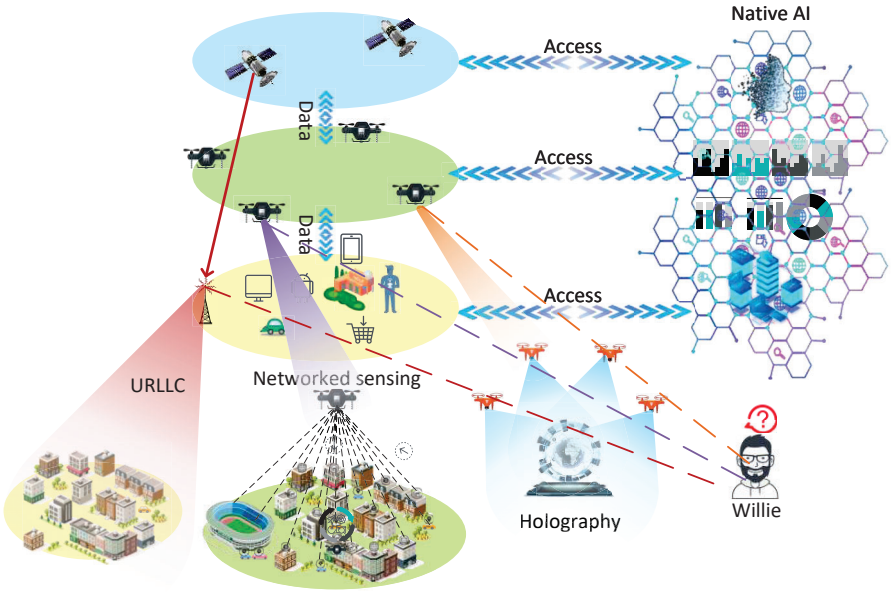

Fig. 18. Utilization of covert communication in 6G.

systems [214]. However, by sharing the radio resource and hardware platform, the interference can be eliminated and the performance can be further improved, which is called the integrated sensing and communication system [215], [216]. One of the possible covert scenarios for integrated sensing and communication is that Alice tries to detect the location of Willie via the sensing signals during her transmission to Bob, Then, Alice can introduce more directional interference at Willie after obtaining its location information. Thus, a covert joint sensing-communication system can treat the active or mobile Willie more efficiently [217]. With the radar detection, Alice can detect Willie and estimate the CSI, which sheds more light on the zero-forcing beamforming towards the warden. Nevertheless, one of the critical problems to be solved in a covert joint sensing-communication system remains as how to send the probing waveform embedding secure information without being detected by the warden. In [218], Du *et al.* applied covert communication to a joint radar communication system to achieve better spectrum utilization and information security.

D. Space Information Networks

Space information networks refer to the data transmission between spacecraft and ground base stations, which can utilize different types and functions of satellites, stratospheric ballons, UAVs and other equipments to combine inter-satellite links and satellite-air-ground links to provide full coverage of the integrated space-ground information systems [219]. Compared with the conventional terrestrial wireless networks, space information networks have the advantages of full coverage, fast configuration, and less environmental limitation. However, the extreme long distance can cause severe time delay, which can be solved by the short-packet transmission. Nevertheless, there still exist some security challenges in space information networks, which can be solved with the help of covert communications [220], as shown in Fig. 19. The critical task of implanting covert communications into space information networks is to prevent detection while guaranteeing high transmission rate, seamless coverage, as well as low latency. Secure signal can be transmitted via covert communications with slot selection, which limits the averaged transmission rate. In addition, the transmit power is also reduced to decrease the risk of being detected in covert communication networks. Therefore, more powerful uncertainty-introducing method should be developed to guarantee the covertness while improving the transmission performance for space information networks.

VII. Future Issues And Open Challenges

With the aforementioned solutions, the covert communications can be guaranteed with a low probability of being detected by the wardens. However, there still exist several challenges to be conquered to improve the covertness performance. The main challenges and potential solutions for covert communications are summarized in Table VIII.

A. Active Willie

Different from the typical scenario where Willie is either at a fixed location or performing passive detection, active Willie can be referred to as a mobile warden or an active attacking warden. As for the mobile Willie, it indicates that Willie can change his detection location and power threshold dynamically according to the received signals [93]. Willie may locate far away from Alice, and can measure his received signal to analyze whether Alice is transmitting. If he finds that Alice has some suspicious behavior, he can move closer

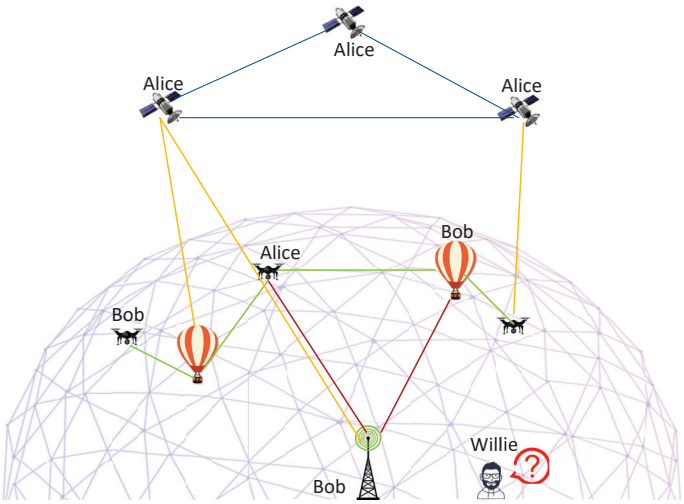

Fig. 19. Fundamental model of remote covert communication networks.

TABLE VIII
FUTURE CHALLENGES AND POTENTIAL SOLUTIONS

Future Issues	Challenges	Potential Solutions
Active Willie	1) Active noise attack; 2) More adaptive detection;	1) Malicious jamming cancellation; 2) Diverse uncertainty techniques;
Utilization of MIMO	Decoding vector design at Bob	More efficient algorithm to derive the decoding vector
Powerful Willie	Higher detection risk	More randomization techniques
Imperfect CSI	Communication quality reduced at Bob	Improve CSI estimation performance
Leakage and blockage of mmWave	Poor performance in NLoS channels	Utilize IRS to assist the transmission
Uncertainty techniques	Limited types of uncertainty techniques	Further development of randomization techniques

and perform further detection and analysis. After a few times of repeating this closer-and-detecting process, he can make a more precise decision of whether Alice is transmitting or not. As for the active attack, it means that Willie is no longer satisfied with the passive detection, and he may generate interference when he finds out the transmission of Alice. After Willie makes the decision that Alice is transmitting, he can send artificial noise to jam the transmission of Alice and influence the receiving at Bob. This can be more frustrating when Willie is much closer to Bob than Alice, where he can jam Bob with considerable low power and have better jamming effect. However, the current research related to covert communications rarely considers the active Willie, which can be further explored to provide more thorough protection for the covert transmission.

B. Utilization of MIMO

By adopting MIMO, the total power of received signal can be boosted significantly via the advantage of wireless channels. In addition, MIMO can also leverage precoding to maximize the SINR at the target receiver while putting the illegal receivers in the null space. However, most of the multi-antenna research regarding covert communications only concerns the multiple-input single-output (MISO) case. In future directions of covert communications, multiple antennas at Willie or Bob should be also considered, which remains a severe challenge. For the multi-antenna Willie, the received signal power distribution requires further discussion, and more analysis of the probability distribution needs to be provided. For the multi-antenna Bob, the design of his decoding vector needs to be studied. Although the design of MIMO decoding vector has been well studied in 5G networks, it still needs to be further considered for a covert wireless network with the uncertainty introduced. Therefore, the future work related to MIMO covert communications should include how to design the decoding vector for Bob and the analysis of Willie with multiple antennas.

C. Powerful Willie

Current analysis usually assumes that Willie sets his power detection threshold as the optimum and stays fixed. This situation will become worse when Willie can utilize machine learning, and alternatively adapt the threshold for more precise detection. Machine learning can help Willie reduce the probability of error detection, which will pose a great threat to Alice. Currently, machine learning still faces some problems of high training overhead, less stability, difficulty in adaptivity, as well as sample limitation. For legitimate surveillance, the legal warden can utilize machine learning to estimate the CSI more precisely to help the detection. Through passive detection, the legitimate warden cannot obtain the CSI between himself and the illegal Alice. Thus, if he can adopt machine learning for detecting, his detection will be more accurate.

D. Imperfect CSI

A weak Alice can also result in a bad performance of covert communications. Previous works usually assume that Alice, the jammer or the legitimate relay has the full knowledge of CSI among legitimate users. They assume that the real-time CSI can be obtained by sending pilots, which is somewhat impractical. Forouzesh *et al.* in [81] studied the cases when the transmitter cannot obtain the perfect CSI, where they discussed three cases: 1) the channel distribution information (CDI) is available within a specific range, 2) the mean and variance of CDI are available, 3) the variance is unknown to the transmitter. Refer to [81], more research related to a weak Alice can be conducted to provide a more thorough covertness protection to the wireless transmission. In addition, the legitimate warden for surveillance also would like to have a more perfect CSI estimation between itself and the illegal transmitter [85].

E. Leakage and Blockage in mmWave

mmWave emerges as a key technique for wireless communications owing to its characteristics of short wavelength and high directionality. Although mmWave suffers strong absorption and cannot provide satisfied performance under NLoS channels, it is still widely utilized in personal area wireless networks benefiting from its short wavelength. A highly directional beam allows mmWave to transmit to its desired receiver directly and accurately without scattering to other users, which can guarantee the transmission security. Nevertheless, the information leakage problem still exists, which may post the transmission of Alice under the discovery of Willie. In addition, the transmission in mmWave between Alice and Bob may be blocked in NLoS links. Future research can further consider to utilize IRS or other techniques to solve this inherent problem of mmWave.

F. Uncertainty Techniques

The reason why Alice can transmit to Bob without being detected by Willie is that she can hide her signal in the environmental or artificial noise to avoid the detection of Willie. However, the hiding-and-detecting mode is a competitive game between Alice and Willie, where Willie is fighting for more precise detection, and Alice is trying her best to make her signal disappear at Willie. Besides the environmental noise, the typical solutions used in covert communications include: 1) the uncertainty from small-scale channel fading, 2) the transmit power randomization, 3) the location variation, and 4) the jamming power randomization. The above-mentioned uncertainty solutions can be utilized alone or combined. In [221], Wang *et al.* proposed a probabilistic accumulate-then-transmit scheme, where Alice can adjust the prior of energy harvesting and information transmission to confuse the detection of Willie to realize covertness. However, the covert communication networks still require more effective techniques to bring uncertainty and provide more solid covertness in the future.

VIII. Conclusion

This survey has provided an extensive review of covert communication, which is a pivotal security technique that can provide comprehensive security protection via hiding the existence of transmission. First, we explain the fundamental knowledge of the covertness theory and compare the difference with other security methods. Then, different branches of covert communication research are introduced and compared in detail. An overview of diverse applications of covert communication in different networks is presented. In particular, the techniques leveraged in covert communications to hide the stealthy signal from the detection of wardens are summarized and explained. Furthermore, the emerging applications of covert communication and the potential scenarios are analyzed and discussed. Finally, we discuss the possible future issues of covert communications, and demonstrate the potential research directions.

References

[1] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Towards dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, to appear.

[2] Y. Heng, J. G. Andrews, J. Mo, V. Va, A. Ali, B. L. Ng, and J. C. Zhang, "Six key challenges for beam management in 5.5G and 6G systems," *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 74–79, Jul. 2021.

[3] Y. Liu, X. Wang, G. Boudreau, A. B. Sediq, and H. Abou-Zeid, "A multi-dimensional intelligent multiple access technique for 5G beyond and 6G wireless networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 2, pp. 1308–1320, 2021.

[4] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

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

[6] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[7] R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, "A steganography algorithm based on CycleGAN for covert communication in the internet of things," *IEEE Access*, vol. 7, pp. 90574–90584, 2019.

[8] J.-W. Ho, "Covert channel establishment through the dynamic adaptation of the sequential probability ratio test to sensor data in IoT," *IEEE Access*, vol. 7, pp. 146093–146107, 2019.

[9] J. Peng and S. Tang, "Covert communication over voip streaming media with dynamic key distribution and authentication," *IEEE Trans. Ind. Electron.*, vol. 68, no. 4, pp. 3619–3628, Apr. 2021.

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

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

[12] M. Li, G. Ti, X. Tian, and Q. Liu, "QoS-based binary signature design for secure CDMA systems," *IEEE Trans. Veh. Tech.*, vol. 66, no. 11, pp. 10011–10023, Nov. 2017.

[13] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.

[14] Z. Xiang, W. Yang, Y. Cai, Z. Ding, Y. Song, and Y. Zou, "Noma-assisted secure short-packet communications in IoT," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 8–15, Aug. 2020.

[15] H. Peng, Z. Wang, S. Han, and Y. Jiang, "Physical layer security for MISO NOMA VLC system under eavesdropper collusion," *IEEE Trans. Veh. Tech.*, vol. 70, no. 6, pp. 6249–6254, Jun. 2021.

[16] N. Zhao, X. Pang, Z. Li, Y. Chen, F. Li, Z. Ding, and M.-S. Alouini, "Joint trajectory and precoding optimization for UAV-assisted NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3723–3735, May 2019.

[17] X. Liu, J. Wang, N. Zhao, Y. Chen, S. Zhang, Z. Ding, and F. R. Yu, "Placement and power allocation for NOMA-UAV networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 965–968, Jun. 2019.

[18] W. Wang, J. Tang, N. Zhao, X. Liu, X. Y. Zhang, Y. Chen, and Y. Qian, "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

[19] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos based spread spectrum image steganography," *IEEE Trans. Consum. Electron*, vol. 50, no. 2, pp. 587–590, May 2004.

[20] C. Wang, E. K. Au, R. D. Murch, W. H. Mow, R. S. Cheng, and V. Lau, "On the performance of the MIMO zero-forcing receiver in the presence of channel estimation error," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 805–810, Mar. 2007.

[21] C.-K. Wen, W.-T. Shih, and S. Jin, "Deep learning for massive MIMO CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 748–751, Oct. 2018.

[22] 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, Sept. 2013.

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

[24] O. A. Topal and G. K. Kurt, "Covert communication in cooperative NOMA networks," in *Proc. IEEE SIU'20*, pp. 1–4, Gaziantep, Turkey, Oct. 2020.

[25] S. A. Ahmadzadeh and G. Agnew, "Turbo covert channel: An iterative framework for covert communication over data networks," in *Proc. IEEE INFOCOM'13*, pp. 2031–2039, Turin, Italy, Jul. 2013.

[26] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *Proc. IEEE VTC'17 Spring*, pp. 1–5, Sydney, NSW, Jun. 2017.

[27] 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.

[28] 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.

[29] L. Wang, "Covert communication over the Poisson channel," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 1, pp. 23–31, Mar. 2021.

[30] 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 ICC'18*, pp. 1–6, Kansas City, MO, USA, May 2018.

[31] 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.

[32] A. Abdelaziz and C. E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel," in *Proc. IEEE CCNS'17*, pp. 1–9, Las Vegas, NV, USA, Dec. 2017.

[33] H. Q. Ta, Q.-V. Pham, K. Ho-Van, and S. W. Kim, "Covert communication with noise and channel uncertainties," *Wireless Netw.*, vol. 28, no. 1, pp. 161–172, Jan. 2022.

[34] 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.

[35] 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.

[36] 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, Sept. 2021.

[37] 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 ICCC'19*, pp. 912–916, Chengdu, China, Dec. 2019.

[38] 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.

[39] 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, Sept. 2018.

[40] 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.

[41] Y. Li, Y. Zhang, J. Wang, W. Xiang, S. Xiao, L. Chang, and W. Tang, "Performance analysis for covert communications under faster-than-nyquist signaling," *IEEE Commun. Lett.*, to appear.

[42] W. Yang, X. Lu, S. Yan, F. Shu, and Z. Li, "Age of information for short-packet covert communication," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1890–1894, Sept. 2021.

[43] 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.

[44] 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 Proc.*, vol. 67, no. 16, pp. 4276–4290, Aug. 2019.

[45] O. A. Topal and G. K. Kurt, "A countermeasure for traffic analysis attacks: Covert communications with digital modulation," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 441–445, Feb. 2021.

[46] Y. Fu, S. Guo, and Z. Yu, "The modulation technology of chaotic multi-tone and its application in covert communication system," *IEEE Access*, vol. 7, pp. 122289–122301, 2019.

[47] X. Lu, W. Yang, S. Yan, L. Tao, and D. W. K. Ng, "Joint packet generation and covert communication in delay-intolerant status update systems," *IEEE Trans. Veh. Tech.*, vol. 71, no. 2, pp. 2170–2175, Feb. 2022.

[48] R. Li, J. Cui, T. Huang, L. Yang, and S. Yan, "Optimal pulse-position modulation order and transmit power in covert communications," *IEEE Trans. Veh. Tech.*, to appear.

[49] 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.

[50] M. V. Jamali and H. Mahdavifar, "Covert millimeter-wave communication: Design strategies and performance analysis," *IEEE Trans. Wireless Commun.*, to appear.

[51] 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, Sept. 2020.

[52] 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.*, to appear.

[53] T.-X. 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.

[54] 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.

[55] 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.

[56] Y. Wang, S. Yan, W. Yang, and Y. Cai, "Covert communications with constrained age of information," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 368–372, Feb. 2021.

[57] 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.

[58] 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.

[59] 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.

[60] S. Ma, Y. Zhang, H. Li, S. Lu, N. Al-Dhahir, S. Zhang, and S. Li, "Robust beamforming design for covert communications," *IEEE Trans. Inf. Forens. Security*, vol. 16, pp. 3026–3038, 2021.

[61] 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.

[62] 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.

[63] K. Shahzad and X. Zhou, "Covert wireless communications under quasi-static fading with channel uncertainty," *IEEE Trans. Inf. Forens. Security*, vol. 16, pp. 1104–1116, 2021.

[64] 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.

[65] X. Jiang, X. Chen, J. Tang, N. Zhao, X. Y. Zhang, D. Niyato, and K.-K. Wong, "Covert communication in UAV-assisted air-ground networks," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 190–197, Aug. 2021.

[66] 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.

[67] C. Wu, S. Yan, X. Zhou, R. Chen, and J. Sun, "Intelligent reflecting surface (IRS)-aided covert communication with wardens statistical CSI," *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1449–1453, Jul. 2021.

[68] X. Chen, W. Sun, C. Xing, N. Zhao, Y. Chen, F. Richard Yu, and A. Nallanathan, "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.

[69] L. Sun, T. Xu, S. Yan, J. Hu, X. Yu, and F. Shu, "On resource allocation in covert wireless communication with channel estimation," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6456–6469, Oct. 2020.

[70] 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.

[71] 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.

[72] K.-W. Huang, H. Deng, and H.-M. Wang, "Jamming aided covert communication with multiple receivers," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4480–4494, Jul. 2021.

[73] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Trans. Veh. Tech.*, vol. 68, no. 12, pp. 12432–12436, Dec. 2019.

[74] Y. Wang, S. Yan, W. Yang, Y. Huang, and C. Liu, "Energy-efficient covert communications for bistatic backscatter systems," *IEEE Trans. Veh. Tech.*, vol. 70, no. 3, pp. 2906–2911, Mar. 2021.

[75] X. Lu, W. Yang, Y. Cai, and X. Guan, "Proactive eavesdropping via covert pilot spoofing attack in multi-antenna systems," *IEEE Access*, vol. 7, pp. 151295–151306, 2019.

[76] 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. Tech.*, vol. 71, no. 1, pp. 533–544, Jan. 2022.

[77] S. Ma, Y. Zhang, H. Li, J. Sun, J. Shi, H. Zhang, C. Shen, and S. Li, "Covert beamforming design for intelligent reflecting surface assisted IoT networks," *IEEE Internet Things J.*, to appear.

[78] D. Wang, P. Qi, Y. Zhao, C. Li, W. Wu, and Z. Li, "Covert wireless communication with noise uncertainty in space-air-ground integrated vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2784–2797, Mar. 2022.

[79] 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.

[80] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information-theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7170–7181, May 2021.

[81] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Robust power allocation in covert communication: Imperfect CDI," *IEEE Trans. Veh. Tech.*, vol. 70, no. 6, pp. 5789–5802, Jun. 2021.

[82] 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.

[83] J. Si, Z. Li, Y. Zhao, J. Cheng, L. Guan, J. Shi, and N. Al-Dhahir, "Covert transmission assisted by intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394–5408, Aug. 2021.

[84] 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. Tech.*, vol. 70, no. 11, pp. 11619–11631, Nov. 2021.

[85] Z. Cheng, J. Si, Z. Li, L. Guan, Y. Zhao, D. Wang, J. Cheng, and N. Al-Dhahir, "Covert surveillance via proactive eavesdropping under channel uncertainty," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4024–4037, Jun. 2021.

[86] 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.

[87] J. Zhang, X. Chen, M. Li, and M. Zhao, "Optimized throughput in covert millimeter-wave UAV communications with beam sweeping," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 720–724, Apr. 2021.

[88] S. Yan, S. V. Hanly, and I. B. Collings, "Optimal transmit power and flying location for UAV covert wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3321–3333, Nov. 2021.

[89] 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.

[90] 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.

[91] W. Liang, J. Shi, Z. Tie, and F. Yang, "Performance analysis for UAV-jammer aided covert communication," *IEEE Access*, vol. 8, pp. 111394–111400, 2020.

[92] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Inf. Forens. Security*, to appear.

[93] Y. Zhao, Z. Li, N. Cheng, W. Wang, C. Li, and X. Shen, "Covert localization in wireless networks: Feasibility and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6549–6563, Oct. 2020.

[94] W. Ma, Z. Niu, W. Wang, S. He, and T. Jiang, "Covert communication with uninformed backscatters in hybrid active/passive wireless networks: Modeling and performance analysis," *IEEE Trans. Commun.*, to appear.

[95] Y. Zhao, Z. Li, D. Wang, and N. Cheng, "Tradeoffs in covert wireless communication with a controllable full-duplex receiver," *China Commun.*, to appear.

[96] K. Li, T. Sobers, D. Towsley, and D. Goeckel, "Covert communication in continuous-time systems in the presence of a jammer," *IEEE Trans. Wireless Commun.*, to appear.

[97] 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, Sept. 2017.

[98] 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.

[99] 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. Tech.*, vol. 69, no. 3, pp. 2980–2992, Mar. 2020.

[100] J. Zhang, M. Li, S. Yan, C. Liu, X. Chen, M.-J. Zhao, and P. Whiting, "Joint beam training and data transmission design for covert millimeter-wave communication," *IEEE Trans. Inf. Forens Security*, vol. 16, pp. 2232–2245, 2021.

[101] W. Xiong, Y. Yao, X. Fu, and S. Li, "Covert communication with cognitive jammer," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1753–1757, Oct. 2020.

[102] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Trans. Inf. Forens. Security*, vol. 14, no. 1, pp. 129–140, Jan. 2019.

[103] 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.

[104] 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.

[105] 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.*, to appear.

[106] 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. Tech.*, vol. 70, no. 2, pp. 1989–1994, Feb. 2021.

[107] 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.

[108] 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.

[109] R. Xu, D. Guo, B. Zhang, and G. Ding, "Finite blocklength covert communications with random selection of channel use," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 2085–2089, Sept. 2021.

[110] S. W. Kim and H. Q. Ta, "Covert communications over multiple overt channels," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1112–1124, Feb. 2022.

[111] 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.*, to appear.

[112] 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.*, to appear.

[113] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," in *Proc. IEEE GLOBECOM'17*, pp. 1–6, Singapore, Dec. 2017.

[114] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communication with interference uncertainty," in *Proc. IEEE ICC'18*, pp. 1–6, Kansas City, MO, USA, Dec. 2018.

[115] 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. IEEE ACSSC'15*, pp. 625–629, Pacific Grove, CA, USA, Nov. 2015.

[116] L. Wang, G. W. Wornell, and L. Zheng, "Limits of low-probability-of-detection communication over a discrete memoryless channel," in *Proc. IEEE ISIT'15*, pp. 2525–2529, Hong Kong, China, Jun. 2015.

[117] H. Q. Ta and S. W. Kim, "Covert communication under channel uncertainty and noise uncertainty," in *Proc. IEEE ICC'19*, pp. 1–6, Shanghai, China, May 2019.

[118] 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 ICC'19*, pp. 1–6, Shanghai, China, May 2019.

[119] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Commun. Surv. Tut.*, vol. 9, no. 3, pp. 44–57, 3rd Quart. 2007.

[120] S. Zander, G. Armitage, and P. Branch, "Covert channels and countermeasures in computer network protocols," *IEEE Commun. Mag.*, vol. 45, no. 12, pp. 136–142, Dec. 2007.

[121] W. Mazurczyk and L. Caviglione, "Steganography in modern smartphones and mitigation techniques," *IEEE Commun. Surv. Tut.*, vol. 17, no. 1, pp. 334–357, 1st Quart. 2015.

[122] J. Ullrich, T. Zseby, J. Fabini, and E. Weippl, "Network-based secret communication in clouds: A survey," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1112–1144, 2nd Quart. 2017.

[123] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology: Proceedings of CRYPTO'83*, pp. 51–67, Plenum, 1983.

[124] R. Anderson, *Information Hiding, First International Workshop, Cambridge, U.K., May 30 - June 1, 1996, Proceedings*. Springer-Verlag, 1996.

[125] D. Schilling, L. Milstein, R. Pickholtz, M. Kullback, and F. Miller, "Spread spectrum for commercial communications," *IEEE Commun. Mag.*, vol. 29, no. 4, pp. 66–79, Apr. 1991.

[126] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[127] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread spectrum communications handbook*. McGraw-Hill Education, 2002.

[128] 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.

[129] K.-W. Huang, H.-M. Wang, and H. V. Poor, "On covert communication against sequential change-point detection," *IEEE Trans. Inf. Theory*, vol. 67, no. 11, pp. 7285–7303, Nov. 2021.

[130] 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.

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

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

[133] W. Chen, H. Ding, S. Wang, and F. Gong, "On the limits of covert ambient backscatter communications," *IEEE Commun. Lett.*, vol. 11, no. 2, pp. 308–312, Feb. 2022.

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

[135] 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.

[136] 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.

[137] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, "Covert communication over classical-quantum channels," in *Proc. IEEE ISIT'16*, pp. 2064–2068, Barcelona, Spain, Jul. 2016.

[138] 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.

[139] K. S. Kumar Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Trans Inf. Forens. Security*, vol. 14, no. 10, pp. 2787–2801, Oct. 2019.

[140] V. Y. F. Tan and S.-H. Lee, "Time-division is optimal for covert communication over some broadcast channels," *IEEE Trans. Inf. Forens. Security*, vol. 14, no. 5, pp. 1377–1389, May 2019.

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

[142] R. W. Smith and S. G. Knight, "Predictable three-parameter design of network covert communication systems," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 1, pp. 1–13, Mar. 2011.

[143] A. V. Nikitin and R. L. Davidchack, "Pulsed waveforms and intermittently nonlinear filtering in synthesis of low-SNR and covert communications," *IEEE Access*, vol. 8, pp. 173250–173266, 2020.

[144] 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.

[145] S. Huang, X. Hou, W. Liu, G. Liu, Y. Dai, and W. Tian, "Mimicking ship-radiated noise with chaos signal for covert underwater acoustic communication," *IEEE Access*, vol. 8, pp. 180341–180351, 2020.

[146] G. Leus and P. A. van Walree, "Multiband OFDM for covert acoustic communications," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 9, pp. 1662–1673, Dec. 2008.

[147] 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.

[148] X. Luo, P. Zhang, M. Zhang, H. Li, and Q. Cheng, "A novel covert communication method based on bitcoin transaction," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2830–2839, Apr. 2022.

[149] K.-H. Cho and S.-H. Lee, "Treating interference as noise is optimal for covert communication over interference channels," *IEEE Trans. Inf. Forens. Security*, vol. 16, pp. 322–332, 2021.

[150] 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.

[151] X. Yu, S. Wei, and Y. Luo, "Finite blocklength analysis of Gaussian random coding in AWGN channels under covert constraint," *IEEE Trans. Inf. Forens. Security*, vol. 16, pp. 1261–1274, 2021.

[152] Z. Xu, W. Lu, Y. Gong, J. Hua, and W. Jin, "A covert communication system using non-zero mean normal distributions," *Radioengineering*, vol. 29, pp. 580–588, Sep. 2020.

[153] H.-S. Im and S.-H. Lee, "Mobility-assisted covert communication over wireless Ad Hoc networks," *IEEE Trans. Inf. Forens. Security*, vol. 16, pp. 1768–1781, 2021.

[154] K.-H. Cho, S.-H. Lee, and V. Y. F. Tan, "Throughput scaling of covert communication over wireless adhoc networks," *IEEE Trans. Inf. Theory*, vol. 66, no. 12, pp. 7684–7701, Dec. 2020.

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

[156] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Covert communication using null space and 3D beamforming: Uncertainty of Willie's location information," *IEEE Trans. Veh. Tech.*, vol. 69, no. 8, pp. 8568–8576, Aug. 2020.

[157] Z. Liu, S. Li, Y. Zeng, and J. Ma, "Covert wireless communications in the presence of an active adversary," in *Proc. IEEE ICC'21*, pp. 1–6, Montreal, QC, Canada, Jun. 2021.

[158] M. Tahmasbi and M. R. Bloch, "Covert secret key generation with an active warden," *IEEE Trans. Inf. Forens. Security*, vol. 15, pp. 1026–1039, 2020.

[159] X. Chen, Z. Chang, N. Zhao, Y. Chen, F. R. Yu, and T. Hämäläinen, "Multi-antenna covert communication with jamming in the presence of a mobile warden," in *Proc. IEEE VTC'21-Spring*, pp. 1–6, Helsinki, Finland, Apr. 2021.

[160] X. Chen, M. Sheng, N. Zhao, W. Xu, and D. Niyato, "Finite-blocklength multi-antenna covert communication aided by a UAV relay," in *Proc. IEEE GLOBECOM'21*, pp. 1–6, Madrid, Spain, Dec. 2021.

[161] X. Chen, Z. Chang, J. Tang, N. Zhao, and D. Niyato, "UAV-aided multi-antenna covert communication against multiple wardens," in *Proc.IEEE ICC'21*, pp. 1–6, Montreal, QC, Canada, Jun. 2021.

[162] R. Xu, D. Guo, B. Zhang, and G. Ding, "Finite blocklength covert communications in interweave cognitive radio networks," *IEEE Commun. Lett.*, vol. 26, no. 9, pp. 1989–1993, Sept. 2022.

[163] Y. Zhang, W. He, X. Li, H. Peng, K. Rabie, G. Nauryzbayev, B. M. ElHalawany, and M. Zhu, "Covert communication in downlink NOMA systems with channel uncertainty," *IEEE Sensors J.*, vol. 22, no. 19, pp. 19101–19112, Oct. 2022.

[164] 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.

[165] X. Zhou, S. Yan, D. W. K. Ng, and R. Schober, "Three-dimensional placement and transmit power design for UAV covert communications," *IEEE Trans. Veh. Tech.*, vol. 70, no. 12, pp. 13424–13429, Dec. 2021.

[166] D. Wang, Q. Fu, J. Si, N. Zhang, and Z. Li, "Improper Gaussian signaling based covert wireless communication in IoT networks," in *Proc. IEEE GLOBECOM'21*, pp. 1–6, Madrid, Spain, Dec. 2021.

[167] S. Sodagari, "Covert communications against an adversary with low-SNR sensing capability in nakagami fading," *IEEE Sensors Lett*, vol. 4, no. 5, pp. 1–4, May 2020.

[168] J. Shelley, H. Mohammed, L. Zink, S. R. Hasan, and O. Elkeelany, "Covert communication channel detection in low-power battery operated IoT devices: Leveraging power profiles," in *Proc. IEEE SoutheastCon'18*, pp. 1–6, St. Petersburg, FL, USA, Apr. 2018.

[169] 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. Tech.*, vol. 69, no. 1, pp. 1080–1085, Jan. 2020.

[170] J. Hu, L. Wu, F. Shu, Y. Chen, and H. Zheng, "UAV-relay assisted covert communication with finite block-length," *J. Electronic Inf. Tech.*, vol. 44, no. 3, pp. 1006–1013, Mar. 2022.

[171] D. Mallikarachchi, K. Wong, and J. M.-Y. Lim, "Covert communication in multi-hop UAV network," *Ad Hoc Networks*, vol. 128, p. 102788, Apr. 2022.

[172] B. Kang, N. Ye, and B. Qi, "Comparisons on covert performances of NOMA in satellite internet of things," in *Proc. IEEE ComComAp'21*, pp. 318–322, Shenzhen, China, Nov. 2021.

[173] C. Chen, S. Wang, L. Li, S. Ke, C. Wang, and X. Bu, "Intelligent covert satellite communication for military robot swarm," *IEEE Access*, vol. 8, pp. 5363–5382, Dec. 2020.

[174] J. Wu, C. Chen, and X. Bu, "Polar code-aided frequency offset estimation algorithm in satellite covert communication carrier synchronization," in *Proc. IEEE ITNEC'20*, pp. 1340–1344, Chongqing, China, Jun. 2020.

[175] X. Lu, S. Yan, W. Yang, C. Liu, and D. W. K. Ng, "Short-packet covert communication in interweave cognitive radio networks," *IEEE Trans. Vehi. Tech.*, vol. 72, no. 2, pp. 2649–2654, Feb. 2023.

[176] 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.

[177] 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. Tech.*, vol. 71, no. 7, pp. 7936–7941, Jul. 2022.

[178] X. Chen, J. An, N. Zhao, C. Xing, D. B. d. Costa, Y. Li, and F. R. Yu, "UAV relayed covert wireless networks: Expand hiding range via drones," *IEEE Network*, to appear.

[179] L. Jiao, R. Zhang, M. Liu, Q. Hua, N. Zhao, A. Nallanathan, and X. Wang, "Placement optimization of UAV relaying for covert communication," *IEEE Trans. Veh. Technol.*, to appear.

[180] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, "A survey on technologies, standards and open challenges in satellite IoT," *IEEE Commun. Surv. Tut.*, vol. 23, no. 3, pp. 1693–1720, 3rd Quart. 2021.

[181] X. Yu, Y. Luo, and W. Chen, "Covert communication with beamforming over MISO channels in the finite blocklength regime," *Sci. China Inf. Sci.*, vol. 64, no. 9, pp. 1–15, Aug. 2021.

[182] 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.

[183] L. Yang, W. Yang, J. Tu, X. Lu, L. Tang, and Z. He, "Covert communication achieved by a full-duplex multi-antenna receiver in wireless networks," *J. Circuits, Systems Computers*, vol. 30, no. 14, p. 2150258, May. 2021.

[184] L. Yang, W. Yang, L. Tang, L. Tao, X. Lu, and Z. He, "Covert communication for wireless networks with full-duplex multiantenna relay," *Complexity*, vol. 2022, Jan. 2022.

[185] H. Du, D. Niyato, Y.-A. Xie, Y. Cheng, J. Kang, and D. I. Kim, "Performance analysis and optimization for jammer-aided multiantenna UAV covert communication," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 10, pp. 2962–2979, Oct. 2022.

[186] Q. Zhang, M. Bakshi, and S. Jaggi, "Covert communication over adversarially jammed channels," *IEEE Trans. Inf. Theory*, vol. 67, no. 9, pp. 6096–6121, Sept. 2021.

[187] W. He, J. Chen, G. Li, H. Wang, X. Chu, R. He, Y. Xu, and Y. Jiao, "Optimal transmission probabilities of information and artificial noise in covert communications," *IEEE Commun. Lett.*, to appear.

[188] C. Wang, Z. Li, and D. W. K. Ng, "Covert rate optimization of millimeter wave full-duplex communications," *IEEE Trans. Wireless Commun.*, to appear.

[189] X. Lu, E. Hossain, T. Shafique, S. Feng, H. Jiang, and D. Niyato, "Intelligent reflecting surface enabled covert communications in wireless networks," *IEEE Network*, vol. 34, no. 5, pp. 148–155, Sept./Oct. 2020.

[190] L. Zou, D. Zhang, M. Cui, G. Zhang, and Q. Wu, "IRS-assisted covert communication with eavesdroppers channel and noise information uncertainties," *Physical Commun.*, vol. 53, p. 101662, Aug. 2022.

[191] M. Li, X. Tao, N. Li, and H. Wu, "Energy-efficient covert communication with the aid of aerial reconfigurable intelligent surface," *IEEE Commun. Lett.*, vol. 26, no. 9, pp. 2101–2105, Sept. 2022.

[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. Forens. Security*, vol. 16, pp. 1959–1972, 2021.

[193] H. Rao, S. Xiao, S. Yan, J. Wang, and W. Tang, "Optimal geometric solutions to UAV-enabled covert communications in line-of-sight scenarios," *IEEE Trans. Wireless Commun.*, to appear.

[194] 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. Tech.*, vol. 68, no. 12, pp. 12135–12149, Dec. 2019.

[195] M. Wang, W. Yang, Y. Wang, L. Tao, and R. Ma, "Covert communications in uplink NOMA systems with channel inversion power control," in *Proc. IEEE ICCC'20*, pp. 317–321, Chengdu, China, Dec. 2020.

[196] C. Xing, S. Wang, S. Chen, S. Ma, H. V. Poor, and L. Hanzo, "Matrix-monotonic optimization — part I: Single-variable optimization," *IEEE Trans. Signal Process.*, vol. 69, pp. 738–754, 2021.

[197] C. Xing, S. Wang, S. Chen, S. Ma, H. V. Poor, and L. Hanzo, "Matrix-monotonic optimization — part II: Multi-variable optimization," *IEEE Trans. Signal Process.*, vol. 69, pp. 179–194, 2021.

[198] C. Xing, S. Ma, and Y. Zhou, "Matrix-monotonic optimization for MIMO systems," *IEEE Trans. Signal Process.*, vol. 63, no. 2, pp. 334–348, Jan. 2015.

[199] B. Yang, T. Taleb, Y. Fan, and S. Shen, "Mode selection and cooperative jamming for covert communication in D2D underlaid UAV networks," *IEEE Network*, vol. 35, no. 2, pp. 104–111, Mar./Apr. 2021.

[200] 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.

[201] 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.

[202] D. Deng, X. Li, S. Dang, M. C. Gursoy, and A. Nallanathan, "Covert communications in intelligent reflecting surface-assisted two-way relaying networks," *IEEE Trans. Veh. Tech.*, to appear.

[203] Y. Wu, S. Wang, J. Luo, and W. Chen, "Passive covert communications based on reconfigurable intelligent surface," *IEEE Wireless Commun. Lett.*, to appear.

[204] S. Pejoski, Z. Hadzi-Velkov, and N. Zlatanov, "Full-duplex covert communications assisted by intelligent reflective surfaces," *IEEE Commun. Lett.*, to appear.

[205] C. Wang, X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, and D. Niyato, "Covert communication assisted by UAV-IRS," *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 357–369, Jan. 2023.

[206] M. Wang, J. Tu, M. Wang, Y. Wang, H. Shi, and W. Yang, "Covert communications with channel inversion power control in uplink noma systems," *Electronics Lett.*, vol. 57, no. 9, pp. 360–362, Apr. 2021.

[207] Z. Hadzi-Velkov, S. Pejoski, and N. Zlatanov, "Achieving near ideal covertness in NOMA systems with channel inversion power control," *IEEE Commun. Lett.*, to appear.

[208] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14399–14417, Sept. 2021.

[209] B. Ji, Y. Wang, K. Song, C. Li, H. Wen, V. G. Menon, and S. Mumtaz, "A survey of computational intelligence for 6G: Key technologies, applications and trends," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7145–7154, Oct. 2021.

[210] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 65–71, Apr. 2022.

[211] H. Elayan, O. Amin, B. Shihada, R. M. Shubair, and M.-S. Alouini, "Terahertz band: The last piece of RF spectrum puzzle for communication systems," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1–32, Nov. 2020.

[212] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, Oct. 2018.

[213] 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.
[214] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling joint communication and radar sensing in mobile networksa survey," *IEEE Commun. Surv. Tut.*, vol. 24, no. 1, pp. 306–345, 1st Quart. 2022.
[215] C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proc. IEEE*, vol. 99, no. 7, pp. 1236–1259, Jul. 2011.
[216] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30845–30857, Feb. 2021.
[217] S. Ma, H. Sheng, R. Yang, H. Li, Y. Wu, C. Shen, N. Al-Dhahir, and S. Li, "Covert beamforming design for integrated radar sensing and communication systems," *IEEE Trans. Wireless Commun.*, to appear.
[218] 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. Tech. Mag.*, vol. 17, no. 3, pp. 54–64, Sept. 2022.
[219] H. Al-Hraishawi, M. Minardi, H. Chougrani, O. Kodheli, J. F. M. Montoya, and S. Chatzinotas, "Multi-layer space information networks: Access design and softwarization," *IEEE Access*, vol. 9, pp. 158587–158598, Nov. 2021.
[220] J. Shen, C. Wang, S. Ji, T. Zhou, and H. Yang, "Secure emergent data protection scheme for a space-terrestrial integrated network," *IEEE Network*, vol. 33, no. 1, pp. 44–50, Jan./Feb. 2019.
[221] Y. Wang, S. Yan, W. Yang, C. Zhong, and D. W. K. Ng, "Probabilistic accumulate-then-transmit in wireless-powered covert communications," *IEEE Trans. Wireless Commun.*, to appear.