Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6638405, 11 pages
https://doi.org/10.1155/2021/6638405

Research Article

A Survey of Cooperative Jamming-Based Secure Transmission for Energy-Limited Systems

Yuandong Wu and Yan Huo

School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China

Correspondence should be addressed to Yan Huo; yhuo@bjtu.edu.cn

Received 23 November 2020; Revised 25 December 2020; Accepted 7 January 2021; Published 15 January 2021

Academic Editor: Zhuojun Duan

Considering the ongoing development of various devices and rich applications in intelligent Internet of Things (IoT) systems, it is a crucial issue to solve secure transmission of legitimate signals for massive data sharing in the systems. Cooperative jamming-based physical layer security is explored to be a complement of conventional cryptographic schemes to protect private information. Yet, this method needs to solve a game between energy consumption and signal secure transmission. In this paper, we summarize the basics of cooperative jamming and universal security metrics. Using the metrics, we study a series of typical cooperative jamming strategies from two aspects, including power allocation and energy harvesting. Finally, we propose open issues and challenges of further works on cooperative jamming in an IoT system with energy constraints.

1. Introduction

The popularization of smart devices and corresponding applications in Internet of Things (IoT) systems, such as smart city, intelligent industry, and security surveillance, has penetrated modern life [1]. We heavily rely on these wireless smart devices for private information transmission. The rapid development of mobile computing prompts smart devices to receive wireless signals without restriction. Due to the broadcast nature of wireless channels, legitimate wireless signals are vulnerable to unauthorized receivers. Wiretap, caused by an eavesdropper, is a passive attack and does not interfere with legitimate transceivers. Though a legitimate receiver can receive untampered signals, the privacy leakage of these signals is unacceptable along with more attention to information security [2–4].

Multilayer-based mechanisms have been studied to increase the security and integrity of transmitted signals. These mechanisms, designed by traditional cryptography algorithms, are deployed in the high layers of the open system interconnection model [5–7]. However, the distribution and management of secret keys between wireless devices remain a challenge for cryptography-based security mechanisms [8]. Moreover, low-end IoT devices with limited computing capability and hardware resources cannot adopt highly complex cryptographic approaches [9, 10]. These increase the probability to eavesdrop on legitimate signals. Therefore, we need to introduce complementary or alternative information security measures for IoT devices and applications. Physical layer security (PLS) was first presented in Wyner's wiretap channel [11] and then extended to a Gaussian degraded wiretap channel in [12] and a general nondegraded wiretap channel in [13]. These works are a vital foundation for the following studies.

PLS exploits physical inherent characteristics of wireless channels to guarantee information security regardless of eavesdropper computing capability. It can provide low-layer protection without compromising the existing cryptographic technique-based security protection. Signal processing techniques such as beamforming, precoding, and diversity approaches contribute to PLS. Besides, cooperative jamming, first proposed in [14], is a mainstream technology of PLS, whose core idea is to hide legitimate signals within artificial noise (AN). Essentially, the inherent randomness of AN is used to stop eavesdropping to guarantee information security. At the same time, to avoid AN from interfering with legitimate receivers, it should be actively controlled.

Most cooperative jamming schemes interfere with eavesdroppers by AN while exploiting beamforming to cancel interference at destination nodes [15]. This idea should lead to much energy consumption. From the energy perspective, we should focus on not only secure performance but also energy efficiency for such security solutions due to massive deployed devices with low power and limited energy [16]. We summarize three reasons to illustrate why energy efficiency must be concerned in the cooperative jamming design. Firstly, IoT devices are usually designed as small, wireless portable electronics, whose batteries need to be recharged frequently. Next, batteries may pose huge safety risks in some deployments. Finally, it is not environment-friendly to dump billions of waste batteries.

Because energy constraints of low-end IoT devices hinder the application of cooperative jamming, recent works introduced an energy harvesting technology [17] and power allocation strategies to increase energy efficiency. However, there remain significant issues to realize efficient cooperative jamming with energy constraints. For example, current energy harvesting technologies only transfer small amounts of dynamic and unpredictable power for a small wireless device. Thus, in this paper, we need to survey numerous studies of cooperative jamming strategies with energy constraints. Our contributions are as follows.

(i) We formulate a general cooperative jamming model and present main metrics to measure security levels of signal transmission

(ii) We systematically review cooperative jamming strategies for limited energy scenarios in terms of optimal power allocation and wireless-powered methods

(iii) We raise a series of interesting open issues that need to be studied in depth to improve secure energy efficiency for physical layer security

The survey is organized as follows. Section 2 provides a general cooperative jamming model and the corresponding security performance metrics. Next, we present typical cooperative jamming schemes based on power allocation and energy harvesting to cope with energy constraints in a wireless transmission scenario in Section 3. We discuss a few interesting open research issues and the corresponding challenges in Section 4, and the conclusion of our survey will be given in Section 5.

2. Basics of Cooperative Jamming Schemes

In this section, we investigate a general cooperative jamming model and summarize typical secrecy metrics of cooperative jamming.

2.1. A General Cooperative Jamming Model. A typical wiretap model consists of a pair of transceivers (Alice and Bob) and an illegal passive eavesdropper (Eve) [18]. Eve intends to passively wiretap legitimate signals between transceivers. A traditional method is to broadcast encrypted signals to prevent Eve from wiretapping. However, the cryptographic method cannot satisfy security requirements of resource-constrained scenarios due to limited computational capabilities and insufficient energy. As a result, a physical layer-based solution provides additional protection via exploiting characteristic differences between a legitimate channel and a wiretapping channel.

A cooperative jamming scheme is a typical physical layer-based solution to broadcast artificial noise to block eavesdropping while not degrading the receiving performance of legitimate transceivers. The artificial noise is actively transmitted by the transceiver or a selected jammer, which is defined as self-cooperative jamming and non-self-cooperative jamming, shown in Figure 1. In essence, a transceiver in the self-cooperative jamming mode utilizes multiple antennas to transmit legitimate signals and artificial noise simultaneously while a friendly jammer in the non-self-cooperative jamming mode needs to optimize power allocation and design beamforming vectors to cover legitimate signals.

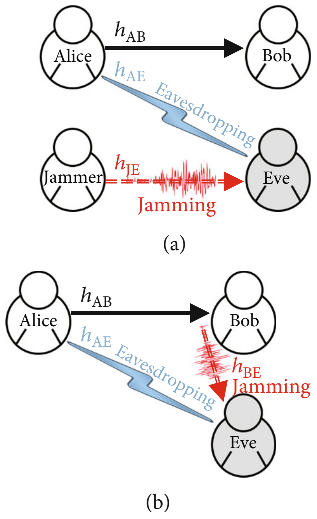
2.2. Security Metrics. Various metrics, i.e., bit error ratio of received signals, secrecy capacity, secrecy outage probability, and intercept probability, are considered to measure security performances of cooperative jamming schemes in different scenarios. We describe these metrics as follows.

2.2.1. Bit Error Ratio (BER). It is defined as a ratio of the number of error bits to the number of total transmitted bits in a certain period. It is used in the scenario where it only focuses on the decode error probability at receivers. BER of a receiver is affected by the signal energy per bit, the spectral density of interference and noise, channel fading parameters, and modulation methods. The received BER of an eavesdropper under BPSK modulation, for example, can be represented as follows:

$$p_e^{\mathrm{BPSK}} = \mathcal{Q}\left(\sqrt{\frac{2|h_{\mathrm{AE}}|^2 E_b}{N_0 + |h_{\mathrm{JE}}|^2 N_{\mathrm{J}}}}\right), \quad (1)$$

where h_{AE} and h_{JE} represent the channel states from Alice and Jammer to Eve, respectively. N_0 is the spectral density of the Gaussian white noise, and N_{J} denotes the time-averaged spectral density of jamming signals. $\mathcal{Q}(\cdot)$ is the complementary distribution function of the standard Gaussian and defined as $\mathcal{Q}(x) = 1/\sqrt{2\pi}\int_x^{\infty} \exp\left(-(t^2/2)\right)dt$.

2.2.2. Secrecy Capacity (SC). It is firstly proposed in [12] and can be defined as the maximum achievable perfect secrecy rate [19], i.e., $C_s = \sup_{p_e<\varepsilon} R_s$, where $p_e \triangleq \Pr(\bar{W} \neq W)$ is the error probability of message W and $\varepsilon > 0$ is a predefined error probability threshold for a given system. Here, W is the



(a)

(b)

Figure 1: Cooperative jamming-based physical layer security.

original messages and $\bar{W}$ represents the decoded messages at Bob. $R_s \triangleq H(W)/n$ is the secrecy rate, and $H(\cdot)$ denotes the entropy of the confidential messages. The secrecy capacity of the general wiretap channel is given by the following expression [20]:

$$C_s = \max_{p(u,x)} I(V\,;Y) - I(V\,;Z), \tag{2}$$

where $I(V\,;Y)$ and $I(V\,;Z)$ are the mutual information of an auxiliary random variable, V, and the received variable at Bob, Y, or the received variable at Eve, Z, when sending X at Alice, respectively. For a given channel, finding the secrecy capacity is equivalent to finding the joint distribution of V and X, i.e., $p(v,x), u \in U, x \in X$, which maximizes the difference in (2). As the result, the secrecy capacity for an average power constraint can be calculated as follows:

$$C_s = (C_Y - C_Z)^+ = \left(\frac{1}{2}\log_2(1+\gamma_B) - \frac{1}{2}\log_2(1+\gamma_E)\right)^+, \tag{3}$$

where γ_U is the signal-to-interference-plus-noise ratio of $U \in \{\text{Bob}, \text{Eve}\}$, $(x)^+$ represents $\max(0,x)$, and C_Y and C_Z, respectively, represent the channel capacities of the main and the wiretap channels. It is used when the state information of both legitimate channels and illegal channels is perfectly known. Note that Eve definitely intercept transmitted signals if the secrecy capacity is negative (i.e., the capacity of a legitimate channel falls below that of a wiretap channel). In this case, signal transmission from Alice to Bob should be insecure [21].

2.2.3. Secrecy Sum Rate (SSR). It is used to characterize the sum of the secrecy rate for n legitimate users when discussing the overall security requirements of a wireless system with several transmitters. It is a metric that optimizes the secrecy rate of the whole system rather than a specific legitimate channel:

$$R_{\text{sum}} = \sum_{i=1}^{n} ⊠R_s^i. \tag{4}$$

2.2.4. Secrecy Outage Probability (SOP). The SOP metric is a probability that the instantaneous security capacity is less than a nonnegative target secrecy rate R_s. It is also named the outage probability of SC. Considering a fading channel with an eavesdropper, SOP is a mainstream metric to analyze secrecy performance [22]. The SOP metric is formulated as follows:

$$P_{\text{out}}(R_s) = \Pr(C_s < R_s). \tag{5}$$

2.2.5. Connection Outage Probability (COP). The COP is defined as the probability that the SINR of the legitimate channel falls below the transmission threshold $\gamma^{\text{th}} = 2^{R_t} - 1$, where R_t represents the transmission minimum target rate [23]. It can be expressed as follows:

$$P_{\text{CO}} = \Pr\left(\gamma_t < \gamma_t^{\text{th}}\right). \tag{6}$$

2.2.6. Intercept Probability (IP). This metric is to describe the probability of an intercept event if the SC falls below zero [24]. Intuitively, it is related to the statistical characteristics of a legitimate channel and a wiretap channel when jamming signals are invalid:

$$P_{\text{int}} = \Pr(C_Y < C_Z). \tag{7}$$

2.2.7. Secrecy Energy Efficiency (SEE). The concept of SEE, η_{SEE}, is defined as a ratio of the secrecy rate to the total power consumption, i.e., the number of securely transmitted bits per unit energy [25]. It is an important metric for a scenario that considers both secure transmission and energy efficiency. We can find an optimal equilibrium between the secrecy rate and the total energy consumption when maximizing this metric:

$$\eta_{\text{SEE}} = \frac{R_s}{P_{\text{tot}}}, \tag{8}$$

where P_{tot} is the total power consumption for the complete transmission.

2.2.8. Secrecy Gap (SG). The secrecy gap is the SNR difference between a legitimate receiver and an eavesdropper. It can be calculated by a tight bound of the maximal secrecy rate [26]:

$$\Delta\gamma = \gamma_B - \gamma_E. \tag{9}$$

2.2.9. Worst-Case Secrecy Rate (WCSR). It is defined as the minimum secrecy rate when there are K eavesdroppers in an uncertain region [27], i.e.,

$$C_s = \left(C_Y - \max_{1\le k\le K} C_Z^k \right)^+ . \tag{10}$$

In addition, we use WCSR to optimize beamforming vectors, energy covariance at a transmitter, and AN covariance at a receiver, to minimize the legitimate channel capacity C_Y with power constraint [28],

$$C_s = \left(\min_{h\in\Omega_h} C_Y(h) - C_Z \right)^+ , \tag{11}$$

where h represents the estimated signal fading coefficient affected by the optimized factors mentioned above and Ω_h is the value range of h.

2.2.10. Secrecy Throughput (ST). This metric determines the average number of bits of confidential information received per unit time. We assume that the secrecy capacity is C_s, and a ratio of the transmission duration to the total time-slot is $(1-\alpha)$; then, the secrecy throughput is calculated as follows [29]:

$$\tau_s = (1-\alpha) C_s . \tag{12}$$

2.2.11. Power Consumption (PC). It is a power constraint to secure signal transmission. We can compare system performance when satisfying the same security requirements. Lower power consumption means higher energy efficiency.

3. Cooperative Jamming in Energy-Constraint Scenarios

The stored energy in devices is the key factor to achieve secure signal transmission, especially in an energy-constraint wireless system. Enough energy can ensure the simultaneous transmission of legitimate signals and artificial noise. There are two perspectives to design secure communication strategies with energy constraints, including optimal power allocation and the efficient wireless-powered method. The former focuses on the reasonable utility of limited energy in one period while the latter is aimed at harvesting much energy from wireless environments to support energy consumption.

3.1. Power Allocation-Based Cooperative Jamming Schemes. Power allocation is one of the mainstream solutions to the optimization problem of cooperative jamming-based physical layer security in an energy-constraint scenario. The transmit power and jamming power are the main factors to affect secrecy performance and transmission efficiency when sending legitimate signals to a wireless network. An unreasonable power allocation scheme may cause much decoding errors at a legitimate receiver or low secure transmission performance. Therefore, it is important to design a feasible power allocation scheme to ensure the effectiveness and security of signal transmission.

The existing works to design optimal power allocation are based on two assumptions. The first one is that the global channel state information (CSI) is perfectly available to all legitimate nodes, and the second one is that the CSI of eavesdroppers in the given networks is imperfect. According to these assumptions, the authors in [30] first proposed a scheme to determine antenna weights and optimize transmit power for a relay communication scenario with limited total system power. Then, the authors in [31] further studied a secure transmission strategy for a multiantenna amplify-and-forward (AF) wireless network with one eavesdropper. Their strategy exploited artificial noise sent by the receiver to superimpose legitimate signal broadcast to the relay in the first phase and perfectly removed the noise via the self-interference cancelation (SIC) technology at the receiver when in the forwarding phase. Their investigation on jamming power allocation strategy depended on either the known perfect CSI or the known statistical CSI. Similarly, the authors in [32] presented a half jamming power scheme to achieve secure transmission for a two-hop relaying network with four nodes. They provided the optimal percentage of jamming power to minimize SOP under different SNR scenarios.

Although a relay can forward legitimate signals and emit AN to degrade the receiving quality of Eve [43–47], it still has potential secrecy threats for signal transmission. For one thing, numerous eavesdroppers may surround a relay to intercept forwarded signals. In this case, the authors in [48] exploited the relay as a pure cooperative jammer without signal forwarding. They optimized power allocation between information-bearing signals at the transmitter and the AN at the relay to cope with the decreasing SC caused by the correlation between eavesdropping channels and legitimate channels. For another, an untrusted relay may intercept and wiretap confidential signals when forwarding these signals. The work of [49] jointly optimized power allocation for all nodes in an untrusted two-way relay network to maximize SEE subject to power and SC constraints.

In Table 1, we summarize a list of feasible power allocation schemes to achieve cooperative jamming in energy-constraint scenarios. We notice that the known perfect CSI is essential to achieve secure communications through optimal power allocation.

3.2. Wireless-Powered Cooperative Jamming. Although power allocation strategies achieve the optimal secure transmission performance with energy constraints, it is difficult to further increase the SC or decrease SOP by using limited energy. Energy harvesting (EH) is a promising technology to recharge their batteries by converting solar, thermoelectric, or electromagnetic energy into electricity [50]. As this technology realizes the proactive energy replenishment of wireless devices, it has advantages to support further cooperative jamming and achieve a self-sustainable secure communication system [51].

Radio frequency-based energy harvesting (RF-EH) is a feasible method to help wireless devices acquire energy from ambient radio signals. A generalized RF-EH network consists of RF energy sources (e.g., Powercast or even TV Tower),

Table 1: An overview of power allocation-based cooperative jamming schemes.

References	Assumptions	Metrics	Contributions
[33]	Perfect CSI	SC	Propose a fast algorithm to obtain asymptotically optimal cooperative jamming.
[34]	Perfect CSI	SC	Improve the SC for a scenario with limited power and a fixed number of antennas.
[35]	Perfect CSI	SC	Prove that the optimal power allocation depends on the global CSI and optimize SC subject to power constraints.
[36]	Perfect CSI	SC	Study the secrecy performance of partial cooperative jamming for single and multiple data transmission scenarios.
[37]	Perfect CSI	SC	Analyze the impact of the distance and the number of eavesdroppers on the secrecy performance for different transmission patterns.
[38]	Unknown CSI	SC	Propose a robust scheme in an unknown CSI scenario and demonstrate the similar secrecy performance between unknown and known CSI.
[39]	Statistical CSI	SOP	Minimize the SOP problem to obtain the optimal power allocation.
[40]	Statistical CSI	SOP	Derive closed-form and asymptotic expressions of the SOP for a dual-hop underlay uplink CRN operating under Nakagami-m fading channels.
[24]	Statistical CSI	IP	Propose a case study of physical layer security for a multiple relay scenario and evaluate the IP in Rayleigh fading environments.
[41]	Perfect CSI	SEE	Propose a beamforming scheme to maximize the SEE-based optimization problem in an underlay CRN cooperative jamming scenario.
[25]	Perfect CSI	SEE	Consider a joint source and relay power allocation scheme to maximize the system SEE.
[26]	Perfect CSI	SG	Demonstrate that a slightly reduced SC sharply decreases the received SNR of an eavesdropper.
[42]	Unknown CSI	WCSR	Optimize the flying trajectories and transmit power of unmanned aerial vehicles to improve the average WCSR of the system.

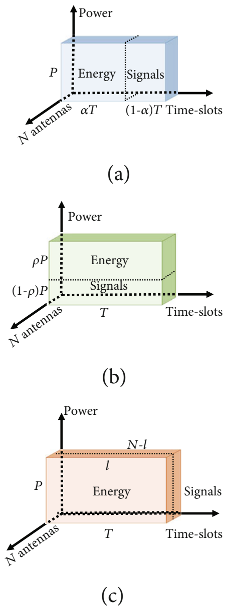
nodes (end users like sensors), and an information gateway (e.g., relay and base stations). The RF energy sources, whose spectrum to carry electromagnetic signals is from 3 kHz to 300 GHz, are the common infrastructures in daily lives. It attracts much attention as a viable solution to extend the lifetime of energy-constrained wireless networks. Though the fact that RF waves are available almost anywhere, the density in the environment is low. For example, the power density of Wi-Fi is only 1 mW/cm^2. In addition, the efficiency of energy harvesting is inversely proportional to the signal propagation distance. As a result, it is much more efficient to exploit a dedicated source as well as multiple-antenna techniques to transfer energy [52, 53].

Simultaneous wireless information and power transfer (SWIPT) is an efficient technology to broadcast information and RF energy signals to communicate with information nodes and power energy receivers [54]. Different from traditional energy harvesting methods, SWIPT harvests dedicated RF energy rather than other environmental energy. Using alternative patterns of information transmission and energy transfer, it prolongs the lifetime for an energy-constrained system with hardware limitations. In particular, three modes are designed to implement SWIPT in a practical scenario, i.e., the time switching (TS) mode, the power splitting (PS) mode, and the antenna switching (AS) mode, which are intuitively compared in Figure 2. The first mode exploits an orthogonal time-slot to receive signals and energy alternately by periodical switching antennas between an EH receiver and an information decoder. The second one splits received signals into two individual streams with different power levels. Last, the AS mode assigns a part of antennas for decoding signals while using the rest of the antennas to harvesting energy.

The SWIPT technology is usually used in a relay node to extend transmission ranges and provide additional services, e.g., cooperative jamming-based secure transmission. The relay node with SWIPT ensures legitimate signal forwarding and AN transmission via continuous energy replenishment. In particular, the existing works on SWIPT-based secure transmission include scenarios of static relay communications and unmanned aerial vehicle- (UAV-) enabled dynamic relay communications.

For static relay communications, the authors of [66] analyzed the impact of the number of antennas of the source, relay, and destination nodes on the secure performance of cooperative jamming for different multiantenna models. Then, the authors in [67] proposed an accumulate-then-transmit communication protocol. They employed a multiantenna power beacon to establish a secure wireless link for energy-constrained sources. In [68], the authors studied an RF-EH power splitting technique for a multiuser multiple-input-single-output interference channel. They designed beamforming vectors and the power allocation strategy to minimize the total transmitted power subject to the quality of service requirements and energy constraints. Similarly, the authors in [69] employed power splitting to design a robust secure transmission scheme for a multiple-input-single-output channel to minimize the WCSR under transmit power constraints and additional worst-case EH constraints.

Yet, the above schemes are based on the half-duplex signal transmission that cannot receive and transmit signals



(a)

(b)

(c)

Figure 2: The typical SWIPT modes.

simultaneously. To improve energy efficiency, some studies proposed full-duplex-based cooperative jamming methods because a jammer can broadcast AN and harvest energy simultaneously. A three-part energy-constrained SWIPT system with full-duplex self-jamming was proposed in [70]. They apply the TS SWIPT technology at the destination to extend battery lifetime. The source transmits the energy-bearing signals to the destination using maximal ratio transmission (MRT) to increase harvested energy in the EH phase. Based on their analysis, they derived the closed-form expressions of SOP and ST and then provided the optimal duration allocation and the maximum ST. Coincidentally, a wireless-powered full-duplex jammer in a four-node system is introduced in [71]. The authors employed the accumulate-and-jam protocol and discussed the impact of antenna allocation at the jammer on secure performance. They believed that increasing the number of antennas used for energy harvesting can enhance security when a source sends legitimate signals with low power.

For dynamic relay communications, relay nodes are deployed based on physical layer characteristics, such as channel state information (CSI), received signal strength (RSS), channel phase response, and channel impulse response (CIR). In [72], the authors considered a novel scenario that has no direct link between transceivers due to heavy shadow fading. They employed an energy-constrained UAV-enabled mobile relay to receive information and harvest energy simultaneously. The UAV exploits PS and TS protocols while the full-duplex destination can simultaneously receive forwarded signals from UAV and transmit AN signals to confuse eavesdroppers without perfect CSI. Their scheme can achieve a significant improvement in the max–min SC compared to the benchmark schemes.

Table 2 lists wireless-powered cooperative jamming schemes for energy-constrained systems.

4. Open Issues and Challenges

In this section, we first discuss a few interesting open research issues and novel technologies to improve energy efficiency and then present challenges to be solved.

4.1. Open Research Issues

4.1.1. The Optimal Friendly Jammer Selection. The optimal jammer selection leads to the best secure performance (the maximal SC or the minimal SOP) with the same energy consumption. The optimal jammer performs better than the other candidate jammers under energy constraints. Therefore, optimal jammer selection is an effective method to improve energy efficiency. In [73], the authors considered a wireless network with multiple sources and multiple relay nodes. Each relay node is equipped with a rechargeable battery. A novel minimum bottleneck matching algorithm and a suboptimal relay selection algorithm are proposed for the group lifetime maximization policy. For an EH-enabled secondary system in cooperative cognitive radio-based IoT, the authors of [74] presented a Vickrey auction-based relay selection strategy. This strategy can select an SU from several EH-enabled candidate SUs as a relay node while the unselected SUs keep harvesting energy. Moreover, works of [75, 76] demonstrate that joint power allocation and relay selection schemes can obtain better secrecy performance than the conventional jamming power allocation. Based on the existing studies, we note that it is a fundamental issue to select the optimal relay and jammer from a set of candidate nodes to extend the lifetime and improve the energy efficiency of a secure transmission system.

4.1.2. Intermittent Friendly Jamming. The optimal design of friendly jamming schemes is the core issue to achieve the best secure transmission performance and energy efficiency. Traditional continuous friendly jamming schemes can maximize SC or minimize SOP under the given energy constraints. However, these algorithms may waste energy to broadcast AN even though there is no legitimate signal transmission. Thus, some researchers studied intermittent jamming schemes to cope with issues of low SEE. Different from continuous jamming, an intermittent jammer transmits jamming signals on demand [77, 78]. Despite energy constraints, we can exploit intermittent jamming to ensure secure transmission and energy efficiency for it utilizes the idle duration of legitimate signal transmission to keep sleeping and harvest energy to improve SEE. The intermittent jammer can theoretically strike a tradeoff between the jamming effectiveness and energy savings by appropriately adjusting durations of transmission and sleeping and, finally, increase the lifetime of devices in an energy-constraint IoT system.

Take an intermittent jamming strategy proposed in [79] as an example. Different from traditional continuous jamming strategies, the intermittent jamming strategy proposed in this article is aimed at increasing the system security by shortening the jamming time but strengthening the jamming power. They compared the BER of intermittent jamming strategies and continuous jamming strategies and developed

Table 2: An overview of energy-constrained wireless-powered cooperative jamming.

References	Scenarios/assumptions	Metrics	Contributions
[29]	PS-based full duplex jamming/imperfect CSI	ST	Prove that a PS-based scheme outperforms a TS-based scheme for a delay-tolerant transmission mode and performs better for delay-constrained transmission only in specific scenario.
[55]	SWIPT-based AF half-duplex relay/perfect CSI	SC	Maximize SC subject to transmit power constraints by optimizing the transmit beamforming matrix of an AF relay and the covariance matrix of AN.
[56]	EH half-duplex relay/perfect CSI	SOP	Obtain a closed-form near-optimal TS ratio and the SOP exact expression for an EH-based jammer-assisted wireless sensor network.
[57]	SWIPT-based AF half-duplex relay/imperfect CSI	WCSR	Maximize WCSR by jointly optimizing the CB and the CJ covariance matrix along with the PS ratios for a relay with static power splitting and dynamic power splitting scenarios.
[58]	EH half-duplex jammer/imperfect CSI	ST	Achieve the best throughput subject to secrecy outage probability constraints by optimizing rate parameters.
[59]	SWIPT-based AF half-duplex relay/imperfect CSI	WCSR	Jointly optimize the AN covariance matrices at harvest-and-jam helpers and the AF relay beamforming matrix to maximize the WCSR.
[60]	SWIPT-based full-duplex relay/perfect CSI	SC	Study optimal power allocation in a secure OFDM-based SWIPT system with the help of a wireless-powered friendly jammer.
[61]	SWIPT-based full-duplex relay/imperfect CSI	PC	Prove that secure performance of the robust beamforming design is better than nonrobust ones for a practical multiradio wireless mesh network.
[62].	SWIPT-based full-duplex self-jamming/perfect CSI	COP, SOP, ST	Analyze COP, SOP, reliable-secure probability, and ST when multiple noncollusion eavesdroppers intercept confidential signals.
[63]	Half duplex destination-based-jamming SWIPT/imperfect CSI	SC	Design an AN-aided multicell coordinated beamforming scheme for SWIPT-enabled centralized and distributed manners by minimizing the total required power.
[64]	SWIPT-based AF half-duplex relay/imperfect CSI	SOP	Investigate the SOP for a TS-based SWIPT and destination-aided-jamming system with an untrustworthy AF relay.
[65]	EH full-duplex relay/imperfect CSI	SC and SOP	Propose a full-duplex jammer protocol whose key feature is that both relay and jammer are powered by source transmissions.

a new metric to jointly measure security requirements and energy cost, formulated an optimization problem with respect to the jamming duration proportion and jamming power, and examined the feasibility of intermittent jamming for different modulation methods. Accordingly, intermittent jamming is a feasible scheme to satisfy the requirements of secure performance and energy constraints. After solving the issues of when to jam and how to jam, it will surely become one of the practical cooperative jamming solutions.

4.1.3. Unknown CSI of an Eavesdropper. Almost all the existing cooperative jamming schemes are based on the assumptions of available perfect CSI or statistical CSI of all nodes in a wireless system. Yet, it is difficult to estimate the CSI of an eavesdropper perfectly especially when it is in the passive wiretapping mode. As a result, the performance with energy constraints in a practical scenario may be worse than its theoretical performance. Thus, the authors of [80] employed the space power synthesis technology to design a multijammer-based model to minimize synthetic jamming power at a legitimate receiver while satisfying predefined interference temperature in other locations. Although this scheme can securely transmit signals for an unknown CSI scenario within a fixed small area, multijammer-based cooperative jamming for a large-scale scenario may highly waste energy, which is difficult to achieve in an energy-limited system. As a result, future studies should consider how to design a cooperative jamming scheme for an unknown CSI scenario with energy constraints.

4.1.4. Cooperative Jamming for Intelligent Reflecting Surface. Intelligent reflecting surface (IRS) is a promising technology to engineer the radio signal propagation in wireless networks. IRS can dynamically alter a wireless channel to enhance communication performance via tuning massive reflecting elements. Different from the AF technology that uses energy to transmit signals, IRS only reflects signals by passive elements rather than generating new signals via a transmitter module. Thus, IRS adapts to an energy-constrained scenario well. In [81], the authors studied an IRS-assisted multiple-input-single-output system with cooperative jamming. They designed jamming beamforming matrices and the IRS phase-shift matrix to maximize energy efficiency. Considering the changeable CSI, the authors of [82] formulated a secure energy efficiency maximization problem subject to available power and the lowest rate constraints. Intuitively, IRS is envisioned to have abundant applications in future wireless networks. We need to consider issues such as how to integrate IRS into existing wireless systems, how to balance between signal transmission and energy consumption, and how many reflecting elements should be introduced.

4.1.5. Polar Code-Based Secure Transmission. The polar code has been regarded as a candidate technology for forward-error-correction (FEC) in the 5G air interfaces due to its excellent encoding/decoding capability and high reliability. Because using the polar code is able to improve the reliability of legitimate signals, a friendly jammer can consume less energy to ensure the transmission. Therefore, we can guarantee secure transmission by an energy-limited friendly jammer. For a discrete memoryless multiple-access wiretap channel, the authors in [83] proved that any feasible rate pair is achievable under strong secrecy with a low-complexity polar coding scheme. In essence, the reason for using polar codes to ensure physical layer security is that polarization creates a series of independent linear deterministic multiple access channels. These channels make it possible to design a resolvability-based code and thus achieve strong secure transmission. In [84], the authors minimized the number of cooperative helpers to fulfill a feasible SC requirement. They employed Tal-Sharov-Vardy implementation of polar codes to implement secure polar coding for a two-user Gaussian wiretap channel. Note that many modules and applications of a digital wireless communication system have the polarization effect that can improve ST and the received signal quality. Thus, it is one of the urgent issues to jointly optimize physical layer technologies with polar codes of future wireless communications to achieve optimal transmission performance.

4.2. Challenges of Future Works. Although the existing works on cooperative jamming with energy constraints have made progress, there are still many challenges unsolved.

Firstly, the study in [40] proved that a friendly jammer cannot contribute to the enhancement of system security in the presence of an important number of eavesdroppers. The reason is that cooperative jamming is to ensure that the average legitimate channel state is better than the wiretap channel state. Yet, multiple eavesdroppers may collude to achieve a better wiretap channel than a legitimate channel. As a result, the number, location, power, and social attributes [85] of selected jammers should be appropriately designed to protect from collusion eavesdropping.

Next, most current studies focus on static system models. Yet, a practical scenario with mobile nodes, such as intelligent industry or smart home, causes a dynamic wireless channel [86], which leads to inaccurate prediction or even difficult to predict. This indicates that the assumption of a perfect/statistical channel state is unrealistic. In addition, a mobile scenario results in wireless-powered nodes without sufficient energy supply [87]. The Doppler shift causes the mismatch between a cooperative node and a receiver, which impacts the performance of cooperative jamming cancelation [88]. Thus, one crux to use cooperative jamming in a practical application is how to design secure transmission for legitimate signals using various characteristics of changeable wireless transmission scenarios.

Finally, recent works merely design the management of harvested energy but ignore feasible scheme design to decide when to switch a relay as a transceiver or to keep idle. Besides, researches on SWIPT-based remote communications remain vacant. The battery power may be insufficient due to low harvesting efficiency caused by long distances.

5. Conclusion

In this article, we investigate cooperative jamming schemes for physical layer security for an IoT system with energy constraints. Our work starts with the necessity of physical layer security and introduces the basic knowledge and security metrics of cooperative jamming. Next, considering limited energy scenarios, we discuss the typical security optimization strategies from two aspects of power allocation and energy harvesting. In essence, the power allocation-based secure transmission focuses on the effective utilization of device energy while the energy harvesting is aimed at employing external energy to recharge. We believe that a feasible cooperative jamming scheme should exploit these two methods to jointly optimize so as to deal with the bottleneck of energy shortage in an IoT system. Finally, we propose related open issues as well as challenges to study cooperative jamming with novel technologies in the future for an IoT system with limited energy.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2019JBZ001, in part by the Beijing Natural Science Foundation under Grant 4202054, and in part by the National Natural Science Foundation of China under Grant 61871023 and Grant 61931001.

References

[1] Z. Cai and X. Zheng, “A private and efficient mechanism for data uploading in smart cyber-physical systems,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.

[2] J. Mao, S. Zhu, X. Dai, Q. Lin, and J. Liu, “Watchdog: detecting ultrasonic-based inaudible voice attacks to smart home systems,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8025–8035, 2020.

[3] X. Zheng, Z. Cai, and Y. Li, “Data linkage in smart internet of things systems: a consideration from a privacy perspective,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.

[4] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, “Follow but no track:Privacy preserved profile publishing in cyber-physical social systems,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1868–1878, 2017.

[5] Z. Cai, Z. He, X. Guan, and Y. Li, “Collective data-sanitization for preventing sensitive information inference attacks in social networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

[6] Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, and Z. Liang, "Man-in-the-browser-cache: persisting HTTPS attacks via browser cache poisoning," *Computer & Security*, vol. 55, pp. 62–80, 2015.

[7] Z. Cai and Z. He, "Trading private range counting over big iot data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.

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

[9] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[10] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.

[11] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[12] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[14] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference*, pp. 1906–1910, Dallas, TX, USA, 2005.

[15] M. Dehghan, D. L. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3025–3029, 2012.

[16] Z. Cai and Q. Chen, "Latency-and-coverage aware data aggregation scheduling for multihop battery-free wireless networks," *IEEE Transactions on Wireless Communications*, 2020.

[17] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure ofdm system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1331–1346, 2018.

[18] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[19] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[20] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[21] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis o cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *2013 IEEE International Conference on Communications (ICC)*, pp. 2183–2187, Budapest, Hungary, 2013.

[22] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, pp. 356–360, Seattle, WA, USA, 2006.

[23] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of csi feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2016.

[24] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[25] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 740–752, 2016.

[26] K. Fytrakis, N. Kolokotronis, K. Katsanos, and N. Kalouptsidis, "Optimal cooperative strategies for phy security maximization subject to SNR constraints," *IEEE Access*, vol. 8, pp. 119312–119323, 2020.

[27] L. Tang and Q. Li, "Wireless power transfer and cooperative jamming for secrecy throughput maximization," *IEEE Wireless Communications Letters*, vol. 5, no. 5, pp. 556–559, 2016.

[28] Z. Deng, Y. Gao, C. Cai, and W. Li, "Optimal transceiver design for swipt system with full-duplex receiver and energy-harvesting eavesdropper," *Physical Communication*, vol. 26, pp. 1–8, 2017.

[29] R. Ma, H. Wu, J. Ou, S. Yang, and Y. Gao, "Power splitting-based SWIPT systems with full-duplex jamming," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9822–9836, 2020.

[30] L. Dong, H. Zhu, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, pp. 417–420, Cardiff, UK, 2009.

[31] K. Park, T. Wang, and M. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1741–1750, 2013.

[32] Y. Choi and J. H. Lee, "Power allocation for cooperative jamming in amplify-and-forward relaying network with eavesdropper," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Glasgow, UK, 2015.

[33] J. Yang, S. Salari, I. Kim, D. I. Kim, S. Kim, and K. Lim, "Asymptotically optimal cooperative jamming for physical layer security," *Journal of Communications and Networks*, vol. 18, no. 1, pp. 84–94, 2016.

[34] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, 2011.

[35] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, Kyoto, Japan, 2011.

[36] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[37] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[38] P. Siyari, M. Krunz, and D. N. Nguyen, "Distributed power control in single-stream MIMO wiretap interference networks with full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 67, no. 3, pp. 594–608, 2019.

[39] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: optimal power allocation and secrecy outage analysis,"

IEEE Transactions on Vehicular Technology, vol. 66, no. 8, pp. 7495–7505, 2017.

[40] M. Bouabdellah, F. el Bouanani, and M.-S. Alouini, "A PHY layer security analysis of uplink cooperative jamming-based underlay CRNs with multi-eavesdroppers," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 704–717, 2020.

[41] Y. Wen, T. Jing, Y. Huo, Z. Li, and Q. Gao, "Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 795–799, Maui, HI, USA, 2018.

[42] Y. Li, R. Zhang, J. Zhang, S. Gao, and L. Yang, "Cooperative jamming for secure UAV communications with partial eavesdropper information," *IEEE Access*, vol. 7, pp. 94593–94603, 2019.

[43] G. Zheng, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.

[44] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.

[45] L. Chen, S. Han, W. Meng, C. Li, and M. Berhane, "Power allocation for single-stream dual-hop full-duplex decode-and-forward mimo relay," *IEEE Communications Letters*, vol. 20, no. 4, pp. 740–743, 2016.

[46] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[47] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu, and P. Zhang, "Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2682–2696, 2019.

[48] S. Xu, S. Han, W. Meng, Z. Li, C. Li, and C. Zhang, "Improving secrecy for correlated main and wiretap channels using cooperative jamming," *IEEE Access*, vol. 7, pp. 23788–23797, 2019.

[49] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: a physical layer approach," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 1861–1874, 2016.

[50] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, 2015.

[51] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: a contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.

[52] L.-G. Tran, H.-K. Cha, and W.-T. Park, "RF power harvesting: a review on designing methodologies and applications," *Micro and Nano Systems Letters*, vol. 5, no. 1, pp. 1–14, 2017.

[53] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative strategies for wireless-powered communications: an overview," *IEEE Wireless Communications*, vol. 25, no. 4, pp. 112–119, 2018.

[54] J. Huang, C.-C. Xing, and C. Wang, "Simultaneous wireless information and power transfer: technologies, applications, and research challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 26–32, 2017.

[55] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: improving security for wireless energy harvesting cooperative networks," in *2014 IEEE Global Communications Conference*, pp. 3145–3150, Austin, TX, USA, 2014.

[56] G. Hu and Y. Cai, "Analysis and optimization of wireless-powered cooperative jamming for sensor network over Nakagami-m fading channels," *IEEE Communications Letters*, vol. 23, no. 5, pp. 926–929, 2019.

[57] H. Xing, K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 7971–7984, 2016.

[58] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 401–415, 2016.

[59] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: a paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Transactions on Signal Processing*, vol. 63, no. 24, pp. 6616–6631, 2015.

[60] M. Liu and Y. Liu, "Power allocation for secure swipt systems with wireless-powered cooperative jamming," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1353–1356, 2017.

[61] L. Li, X. Zhao, S. Geng, Y. Zhang, and L. Zhang, "Robust beamforming design for SWIPT-based multi-radio wireless mesh network with cooperative jamming," *Information*, vol. 11, no. 3, p. 138, 2020.

[62] X. X. Tang, W. Yang, Y. Cai, W. Yang, and Y. Huang, "Security of full-duplex jamming SWIPT system with multiple non-colluding eavesdroppers," in *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 66–69, Macau, 2017.

[63] Y. Lu, K. Xiong, P. Fan, Z. Zhong, and K. B. Letaief, "Coordinated beamforming with artificial noise for secure SWIPT under non-linear EH model: centralized and distributed designs," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1544–1563, 2018.

[64] E. N. Egashira, E. E. B. Olivo, D. P. M. Osorio, and H. Alves, "Secrecy performance of untrustworthy AF relay networks using cooperative jamming and SWIPT," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, Istanbul, Turkey, 2019.

[65] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered fullduplex relay and friendly jamming for secure cooperative communications," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 621–634, 2019.

[66] K. Cao, B. Wang, H. Ding, and J. Tian, "Adaptive cooperative jamming for secure communication in energy harvesting relay networks," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1316–1319, 2019.

[67] Y. Bi and A. Jamalipour, "Accumulate then transmit: toward secure wireless powered communication networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6301–6310, 2018.

[68] S. Timotheou, I. Krikidis, G. Zheng, and B. Ottersten, "Beamforming for MISO interference channels with QoS and RF energy transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2646–2658, 2014.

[69] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and

power transfer in MISO channels," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 906–915, 2015.

[70] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, "Energy-constrained SWIPT networks: enhancing physical layer security with FD self-jamming," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 212–222, 2019.

[71] Y. Bi and H. Chen, "Accumulate and jam: towards secure communication via a wireless-powered full-duplex jammer," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1538–1550, 2016.

[72] W. Wang, X. Li, M. Zhang et al., "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4476–4489, 2020.

[73] S. Gupta and R. Bose, "Energy-aware relay selection and power allocation for multiple-user cooperative networks," in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–7, Doha, Qatar, 2016.

[74] Y. Huo, M. Xu, X. Fan, and T. Jing, "A novel secure relay selection strategy for energy-harvesting-enabled internet of things," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, 18 pages, 2018.

[75] Y. Choi and J. H. Lee, "A new cooperative jamming technique for a two-hop amplify-and-forward relay network with an eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12447–12451, 2018.

[76] D. Li, X. Zhang, and Y. Shang, "Joint physical network coding and destination aided cooperative jamming for secure wireless sensor networks," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Nanjing, China, 2016.

[77] O. Besson, P. Stoica, and Y. Kamiya, "Direction finding in the presence of an intermittent interference," *IEEE Transactions on Signal Processing*, vol. 50, no. 7, pp. 1554–1564, 2002.

[78] Z. Cai, S. Ji, J. He, and A. G. Bourgeois, "Optimal distributed data collection for asynchronous cognitive radio networks," in *2012 IEEE 32nd International Conference on Distributed Computing Systems*, pp. 245–254, Macau, China, 2012.

[79] Q. Gao, Y. Huo, T. Jing, L. Ma, Y. Wen, and X. Xing, "An intermittent cooperative jamming strategy for securing energy-constrained networks," *IEEE Transactions on Communications*, vol. 67, no. 11, pp. 7715–7726, 2019.

[80] L. Huang, X. Fan, Y. Huo, C. Hu, Y. Tian, and J. Qian, "A novel cooperative jamming scheme for wireless social networks without known csi," *IEEE Access*, vol. 5, pp. 26476–26486, 2017.

[81] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy-efficient beamforming and cooperative jamming in irs-assisted miso networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, Dublin, Ireland, 2020.

[82] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network: joint active and passive beamforming design," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Abu Dhabi, United Arab Emirates, 2018.

[83] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7903–7921, 2018.

[84] M. Hajimomeni, K. Kim, H. Aghaeinia, and I.-M. Kim, "Cooperative jamming polar codes for multiple-access wiretap channels," *IET Communications*, vol. 10, no. 4, pp. 407–415, 2016.

[85] X. Zheng, Z. Cai, J. Li, and H. Gao, "Location-privacy-aware review publication mechanism for local business service systems," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.

[86] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[87] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[88] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu, and Y. Tang, "Effect of frequency offset on cooperative jamming cancellation in physical layer security," in *2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–5, Abu Dhabi, United Arab Emirates, 2018.