Secure Wirelessly-Powered Networks at the Physical Layer: Challenges, Countermeasures, and Road Ahead

Xiao Lu, Nguyen Cong Luong, Dinh Thai Hoang, Dusit Niyato, Yong Xiao and Ping Wang

***Abstract*—Harvesting wireless power to energize miniature devices has been envisioned as a promising solution to sustain future-generation energy-sensitive networks, e.g., Internet-of-things systems. However, due to the limited computing and communication capabilities, wirelessly-powered networks (WPNs) may be incapable of employing complex security practices, e.g., encryption, which may incur considerable computation and communication overheads. This challenge makes securing energy harvesting communications an arduous task, and thus limits the use of WPNs in many high-security applications. In this context, security at the physical layer (PHY) that exploits the intrinsic properties of the wireless medium to achieve secure communication has emerged as an alternative paradigm. This article first introduces the fundamental principles of primary PHY attacks, covering jamming, eavesdropping and detection of covert, then presents an overview of the prevalent countermeasures to secure both active and passive communications in WPNs. Furthermore, a number of open research issues are identified to inspire possible future research.**

***Index Terms*—Physical-layer security, jamming, eavesdropping, detection-of-covert, information-theoretical security, denial-of-service, artificial noise, beamforming.**

I. Introduction

Thanks to the recent advances in antenna techniques and realizations of highly efficient energy harvester and antenna designs [1], [2], radio frequency (RF) based wireless power transfer (WPT) becomes a feasible approach to charging miniature wireless devices [3]–[6]. This solution enables energy replenishment, and thus self-sustainable operation [7], of remote low-power devices (e.g., wireless sensors and actuators [8]), facilitating the development of broad applications driven by household and industrial needs. Despite the promising application prospects, securing communications in wirelessly-powered networks (WPNs) is challenging since they may be incapable of employing the current practice of wireless security [9], e.g., encryption, in conventional networks. Considering encryption for instance, the limited computing and communication capability imposed by the hardware and energy constraints make it difficult to manage and distribute the cryptographic keys in WPNs.

To address the challenge, physical-layer (PHY) countermeasures have drawn considerable attention, especially, in the study of WPNs. At the heart of this endeavour is the belief that PHY security approaches have the potential to provide radical protection against attacks. Securing communication at the PHY is fundamentally different from that at the higher layers (e.g., the application layer) which mostly rely on cyber-enabled techniques, e.g., encryption, integrated into the protocol stack [10]. In essence, PHY security approaches shield communications by only exploiting the intrinsic properties of the wireless medium (e.g., noise, fading and interference), which averts incurring the excessive computing and signalling overheads required in higher-layer encryption approaches.

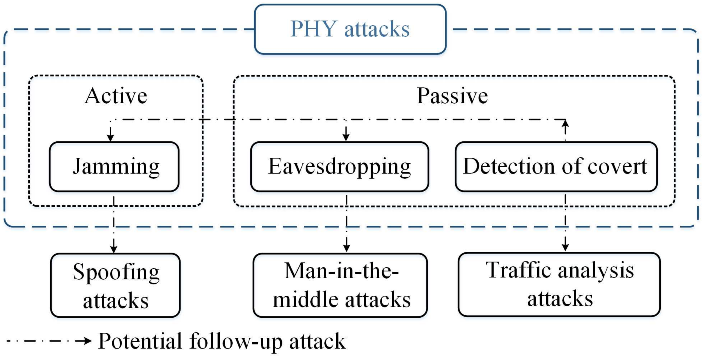


Fig. 1. PHY attacks and potential follow-up attacks.

Jamming, eavesdropping and detection of covert (DoC) are the most common PHY attacks, which can be sorted into two forms, i.e., active and passive, as shown in Fig. 1. Active attacks intentionally cause malfunctions (e.g., denial of service) of the target networks. By contrast, passive attacks intend to extract information by monitoring wireless channels instead of intervening in the network operation. Once legitimate communications are breached at the PHY, an advanced adversary can further initiate various other forms of attacks, which are not limited to PHY security attacks. As exampled in Fig. 1, once identifying the presence of a target through DoC, an adversary can further eavesdrop and jam the target's channel. Instances of cross-layer attacks include 1) Spoofing attacks to falsify the identity of a legitimate node, the signals of which have been blocked through jamming; 2) Man-in-the-middle attacks to inject the tampered data intercepted through eavesdropping; 3) Traffic analysis attacks to deduce information from the communication patterns obtained through DoC attacks. It is evident that safeguarding communication at the PHY is of profound importance as it has the potential to offer built-in protection to complement the upper-layer security designs.

This article aims to provide a comprehensive review of the state-of-the-art countermeasures to PHY attacks in WPNs, directing the interested readers to the fundamentals, existing progress and open issues. Although surveys of wireless security techniques have been well established, systematic reviews on PHY security techniques for WPNs are still lacking. Reference [11] offers an overview of PHY security methodologies for

X. Lu and P. Wang is with York University, Canada. X. Lu is also with Ericsson, Canada. N. C. Luong is with Phenikaa University, Vietnam. D. T. Hoang is with University of Technology Sydney, Australia. D. Niyato is with Nangyang Techngical University, Singapore. Y. Xiao is with Huazhong University of Science and Technology, China. (N. C. Luong is the corresponding author.)

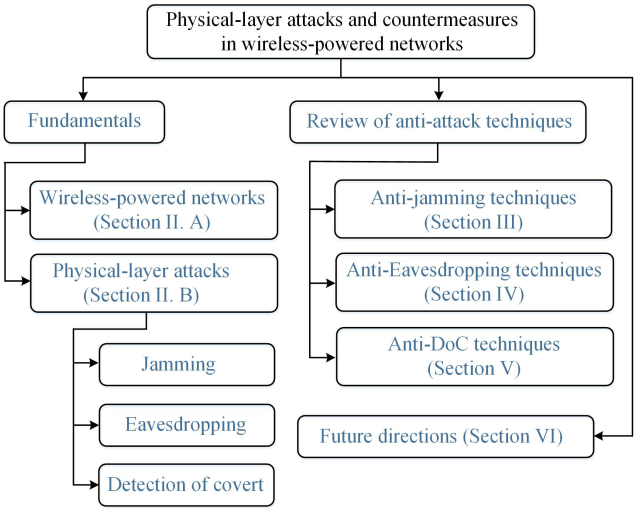

Physical-layer attacks and countermeasures in wireless-powered networks
Fundamentals
Review of anti-attack techniques
Wireless-powered networks (Section II. A)
Physical-layer attacks (Section II. B)
Jamming
Eavesdropping
Detection of covert
Anti-jamming techniques (Section III)
Anti-Eavesdropping techniques (Section IV)
Anti-DoC techniques (Section V)
Future directions (Section VI)

Fig. 2. Organization of this article.

general wireless networks. The comprehensive survey in [12] covers wiretap code, multi-antenna, relaying, key generation, and authentication techniques to address eavesdropping attacks at the PHY. Reference [13] surveys anti-eavesdropping designs at the PHY before 2018. Differently, references [14] and [15] offer specialized surveys on the anti-eavesdropping techniques designed for satellite networks and developed based on optimization methods, respectively. Other than literature addressing eavesdropping attacks, existing efforts have been devoted to reviews and surveys addressing jamming attacks in wireless networks with disparate focuses. A taxonomic survey on jamming and anti-jamming strategies in conventional wireless networks is presented in [16]. Reference [17] presents a review of the detection methods for different types of jamming attacks. Besides, countermeasures of jamming attacks in wireless sensor networks and cognitive radio networks can be found in [18] and [19], respectively. Nevertheless, a survey of anti-DoC approaches is still missing in the literature. To the best of our knowledge, there is no review that particularly explores the PHY security techniques in WPNs, which motivates our efforts in this work.

Contributions: The main contribution of this article is threefold. First, we provide a brief overview of active and passive/backscatter WPNs and the common PHY attacks that they are facing. Second, we present an up-to-date review on the anti-attack techniques for WPNs with their principles, advantages and disadvantage discussed in detail. Third, we discuss addressed issues and highlight future directions. The organization of the remainder of this article is outlined in Fig. 2.

The acronyms used throughout the article are listed in Table I.

TABLE I
List of Acronyms.

Acronym	Full name
WPAC	Wirelessly-powered active communication
WPBC	Wirelessly-powered backscatter communication
WPN	Wirelessly-powered networks
WPT	Wireless power transfer
WPAT	Wireless-powered active transmitter
AN	Artificial noise
SWIPT	Simultaneous wireless information and power transfer
DoC	Detection of covert
PHY	Physical layer
CSI	Channel state information

II. Overview of Security Issues in Wirelessly-Powered Communication Systems

This section first describes the basic principles of wireless-powered communications and then expounds on the PHY attacks in WPNs.

A. *Fundamentals of Wireless-Powered Communications*

Recent developments in WPT and RF energy harvesting hardware [20], [21] have made a substantial impact on low-power communication research as well as commercial applications. From the types of energy sources, wireless-powered communications can be classified as *wireless-powered active communications* (WPAC) and *wireless-powered backscatter communications* (WPBC).

1) WPAC: WPAC uses the harvested RF energy to actively generate RF signals for communication. Compared with conventional battery-powered communication, WPAC involves an energy harvesting process to support RF signal generation. Specifically, equipped with an RF energy harvester, a wireless-powered active transmitter (WPAT) is able to harvest energy from RF signals from a power beacon, i.e., an RF energy source enabled with WPT capability, and store the harvested energy for its circuit operation (e.g., signal processing) and communication purpose.

With a dedicated power beacon, the transmit power, frequency and time in WPAC can be fully controlled to provide reliable WPT according to different quality-of-service (QoS) requirements. This is in contrast to renewable energy-powered communications, in which the energy sources (e.g., solar and wind) can be time-varying and uncontrollable. Compared with battery-powered communication, WPAC eliminates the need for battery replacement or recharging. Nevertheless, deploying a dedicated power beacon incurs an extra infrastructure cost. Another disadvantage is that the WPAT is only functional within the energy provisioning zone of the power beacon. Additionally, the WPAT has to accumulate sufficient energy first before performing communications. This operation causes a time delay and makes WPAC hard to support low-latency communication service [22], [23].

Existing literature has presented comprehensive surveys on WPAC regarding WPT strategies [4], beamforming designs [24], simultaneous wireless information and power transfer (SWIPT) [26] and hardware realizations [21]. Again, none of them discusses security issues.

2) WPBC: Different from WPAC, which relies on active RF generation for transmission, WPBC passively backscatters existing RF signals for transmission based on the impedance mismatching technique [27], [28]. Specifically, a backscatter transmitter can selectively tune the load impedance of the antenna to reflect the incident carrier signals (i.e., continuous waves generated by a carrier emitter), with modified amplitude, frequency, and/or phase to its intended receiver. Different from a WPAT that can initiate a transmission by itself, a backscatter transmitter relies on the carrier signals from the carrier emitter for initiation. Specifically, to perform a backscatter transmis-

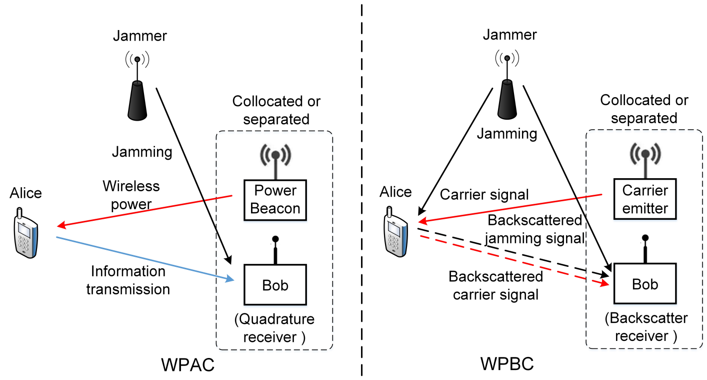


Fig. 3. Illustration of jamming attacks in WPNs.

sion, the carrier emitter needs to generate carrier signals from which the backscatter transmitter can harvest energy through rectifying. Once the rectified voltage reaches the required level, the backscatter transmitter is activated to perform *impedance matching*, generate modulated backscatter based on the carrier signals. Hence, WPBC is capable of simultaneous backscattering and energy harvesting.

Since the RF signal generation is offloaded to an external carrier emitter, a backscatter transmitter can be realized with a simpler and lower-cost hardware design, lower cost, ultra-low power consumption, and small form factor than a battery-power device and a WPAT [29]. Despite these merits, WPBC achieves a low bitrate due to low-order constellations typically supported by the simple hardware [30]. Additionally, due to the two-hop path loss, i.e., from the carrier emitter to the backscatter transmitter and from the backscatter transmitter to the backscatter receiver, the effective transmission range is limited.

A comprehensive survey of the principles, architectures, network protocols, hardware designs and applications of WPBC is available in [30]. Moreover, a tutorial of the backscatter basics and review focused on Internet of things-related backscatter applications can be found in [29]. Additionally, Table II highlights the differences among WPAC, WPBC and battery-powered communication.

B. Physical-layer attacks

1) Jamming: Jamming is a common form of denial-of-service (DoS) attacks launched at the PHY in which intruders flood artificial noise (AN) to harm legitimate use of communication medium [31], [32]. By such, jamming could cause negative effects as follows:

- A legitimate transmitter backs off as it always senses busy channels, and
- The desirable signals are corrupted by the overwhelming AN, making them undecodable at the target receiver.

Both effects damage communication *availability*, making network services unavailable to legitimate users. Wireless transmission is very susceptible to jamming attacks as it is always possible for an attacker to inject AN over the wireless medium. An attacker can generate AN to cause the target nodes to suffer from DoS as long as their operating channels can be identified [33]. The harmfulness of jamming attack can be assessed from several aspects [34], including: 1) energy efficiency; 2) probability of detection (stealthiness); 3) robustness against anti-jamming techniques; and 4) level of resultant DoS.

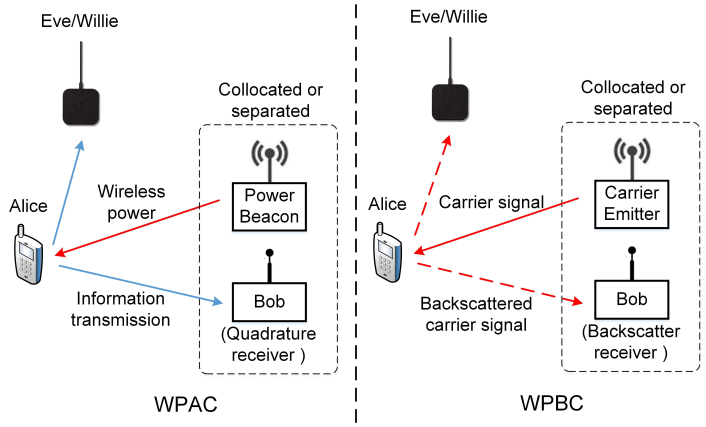


Fig. 4. Illustration of eavesdropping and DoC attacks in WPNs.

A simple illustration of jamming attacks in WPNs is shown in Fig. 3, which consists of four entities: the power beacon, the authorized transmitter (Alice), the intended receiver (Bob) and the malicious jammer. The legitimate transmission (either WPAC or WPBC) between Alice and Bob is the target that the jammer aims to disturb and disrupt. Compared with WPAC, WPBC can be more vulnerable to jamming attacks as both the carrier signal and the modulated backscatter are impaired by the jamming signals.

Different from battery-powered wireless networks where jamming causes only negative effects, notably, a WPAT can harvest energy from jamming signal (i.e., through RF-to-DC conversion) to facilitate legitimate transmission [35]. Hence, through the smart operation of WPNs, it is possible to transform the adversarial jamming into a positive effect. The crux of successfully exploiting jamming signals is to identify the key features of different jamming attacks. The principles of designing anti-jamming schemes in WPNs are detailed in Section III.

2) Eavesdropping: Eavesdropping is a passive form of attack that secretly intercepts private information (e.g., verification code, identification numbers, or application-specific data) over an open wireless medium without authorization. To launch the eavesdropping attack, the attacker requires the knowledge of the encryption key to decipher from the captured signals. Such knowledge may be publicly available, especially for many civilian applications. For instance, open-source software like Wireshark [36] can be configured to snoop WiFi signals. Besides, the hopping sequence adopted for Bluetooth transmission can be determined by third-party devices, such as GNU radio [37]. Eavesdropping attackers breach communication *confidentiality* as private information can be snooped and revealed to the third party and even the public. Compared with the jamming attack, an eavesdropping attack can be hard to detect if the attacker remains silent.

Eavesdropping attacks can be typically addressed through encryption at the application/representation layer and/or information theoretic security approach at the PHY. The former masks confidential contents with secret code so that although

TABLE II
COMPARISON OF COMMUNICATION PARADIGMS.

Communication Paradigm	RF signal generation	Transmit/backscatter power control	Circuit power consumption	Transmission range	Form factor	Limited operation zone
Wirelessly-powered active communication	Yes	Yes	Higher	Longer	Larger	Yes
Wirelessly-powered backscatter communication	No	Yes	Lower	Shorter	Smaller	Yes
Battery-powered communication	Yes	Yes	Higher	Longer	Larger	No

TABLE III
COMPARISON OF PHY ATTACKS.

PHY attacks	Principle	Stealthiness	Breach
Jamming	DoS through AN	Low	Availability
Eavesdropping	Intercepting confidential message	High	Confidentiality
Detection of covert	Detection of presence	High	Stealthiness

the signals can be intercepted by the eavesdropper, their true meaning might not be uncovered. The latter aims to achieve a positive secrecy capacity, which is the difference between the capacity of the legitimate channel and that of the wiretapping channel. Accordingly, a sufficient amount of the secret message can be hidden from the eavesdropper successfully [12]. Thus, in principle, foiling an eavesdropping attack typically involves either or both of boosting the legitimate capacity and diminishing the wiretapping capacity.

A typical eavesdropping attack in WPNs is shown in Fig. 4, where the eavesdropper (Eve) wants to decipher the legitimate transmission (either WPC or modulated backscatter) from Alice. Different from battery-powered networks, wireless power and carrier signals can be exploited to facilitate communication secrecy in WPAC with in-band energy harvesting and WPBC, respectively. Specifically, the power beacon and carrier emitter can generate signals based on the secret key pre-shared with Bob. As such, the generated signals can be eliminated at Bob while causing interference at Eve to detriment its decodability.

3) Detection of covert: A DoC attack aims to detect the presence of a target through passive listening. Due to its stealth nature, discovering a DoC attack can be a challenging task. Wireless communication is more vulnerable to the DoC attack than the eavesdropping attack as even if the transmission is encrypted, its transmission behavior may still be exposed to adversaries. A DoC attack is usually supported by traffic analysis to deduce knowledge from the observed communication patterns. By analyzing the communication patterns, the DoC attack has the potential to deduce some critical information. For instance, bursty and frequent communications may indicate the planning progress for activity, while the absence of communications may hint at activity in progress as scheduled. Some other typical information that can be extracted and/or implied includes position, trajectory and speed, based on which the adversaries can further launch other forms of attacks. Thus, DoC attacks diminish the stealthiness of communication. Generally, making the transmission undetectable provides a stronger level of security than secrecy communication. There appear increasingly more cases where a breach of covertness can lead to grave consequences. Such examples range from exposure of confidential business activities to failure of secret military operations.

A typical DoC attack in WPNs is shown in Fig. 4, where the warden (Willie) aims to determine if Alice is in the transmission or idle status, which is a binary decision problem. To this end, Willie can analyze the signal samples collected over time based on a statistical hypothesis test, with the null and non-null hypotheses inferring that Alice is off and on transmission, respectively. In the process of the hypothesis test, Willie tolerates some errors when his test incorrectly represents the true status of Alice. Specifically, Willie makes two types of errors, namely, false alarm and miss detection, also referred to as Type I error and Type II error, respectively [38]. The former occurs when Alice is idle while Willie rejects the null hypothesis. The latter happens if Alice is on transmission while Willie rejects the non-null hypothesis. The performance of the hypothesis test (i.e., the detection performance of Willie) can be measured by the detection error probability [39], which is the sum probabilities of false alarm and miss detection.

To cope with DoC attacks, and thus ensuring *covert communications* between Alice and Bob, the detection error probability of Willie needs to be maintained at a high value. In principle, the detection error probability can be increased by augmenting the uncertainties of the received signal samples including 1) noises uncertainty, 2) channel uncertainty (e.g., fading), 3) Alice's signal uncertainty (e.g., through power control) and 4) interference uncertainty [40]. Additionally, different from battery-powered networks, the power beacon and carrier emitter in WPNs can be employed to generate AN to increase the uncertainty of signal samples. The detailed techniques are reviewed in Section V.

III. ANTI-JAMMING TECHNIQUES IN WPNS

Existing research efforts mainly focus on addressing jamming attacks for WPAC with that for WPBC left unaddressed. Hence, this section focuses on reviewing the anti-jamming techniques for WPAC.

A. Challenges

The development of WPNs can address many problems for future wireless communication networks with low-power consumptions. However, it also places new challenges, especially problems related to PHY security. In particular, different from conventional wireless communication networks, WPNs often experience two phases. In the first phase, wireless nodes need to harvest energy broadcast from RF sources in surrounding environments. After that, the harvested energy will be stored in energy storage and used to transmit data in the second phase. Consequently, such kind of networks is very vulnerable to radio jamming attacks. The main reason is that, in such networks, jammers only need to focus on the data transmission phase. Furthermore, the amount of energy harvested from RF signals is usually very little compared with the amount of energy supplied from stable energy sources. Thus, the transmit power of a WPAT is usually very low compared with those of conventional wireless communication networks. Thus, jamming attacks can be easily launched through off-the-shelf products. This causes serious concerns for the deployment of WPAC in practice, especially for data-sensitive wireless applications, e.g., healthcare, road traffic control and military operation.

To deal with jamming attacks, existing literature [41] has introduced many solutions, e.g., power control, rate adaption and frequency hopping. However, these solutions may not be effective and sometimes infeasible to deploy for WPAC. For example, power control approaches may be only effective when a transmitter can transmit data at a very high power compared with that of the jammer. Nevertheless, WPATs usually have meager transmission power due to the limited amount of harvested energy. Therefore, such solutions are ineffective, or even infeasible, to implement in practical WPNs. Alternatively, other solutions, e.g., rate adaption and frequency hopping, which are widely considered to be effective anti-jamming solutions in conventional wireless communication networks, may not be suitable to be adopted due to hardware constraints of WPATs. Therefore, novel solutions which can effectively address jamming attacks for WPAC are in urgent need.

B. Emerging Countermeasures

Existing countermeasures to deal with the jamming attacks for WPAC can be sorted into two groups. Specifically, the first group focuses on applying advanced technologies (e.g., ambient backscatter communications and RF energy harvesting techniques) to exploit and utilize jamming signals, and thereby improving system performance for WPAC. The second group focuses on developing deception strategies to lure jammers, thereby undermining them and making them unable to attack with high efficiency. In the following, we will discuss the solutions in detail as well as analyze their pros and cons for implementation.

1) Ambient RF Energy Harvesting and Ambient Backscattering Techniques:

Ambient RF Energy Harvesting Techniques: Ambient RF energy harvesting is an emerging technology that allows wireless devices to harvest energy from RF signals in the surrounding environments [42]–[44]. The key principle of this technique is to transform received ambient RF signals into usable direct current [45], [46]. Inspired by this principle, a novel idea is developed to help WPAC to deal with radio jamming attacks. In particular, when a jammer launches attacks by sending strong jamming signals to the communication channel, the WPAT can harvest energy from jamming signals. As such, when the jammer does not attack the channel, the WPAT can use the harvested energy from jamming signals to transmit data. One interesting point of this solution is that jammers often attack at very high power levels, and thus the amount of harvested energy is usually much higher than that of the normal RF signals (e.g., from WiFi or TV signals). As a result, if we can properly manage jamming signals, they can be used to enhance the performance of WPAC.

One of the very first research works which consider using ambient RF energy harvesting technique to deal with jamming attacks is [41]. In this work, the authors consider a two-way WPAC with a hostile jammer placed in between a base station and WPAT. The base station is assumed to be a powerful device with a fixed power supply, while the WPAT is able to harvest energy from surrounding RF signals (e.g., from the base station and/or from the jammer). In the downlink, when the base station transmits data to the WPAT, the received signals will be split into two parts, one for harvesting energy and another one for extracting information. In the uplink, the WPAT will use all the harvested energy together with its own power supply to transmit data to the base station. Given jamming attacks on both uplink and downlink channels at a fixed jamming power, the authors then formulate a sum-rate maximization problem and propose a low-cost approximation method to find the optimal settings for the considered system, including the optimal power splitting ratio, and the optimal transmit power levels of the base station and WPAT. Both analytical and simulation results then clearly show that by using energy harvesting, the system performance can be significantly improved compared with the approach without using the energy harvesting technique.

In [47], a more complicated scenario is considered for WPAC in the presence of two types of attacks, i.e., jamming and eavesdropper attacks. As illustrated in Fig. 5, the considered system contains a base station acting as a central controller and two sensor clusters, each of which has a cluster head that takes responsibility to collect data from all sensors located in its cluster before sending all the collected data to the base station. In addition to the data collection role, the cluster heads also take responsibility for supplying energy for the sensors through WPT. After harvesting energy from the cluster heads, the sensors will use the harvested energy to transmit data to the cluster heads. To deal with jamming attacks, the authors in [47] propose an intelligent strategy. Specifically, given a set of all available channels between the sensors and the cluster heads, if a channel is under a jamming attack, the sensors will try to harvest energy from jamming signals on this channel if needed. Otherwise, they will choose other channels without interfering with the jammer to transmit data. Similarly, the cluster heads are also able to observe and use the unjammed channels to transmit data to the base station. However, in this scenario, in addition to defeat jamming attacks, the eavesdropping attack needs to be handled as well. To cope with this issue, the authors formulate a secrecy capacity maximization problem and propose a low-cost solution to find the optimal power control for the cluster heads with non-orthogonal multiple access. Through the simulation results, the authors then show the efficiency of using the energy harvesting technique in dealing with both jamming and eavesdropper attacks.

Ambient Backscatter Techniques: Although RF energy harvesting techniques have been proposed as a potential solution in

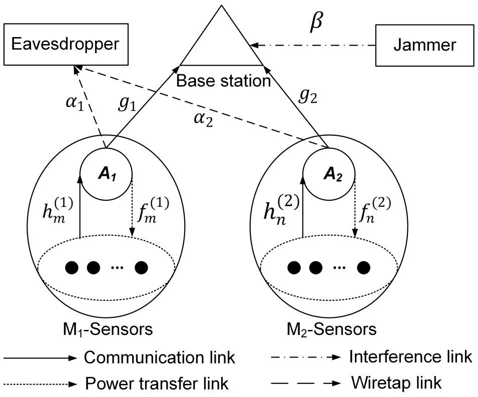


Fig. 5. WPAC in the presence of eavesdropping and jamming attacks [47].

dealing with jamming attacks, it suffers an intractable problem in dealing with jamming attacks. In particular, this technique only allow the WPATs to transmit data while the jammers are idle. If a jammer is equipped with a ample power supply and can continuously attack the channel, the WPATs will have no chance to transmit data. To address this problem, ambient backscattering technology [48]–[50] has been recently employed to defeat jamming attacks for WPAC.

Inspired by the operation principle of ambient backscatter communication technology, the authors in [51]–[53] propose the idea of leveraging jamming signals to facilitate WPAC when jammers attack the communication channels. In particular, the authors in [53] consider a scenario in which there is a jammer located near a system with one backscatter transmitter and one receiver. The transmitter is assumed to be equipped with an energy harvesting circuit and an ambient backscatter circuit in order to harvest energy and transmit data by backscattering surrounding signals, respectively. In this case, when the jammer attacks the channel, the transmitter can backscatter RF signals to transmit data or harvest energy from jamming signals and use the harvested energy to actively transmit data to the receiver when the jammer stops jamming. However, in practice, the jammer can attack the communication channel at different power levels at different times. Here, it is important to note that when the jammer attacks at high power levels, energy harvesting and ambient backscatter techniques can be used very effectively to improve performance for the system. However, when the jammer attacks the channel at low power levels, these techniques may not be efficient anymore. In this case, the rate adaption technique [41] can be used. In particular, under low-power jamming attacks, the transmitter can reduce its transmission rate, so that the receiver can still receive and decode the transmitted information. Nevertheless, in practice, the jamming attack power is unknown in advance. Thus, the authors propose to use a Markov decision process framework together with a Q-learning algorithm to help the transmitter make optimal actions under the uncertainty and dynamic of jamming attacks. This work is then extended in [51], [52] by using deep neural networks and deep dueling architectures to speed up the learning process at the transmitter. Through simulation results, the authors clearly demonstrate the superior performance of using ambient backscatter and energy harvesting techniques in dealing with jamming attacks for WPAC.

2) Deception Strategies: In the previous section, we have discussed two advanced techniques which have been recently introduced to deal with jamming attacks for WPAC. Although these techniques can show efficiency, they are only applicable to proactive jammers, i.e., jammers will attack the channels no matter whether the transmitters transmit signals or not. However, in practice, modern jammers are often equipped with smart sensors to detect activities of targets on the targeted channels, and they only attack the channels once they detect the activities of targets on the channels. Such kind of jamming attacks is known as reactive jamming attacks, and they are especially efficient in practice because they can focus their energy to attack the channels at the right time, thereby maximizing attack efficiency. Furthermore, as the jammers only attack the channels after the transmitters transmit signals, it is impossible to detect the locations of jammers ahead of transmission. Consequently, dealing with reactive jamming attacks for WPAC is more challenging than proactive jamming attacks.

To deal with reactive jamming attacks, deception strategies can be considered to be the most effective way for WPAC. Deception, as the art of military, allows a small army to defend or even defeat large foes by using smart tactics to weaken the enemy. Inspired by this military tactic, some deception strategies are developed to deal with jamming attacks for WPAC [35], [54]–[57]. Specifically, the authors in [54] consider a WPAC system consisting of one energy source and multiple WPATs. The energy source continuously transfers energy to the WPATs. The WPATs then use the harvested energy to transmit data to a dedicated channel. However, in this scenario, it is assumed that there are multiple jammers located near the energy source, and they can also harvest energy from the energy source to launch attacks. To deal with jammer attacks, the authors propose an intelligent deception strategy in which a WPAT can send a "fake" signal at the beginning of a time slot to mislead the jammer. A fake signal is only transmitted for a short period of time to lure the jammers to attack the channel. In this way, the WPATs can possibly attract the jammers to attack and weaken them by wasting their energy. As a result, when the WPATs transmit actual data, the jammers may not have sufficient energy to attack, and thus the system performance can be improved even under multiple jamming attacks.

Unlike the approach proposed in [54] which only deal with resource-constrained jammers (i.e., jammers need to harvest energy to attack the channel), the authors in [54] and [56] develop a solution that can help WPAC to be more effective in defeating strong jamming attacks. In particular, similar to the approach proposed in [54], a "fake" signal can be used at the beginning of a time slot to lure the jammer to attack the channel. However, unlike [54], when the jammer attacks the channel, the transmitter can backscatter the jammer signals to transmit data or harvest energy from the jamming signals as illustrated in Fig. 6. The harvested energy will be then used to actively transmit data to the receiver when the jammer does not attack the channel. To deal with the dynamic and uncertainty of the jammer, the Markov decision process framework is adopted where states (including its energy and data queues) of the

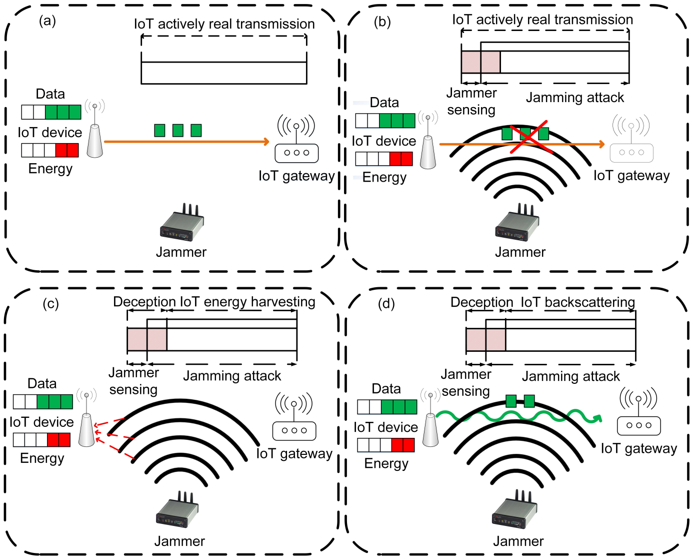


Fig. 6. Deception strategy to defeat jamming attacks (the figure is adopted from [56]).

transmitter are taken into considerations. In this way, a deep reinforcement learning algorithm [58] is proposed to help the transmitter determine the best action to take given its current state without requiring completed information about the jammer's attacks in advance. However, this solution does not take the state of jammer into considerations, and thus the efficiency in defeating jamming attacks may not be as high as expected. To overcome this limitation, reference [57] proposes an advanced MDP model with two decision-epochs. Specifically, there are two periods in each time slot. The first period, i.e., deception period, is used to lure the jammer by sending "fake" signals to the channel. Then, in the second period, after observing the actual state of the jammer (e.g., attack or not and which power level the jammer uses to attack the channel), the transmitter can make optimal actions (e.g., actively transmit data, backscatter data, harvest energy or just stay idle) in order to maximize its average long-term throughput. Through simulation results, the authors show that the proposed deception anti-jamming approach can not only very effectively defeat strong jamming attacks, but also smartly leverage jamming attacks to enhance the overall system performance.

Finally, we summarize the anti-jamming techniques by highlighting their pros and cons in Table IV.

IV. Anti-Eavesdropping Techniques In WPNs

Compared with the conventional wireless networks, WPNs are more vulnerable to the eavesdropping attack due to the presence of energy harvesters. In WPNs, the energy harvesters are typically located much closer to the base station, i.e., information and energy source, than information receiver. Due to the "near-far" effect, untrusted energy harvesters can easily eavesdrop on the information intended for information receivers.

Generally, anti-eavesdropping approaches leverage AN to increase the interference at the eavesdropper, suppressing the wiretapping rate. By using AN, several anti-eavesdropping approaches have been proposed for WPNs to combat the eavesdropping attack. In general, they are grouped into three major classes: beamforming design, system deployment, and transmit antenna selection. The applicability of these approaches in different WPNs is to be discussed in the following subsections. Note that although similar approaches have been proposed for conventional wireless networks, they may not be directly applied to WPNs. In particular, the anti-eavesdropping approaches in WPNs need to take into account the energy constraints strictly. Besides, in WPBC systems, the propagation models are different from those in conventional wireless networks. Therefore, implementing the security approaches in WPNs is much more challenging. For example, with the beamforming technique, the CSI of the network entities is required to enhance the security performance. However, the CSI acquisition is hard to achieve in WPNs. The reason is that in WPNs, energy harvesters may not be equipped with an information transceiver to feedback their own CSI to the source. Even if they possess the information transceiver, the availability of CSI is still subject to the energy constraint of the energy harvesters.

A. Beamforming Design

Beamforming is a common technique in MIMO cellular systems that exploit multi-antenna techniques to steer RF signals toward a targeted destination [59]. Due to its directional transmission capability, the beamforming technique is more energy-efficient than omni-directional broadcast in transmission. The key idea of beamforming-based anti-eavesdropping design is to direct the information signals from an information source toward its legitimate destinations and the AN signals toward illegitimate destinations. With the capability of increasing the signal-to-interference-and-noise-ratio (SINR) values at the legitimate destinations while reducing those at the illegitimate destinations, beamforming approaches can improve the secrecy rate of the system.

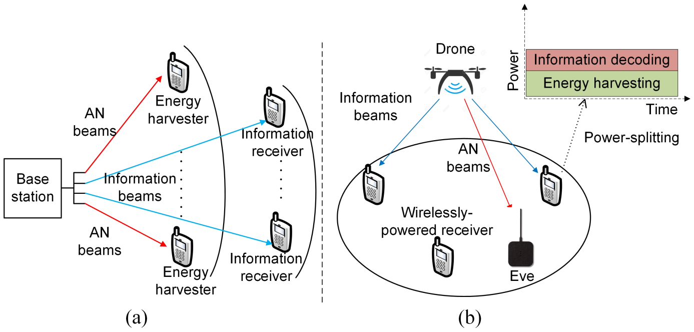


Fig. 7. (a) Beamforming for a secure MISO-SWIPT network [75] and (b) Joint beamforming and PS factor for a secure drone-aided SWIPT network with non-orthogonal multiple access [66].

As an example, we illustrate a wiretapping scenario in a multiple-input-multiple-output (MISO) SWIPT system, as shown in Fig. 7(a) [60]. The system consists of a base station, multiple information receivers, and multiple energy harvesters. The objective of the base station is to simultaneously transmit information to the information receivers and wireless power to the energy harvesters. As the energy harvesters can be untrusted, they possess the potential to intercept the intended

TABLE IV
COMPARISON OF ANTI-JAMMING TECHNIQUES FOR WPAC

Countermeasures	Principle	Advantages	Disadvantages
RF energy harvesting	Harvest energy from jamming signals and use the harvested energy to transmit data	Easy to deploy as RF energy harvesting circuits can be easily integrated on wireless devices	Only effective to deal with jammers which cannot attack the channel continuously. Cannot deal with reactive jammers
Ambient backscatter	Backscatter jamming signals to transmit data	Easy to deploy as ambient backscatter circuit can be easily integrated on wireless devices. Still can work well even when jammers attack constantly the channel with high powers	Cannot deal with reactive jammers. Require a new way for decoding information (due to backscatter communications)
Deception strategy	Send the deceptive signals to lure the jammer to attack, and then leverage jamming to improve system performance	Easy to deploy and combine with other methods like RF energy harvesting and ambient backscatter techniques. Can deal with both proactive and reactive jammers	Need to modify transmission framework. Need to combine with other techniques to maximize efficiency

information for the information receivers. To mitigate the information leakage to the energy harvesters, the base station can employ transmit beamforming to steer the information signal beams toward the information receivers along with the AN beams directed toward the energy harvesters to degrade their received information signal quality. For this, the base station first needs to achieve the CSI of both the information receivers and energy harvesters. Then, the beamforming matrices for both information signal and AN signal can be optimized based on the objective of the system. For example, reference [60] maximizes the sum secrecy rate of the information receivers given the harvested energy requirements of the energy harvesters. Differently, reference [61] maximizes the totally harvested energy of the energy harvesters under the sum secrecy rate requirements of the information receivers. Moreover, reference [62] maximizes both the sum secrecy rate of the information receivers and the totally harvested energy of the energy harvesters. It is worth noting that AN signals should be randomly generated following a distribution with a covariance that can be jointly optimized with the beamforming matrices to maximize the secrecy rate of the information receivers [63], [64].

Apart from dedicated information and energy transmission, a wirelessly-powered receiver may require information and energy concurrently in WPNs. To accommodate the reception, there are two common receiver architectures, namely, time switching (TS) and power splitting (PS) [65]. With TS, a wirelessly-powered receiver switches over time between information decoding and energy harvesting. With PS, the user splits the received signal into two streams for information decoding and energy harvesting. In general, the TS and PS coefficients affect the energy harvesting performance and the SINR of the wirelessly-powered receiver. Thus, the TS/PS coefficients at the wirelessly-powered receivers can be jointly optimized with the transmit beamforming matrices to improve the secrecy performance. For example, the authors in [66] consider a drone performs SWIPT to multiple wirelessly-powered receivers with non-orthogonal multiple access in the presence of an eavesdropper (Eve) as shown in Fig. 7(b). The drone performs SWIPT to the wirelessly-powered receivers while transmits AN towards the eavesdropper. Each wirelessly-powered receiver uses PS to perform the information decoding and energy harvesting simultaneously. Since the wirelessly-powered receivers consume the harvested energy to decode and cancel the received AN signal, there exists a tradeoff between extracting energy and information from the received signals to maximize the secrecy rate. To balance the tradeoff, reference [66] jointly optimizes the SWIPT beamforming matrices and the PS factors at the wirelessly-powered receivers. Besides single-cell designs, joint transmit beamforming and receiver coefficient designs for multi-cell networks with SWIPT can be found in [67] and [68].

Note that the aforementioned beamforming techniques are typically designed for MIMO systems. In single-input-single-output (SISO) systems, power allocation techniques can be an appropriate solution to enhance the secrecy performance. As an example, the authors in [69] consider a SWIPT system including a base station, one information receiver, and one energy harvester, each equipped with one antenna. To prevent the energy harvester from eavesdropping the information intended to the information receiver, the authors develop a power allocation scheme to optimize the power portions allocated to the information signal and AN for the maximization of the secrecy rate of the information receiver, subject to an average harvested power requirement at the energy harvester.

In large-scale SWIPT systems, e.g., with cell-free massive MIMO, in which a large number of base stations are deployed to serve multiple information receivers and energy harvesters, the power allocation techniques can be used to determine the power allocated to the information transmission, AN signal and energy signal to improve the system secrecy rate [70]. In the presence of an advanced attacker that can launch different types of attacks such as eavesdropping, jamming, and spoofing, the power allocation techniques can be used as a security solution. For this, a game theory with the Nash equilibrium can be adopted that allows the base station to find its best transmit power allocation strategy given the attack strategy [71]. The base station can be limited in energy, and it may need to rent an external friendly jammer to transmit the AN signal to confuse the energy harvester. The power allocation strategy is adopted to determine the optimal amount of jamming power for a tradeoff between the security performance and the power cost paid to the friendly jammer [72].

In addition to WPAC, the use of beamforming and power allocation techniques have also been introduced to cope with the eavesdropping attack for WPBC. Fig. 8 shows a bistatic radio frequency identification (RFID) system consisting of a reader, a colocated carrier emitter and a backscatter receiver, and a tag, i.e., backscatter transmitter. To cope with the eavesdropping attack, the reader can generate AN along with the carrier signal

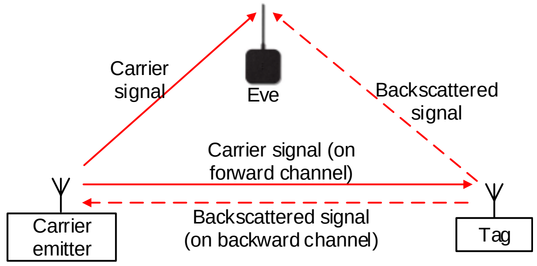

Carrier signal
Eve
Backscattered signal
Carrier signal (on forward channel)
Carrier emitter
Backscattered signal (on backward channel)
Tag

Fig. 8. An illustration of a WPBC network with an eavesdropper.

to disturb Eve. In particular, to interfere with the eavesdropper's reception of the tag's backscatter information signal, the reader can 1) optimize the transmit powers of carrier signal and AN to maximize the secrecy rate in SISO system [73] or 2) optimize the carrier signal power and AN covariance matrix to maximize the secrecy rate in MIMO system [74]. Generally, implementing beamforming for WPBC is more challenging than that for WPAC due to more complicated signal patterns caused by backscattering. Specifically, the injected AN distort not only the carrier signals but also the reflected version, making instant channel estimation and backscatter demodulation more difficult.

B. System Deployment

In SWIPT systems, the locations of information/energy sources, e.g., base stations, play a pivotal role in the secrecy rate of the information receivers. In particular, when the information/energy source is located close to the information receivers and far from the eavesdropping energy harvesters the secrecy capacity of the information receivers is high. However, in this case, the harvested energy of the energy harvesters may be too low to meet their energy requirements. Thus, the system deployment approach can be adopted to optimize the coordinates of network entities, e.g., information/energy sources, information receivers, and energy harvesters, for the tradeoff between security performance and energy performance. For example, the authors in [75] consider a drone-assisted SWIPT system, as shown in Fig 9(a). The system consists of a drone, an information receiver, and multiple energy harvesters. The drone transmits confidential information to the information receiver, which can be intercepted by the energy harvesters. Then, the optimization problem is formulated to determine the positions and the transmit power of the drone to maximize the secrecy rate of the information receiver, given the energy constraints of the energy harvesters and the drone. To enhance the secrecy rate of the information receiver, another drone can be deployed to send AN signals against the eavesdropping energy harvesters [76]. In this case, the positions of the drones and their transmit power need to be jointly optimized.

The information receiver can be enabled with full-duplex operation that adopts the PS protocol to receive confidential signals from the drone and cooperatively transmits AN to confuse the energy harvesters. In this scenario, the system deployment technique can be used to jointly optimizes the drone position, AN transmit power, and PS ratios [77]. This technique can also be used in WPBC networks [78]. In the network, a drone as an energy source and an information receiver emits RF signals which are backscattered by ground backscatter transmitters for uploading their own information to the drone. The backscatter transmitters adjust their backscatter coefficients for balancing the reflected signal and the harvested energy. To guarantee the secrecy rate of the backscatter links, the system deployment technique jointly optimizes the position and transmit power of the drone along with the backscatter coefficients of backscatter transmitters.

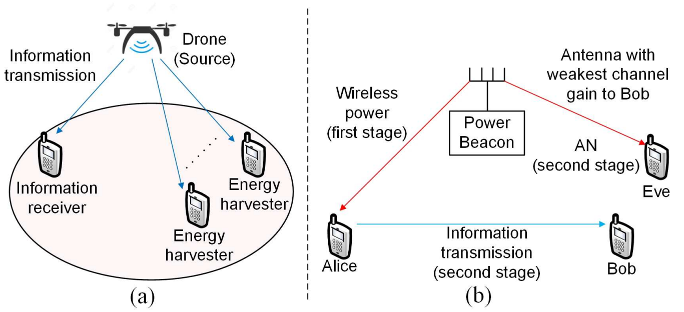


Fig. 9. (a) Position optimization-based security in a drone-assisted SWIPT system [75] and (b) Transmit antenna selection [79] for a secure WPN.

C. Transmit Antenna Selection

In addition to the aforementioned techniques, transmit antenna selection technique can be used to secure communications for multi-antenna WPNs. With this technique, the source can work as a friendly jammer to transmit AN with the selected antenna(s). Specifically, depending on the channel condition, the source selects one (or more) of its antennas to transmit AN to jam the eavesdropper while causing minimal interference to its legitimate destination. As an example, the authors in [79] consider the WPAC, as shown in Fig 9(b), in which Alice powered by a power beacon intends to transmit information to Bob in the presence of Eve. The PB, equipped with multiple antennas, acts as both a power source and a friendly jammer. A two-stage time-division communication protocol is adopted. Alice is charged by the power beacon in the first stage and transmits to Bob in the second stage, during which the power beacon transmits AN. For transmit antenna selection, the power beacon first retrieves the CSI between itself and Bob and then selects the antenna with the weakest channel gain to transmit AN. As such, the secrecy capacity is maximized by suppressing the wiretapping capacity while imposing minimal AN towards Bob. In addition to secrecy capacity maximization, a transmit antenna selection approach is also found in [80] that is designed to minimize Alice's secrecy outage probability, defined as the probability that the instantaneous secrecy capacity drops below a threshold value. It is evaluated in [79] that compared with the beamforming and power allocation techniques, the transmit antenna selection is a low-complexity solution and may not require the CSI of the communication link between the source and eavesdroppers.

D. Summary

In summary, when the CSI of all network entities is available, the beamforming technique serves as an energy-effective solution, especially for static networks. In the scenario with

TABLE V
COMPARISON OF ANTI-EAVESDROPPING TECHNIQUES FOR WPNS

Technique	Principe	Communication overhead	Computational overhead	Implementation scalability
Beamforming	Direct signals toward target destinations	High	High	High
System deployment	Optimize locations of network entities	High	High	High
Transmit antenna selection	Select antennas to transmit AN signals	Low	Low	High

mobile information sources, e.g., drones, the system deployment approach can be adopted in conjunction with the beamforming technique. Conversely, when the CSI of the wiretapping channels are unavailable, the transmit antenna selection can be a more suitable choice to be adopted. Table V compares the reviewed anti-eavesdropping techniques for WPNs. As can be seen, the transmit antenna selection technique has the advantage of less computational overhead than those of the other techniques. However, the secrecy performance obtained by the transmit antenna selection technique may not be desirable when it does not accurately identify the weakest channel gain between the AN source and the legitimate destination.

V. ANTI-DOC TECHNIQUES IN WPNS

Covert communication has been conventionally realized through spread-spectrum techniques, such as direct sequence and frequency hopping [81], which suppress the average power spectral density of legitimate transmission under the noise floor by spreading the signals across a wide frequency range. As such, Willie is hard to differentiate the information-bearing signal from ambient noise. However, spread-spectrum techniques 1) require a large frequency band; 2) increase the computational complexity; and 3) need synchronization between Alice and Bob [82]. These requirements make spread spectrum less suitable for WPNs which usually have low computation capability (e.g., due to hardware incapability and energy constraint) and operates with limited bandwidth (e.g., Narrowband Internet of Things [83]).

This section focuses on reviewing the anti-DoC techniques for WPNs. Generally, there are two fundamental principles to impair the detectability of Willie so as to alleviate DoC attacks. One is to suppress the signal leakage towards Willie. The other is to intensify interference variation such that the signal leakage becomes hard to be detected. In the following, we review the covertness approaches that exploit the two principles in WPNs.

A. Directional Transmission

Directional transmission is a technique that focuses and radiates the signal beams towards the direction of the target receiver. Compared with the omni-directional transmission that broadcasts signals in all directions, directional transmission not only curtails the signal leakage to Willie but also strengthens the power intensity and thus transmission rate at target receiver. Common techniques to realize directional transmission include the following.

- Adopting a directional antenna at the transmitter which concentrates the radiation in the desired direction. Note that a directional antenna can also be used at the receiver to further improve the received signal strength[1].
- Multi-antenna beamforming tailors the phase and amplitude of the transmitted signals at different antennas such that the aggregated waves are constructive (i.e., stronger) in the target direction and destructive (i.e., weaker) towards other areas [39]. Receive beamforming, which coherently combines the received signal components at the legitimate receiver, can be adopted in combination with transmit beamforming to create the desired pattern[2].
- Millimeter-wave (mmWave) communication [84] (with frequency ranging from 30 to 300GHz) entails narrow and steerable beams, which naturally benefit directional transmission. Compared with the microwave counterpart, mmWave signal leakage in the directions off-boresight can be easily suppressed [40].

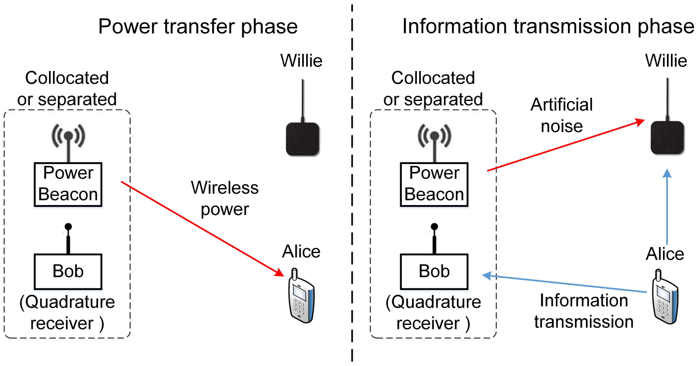


Fig. 10. Covert WPAC with AN generation.

As discussed above, directional transmission techniques impose requirements on the hardware, e.g., directional antennas, multiple antennas and mmWave circuits. Since usually transmitter-side implementation is needed, the implementation scalability of directional transmission techniques is high. The above-mentioned techniques can be applied for both WPAC and WPBC with prototype examples demonstrated in [85]–[89].

B. Artificial Noise Generation

Random AN can be created to ruin the effectiveness of Willie's hypothesis test at the cost of Bob's performance degradation. Thus, lessening the negative impact of AN on legitimate transmission is of paramount importance to an applicable AN design. For this, directional transmission techniques discussed

[1] If directional antennas are equipped at both transmitter and receiver, a fine alignment of the two antennas is needed to achieve efficient transmission.

[2] It is worth noting that beamforming performance heavily relies on the availability and accuracy of timely CSI.

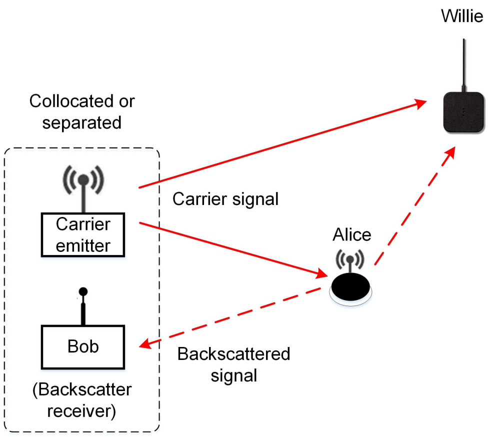


Fig. 11. Covert WPBC with AN generation.

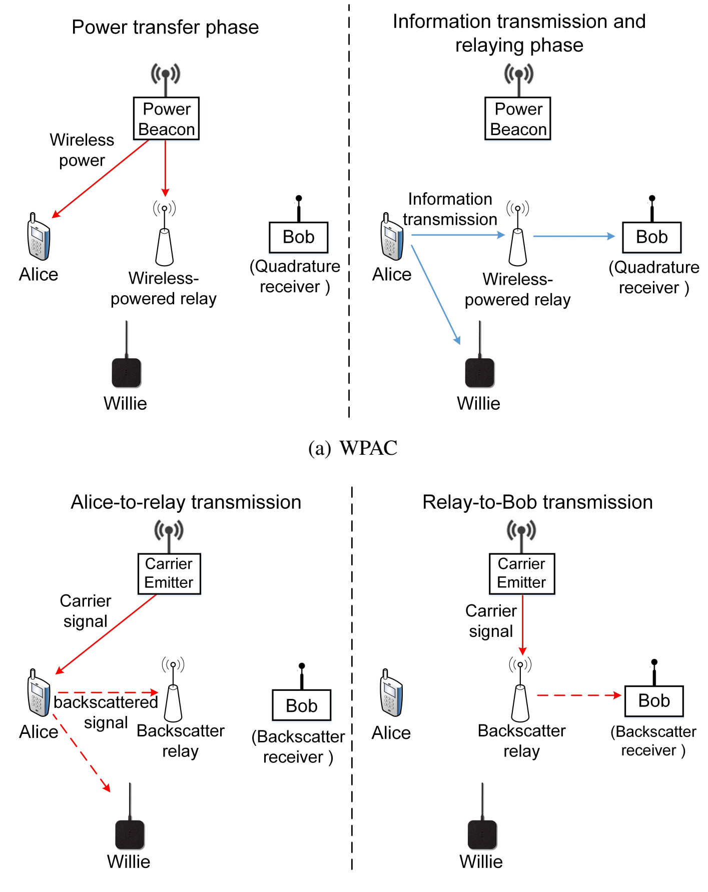
previously can be employed to generate AN specifically towards Willie if its location is known and towards non-Bob directions otherwise.

In WPNs, the off-the-shelf power beacon/carrier emitter serves as a natural choice for the AN generation. In the following, we introduce instances of power beacon-assisted AN generation in WPNs.

- For WPAC, as shown in Fig. 10, the power beacon first performs wireless charging to Alice as usual during the power transfer phase. In the information transmission phase, the power beacon continues to inject AN to shield Alice's transmission. To mitigate the damage of AN on legitimate transmission, AN nulling [90] towards Bob based on multi-antenna techniques can be adopted if the power beacon and Bob are separated, and self-interference cancellation [91] can be employed if the power beacon and Bob are collocated. Additionally, the transmit powers of the power beacon, and Alice can be jointly optimized, taking into account the communication and covertness requirement.
- For WPBC, as shown in Fig. 11, a carrier emitter can produce AN based on a secret key to increase the interference uncertainty at Willie [92]. The secret key needs to be pre-shared with Alice and Bob by secret means so that the AN can be eliminated at Bob through successive interference cancellation. Additionally, to disturb the decision of Willie, the carrier emitter can adopt time-varying transmit power [93] so that the increase and decrease of the received signal density may not necessarily indicate Alice is on and off, respectively. On Alice side, its backscatter coefficient can be tuned in a real-time manner based on the instant transmit power of the carrier emitter. Furthermore, the transmit power of the carrier emitter and backscatter coefficient of Alice can be jointly optimized based on the instantaneous CSI.

Other than the power beacon-assisted AN scheme as discussed above, a WPN can implement other AN schemes, which include 1) equipping a full-duplex jamming receiver [64], [94] at Bob that enables data reception from Alice and AN generation for Willie simultaneously; 2) performing AN injection [95], [96] at Alice to concurrently transmit data symbols to Bob and AN to Willie; and 3) deploying a third-party wireless-powered jammer [97]–[99] utilizing the broadcast energy from the power beacon to generate AN towards Willie.

C. Relay-aided Transmission



(a) WPAC

(b) WPBC

Fig. 12. Relay-aided covert communication in WPNs.

Relay-aided transmission involves the use of intermediate relay node(s) to facilitate covertness. Through multi-hop data forwarding, the link distance of each hop is shortened. As a consequence, the transmit power and thus signal leakage of each hop can be kept low, making Alice a low probability of being detected. Next, we discuss the relay-aided transmission approaches.

- For WPAC, as shown in Fig. 12(a), one (or multiple) wireless-powered relay(s) can be deployed to lessen the transmission distance of Alice. During the power transfer phase, the power beacon wirelessly charges both Alice and relay(s) wirelessly. Subsequently, Alice performs transmission to Bob with the assistance of the relay(s) with low transmit power. It is worth noting that the relay-aided covert communication is greatly affected by the implemented relaying protocol (e.g., amplify-and-forward and decode-and-forward) and duplex operation (i.e., half-duplex and full-duplex). Different combinations lead to disparate end-to-end SINRs, and thus secrecy capacity. The transmit power of Alice can be optimized, taking into account these configurations and the harvested energy at the relay(s).

TABLE VI
COMPARISON OF COVERTNESS TECHNIQUES FOR WPNS.

Technique	Principle	Communication overhead	Computational overhead	Implementation Scalability
Directional transmission	Suppressing signal leakage	High if beamforming/precoding is involved and low otherwise.	High if beamforming/precoding is involved and low otherwise.	High
AN generation	Intensify interference dynamics	High if a third-party device is involved and low otherwise.	High if AN injection is involved and low otherwise	Low if using a third-party device and high otherwise
Relay-aided transmission	Suppressing signal leakage	High	Low	Low

- For WPBC, as shown in Fig. 12(b), the system can deploy a backscatter relay that is capable of backscatter modulation and demodulation. During the first-hop transmission, Alice modulates the incident carrier signal and reflects it to the backscatter relay with a reduced backscatter coefficient compared with direct Alice-to-Bob reflection (i.e., by adjusting its load impedance). The relay demodulates the backscatter into information bits upon reception. Then, the relay re-modulates the bits on the carrier signal and reflects it to Bob.

Compared with the multi-antenna beamforming and AN injection techniques, relay-aided transmission incurs low computational complexity, e.g., signal processing overhead. However, owing to the use of additional relay(s), this approach has limited implementation scalability and may not apply efficiently in mobile systems, e.g., portable WPATs [100], [101].

Table VI summarizes and compares the characteristics of the reviewed covertness techniques for WPNs. As can be seen, each technique, though, has its advantages, exhibits limitations. These techniques can be applied in a complementary manner to each other for performance enhancement at the cost of increased complexity.

VI. FUTURE DIRECTIONS

In this section, we discuss future opportunities of anti-attack designs for WPNs.

A. Attacks in emerging scenarios

Although PHY attacks have attracted considerable research attention over the years, some critical directions have been left unaddressed. Such examples are discussed as follows.

- *Emerging jamming attacks*: With the rapid development of technologies, many attacks at the PHY have also evolved worrisomely, which has caused many difficulties in preventing. For example, due to the development of full-duplex technology, a new kind of jammer, namely, "super-reactive jammers" [102], has been introduced recently. Unlike conventional reactive jammers, a super-reactive jammer can attack the channel by sending its jamming signals over the channel and at the same time listen to the channel to detect activities of the transmitter. Consequently, current deception solutions [56], [57] might not be effective in dealing with such a kind of attack. In this case, the combination of machine learning and ambient backscatter technologies can be a potential solution to defeat super-reactive jamming attacks [102].
- *Jamming attacks for WPBC*: As mentioned in Section III, countermeasures to jamming attacks for WPBC is missing in the existing literature. Handling jamming attacks for WPBC can be an arduous mission, especially in a multiple backscatter transmitter system, due to the aggregated interference caused by backscattering. Inter-device coordination can be explored to cope with the jamming signals collectively.
- *Wireless-powered passive attacks*: Similar to wireless-powered jammers, an adversary can also be powered by the RF energy from power sources or legitimate transmitters, i.e., performing eavesdropping/DoC attacks after harvesting sufficient energy. In this context, WPT may not only benefit legitimate users but also increase the chance of DoC attacks. To cope with RF-powered DoC attacks, an omni-directional power source needs to balance the tradeoff between user performance and activation of Willie. Besides, a directional power source should endeavour to minimize the power leakage towards the adversary.

B. Incentive mechanism for security in WPNs

In WPNs, distributed WPATs can establish cooperation to defend against security attacks. For example, to mitigate jamming attacks, WPATs can expedite the energy depletion of jammers collectively based on the deception strategies (introduced in Section III-B2). Moreover, to alleviate passive PHY attacks (e.g., eavesdropping and DoC attacks), idle WPATs can serve as friendly jammers to transmit AN to disturb the attackers. The key to establishing such cooperation is the incentive mechanism that will benefit each individual WPAT. Economic mechanisms (e.g., pricing [103], [104] and game-theoretical approaches [105], [106]) can be utilized to design effective solutions.

C. Reconfigurable environments

Metasurface [107] is an emerging technology that can dynamically change the electromagnetic behavior of the incident signals by electronically tuning the responses of its passive scattering particles. By coating environmental objects with the metasurface, a controllable propagation environment can be created to facilitate secure communication. In this context, joint control of the metasurface's configuration with the security techniques reviewed in this article would be a promising research direction. For instance, the responses of the scattering particles and the resource allocation of the WPN can be jointly optimized under security concerns.

It is worth noting that metasurface could also be leveraged by adversaries to facilitate hostile attacks. For instance, metasurface-assisted eavesdropping can strengthen the reflected signals towards the eavesdropper. Thus, it is imperative to develop novel solutions to defeat metasurface-assisted PHY attacks.

D. Hardware implementation

Although the PHY security consumes a remarkably lower computational load compared with higher-layer cryptographic techniques, the required hardware complexity and cost remain critical factors in its implementation. The realization of PHY security in WPNs necessitates the advances of hardware fabrication in many ways, including antenna gain, detection sensitivity, energy harvesting efficiency, computation capacity and circuit power consumption. Furthermore, low-complexity and low-cost implementation of modern PHY security approaches to facilitate the practical development of WPNs is of crucial importance.

E. Experimental evaluation and validation

Practical WPATs and backscatter transmitters unavoidably expose security vulnerabilities that have not been taken into consideration by the theoretical studies in the existing literature. For example, the analytical models, e.g., propagation channels, channel estimation and co-channel interference distribution, might deviate from the real-world behaviors, resulting in inefficiency, or even failure, of the designed security techniques. Therefore, more extensive evaluation in prototype systems is imperative to validate the effectiveness of novel PHY countermeasures.

F. Standardization

Promising applications of PHY security entail the efforts to standardize the PHY protocol suite. This mainly includes designing hardware and software components to implement PHY security techniques interoperable with the higher layer, taking into account regulatory aspects in the context of 6G privacy. The emerging cyber-physical systems [108] may serve as a suitable framework to implement novel security techniques at the PHY, resolving the integration issue conveniently.

VII. Conclusion

This article has discussed PHY security for WPNs in a review manner. Specifically, we first explicate the radical principles of WPAC and WPBC as well as their exposure to PHY attacks. Subsequently, we present a systematic overview of the up-to-date countermeasures to address the most common PHY attacks, including jamming, eavesdropping and DoC. Additionally, we shed light on the rich opportunities of PHY anti-attack designs for the emerging WPNs.

References

[1] B. Clerckx, R. Zhang, R. Schober, D. W. K. NG, D. I. Kim, and H. V. Poor, "Fundamentals of wireless information and power transfer: From RF energy harvester models to signal and system designs," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 4-33, Jan. 2019

[2] H. J. Visser and Ruud J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: Principles and requirements," *Proceedings of the IEEE*, vol. 101, no. 6, pp. 1410-1423, June 2013

[3] S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, and K. Huang, "Energy harvesting wireless communications: A review of recent advances," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 3, pp. 360-381, Mar. 2015.

[4] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless charging technologies: Fundamentals, standards, and network applications," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 2, pp. 1413-1452, Secondquarter 2016.

[5] X. Lu, P. Wang, G. Li, D. Niyato, and Z. Li, "Short-Packet Backscatter Assisted Wireless-Powered Relaying with NOMA: Mode Selection with Performance Estimation," *IEEE Transactions on Cognitive Communications and Networking*, to appear.

[6] G. Li, X. Lu and D. Niyato, "A Bandit Approach for Mode Selection in Ambient Backscatter-Assisted Wireless-Powered Relaying," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, Aug. 2020.

[7] X. Lu, I. Flint, D. Niyato, N. Privault and P. Wang, "Self-sustainable communications with RF energy harvesting: Ginibre point process modeling and analysis," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1518-1535, May 2016.

[8] D. Niyato, X. Lu, P. Wang, D. I. Kim and Z. Han, "Distributed wireless energy scheduling for wireless powered sensor networks," in *Proc. of IEEE ICC*, Kuala Lumpur, Malaysia, May 2016.

[9] 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, Sept. 2016.

[10] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing physical layer security in wireless cellular networks: insurance approach," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1648-1661, July 2018.

[11] Y.-S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen "Physical layer security in wireless networks: A tutorial," *IEEE Wirel. Comm.*, vol. 18, no. 2, pp. 66-74, April 2011.

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

[13] Y. Wu, A. Khisti, C. Xiao, G. Caire, and K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679-695, April 2018.

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

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

[16] S. Vadlamani, B. Eksioglu, H. Medala, and A. Nandia, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76-94, Feb. 2016.

[17] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surv. Tutor.*, vol. 13, no. 2, pp. 245-257, Second Quarter 2011.

[18] A. Mpitziopoulos, D. Gavalas; C. Konstantopoulos, G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Commun. Surv. Tutor.*, vol. 11, no. 4, pp. 42-56, Fourth Quarter 2009.

[19] M. A. Aref, S. K. Jayaweera, and E. Yepez, "Survey on cognitive anti-jamming communications," *IET Communications*, vol. 14, no. 18, pp. 3110-3127, 2020.

[20] J. C. O. Galvan, C. Juan, E. C. Littlewood, S. Maximov, S. M. Adame, and W. Xu, "Wireless power transfer: Literature survey," in *Proc. of IEEE International Autumn Meeting on Power Electronics and Computing (ROPEC)*, Morelia, Mexico, Nov. 2013.

[21] P. Nintanavongsa, "A survey on RF energy harvesting: circuits and protocols," *Energy Procedia*, vol. 56, pp. 414-422, 2014.

[22] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and Z. Han, "Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1528-1544, March 2018.

[23] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and P Wang, "Analysis of wireless-powered device-to-device communications with ambient backscattering," in *Proc. of IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, ON, Canada, Sept. 2017.

[24] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, "Beamforming in wireless energy harvesting communications systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2., pp. 1329-1360, Secondquarter 2018.

[25] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, "Beamforming in wireless energy harvesting communications systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, vol. 2, pp. 1329-1360, Second quarter 2018.

[26] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 264-302, Firstquarter 2018.

[27] B. Clerckx, Z. B. Zawawi, and K. Huang, "Wirelessly powered backscatter communications: Waveform design and SNR-energy tradeoff," *IEEE Communications Letters*, vol. 21, no. 10, pp. 2234-2237, Oct. 2017.

[28] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient backscatter assisted wireless powered communications," *IEEE Wireless Communications*, vol. 25, no.2, pp. 170-177, Jan. 2018.

[29] C. Xu, L. Yang, and P. Zhang, "Practical backscatter communication systems for battery-free internet of things: A tutorial and survey of recent research," *IEEE SPM*, vol. 35, no. 5, pp. 16-27, Sept. 2018.

[30] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 2889-2922, Fourthquarter 2018.

[31] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. of ACM Mobihoc*, pp. 46-57, May 2005.

[32] D. Niyato, P. Wang, D. I. Kim, Z. Han, and L. Xiao, "Performance analysis of delay-constrained wireless energy harvesting communication networks under jamming attacks," in *IEEE WCNC*, New Orleans, LA, USA, June 2015.

[33] C. S. R. Murthy and B. Manoj, "Ad hoc wireless networks: Architectures and protocols, portable documents," *Pearson education*, 2004.

[34] M. Acharya and D. Thuente, "Intelligent jamming attacks, counterattacks and (counter) 2 attacks in 802.11 b wireless networks," in *Proc. of OPNETWORK*, Washington DC, USA, 2005.

[35] J. Guo, N. Zhao, F. R. Yu, X. Liu, and V. C. Leung, "Exploiting adversarial jamming signals for energy harvesting in interference networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1267-1280, Dec. 2016.

[36] Wireshark (https://www.wireshark.org)

[37] D. Spill and A. Bittau, "Bluesniff: Eve meets alice and bluetooth." WOOT, vol. 7, pp. 1-10, 2007.

[38] B. A. Bash, D. Goeckel, and D. Towsley , "Limits of reliable communication with low probability of detection on awgn channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921-1930, September 2013.

[39] M. Forouzesh, P. Azmi, A. Kuhestani, P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737-3749, June 2020.

[40] 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, September/October 2020.

[41] Z. Fang, T. Song, and T. Li, "Energy harvesting for two-way ofdm communications under hostile jamming," *IEEE Signal Processing Letters*, vol. 22, no. 4, pp. 413-416, April 2015.

[42] I. Flint, X. Lu, N. Privault, D. Niyato, and P. Wang, "Performance analysis of ambient RF energy harvesting with repulsive point process modelling," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5402-5416, May 2015.

[43] X. Lu, I. Flint, D. Niyato, N. Privault, and P. Wang, "Performance analysis for simultaneously wireless information and power transfer with ambient RF energy harvesting," in *Proc. of IEEE WCNC*, New Orleans, LA, USA, March 2015.

[44] I. Flint, X. Lu, N. Privault, D. Niyato, and P. Wang, "Performance analysis of ambient RF energy harvesting: A stochastic geometry approach," in *Proc. of IEEE Globecom*, Austin, USA, December 2014.

[45] X. Lu, P. Wang, D. Niyato, and Z. Han, "Resource allocation in wireless networks with RF energy harvesting and transfer," *IEEE Network*, vol. 29, no. 6, pp. 68-75, Dec. 2015.

[46] X. Lu, P. Wang, D. Niyato, and E. Hossain, "Dynamic spectrum access in cognitive radio networks with RF energy harvesting," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 102-110, June 2014.

[47] H. Tran, H. Tran, V. L. Dao, C. S. In, D. D. Tran, and E. Uhlemann, "On communication performance in energy harvesting WSNs under a cooperative jamming attack," *IEEE Systems Journal*, vol. 14, no. 4, pp. 4955-4966, Feb. 2020.

[48] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM*, Hong Kong, China, Aug. 2013.

[49] X. Lu, G. Li, H. Jiang, D. Niyato, and P. Wang, "Analysis of wireless-powered relaying with ambient backscattering," *IEEE International Conference on Communications*, Kansas City, MO, July 2018.

[50] X. Lu, H. Jiang, D. Niyato, E. Hossain, and P. Wang "Ambient backscatter-assisted wireless-powered relaying," *IEEE Transactions on Green Communications and Networking*, vol. 3, no. 4, pp. 1087-1105, Dec. 2019.

[51] N. V. Huynh, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Jam me if you can: Defeating jammer with deep dueling neural network architecture and ambient backscattering augmented communications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2603-2620, Nov. 2019.

[52] N. V. Huynh, D. N. Nguyen, D. T. Hoang, E. Dutkiewicz, and M. Mueck, "Ambient backscatter: A novel method to defend jamming attacks for wireless networks," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 175-178, Feb. 2020.

[53] N. V. Huynh, D. N. Nguyen, D. T. Hoang, E. Dutkiewicz, M. Mueck, and S. Srikanteswara, "Defeating jamming attacks with ambient backscatter communciations," in *IEEE ICNC*, Big Island, Hawaii, USA, Feb. 2020.

[54] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Performance analysis of wireless energy harvesting cognitive radio networks under smart jamming attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, no. 2, pp. 200-216, Oct. 2015.

[55] D. T. Hoang, M. A. Alsheikh, S. Gong, D. Niyato, Z. Han, and Y. C. Liang, "Defend jamming attacks: How to make enemies become friends," *IEEE GLOBECOM*, Waikoloa, HI, USA, 9-13 December 2019.

[56] D. T. Hoang, D. N. Nguyen, M. A. Alsheikh, S. Gong, D. Dutkiewicz, D. Niyato, and Z. Han, "Borrowing arrows with thatched boats: The art of defeating reactive jammers in IoT networks," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 79-87, June 2020.

[57] N. V. Huynh, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "DeepFake: Deep dueling-based deception strategy to defeat reactive jammers," *IEEE Transactions on Wireless Communications*, to appear.

[58] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y. C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3313-3174, May 2019.

[59] X. Lu, D. Niyato, N. Privault, H. Jiang, and S. S. Wang, "A cyber insurance approach to manage physical layer secrecy for massive MIMO-enabled cellular networks," in *Proc. of IEEE ICC*, Kansas city, MO, May 2018.

[60] M. Alageli, A. Ikhlef, and J. Chambers, "Optimization for maximizing sum secrecy rate in mu-miso swipt systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 537-553, Jan. 2018.

[61] M. R. Khandaker and K.-K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 10-13, Feb. 2015.

[62] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with miso beamforming," *IEEE Transactions on Signal Processing*, vol. 62, no. 7, pp. 1850-1863, April 2014.

[63] Y. Cai, F. Cui, Q. Shi, Y. Wu, B. Champagne, and L. Hanzo, "Secure hybrid a/d beamforming for hardware-efficient large-scale multipleantenna swipt systems," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6141-6156, Oct. 2020.

[64] 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, 2018.

[65] 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, Secondquarter 2015.

[66] 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 Transactions on Communications*, vol. 68, no. 8, pp. 5028-5040, April 2020.

[67] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secure and energy-efficient beamforming for simultaneous information and energy

transfer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7523-7537, Nov. 2017.

[68] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Transactions on Signal Processing*, vol. 65, no. 3, pp. 677-689, Feb. 2017.

[69] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180-190, Jan. 2016.

[70] M. Alageli, A. Ikhlef, F. Alsifiany, M. A. M. Abdullah, G. Chen, and J. Chambers, "Optimal downlink transmission for cell-free swipt massive mimo systems with active eavesdropping," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1983-1998, November 2019.

[71] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting secure communication under uav smart attack with imperfect channel estimation," *IEEE Access*, vol. 6, pp. 76 395-76 401, Nov. 2018.

[72] Y. Zhong, F. Zhou, Y. Wang, X. Deng, N. A. Dhahir, "Cooperative jamming-aided secure wireless powered communication networks: A game theoretical formulation," *IEEE Communications Letters*, vol. 24, no. 5, pp. 1081-1085, May 2020.

[73] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3442-3451, June 2014.

[74] Q. Yang, H. M. Wang, Y. Zhang, and Z. Han, "Physical layer security in mimo backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7547-7560, Nov. 2016.

[75] X. Hong, P. Liu, F. Zhou, S. Guo, and Z. Chu, "Resource allocation for secure uav-assisted swipt systems," *IEEE Access*, vol. 7, pp. 24248-24257, Feb. 2019.

[76] M. T. Mamaghani and Y. Hong, "Improving phy-security of uav-enabled transmission with wireless energy harvesting: robust trajectory design and communications resource allocation," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8586-8600, Aug. 2020.

[77] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. K. Ng, G. Zhang, J. Tang, and O. A. Dobre "Energy-constrained uav-assisted secure communications with position optimization and cooperative jamming," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4476-4489, April 2020.

[78] J. Hu, X. Cai, and K. Yang "Joint trajectory and scheduling design for uav aided secure backscatter communications," *IEEE Wireless Communications Letters*, vol. 9, no. 12, pp. 2168-2172, Dec. 2020.

[79] X. Jiang, C. Zhong, Z. Zhang, and G. K. Karagiannidis, "Power beacon assisted wiretap channels with jamming," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8353-8367, Dec. 2016.

[80] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Secrecy outage of a simultaneous wireless information and power transfer cognitive radio system," *IEEE Wireless Communications Letters*, vol. 5, no. 3, pp. 288-291, June 2016.

[81] D. Kirovski and H. Malvar, "Robust covert communication over a public audio channel using spread spectrum," in *nternational Workshop on Information Hiding*, Springer, 2001.

[82] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1020-1033, April 2003.

[83] A. Haridas, V. S. Rao, R. V. Prasad, and C. Sarkar, "Opportunities and challenges in using energy-harvesting for NB-IoT," *ACM Sigbed Review*, vol. 15, no. 5, pp. 7-13, 2018.

[84] S. L. Cotton, W. G. Scanlon, and B. K. Madahar, "Millimeter-wave soldier-to-soldier communications for covert battlefield operations," *IEEE Communications*, vol. 47, no. 10, pp. 72-81, Oct. 2009.

[85] S. Ladan, A. B. Guntupalli, and K. Wu "A high-efficiency 24 ghz rectenna development towards millimeter-wave energy harvesting and wireless power transmission," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 12, pp. 3358-3366, Dec. 2014.

[86] M. Wagih, A. S. Weddell, and S. Beeby "Rectennas for rf energy harvesting and wireless power transfer: A review of antenna design," *IEEE Antennas and Propagation Magazine*, vol. 62, no. 5, pp. 95-107, Oct. 2020.

[87] M. H. Mazaheri, A. Chen, and O. Abari, "Millimeter wave backscatter: Toward batteryless wireless networking at gigabit speeds," in *ACM HotNets*, November 2020.

[88] V. Mangal, G. Atzeni, and P. R. Kinget. "Multi-antenna directional backscatter tags," in *IEEE European Microwave Conference (EuMC)*, Madrid, Spain, Sept. 2018.

[89] T. Liu, L. Yang, Q. Lin, Y. Guo, and Y. Liu, "Anchor-free backscatter positioning for RFID tags with high accuracy," in *Proc. of IEEE INFOCOM*, Toronto, Canada, May 2014.

[90] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3901-3911, July 2015.

[91] S. Hong, S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman; S. Katti; and P. Levis, "Applications of self-interference cancellation in 5g and beyond," *IEEE Communications*, vol. 52, no. 2, pp. 114-121, Feb. 2014.

[92] Y. Wang, S. Yan, W. Yang, Y. Huang, and C. Liu, "Energy-efficient covert communications for bistatic backscatter systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, March 2021.

[93] K. Shahzad and X. Zhou, "Covert communication in backscatter radio," in *Proc. of IEEE International Conference on Communications (ICC)*, Shanghai, China, May 2019.

[94] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517-8530, Dec. 2018.

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

[96] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6658-6662, July 2018.

[97] H. Xing, K. 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, Dec. 2016.

[98] 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, Mar. 2015.

[99] 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, Dec. 2015.

[100] H. E. Lee, D. Lee, T. I. Lee, J. H. Shin, G. M. Choi, C. Kim, S. H. Lee, J. H. Lee, Y. H. Kim, S. M. Kang, and S. H. Park, "Wireless powered wearable micro light-emitting diodes," *Nano Energy*, vol. 55, pp. 454-462, 2019.

[101] L. Sigrist, A. Gomez, R. Lim, S. Lippuner, M. Leubin, and L. Thiele, "Measurement and validation of energy harvesting iot devices," in *IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Lausanne, Switzerland, March 2017.

[102] N. V. Huynh, D. N. Nguyen, D. T. Hoang, T. X. Vu E. Dutkiewicz, S. Chatzinotas, "Defeating super-reactive jammers with deception strategy: Modeling, signal detection, and performance analysis." Available online at ArXiv:2105.01308, 2021.

[103] S. Feng, D. Niyato, X. Lu, P. Wang, and D. I. Kim, "Dynamic Game and Pricing for Data Sponsored 5G Systems with Memory Effect," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 4, April 2020.

[104] S. Feng, D. Niyato, X. Lu, P. Wang, and D. I. Kim, "Dynamic Model for Network Selection in Next Generation HetNets with Memory-affecting Rational Users," *IEEE Transactions on Mobile Computing*, April 2021.

[105] D. T. Hoang, X. Lu, D. Niyato, P. Wang, and Z. Han, "Applications of repeated games in wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2102-2135, Fourth quarter 2015.

[106] D. Niyato, P. Wang, D. I. Kim, Z. Han, and X. Lu, "Game theoretic modeling of jamming attack in wireless powered networks," in *Proc. of IEEE ICC*, London, UK, June 2015.

[107] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y. C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2283-2314, Fourthquarter 2020.

[108] Q. Shafi, "Cyber physical systems security: A brief survey," *IEEE ICCSA*, 2012.