IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES ON RADIO ACCESS AND SECURITY METHODS IN 5G NETWORKS

Received September 13, 2017, accepted October 18, 2017, date of publication October 27, 2017, date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2767283

Power-Efficient Secure Transmission Against Full-Duplex Active Eavesdropper: A Game-Theoretic Framework

XIAO TANG[1,2], (Student Member, IEEE), PINYI REN[1,2], (Member, IEEE), AND ZHU HAN[3,4], (Fellow, IEEE)

[1]School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[2]Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China
[3]Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA
[4]Department of Computer Science and Engineering, Kyung Hee University, Seoul 02447, South Korea

Corresponding author: Pinyi Ren (pyren@mail.xjtu.edu.cn)

The work of X. Tang and P. Ren was supported in part by the National Natural Science Foundation of China under Grant 61431011, in part by the National Science and Technology Major Project of China under Grant 2016ZX03001016-005, in part by the Key Research and Development Program of Shannxi Province under Grant 2017ZDXM-GY-012, and in part by the Fundamental Research Funds for the Central Universities. The work of Z. Han was supported in part by the U.S. National Science Foundation (NSF) under Grant CNS-1717454, Grant CNS-1731424, Grant CNS-1702850, Grant CNS-1646607, Grant ECCS-1547201, Grant CMMI-1434789, Grant CNS-1443917, and Grant ECCS-1405121.

ABSTRACT Information security is of paramount importance yet significant challenge for wireless communications. In this paper, we investigate the power-efficient transmissions with security concerns in the presence of a full-duplex (FD) active eavesdropper. With FD capability, the eavesdropper can launch jamming attacks while eavesdropping, which affects the legitimate transmissions, such that the legitimate power allocation becomes more favorable for eavesdropping. However, the jamming attacks require additional power consumption and result in self-interference at the eavesdropper itself. The legitimate user intends for a power-efficient manner to effectively guarantee the secure transmissions to defend against the simultaneous eavesdropping and jamming attacks. We formulate the problem within a Stackelberg game framework, where the eavesdropper takes action first as the leader and the legitimate user acts as the follower. We analyze the security game model for both single-channel and multi-channel cases. Furthermore, by exploring the properties of the game equilibrium, we propose the optimal transmission strategy and jamming strategy for the legitimate transmission and eavesdropping, respectively. Finally, we provide extensive simulation results to corroborate our theoretical analysis and evaluate the security performance.

INDEX TERMS Physical layer security, full-duplex, active eavesdropper, Stackelberg game, equilibrium.

I. INTRODUCTION

The rapid development of wireless technology in recent years has empowered the significant advancement of wireless industry [1]. Along with the emergence of numerous wireless devices and various wireless services, there have raised growing concerns on wireless security [2]. However, the wireless signal, which is transmitted in the open and shared wireless medium, can be easily intercepted by the unintended third parties. In this respect, physical layer security has emerged as a promising solution to safeguard wireless informations security, which complements the conventional encryption-based approaches implemented at the higher protocol layers [3]. The physical layer security techniques exploit the intrinsic randomness of wireless medium for security, which can be easily implemented and have the capability to quickly adapt to different wireless scenarios [4].

On the other hand, the full-duplex (FD) technology is widely regarded as one of the essentials for future wireless networks. The FD technology enables simultaneous transmissions and receptions, which thus has the potential to double the spectral efficiency [5]. With the recently reported results to effectively suppress the self-interference by novel cancellation techniques, we can expect the wide applications of FD communications in the near future [6], [7].

In the literature, most of the existing works on physical layer security are based on the assumption of half-duplex (HD) transmission at the legitimate side as well as its adversary [8]. In the HD scenario, the adversary may

remain passive as an eavesdropper to overhear the legitimate transmission, or launch jamming attacks to degrade the legitimate reception. For the threat from an eavesdropper, the multiple-antenna transmission technique [9]–[17] or cooperative security mechanism [18]–[20] are usually adopted to defend against eavesdropping. While to mitigate jamming attacks, there are also different countermeasures proposed, such as frequency hopping [21], power control [22], reactive transmission [23], and so forth. Recently, there have also emerged the research works that consider the secure transmission under the FD scenario [24]. For these research efforts, most of them have been devoted to the FD-enabled security enhancement strategy, such as the FD transmitter [25], FD receiver [26], [27], FD relay [28], [29].

Although FD capability can be exploited to enhance the wireless security, it may also be potentially applied at the adversary to induce serious security challenges [30]–[32]. These issues, however, have not been sufficiently addressed among the existing research works. Particularly, with FD capability, the eavesdropper can *actively* launch jamming attacks while performing the *passive* eavesdropping, and thus known as an *active eavesdropper*. Facing with an active eavesdropper, the legitimate transmissions are directly degraded due to the jamming attacks, apart from the wiretapping threats. While for the eavesdropper, the active jamming results in self-interference at its own receiver, which negatively affects the eavesdropping as well. Besides the more complicated security threats, the modeling of the security problem has been fundamentally changed when the eavesdropper becomes active. Specifically, a passive eavesdropper generally stays silent without any explicit actions, which allows us to concentrate on the analysis regarding the strategy on the legitimate side. In contrast, when the eavesdropper becomes active with explicit jamming actions, the modeling of jamming actions must be considered in parallel with the investigation on security countermeasures. Further, we need to analyze the interactions between the legitimate transmission behavior and actions by the active eavesdropper. In this respect, game theory is an effective tool to explore such interest-conflicting scenarios. Within the game-theoretical framework, the interactions between the legitimate user and active eavesdropper can be tracked through the game playing. Moreover, the equilibrium reveals the steady states of the playing between them and allows to evaluate the security performance.

Meanwhile, most of the research works on physical layer security intend to optimize the secure transmissions, typically, to maximize of secrecy rate. However, since the eavesdropping usually has evident side effect over the legitimate transmissions, and thus the secure wireless transmissions can be significantly power-consuming. Those approaches, although effective in protecting wireless security, may not be as appropriate for the energy-sensitive wireless scenarios. In this respect, we need to instead consider the power-efficient secure transmissions. While on the other hand, since the active eavesdropper requires additional power consumption to conduct jamming attacks, as compared with a conventional passive eavesdropper, we also need to consider the power consumption issue at the active eavesdropper to investigate the security problem.

Targeting at the aforementioned issues for the power-efficient secure transmissions against a FD active eavesdropper, we investigate this problem by employing game theory. We consider a novel FD active eavesdropper[1] model that the eavesdropper with FD capability intends to improve its wiretap rate by launching jamming attacks, which is different from the conventional active eavesdropper model that attempts to minimize the secrecy rate [31], [32]. With FD empowered jamming attacks conducted simultaneously with eavesdropping, it stimulates the legitimate user to change its transmitting behavior to the desired pattern for the eavesdropping. Meanwhile, the active jamming also results in residual self-interference at the eavesdropper itself and is also charged with a price for jamming power consumption. In particular, the main contribution of this paper can be summarized as follows.

- We investigate the power-efficient secure transmission issue to defend against the active eavesdropping. Specially, we consider a novel jamming-assisted eavesdropping model that the eavesdropper launches the jamming attacks to affect the legitimate transmissions so as to facilitate the eavesdropping. The legitimate user aims at the secure transmission with efficient power utilization while defending against the simultaneously conducted eavesdropping and jamming attacks.
- We consider the single-channel case and formulate the interactions between the legitimate user and eavesdropper as a Stackelberg game where the eavesdropper takes action first as the leader while the eavesdropper is the follower. We analyze the properties of the equilibrium for the game and derive the optimal legitimate transmission strategy and jamming strategy with the closed-form expressions.
- We further extend the Stackelberg game model to the multi-channel scenario. Despite the lack of the closed-form expression, we propose effective algorithms to determine the strategies for the legitimate transmissions as well as jamming attacks.

The remainder of this paper is organized as follows. In Sec. II, we review the related works. In Sec. III, we provide the system model with the FD active eavesdropper. In Sec. IV, we focus on the single-channel scenario, while in Sec. V, we deals with the multi-channel problem. In Sec. VI, the simulation results are provided, and this paper is concluded in Sec. VII.

II. RELATED WORKS

The conventional research works on physical layer security are mostly based on the HD assumption [8]. Under this

[1]For the rest of this paper, we will refer the "FD active eavesdropper" as "active eavesdropper" or "eavesdropper" for simplicity.

assumption, the secure transmission can only be challenged by one single type of attack at each time, i.e., either eavesdropping or jamming. To cope with eavesdropping, one common approach is to adopt the multiple-antenna techniques to perform security-oriented beamforming. In this respect, the legitimate transmission can be directly improved through signal beamforming, or indirected benefited through the artificial noise to confuse the eavesdropper [9]. In [10], the authors consider the secure multiple-input-single-output (MISO) transmission in a multi-cell scenario with extensive performance analysis. In [11], the authors investigate the MISO transmission with imperfect channel state information and propose the robust secure beamforming strategy. In [12], the distributed beamforming strategy is proposed for MISO simultaneous wireless information and power transmission system. In [13], the physical layer security issue is addressed for multi-input multi-output (MIMO) systems. Besides the signal beamforming, the artificial-noise based methods are also widely applied [14]. In [15], the authors investigate the artificial noise assisted secure transmission in small cell networks with stochastic geometry based performance analysis. In [16], the security issue is jointly considered with energy efficient wireless transmission, where the utilization of artificial noise is evaluated for both security and energy concerns. The authors of [17] propose to jointly apply the artificial noise and feedback to enhance the wireless security in the absence of eavesdropper's channel state information. Meanwhile, secure transmission can also be guaranteed with the cooperation from external nodes [18]. In [19], the cooperative beamforming is proposed with multiple relay nodes to achieve secure wireless communications. In [20], the cooperative security issue is jointly investigated with signal and jamming under multiple relaying transmissions. Moreover, there also exist some signal processing based security enhancement mechanisms, such as Fountain coding [33] and constellation rotation [34].

While more recently, there has been more research interest on physical layer security issue for FD transmissions. In [25], the secure transmission strategy at the FD base station is investigated by the joint beamforming over information signals and jamming signals. In [26], the receiver is enabled with FD capability, and thus transmit jamming noise towards the eavesdropper while performing legitimate reception, which improves the secure transmissions. Also, the hybrid HD/FD model receiver assisted secure transmission is investigated for a two-tire decentralized network in [27]. In [28], the wireless security is safeguarded by the FD relay, which demonstrates substantial security performance gain on condition of sufficiently suppressed self-interference. In [29], the FD relay node sends jamming signal to the eavesdropping while relaying the legitimate signal to improve the security. Compared with the blooming researches on employing FD techniques to improve security, the studies on the threats along with FD techniques at the adversary are relatively less. In [31], authors investigate the security problem for a FD eavesdropper who performs eavesdropping and jamming simultaneously to degrade the secrecy performance. In [32], the security degree of freedom is analyzed for the secure transmission in the presence of eavesdropping and jamming attacks.

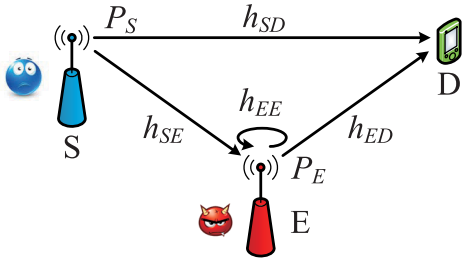


FIGURE 1. System Model.

III. SYSTEM MODEL

We consider a wireless network that consists of a legitimate transmission pair as well as an eavesdropper. We denote the legitimate source node as S, legitimate destination node as D, and the eavesdropper as E, as shown in Fig. 1. For the legitimate nodes S and D, they can only perform HD transmission and reception, respectively. While for the eavesdropper, we assume that it has FD capability, which enables it to perform the simultaneous eavesdropping and jamming attacks. For the legitimate transmission, we assume that the transmit power is P_S which is constrained by the maximum transmit power $P_S^{\max}$. Also, the legitimate link gain from the legitimate source to destination is h_{SD}. In the meantime, the legitimate transmissions are overheard by the eavesdropper, for which we assume the wiretap link gain is h_{SE}. For the eavesdropper, who exploits its FD capability to conduct jamming attacks while eavesdropping, we assume the jamming power is P_E, which is constrained by the maximum allowed power $P_E^{\max}$. For the jamming signal, it affects the legitimate receptions with link gain denoted by h_{ED}. Also, since the jamming and eavesdropping are conducted at the same time at the eavesdropper, the former also negatively influences the latter, known as self-interference, where we denote the self-interference link gain as h_{EE}. Due to the hardware limits, the self-interference cannot be canceled completely. In this respect, we describe the residual self-interference with the self-interference link h_{EE} and a linear coefficient ρ.

We assume the legitimate signal and jamming signal are given by s and w, respectively. Both s and w are of normalized power, i.e., $|s|^2 = 1$ and $|w|^2 = 1$. Then the received signal at the legitimate destination and eavesdropper can be written as

$$x_D = \sqrt{P_S} h_{SD} \cdot s + \sqrt{P_E} h_{ED} \cdot w + z_D, \tag{1}$$

and

$$x_E = \sqrt{P_S} h_{SE} \cdot s + \sqrt{\rho P_E} h_{EE} \cdot w + z_E, \tag{2}$$

respectively, where z_D and z_E denote the noise at the legitimate destination and eavesdropper. Then for the

legitimate link and wiretap link, the corresponding signal-to-interference-plus-noise ratio (SINR) are given as[2],

$$\gamma_D = \frac{P_S \left|h_{SD}\right|^2}{P_E \left|h_{ED}\right|^2 + \sigma_0^2}, \tag{3}$$

and

$$\gamma_E = \frac{P_S \left|h_{SE}\right|^2}{\rho P_E \left|h_{EE}\right|^2 + \sigma_0^2}, \tag{4}$$

respectively, where σ_0^2 denotes the noise power and we assume the same noise power at D and E. For notation simplicity, we define $\alpha_{XY} \triangleq \frac{|h_{XY}|^2}{\sigma_0^2}, X \in \{S, E\}, Y \in \{E, D\}$, as the channel-to-noise ratio. As such, the previously obtained SINRs can be then rewritten as $\gamma_D = \frac{P_S \alpha_{SD}}{P_E \alpha_{ED}+1}$ and $\gamma_E = \frac{P_S \alpha_{SE}}{\rho P_E \alpha_{EE}+1}$. Following the discussions above, we can obtain the transmission rate for the legitimate communication and eavesdropping as

$$R_D = \log_2 (1 + \gamma_D) \tag{5}$$

and

$$R_E = \log_2 (1 + \gamma_E), \tag{6}$$

respectively. Here we assume the channel is of unit bandwidth. Then the secrecy rate for the legitimate transmissions can be obtained as

$$\begin{aligned} R_S &= (R_D - R_E)^+ \\ &= \left(\log_2 \frac{1 + \gamma_D}{1 + \gamma_E}\right)^+, \end{aligned} \tag{7}$$

where the operator $(\cdot)^+$ is equivalent to $\max(\cdot, 0)$.

IV. SINGLE-CHANNEL GAME

In this section, we consider the power-efficient secure communication issue for the single-channel wireless scenario. Then, we formulate the competition between the legitimate user and eavesdropper as a Stackelberg game and derive the equilibrium with the closed-form expressions.

A. GAME MODEL FORMULATION

For the legitimate user, it concerns the secure wireless communication as well as the power consumption. To this end, it specifies a target secrecy rate, denoted by R_0, based on its evaluation on the security requirement. Then, it seeks for the most power-efficient way to achieve such a target, and the problem formulation can thus be given as

$$\min \quad P_S \tag{8a}$$
$$s.t. \quad R_S \geq R_0, \tag{8b}$$
$$0 \leq P_S \leq P_S^{\max}. \tag{8c}$$

[2]Here we adopt the assumption that the legitimate user and active eavesdropper both have the knowledge on the legitimate link and wiretap link. This can be interpreted as the practical scenario that both the legitimate user and eavesdropper belong to the same wireless system. Moreover, as we in this paper emphasize on the competition and interaction among the them, the information availability issue is beyond our main focus.

Meanwhile, the eavesdropper intends for the maximum wiretap rate. To this end, it imposes a jamming signal over the legitimate receiver to affect legitimate transmission in order to facilitate the eavesdropping, which also induces residual self-interference at its own receiver. Moreover, the jamming attack requires additional power consumption as compared with a conventional passive eavesdropper, which is taken into consideration in the form of a linear power price. Therefore, the problem at the eavesdropper can be given as

$$\max \quad U_E = R_E - \theta_E P_E \tag{9a}$$
$$s.t. \quad 0 \leq P_E \leq P_E^{\max}, \tag{9b}$$

where U_E is the utility function of the eavesdropper and θ_E is the coefficient for power price. The utility function incorporates the wiretap rate as the gain and the allocated jamming power as cost. Note when $P_E = 0$, the active eavesdropper reduces to the passive one, and the utility function corresponds to the wiretap rate. Thus our active eavesdropper model here is naturally compatible with the conventional model.

Now we have established the problem for the legitimate user as well as the eavesdropper. We know that in such a communication diagram, the legitimate user needs to adapt to the jamming attacks to achieve the security. Meanwhile, the eavesdropper can only improve its eavesdropping by affecting the legitimate transmission through jamming. Thus, it has to take into account the potential reaction of the legitimate user to determine its strategy. In this regard, the Stackelberg game [35] is perfectly suitable to model such a hierarchical decision-making process. In particular, the eavesdropper takes action first as the leader in the game model and the legitimate user acts as the follower. The follower only needs to react to the action by the leader while the leader needs to consider the follower's action to determine its strategy. The game model is mathematically expressed with problems in (8) and (9). However, we cannot solve these two problems separately, as the behavior of the legitimate user and eavesdropper mutually affects each other, or mathematically, the two problems are coupled. In the following, we will derive the equilibrium of the game, based on which the optimal strategy for the both sides can be derived.

B. THE EQUILIBRIUM

Due to the leader-follower's sequential playing in the Stackelberg game model, we here adopt the backward induction method to solve for the equilibrium.

The backward induction begins with the follower's problem, assuming that the leader's strategy is fixed. Specially for our problem, with fixed jamming power P_E, considering the monotonic relationship between the secrecy rate and legitimate power, the minimum legitimate power is readily obtained by letting the secrecy rate equal the target, i.e., $R_S = R_0$. We can then derive the legitimate power as

$$\bar{P}_S = \left[\frac{1 - \gamma_0}{\frac{\gamma_0 \alpha_{SE}}{\rho P_E \alpha_{EE}+1} - \frac{\alpha_{SD}}{P_E \alpha_{ED}+1}}\right]_0^{P_S^{\max}}, \tag{10}$$

$$P_E^{th} = \frac{-\left((1-\gamma_0)\left(\alpha_{ED}+\rho\alpha_{EE}+P_S^{\max}\alpha_{SD}\rho\alpha_{EE}-P_S^{\max}\gamma_0\alpha_{SE}\alpha_{ED}\right)\right)-\sqrt{\Delta_1}}{2\rho\alpha_{EE}\alpha_{ED}\left(1-\gamma_0\right)} \tag{13}$$

$$\Delta_1 = \left((1-\gamma_0)\left(\alpha_{ED}+\rho\alpha_{EE}+P_S^{\max}\alpha_{SD}\rho\alpha_{EE}-\gamma_0 P_S^{\max}\alpha_{SE}\alpha_{ED}\right)\right)^2 - 4\rho\alpha_{EE}\alpha_{ED}\left(1-\gamma_0\right)\left(1-\gamma_0+P_S^{\max}\alpha_{SD}-\gamma_0 P_S^{\max}\alpha_{SE}\right) \tag{14}$$

$$\frac{\partial U_E}{\partial P_E} = \frac{1}{\log 2}\cdot\frac{\xi\left(1-\gamma_0\right)\left(\rho\alpha_{EE}-\alpha_{ED}\right)}{\left(\left(P_E\alpha_{ED}+1\right)-\xi\left(\rho P_E\alpha_{EE}+1\right)\right)\cdot\left(\gamma_0\left(P_E\alpha_{ED}+1\right)-\xi\left(\rho P_E\alpha_{EE}+1\right)\right)}-\theta_E \tag{17}$$

$$\frac{\partial^2 U_E}{\partial P_E^2} = -\frac{1}{\log 2}\cdot\frac{\xi^2\left(1-\gamma_0\right)^2\left(\rho\alpha_{EE}-\alpha_{ED}\right)^2}{\left(\left(P_E\alpha_{ED}+1\right)-\xi\left(\rho P_E\alpha_{EE}+1\right)\right)^2\cdot\left(\gamma_0\left(P_E\alpha_{ED}+1\right)-\xi\left(\rho P_E\alpha_{EE}+1\right)\right)^2} \tag{18}$$

$$\tilde{P}_E = \frac{-\left(1-\xi\right)\left(\gamma_0\alpha_{ED}-\xi\rho\alpha_{EE}\right)-\left(\gamma_0-\xi\right)\left(\alpha_{ED}-\xi\rho\alpha_{EE}\right)+\sqrt{\Delta_2}}{2\left(\alpha_{ED}-\xi\rho\alpha_{EE}\right)\left(\gamma_0\alpha_{ED}-\xi\rho\alpha_{EE}\right)} \tag{21}$$

$$\Delta_2 = \left[\left(1-\xi\right)\left(\gamma_0\alpha_{ED}-\xi\rho\alpha_{EE}\right)-\left(\gamma_0-\xi\right)\left(\alpha_{ED}-\xi\rho\alpha_{EE}\right)\right]^2 + \frac{4\,\xi}{\theta_E\log 2}\left(\alpha_{ED}-\xi\rho\alpha_{EE}\right)\left(\gamma_0\alpha_{ED}-\xi\rho\alpha_{EE}\right)\left(1-\gamma_0\right)\left(\rho\alpha_{EE}-\alpha_{ED}\right) \tag{22}$$

where $\gamma_0 \triangleq 2^{R_0}$ and $(\,\cdot\,)_a^b = \min\left(\max\left(\,\cdot\,, a\right), b\right)$. Obviously, $\gamma_0 > 1$ needs to be satisfied for a positive secrecy rate, which then yields that the following condition has to hold for a feasible legitimate power allocation

$$\frac{P_E\alpha_{ED}+1}{\rho P_E\alpha_{EE}+1} < \frac{\alpha_{SD}}{\gamma_0\alpha_{SE}}. \tag{11}$$

For the condition above, we can see that due to the monotonous relationship between the left-hand side expression and jamming power P_E, we then obtain the sufficient condition for (11), given as

$$\begin{cases}\gamma_0 < \xi,\\ \frac{\gamma_0}{\xi}\alpha_{ED} < \rho\alpha_{EE},\end{cases} \tag{12}$$

where we define $\xi \triangleq \frac{\alpha_{SD}}{\alpha_{SE}}$ for notation simplicity. The condition in (12) is obtained by considering that (11) holds for the extreme cases corresponding to $P_E = 0$ and $P_E \to \infty$. Then we know that (12) guarantees that (11) holds for any jamming power. Also, from (10), we can see that the threshold jamming power to let the legitimate transmit power exactly equals its maximum is P_E^{th}, given by (13), shown at the top of this page.[3] Obviously, the jamming power should not exceed P_E^{th}, otherwise, the secrecy target is no longer achievable, which further results in the legitimate user ceasing its transmissions and thus the eavesdropper has nothing to wiretap. Then we know that the jamming power should be bounded by

$$P_E^{bound} = \min\left\{P_E^{th}, P_E^{\max}\right\}. \tag{15}$$

Furthermore, if $P_E^{th} < 0$, it implies that even the eavesdropper remains passive, the target secrecy rate is unachievable for the legitimate user under current channel conditions, then both the legitimate user and eavesdropper will terminate their activities.

With the derived optimal power allocation for the legitimate user with respect to a fixed leader's strategy, we can then take such reactions into the leader's problem to determine its strategy. Specifically, by substituting (10) into the eavesdropper's utility function, we then obtain that

$$U_E = \log_2\left(1+\frac{1-\gamma_0}{\gamma_0-\xi\frac{\rho P_E\alpha_{EE}+1}{P_E\alpha_{ED}+1}}\right)-\theta_E P_E. \tag{16}$$

For the eavesdropper's utility function appearing in the form given above, we have the following proposition.

Proposition 1: The eavesdropper's utility function U_E, given by (16), is concave with respect to its jamming power P_E.

Proof: We can easily obtain the first and second derivative of U_E against P_E, given by (17) and (18), shown at the top of this page, respectively. Obviously, we can see that $\frac{\partial^2 U_E}{\partial P_E^2} < 0$, which guarantees that $U_E\left(P_E\right)$ is concave. ■

To derive the optimal jamming power, we first explore some special cases. First, we consider zero jamming power cost, i.e., $\theta_E = 0$. In this case, we can easily prove that the utility function is monotonously increasing with P_E when $\rho\alpha_{EE} < \alpha_{ED}$, and otherwise, monotonously decreasing. Then, obviously, the optimal jamming strategy will be $\bar{P}_E = P_E^{\max}$, if $\rho\alpha_{EE} < \alpha_{ED}$, and $\bar{P}_E = 0$, otherwise. This conclusion can be interpreted as follows. Without the jamming power cost, there only remains the residual self-interference. In this regard, when $\rho\alpha_{EE} < \alpha_{ED}$, which implies that jamming affects the legitimate receiver more than the eavesdropper itself, full jamming power will be used. Otherwise, the jamming negatively influences the eavesdropper itself even more, and thus it is optimal to cease the jamming attacks. Moreover, we inspect the highest jamming price the eavesdropper can afford. To this end, we notice that $\frac{\partial U_E}{\partial P_E}$ is decreasing because of the concavity of the utility function,

[3] Generally, letting $P_S\left(P_E\right) = P_S^{\max}$ results in two roots, denoted by $P_{E,1}^{+}$ and $P_{E,1}^{-}$ with the latter smaller than the former, and we can prove that the latter must be negative. Then the former is selected, given by P_E^{th}. The mathematical details are omitted here for space limitation.

from which we have

$$\frac{\partial U_E}{\partial P_E} \leq \left.\frac{\partial U_E}{\partial P_E}\right|_{P_E=0}. \tag{19}$$

Thus, to ensure the existence of positive extreme point for U_E, i.e., zero point of $\frac{\partial U_E}{\partial P_E}$, we need $\left.\frac{\partial U_E}{\partial P_E}\right|_{P_E=0} > 0$, which implies that

$$\theta_E \leq \frac{1}{\log 2} \cdot \frac{\xi\left(1-\gamma_0\right)\left(\rho\alpha_{EE}-\alpha_{ED}\right)}{\left(1-\xi\right)\left(\gamma_0-\xi\right)}. \tag{20}$$

We denote the right-hand side of (20) as θ_E^{th}. Then, if the jamming power price exceeds θ_E^{th}, it becomes too high for the eavesdropper to launch jamming attacks. In this case, the eavesdropper will stay silent as a passive eavesdropper. When the jamming price is reasonable as $0 \leq \theta_E \leq \theta_E^{th}$, by letting $\frac{\partial U_E}{\partial P_E} = 0$, we obtain the extreme point of U_E given in (21), shown at the top of the previous page,[4] where Δ_2 is represented by (22), shown at the top of the previous page.

Based on the discussions above for different situations, we obtain the optimal jamming power of the active eavesdropper, which is given by

$$\bar{P}_E = \begin{cases} P_E^{\max}, & \text{if } \theta_E = 0 \text{ and } \rho\alpha_{EE} < \alpha_{ED}; \\ \left(\tilde{P}_E\right)_0^{P_E^{bound}}, & \text{if } 0 < \theta_E < \theta_E^{th} \text{ and } \\ & \frac{\gamma_0}{\xi}\alpha_{ED} < \rho\alpha_{EE} < \alpha_{ED}; \\ 0, & \text{otherwise}, \end{cases} \tag{23}$$

where the power allocation $\tilde{P}_E$, naturally, is bounded by the maximum allowed power P_E^{bound}. Here, we can see that the jamming power price should be sufficiently low so as to launch jamming attacks. While for the self-interference, we can see that, on one hand, the existence of certain level self-interference helps guarantee the reachability of the target secrecy rate, as suggested by condition (12). While on the other hand, if the self-interference is too high, exceeding a certain threshold, the jamming has more significant negative effects on the eavesdropper itself as compared with that on the legitimate user. Consequently, the self-interference is both upper-bounded and lower-bounded conditioned for the eavesdropper to launch jamming attacks.

On obtaining the optimal strategy of the jamming power, we can then substitute it into the legitimate user's optimal strategy, given by (10), whose expression is given on condition of fixed jamming power. Then the optimal legitimate power is derived as $\bar{P}_S\left(\bar{P}_E\right)$. Here, we omit the complicated mathematical expression for $\bar{P}_S\left(\bar{P}_E\right)$ to economize the space.

Based on our previous discussions to solve for the optimal strategies for both the legitimate user and eavesdropper, we can have the following conclusion.

Proposition 2: The single-channel Stackelberg game between the legitimate user and active eavesdropper has the unique equilibrium, given by $\left(\bar{P}_S\left(\bar{P}_E\right), \bar{P}_E\right)$.

[4]Generally, solving $\frac{\partial U_E}{\partial P_E} = 0$ implies too roots, denoted by $P_{E,2}^+$ and $P_{E,2}^-$ with $P_{E,2}^+ > P_{E,2}^-$. We can then easily prove that $P_{E,2}^-$ must be negative, and thus the $P_{E,2}^+$ is the only possible solution. When $\theta_E \leq \theta_E^{th}$, $P_{E,2}^+ \geq 0$ is guaranteed, represented by (21), and is the optimal. The mathematical derivations are omitted here for space limitation.

Proof: For the Stackelberg game model, we know from [36] that the equilibrium exists on condition that the follower's best-response strategy with respect to any fixed leader's action is unique. Then, for our formulated game model, we can see that the legitimate user, as the follower, has the unique reaction given in (10) against the eavesdropper's jamming attacks. As such, we can assure the existence of the equilibrium for the game.

While for the leader, we can see that the optimal jamming power, taking the reaction of the follower into consideration, given by (23), is also uniquely determined. Therefore, the equilibrium of the game is thus unique, as given by $\left(\bar{P}_S\left(\bar{P}_E\right), \bar{P}_E\right)$. ■

V. MULTI-CHANNEL GAME

We now focus on the wireless scenario where there are multiple channels available to users. Similar to the single-channel case, we will investigate the security problem against the FD active eavesdropper, who employs jamming attacks to improve eavesdropping. Similarly, we analyze their behavior and track their interactions within the Stackelberg game framework.

A. GAME MODEL FORMULATION

As we consider the multi-channel scenario, we denote the channel set as $\mathcal{N}$, where $|\mathcal{N}| = N$. The notations used in this section have the same interpretation with those in the previous section, while we use a superscript-$n \in \mathcal{N}$ to distinguish the metrics corresponding to different channels.

Similar to the single-channel case, we model the interactions between the interest-conflicting sides as a Stackelberg game where the eavesdropper takes actions first and acts as the leader while the legitimate user is the follower. For the eavesdropper, who intends to maximize its wiretap rate while is confronted with residual self-interference and jamming power price, the problem can be summarized as

$$\max_{\boldsymbol{P}_E} \quad U_E = \sum_{n\in\mathcal{N}} R_E^{(n)} - \theta_E \sum_{n\in\mathcal{N}} P_E^{(n)} \tag{24a}$$

$$s.t. \quad P_E^{(n)} \geq 0, \quad \forall\, n \in \mathcal{N}, \tag{24b}$$

$$\sum_{n\in\mathcal{N}} P_E^{(n)} \leq P_E^{\max}, \tag{24c}$$

where $\boldsymbol{P}_E \triangleq \left[P_E^{(n)}\right]_{n\in\mathcal{N}}$. The eavesdropper needs to optimize the utility function in the multi-channel environment while facing with the maximum jamming power constraint. For the legitimate user, it attempts to minimize the power consumption over all channels while subject to the target secrecy rate constraint, for which the problem can be mathematically given as

$$\min_{\boldsymbol{P}_S} \quad \sum_{n\in\mathcal{N}} P_S^{(n)} \tag{25a}$$

$$s.t. \quad R_S \geq R_0, \tag{25b}$$

$$P_S^{(n)} \geq 0, \quad \forall\, n \in \mathcal{N}, \tag{25c}$$

$$\sum_{n\in\mathcal{N}} P_S^{(n)} \leq P_S^{\max}, \tag{25d}$$

where $\boldsymbol{P}_S \triangleq \left[P_S^{(n)}\right]_{n\in\mathcal{N}}$ and $R_S = \sum_{n\in\mathcal{N}} R_S^{(n)}$. Note the target secrecy rate is constrained on the sum secrecy rate over all channels, rather than at each single channel. In the game, the eavesdropper and legitimate user, respectively, are faced with the problem in (24) and (26). Also, they follow the sequential decision-making process that the eavesdropper takes action first, followed by the legitimate user. However, similar to the single-channel case, we cannot solve those two problems solely as they are coupled, i.e., the determination of jamming power allocation needs to consider the legitimate power allocation as the reaction over different channels, while in turn, the jamming power affects the legitimate power distribution over the channels, as well.

B. THE EQUILIBRIUM

To solve for the equilibrium of the game under multi-channel transmission, we resort to the backward induction method due to the sequential game structure. First, we fix the strategy of the leader and solve for the optimal strategy for the follower, i.e., to solve (25a) on condition of fixed jamming power.

However, before solving the optimization given in (25a), we first need to check its feasibility, i.e., to determine whether the feasible region jointly defined by (25b), (25c), and (25d) is empty. To this end, we consider the problem

$$\max_{\boldsymbol{P}_S} \quad R_S = \sum_{n\in\mathcal{N}} R_S^{(n)} \tag{26a}$$

$$s.t. \quad P_S^{(n)} \geq 0, \quad \forall\, n \in \mathcal{N}, \tag{26b}$$

$$\sum_{n\in\mathcal{N}} P_S^{(n)} \leq P_S^{\max}, \tag{26c}$$

to evaluate the maximum secrecy rate under the given power constraint. To facilitate our discussion, we rewrite the problem above as

$$\max_{\boldsymbol{P}_S} \quad R_S = \sum_{n\in\mathcal{N}} \log_2 \frac{1 + P_S^{(n)} \cdot a_D^{(n)}}{1 + P_S^{(n)} \cdot b_E^{(n)}} \tag{27a}$$

$$s.t. \quad P_S^{(n)} \geq 0, \quad \forall\, n \in \mathcal{N}, \tag{27b}$$

$$\sum_{n\in\mathcal{N}} P_S^{(n)} \leq P_S^{\max}, \tag{27c}$$

where

$$a_D^{(n)} \triangleq \frac{\alpha_{SD}^{(n)}}{P_E^{(n)}\alpha_{ED}^{(n)} + 1} \quad \text{and} \quad b_E^{(n)} \triangleq \frac{\alpha_{SE}^{(n)}}{\rho P_E^{(n)}\alpha_{EE}^{(n)} + 1} \tag{28}$$

can be regarded as the functions with respect to the fixed jamming power $P_E^{(n)}$.

Obviously, in order to achieve positive secrecy rate over a certain channel-n, it requires $a_D^{(n)} > b_E^{(n)}$. Without loss of generality, we assume this condition holds for all channels. Otherwise, we can exclude the channels that violate this condition from the power allocation. For the remaining channels, the following derivations still apply. Then, we can easily verify the inequalities given by

$$\frac{\partial R_S}{\partial P_S^{(n)}} = \sum_{n\in\mathcal{N}} \frac{1}{\log 2} \cdot \frac{a_D^{(n)} - b_E^{(n)}}{\left(1 + P_S^{(n)} a_D^{(n)}\right)\left(1 + P_S^{(n)} b_E^{(n)}\right)} > 0 \tag{29}$$

$$\frac{\partial^2 R_S}{\partial P_S^{(n)} \partial P_S^{(n')}} = 0 \tag{30}$$

and (31), shown at the bottom of this page, which prove that the utility function is increasing and concave with respect to the legitimate power allocation.

On the other hand, the constraints of problem in (27) are obviously convex, which then confirms that the optimization in (27) is a concave problem.

Thanks to the concavity of the optimization (27), we can thus adopt the Lagrange multiplier method [37]. Specially, the Lagrange function can be constructed as

$$\begin{aligned} \mathsf{L}(\boldsymbol{P}_S, \lambda, \boldsymbol{\mu}) = &\sum_{n\in\mathcal{N}} \log_2 \frac{1 + P_S^{(n)} \cdot a_D^{(n)}}{1 + P_S^{(n)} \cdot b_E^{(n)}} \\ &- \lambda\left(\sum_{n\in\mathcal{N}} P_S^{(n)} - P_S^{\max}\right) + \sum_{n\in\mathcal{N}} \mu^{(n)} P_S^{(n)}, \end{aligned} \tag{32}$$

where λ and $\boldsymbol{\mu} = \left[\mu^{(n)}\right]_{n\in\mathcal{N}}$ are the multipliers associated with the sum power constraint and the power constraint over each channel. Then, the optimal solution is required to satisfy the Karush-Kuhn-Tucker condition, specified as

$$\begin{cases} 0 \leq P_S^{(n)} \perp \lambda - \dfrac{\partial R_S}{\partial P_S^{(n)}} \geq 0, \quad \forall\, n \in \mathcal{N}, \\ 0 \leq \lambda \perp P_S^{\max} - \displaystyle\sum_{n\in\mathcal{N}} P_S^{(n)} \geq 0, \end{cases} \tag{33}$$

where $0 \leq x \perp y \geq 0$ indicates that $x \geq 0, y \geq 0$, and $x \cdot y = 0$. From the upper equation in (33), we equivalently have

$$a_D^{(n)} b_E^{(n)} \left(P_S^{(n)}\right)^2 + \left(a_D^{(n)} + b_E^{(n)}\right) P_S^{(n)} = \frac{a_D^{(n)} - b_E^{(n)}}{\lambda \log 2} - 1. \tag{34}$$

$$\frac{\partial^2 R_S}{\partial \left(P_S^{(n)}\right)^2} = -\sum_{n\in\mathcal{N}} \frac{1}{\log 2} \cdot \frac{\left(a_D^{(n)} - b_E^{(n)}\right)\left(2a_D^{(n)} b_E^{(n)} \left(P_S^{(n)}\right)^2 + \left(a_D^{(n)} + b_E^{(n)}\right) P_S^{(n)}\right)}{\left(1 + P_S^{(n)} a_D^{(n)}\right)\left(1 + P_S^{(n)} b_E^{(n)}\right)} < 0 \tag{31}$$

$$\bar{P}_S^{(n)} = \left[\frac{1}{2a_D^{(n)} b_E^{(n)}}\left[-\left(a_D^{(n)} + b_E^{(n)}\right) + \sqrt{\left(a_D^{(n)} - b_E^{(n)}\right)^2 + \frac{4}{\lambda \log 2} a_D^{(n)} b_E^{(n)}\left(a_D^{(n)} - b_E^{(n)}\right)}\right]\right]^+ \tag{36}$$

We can then derive that the equation in (34) has too roots, which are denoted as $P_{S+}^{(n)}$ and $P_{S-}^{(n)}$, with $P_{S+}^{(n)} \geq P_{S-}^{(n)}$. Through basic algebraic operations [38], we can derive that $P_{S+}^{(n)} + P_{S-}^{(n)} = -\frac{a_D^{(n)} + b_E^{(n)}}{a_D^{(n)} b_E^{(n)}} < 0$, which implies that $P_{S-}^{(n)}$ must be negative. Meanwhile, we have $P_{S+}^{(n)} \cdot P_{S-}^{(n)} = 1 - \frac{a_D^{(n)} - b_E^{(n)}}{\lambda \log 2}$, which indicates that the condition for $P_{S+}^{(n)} > 0$ is that $1 - \frac{a_D^{(n)} - b_E^{(n)}}{\lambda \log 2} < 0$, or equivalently,

$$a_D^{(n)} > b_E^{(n)} + \lambda \log 2. \tag{35}$$

The inequality above can be regarded as the sufficient and necessary condition to determine whether or not to transmit over a channel. Denote the channel set satisfying the above condition by $\mathcal{N}'$ for given λ, then the transmit power for legitimate link $n \in \mathcal{N}'$ is derived as (36), shown at the bottom of the previous page, by solving (34). While for $n \in \mathcal{N} \backslash \mathcal{N}'$, we have $P_S^{(n)} = 0$. Due to the fact that utility function is increasing with legitimate transmit power, the Lagrange multiplier λ must satisfy

$$\sum_{n \in \mathcal{N}'} \bar{P}_S^{(n)} = P_S^{\max}. \tag{37}$$

Although we cannot derive the closed-form expression for λ, we can apply numeric method such as the bi-direction search to efficiently find the solution.

Upon obtaining the optimal legitimate transmit power allocation based on (36) and (37), we can then calculate the highest secrecy rate, denoted by $\bar{R}_S$ under the power constraints (25c) and (25d). Then, we compare $\bar{R}_S$ and R_0. Obviously, if the former is larger than the latter, then the target secrecy rate R_0 is achievable, and thus the problem in (26) is feasible. Otherwise, the target secrecy rate R_0 is unachievable.

We then consider the case that the problem in (26) is feasible and revisit the original problem in (25a) to investigate the optimal transmission strategy for the legitimate user. By utilizing the results above regarding problem in (26), we know that the optimal power allocation to maximize the secrecy rate with respect to the power constraint is given by (36) and (37). Then, it indicates that the most power-efficient way to achieve certain secrecy rate also follows the power allocation pattern in (36) with a different multiplier λ that satisfies a certain constraint. On the other hand, we know that the most power-efficient transmission for the problem in (25a) is achieved when the constraint in (25b) is satisfied with equality. Therefore, based on the discussions above that the power allocation pattern satisfies (36) and the constraint in (25c) is satisfied with equality, we know that the optimal power allocation can also be given as (36) with λ replaced by $\bar{\lambda}$ which satisfies

$$\sum_{n \in \mathcal{N}''} R_S^{(n)} \left(\bar{P}_S^{(n)} \right) = P_S^{\max}, \tag{38}$$

where $\mathcal{N}''$ includes the channels that satisfies

$$a_D^{(n)} > b_E^{(n)} + \bar{\lambda} \log 2. \tag{39}$$

Based on the discussions above on the follower's problem, we then have the following proposition regarding the equilibrium of the game.

Proposition 3: The equilibrium of the Stackelberg security game under multi-channel transmission scenario always exists.

Proof: Obviously, we can see that the power allocation in (36) is monotonous with respect to λ (also $\bar{\lambda}$), and then we can obtain the unique root for $\bar{\lambda}$ by solving (38). As such, we know that the optimal power allocation strategy for the power-efficient secure transmission problem in (25a) at the legitimate user is unique. Then, similar to the proof of Proposition 2, we know that the follower's strategy being unique guarantees the existence of equilibrium for the game. Therefore, we can assure the existence of equilibrium for the multi-channel game model. ■

Despite the power allocation appears in the closed-form in (36), we cannot calculate it directly due to the lack of closed-form expression for the multiplier λ (also $\bar{\lambda}$). Then, to obtain the optimal transmission strategy for the legitimate transmission, we can adopt the numeric method. In particular, based on the monotonous relation between power allocation and the multiplier, we can apply the bi-direction search to obtain the desired multiplier $\bar{\lambda}$, following which the power allocation can be obtained efficiently. This process can be summarized below in Algorithm 1.

Algorithm 1 Legitimate Transmission Strategy

```
Initialization: select appropriate minimum and
maximum value for λ̄, given as as λ̄_l and λ̄_r; define a
sufficiently small threshold σ; calculate a_D^(n) and b_E^(n) for
all channels based on given P_E;
repeat
    λ̄ ← (λ̄_l + λ̄_r)/2;
    Determine the temporary transmission strategy
    based on (36) with λ = λ̄;
    for ∀ n ∈ N do
        if (39) fails for channel-n then
            P̄_S^(n) ← 0;
    if Σ_{n∈N} R_S^(n) (P̄_S^(n)) = P_S^max then
        λ̄_r ← λ̄;
    else
        λ̄_l ← λ̄;
until |λ̄_r − λ̄_l| / |λ̄_r| < σ;
Finalize the legitimate transmission strategy according
to (36) with λ = λ̄.
```

For the leader's problem, we then need to substitute the follower's optimal strategy into the leader's problem and solve for the optimal. Specifically, we substitute $\bar{P}_S(P_E)$ given by (36) into the eavesdropper's objective function

and have

$$U_E = \sum_{n\in\mathcal{N}} \log_2\left(1+\frac{\bar{P}_S^{(n)}\left(P_E^{(n)}\right)\alpha_{SE}^{(n)}}{\rho P_E^{(n)}\alpha_{EE}^{(n)}+1}\right) - \theta_E \sum_{n\in\mathcal{N}} P_E^{(n)}. \tag{40}$$

Now we need to maximize U_E given by (40) subject to the constraints (24b) and (24c). Unfortunately, we cannot obtain a well-defined expression for utility function in (40) because of the lack of closed-form expression of $\bar{\lambda}$ in (36). Consequently, we can then only resort to the numeric method searching for the optimal. Similar to some other works [39], we here apply the simulated annealing method, which is specified as Algorithm 2.

Algorithm 2 Jamming Strategy

1 Initialization: setting T, τ, τ^{th}, κ, and δ, randomly generating the power vector $\boldsymbol{P}_E$ and regarding it as the optimal $\bar{\boldsymbol{P}}_E \leftarrow \boldsymbol{P}_E$;
2 **repeat**
3 **for** $t = 1$ *to* T **do**
4 Generate $\boldsymbol{P}'_E$ according to Neighbor $(\boldsymbol{P}_E, \delta)$;
5 Randomly generate χ from the interval $(0, 1)$;
6 **if** $U_E\left(\boldsymbol{P}'_E\right) > U_E\left(\boldsymbol{P}_E\right)$ *or* $\chi < \exp\left(\left(U_E\left(\boldsymbol{P}'_E\right) - U_E\left(\boldsymbol{P}_E\right)\right)/\tau\right)$ **then**
7 $\boldsymbol{P}_E \leftarrow \boldsymbol{P}'_E$;
8 **if** $U_E\left(\boldsymbol{P}_E\right) > U_E\left(\bar{\boldsymbol{P}}_E\right)$ **then**
9 $\bar{\boldsymbol{P}}_E \leftarrow \boldsymbol{P}_E$;
10 $\tau \leftarrow \kappa \cdot \tau$;
11 **until** $\tau < \tau^{th}$;

Due to space limitation, we here do not penetrate into the details of the simulated annealing algorithm, but briefly explain Algorithm 2 below. In the algorithm, T is the maximum iteration times for each temperature and τ represents the temperature. After each round of iteration, the temperature is dropped by factor κ. The temperature has a threshold, given by τ^{th}, which claims the termination of the algorithm. In each iteration, we apply the function Neighbor $(\cdot)$ to select an adjacent power vector with parameter δ. If negative power is allocated for a certain channel (violating constraint (24b)), it is forced to zero. If the sum of jamming power exceeds the maximum power (violating constraint (24c)), we simply adjust the power for each channel by scaling it by factor $P_E^{\max}/\left|\boldsymbol{P}'_E\right|$, where $|\cdot|$ is the sum of all elements for its vector argument. Note from Line 6 of Algorithm 2, we can see that even if the newly selected power vector is not as good as the current one, it is still of positive probability to replace current power vector. This is the key for the algorithm not to be trapped by local optimal which thus enables it to reach the global optimal. Based on [40], we know that the simulated annealing method converges to the global optimal with probability 1, when the time of iteration is sufficiently large.

Now that we have obtained the optimal strategy for the leader, i.e., the jamming power allocation $\bar{\boldsymbol{P}}_E$, based on Algorithm 2. Then, we substitute $\bar{\boldsymbol{P}}_E$ into $\boldsymbol{P}_S\left(\bar{\boldsymbol{P}}_E\right)$ as specified by (36) along with (38), the legitimate transmission strategy $\bar{\boldsymbol{P}}_S\left(\bar{\boldsymbol{P}}_E\right)$ can be then derived accordingly. Finally, $\left(\bar{\boldsymbol{P}}_S\left(\bar{\boldsymbol{P}}_E\right), \bar{\boldsymbol{P}}_E\right)$ constitutes the equilibrium for the Stackelberg security game under the multi-channel scenario.

VI. SIMULATION RESULTS

In this section, we evaluate the security performance with respect to a FD active eavesdropper. We consider the system as illustrated by Fig. 1. The coordinates of legitimate transmitter are (0, 0), while the coordinates of the destination node are (100, 0) (distance in meter). We will consider the cases that the eavesdropper locates at different positions. For the transmission links, we assume the power attenuation exponent is 4 and the transmission experiences Rayleigh flat fading. For the self-interference link at the eavesdropper, we assume the expectation of the link gain is normalized. Also, the background noise power is -100 dBm. The other simulation settings and results will then be specified, respectively, for the single-channel case and multi-channel case.

A. SINGLE-CHANNEL CASE

We first inspect the performance while the eavesdropper locates at different positions with different secrecy targets of the legitimate user. We assume the eavesdropper moves along the straight line from $(0, -150)$ to $(100, -150)$ and we consider the target is $\gamma_0 = 3.5$ or $\gamma_0 = 4.0$ (corresponding to the secrecy rate 1.8 and 2). Meanwhile, we assume the coefficient of residual self-interference is $\rho = 1 \times 10^{-9}$ and the power price coefficient is 1. Also, the maximum transmit power at the legitimate user and maximum jamming power at the eavesdropper is 1 W.

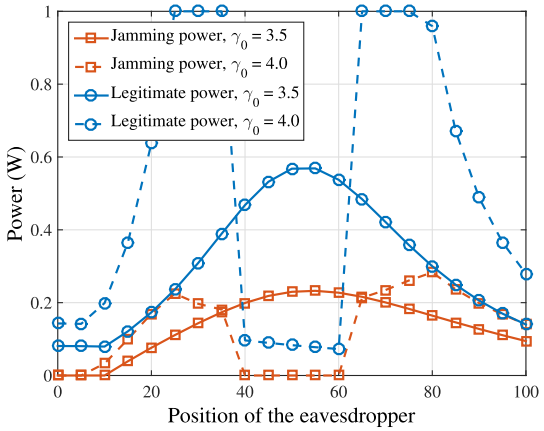


FIGURE 2. Power allocation of legitimate user and eavesdropper when the eavesdropper locates at different positions.

The results are depicted in Figs. 2, 3, and 4. As we can see from Figs. 2 and 3, when secrecy target is 3.5, it can be achieved regardless of the eavesdropper's position. Specially, when the eavesdropper locates near the center

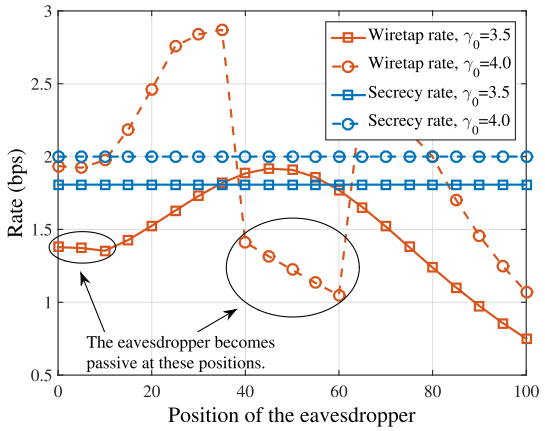


FIGURE 3. The legitimate user's secrecy rate and eavesdropper's wiretap rate when the eavesdropper locates at different positions.

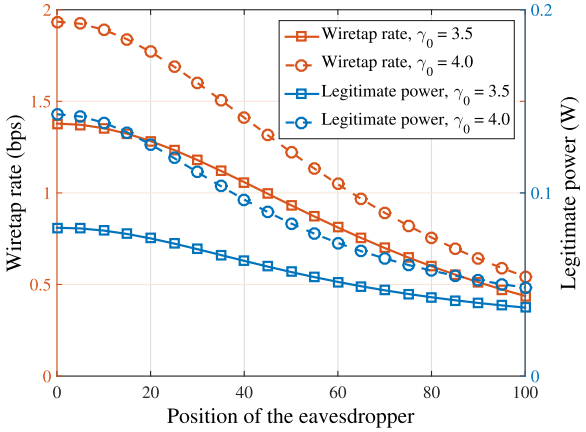


FIGURE 4. The wiretap rate and legitimate power allocation with a passive eavesdropper locating at different positions.

area, it will use relatively high jamming power to obtain a higher wiretap rate. Correspondingly, the legitimate transmit power is also relatively high so as to achieve the secrecy target. This is because that at these positions, the wiretap channel and jamming channel are both in relatively favorable conditions. In contrast, when the eavesdropper is near the boundary, either the eavesdropping link or the jamming link is poor, which limits the effectiveness of improving eavesdropping through jamming. In particular, we notice that, when the secrecy target is 4, there generally requires relatively higher legitimate power to achieve the target. Also, we can see that when the eavesdropper locates from $(25, -150)$ to $(35, -150)$ and from $(65, -150)$ to $(75, -150)$, the eavesdropper can adjust the jamming power such that the legitimate user has to transmit with its maximum power. While the eavesdropper locates around the center area, from $(40, -150)$ to $(60, -150)$, the target secrecy rate cannot be guaranteed with jamming attacks. Then the eavesdropper ceases the jamming attacks and becomes a passive eavesdropper.

In order to more clearly demonstrate the security threats coming from the FD active eavesdropper, in Fig. 4, we present the wiretap rate and the required legitimate transmit power in the presence of a passive eavesdropper. Naturally, the jamming power in this case is zero and the secrecy target is achieved, and these two metrics are thus omitted in the figure. Comparing the results in Fig. 4 and those in Figs. 2 and 3, we can see that the required transmit power will be much lower for the legitimate user to achieve the target facing with a passive eavesdropper. Also, the attainable wiretap rate of the eavesdropper in this case is much lower. Moreover, with the passive eavesdropper moving from left to right, i.e., farther from the legitimate transmitter, the wiretap rate decreases monotonously. While in comparison, the active eavesdropper has chances to even improve the eavesdropping with the assistance from jamming when it moves in the same direction.

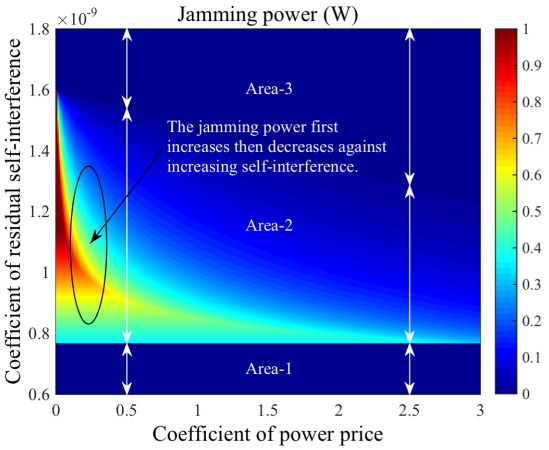


FIGURE 5. Jamming power against coefficients of residual self-interference and jamming power price.

Then, we emphasize the influence of the coefficients of residual self-interference and power price on the performance of the eavesdropper. The basic simulation settings are identical with those we have introduced before, while here we locate the eavesdropper at $(50, -150)$ and set the legitimate user's target as $\gamma_0 = 3$. The results are presented in Figs. 5 and 6. Generally, the behavior of the eavesdropper can be categorized into three types, corresponding to the three areas noted in Figs. 5 and 6. The *Area-1* corresponds to the situation that there is no jamming attack from the eavesdropper, i.e., the passive eavesdropper mode. The legitimate transmission will be suspended if there occur jamming attacks. The eavesdropper, consequently, stays passive to maintain a certain wiretap rate. When it comes to *Area-2*, the jamming attack will be launched as it improves the eavesdropping without causing outage at the legitimate link. We can see from Fig. 6 that the wiretap rate can be significantly increased with the aid of jamming. For *Area-3*, the self-interference is too high that the eavesdropper has to return to the passive mode. The legitimate link needs to be protected from jamming in *Area-1* while the performance of eavesdropper needs protection in *Area-3*. Note that in Fig. 5, we notice the jamming power first increases with the coefficient of residual self-interference and then decreases. This is due to the fact that the jamming power affects the eavesdropper's utility function indirectly, which takes effect through changing the legitimate transmit power.

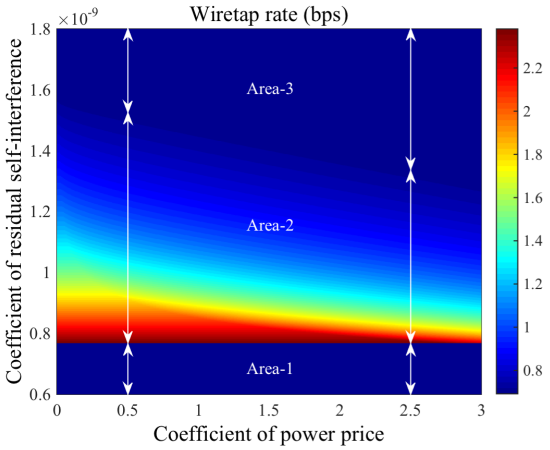


FIGURE 6. Wiretap rate against coefficients of residual self-interference and jamming power price.

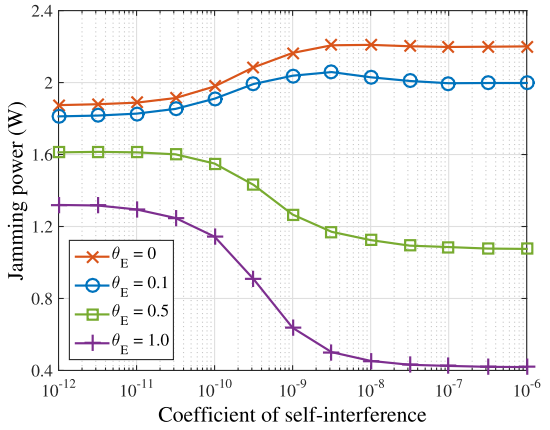


FIGURE 7. Jamming power allocation with respect to the coefficients of self-interference and power price.

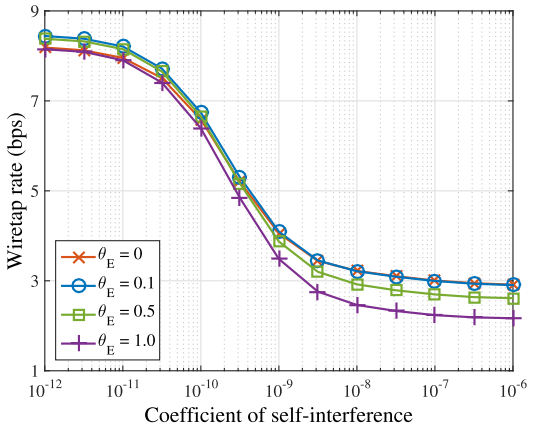


FIGURE 8. Achieved wiretap rate with respect to the coefficients of self-interference and power price.

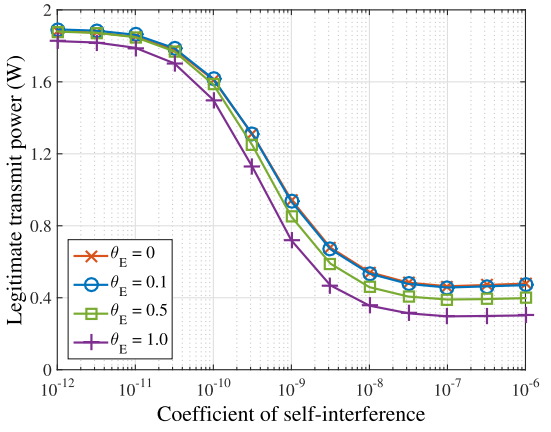


FIGURE 9. Legitimate power allocation with respect to the coefficients of self-interference and power price.

B. MULTI-CHANNEL CASE

For the multi-channel wireless scenario, the basic simulation parameters are the same with those in single-channel cases. Here we consider there are 5 channels available, each is of unit bandwidth. The maximum transmit power for the transmitter and eavesdropper is 2.5 W. The target secrecy rate of the legitimate user is 5 bps.

We first consider the case that the eavesdropper is located with the coordinates $(50, -150)$, and evaluate the security performance with different coefficients of self-interference and power price coefficients. The results are shown in Figs. 7, 8, and 9. In Fig. 7, we show the allocated jamming power at the eavesdropper. Obviously, we can see that when the power price grows higher, the jamming power allocation becomes lower, which is as expected as the price negatively affects the jamming attacks. In particular, when the coefficient of price is relatively high, i.e., $\theta_E = 0.5$ and $\theta_E = 1.0$, the jamming power allocation monotonously decreases as the coefficient of self-interference becomes larger. This is also as expected as the jamming attacks become more conservative when the self-interference is higher. Note the jamming power does not change much when the coefficient of self-interference is sufficiently small, because under these cases, the self-interference has insignificant influence. The similar phenomenon can be observed when the coefficient of self-interference is sufficiently high, which is for the reason that the self-interference now becomes the dominant negative factor for the active eavesdropping. On the other hand, for the cases that the coefficient of power price is sufficiently small, i.e., $\theta_E = 0$ and $\theta_E = 0.1$, we can observe an evident increment of jamming power as the coefficient of self-interference becomes larger. The reason is that, when the self-interference is small, it allows for higher jamming power at the eavesdropper. However, if the eavesdropper follows such actions, it will induce outage at the legitimate user, i.e., the target secrecy rate cannot be achieved. In this case, the eavesdropper has nothing to wiretap, which is against its goal to maximize the wiretap rate. As such, it will elaborately determine its jamming power such that it can achieve the highest wiretap rate with the target secrecy rate at the legitimate user being guaranteed.

The achieved wiretap rate and legitimate transmit power with different coefficients of self-interference and power price at the eavesdropper is shown in Figs. 8 and 9, respectively. As we can see in these two figures, the achieved wiretap rate and the legitimate transmit power decreases

as the coefficients of self-interference and power price increases. This can be explained that, with higher self-interference and power price, the jamming attacks become more conservative as the effectiveness of jamming-aided eavesdropping becomes weaker. Moreover, when the self-interference and power price are higher, the side effect of jamming attacks at the eavesdropper becomes more significant. Then, the achieved wiretap rate can only be smaller and correspondingly, the legitimate power consumption for the target secrecy rate can be lower.

Then, we show the security performance when the eavesdropper locates at different positions and compare the security performance under different schemes. Specifically, we consider the position of the eavesdropper moves from the coordinates $(0, -150)$ to $(100, -150)$. Note that when the eavesdropper locates at $(0, -150)$, it is near the legitimate transmitter while far way from the legitimate receiver, and the thus the wiretap links are in relatively favorable conditions while the jamming links are in poor conditions. The contrary situation holds when the eavesdropper is with the coordinate $(100, -150)$. We fix the coefficient of jamming power price at 0.5. We compare the performance that the active eavesdropper experience the self-interference with the corresponding coefficient being 1×10^{-9} as well as the case that the self-interference is perfectly canceled. Also, we consider the case that the eavesdropper stays silent without any jamming attacks, i.e., as a passive eavesdropper. Moreover, we consider the legitimate user allocates its power according to the water-filling algorithm. The results are shown in Figs 10, 11, 12, and 13.

In Fig. 10, we show the jamming power allocation. For the active eavesdropper without self-interference, we can see that the jamming power slightly increases when it locates near the legitimate receiver. This is as expected as the jamming attacks can be more effectively conducted when it is near the legitimate receiver on condition that the side effect of self-interference is perfectly eliminated. When the active eavesdropper experiences the self-interference, we can see that the jamming power first increases and then decreases as the eavesdropper moves from the left end to the right end. In this case, although the jamming attack improves the eavesdropping, the self-interference also degrades the eavesdropping. As such, the eavesdropper has to trade off these factors, and thus allocates the highest jamming power near the center area. When the eavesdropper stays passive, the jamming power is naturally zero. For the case that the legitimate user follows the water-filling approach, which has deviated from its optimal strategy, we will discuss the results by jointly consider Figs. 10, 11, 12, and 13, given at the end of this section.

In Fig. 11, we show the achieved wiretap rate at the eavesdropper. As we can see, for the cases with active eavesdropping, the achieved wiretap rate first increases and then decreases as the eavesdropper moves from the left end to the right end. As such, we know that for our considered jamming-aided eavesdropping, the wiretap links and jamming links have to be well balanced to obtain the optimal performance. Moreover, the achieved wiretap rate at the left end is higher than that at the right end, which suggests that the quality of wiretap links being favorable is more important than the jamming links being in good condition. The reason is that, the better wiretap link quality benefits the eavesdropping directly, while the jamming attacks can only improve the eavesdropping in an indirect manner. For the passive eavesdropper, naturally, the wiretap rate can only be decreased when eavesdropper moves from the left end to the right end, which only induces worse wiretap links.

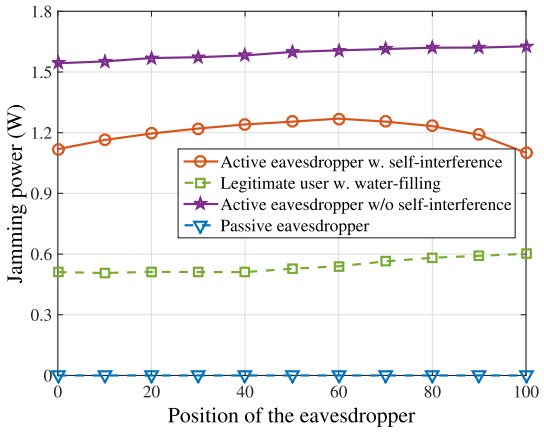


FIGURE 10. Jamming power allocation with respect to the position of the eavesdropper under different schemes.

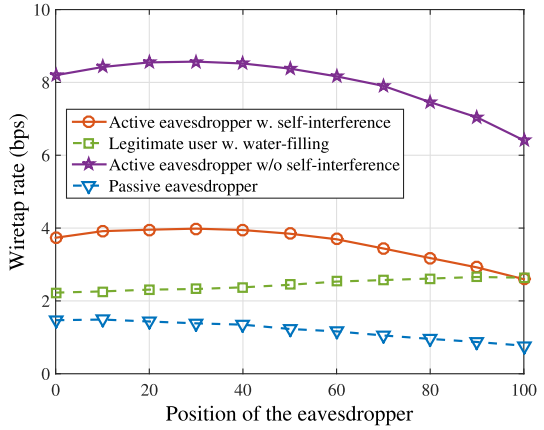


FIGURE 11. Achieved wiretap rate with respect to the position of the eavesdropper under different schemes.

Fig. 12 shows the legitimate transmit power allocation. We first notice that the legitimate transmit power also first increases and then decreases as the eavesdropper moves from left to right, which is of the same trend with the jamming power and the wiretap rate. As we have analyzed before, when the eavesdropper locates near the center area, the jamming-aided eavesdropping is the most effective. Therefore, the legitimate user, which is faced with the target secrecy rate, can only improve the legitimate transmit power as the countermeasure to defend the same target. While for the case with a passive eavesdropper, the target secrecy rate can be easily guaranteed with relatively low legitimate transmit power.

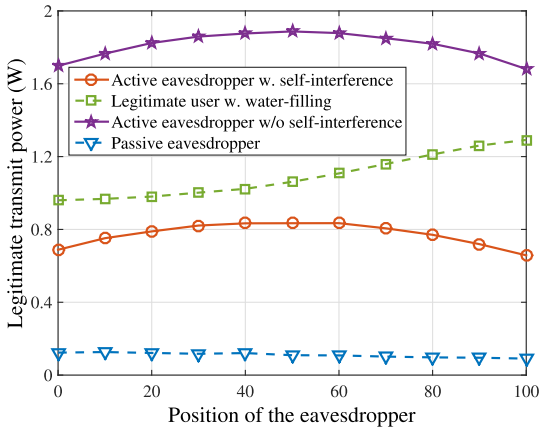


FIGURE 12. Legitimate power allocation with respect to the position of the eavesdropper under different schemes.

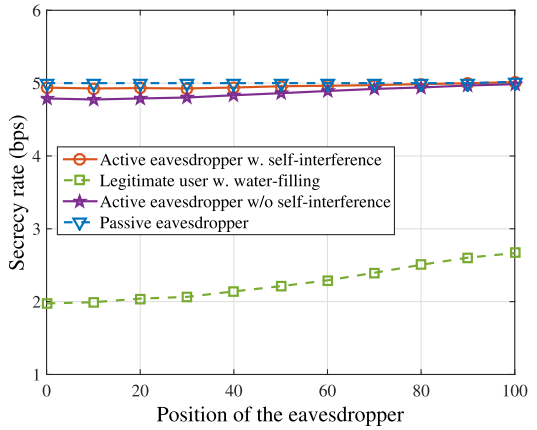


FIGURE 13. Achieved secrecy rate with respect to the position of the eavesdropper under different schemes.

The achieved secrecy rate is shown in Fig. 13. As the legitimate user is with the target secrecy rate, the achieved secrecy rate is thus near the target as long as the legitimate user follows the power allocation in our proposal, regardless of the different situations of the eavesdropper. For the cases the achieved secrecy rate is slightly lower than the target when the eavesdropper is near the left end, it is due to the potential cases that legitimate links are so poor that the target cannot be achieved with the maximum legitimate transmit power, and the results shown in Fig. 13 have to be averaged over such cases.

Now we discuss the case when the legitimate user follows the water-filling approach. Based on our previous analysis regarding Fig. 13, we know that the evidently lower secrecy rate under the water-filling approach is due to the fact that target secrecy rate is often unachievable. For those cases, the legitimate user will cease its transmission and the eavesdropper will stay passive. As the achieved secrecy rate is quit low, we can safely estimate there occur many such simulation trails. Then, revisiting the previous results, we notice that the lower jamming power shown in Fig. 10, and lower wiretap rate shown in Fig. 11, are also due to the numerous simulation trails that the legitimate transmission is canceled and the eavesdropper has nothing to wiretap. However, in Fig. 12, we can see that the legitimate transmit power is relatively high, in spite of the many simulations trials that the legitimate transmission is ceased. It is then implied that, for the cases that legitimate transmissions are conducted, the legitimate transmit power must be quit high. Therefore, the water-filling approach cannot effectively guarantee the security, and cannot achieve power-efficient transmission, neither.

VII. CONCLUSIONS

In this paper, we investigate the power-efficient secure wireless communication in the presence of a FD active eavesdropper. We consider a novel eavesdropping model that the eavesdropper is capable to launch jamming attacks to affect the legitimate transmission so as to improve the eavesdropping. While the eavesdropper also faces the challenges from self-interference and jamming power price. We employ the Stackelberg game problem formulation to model their competition. We analyze the game for the single-channel and multi-channel scenarios. The simulation results demonstrate that, our proposal can effectively guarantee the wireless security with efficient power utilization. Meanwhile, with sufficiently suppressed the self-interference and moderate power price, the jamming attacks can also effectively improve the eavesdropping, which thus presents significant security challenge as compared with the conventional passive eavesdropper model.

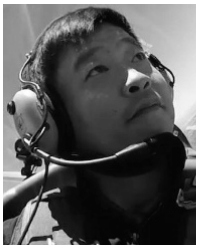
REFERENCES

[1] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[4] 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 Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[5] G. Liu, F. R. Yu, H. Ji, V. C. M. Leung, and X. Li, "In-band full-duplex relaying: A survey, research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 500–524, 2nd Quart., 2015.
[6] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM*, Hong Kong, Aug. 2013, pp. 375–386.
[7] L. Song, R. Wichman, Y. Li, and Z. Han, *Full-Duplex Communications and Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2017.
[8] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.
[9] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.
[10] X. Chen and H.-H. Chen, "Physical layer security in multi-cell MISO downlinks with incomplete CSI—A unified secrecy performance analysis," *IEEE Trans. Signal Process.*, vol. 62, no. 23, pp. 6286–6297, Dec. 2014.
[11] J. Xu, S. Xu, and C. Xu, "Probabilistic robust secure beamforming in MISO channels with imperfect LCSI and statistical ECSI," *IEEE Access*, vol. 5, pp. 10277–10284, 2017.
[12] R. Feng, M. Dai, and H. Wang, "Distributed beamforming in MISO SWIPT system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5440–5445, Jun. 2017.

[13] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[15] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.
[16] A. Zappone, P.-H. Lin, and E. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1462–1477, Dec. 2016.
[17] H. He, P. Ren, Q. Du, and H. Lin, "Joint feedback and artificial noise design for secure communications over fading channels without eavesdropper's CSI," *IEEE Trans. Veh. Technol.*, to be published.
[18] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.
[19] Q. Li, Y. Yang, W. K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.
[20] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition," *IEEE Trans. Veh. Technol.*, to be published.
[21] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 16–30, Jan. 2012.
[22] X. Tang, P. Ren, Y. Wang, Q. Du, and L. Sun, "Securing wireless transmission against reactive jamming: A Stackelberg game framework," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.
[23] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: A game-theoretic analysis," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2337–2352, May 2015.
[24] X. Tang, P. Ren, and Z. Han, "Distributed power optimization for security-aware multi-channel full-duplex communications: A variational inequality framework," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 4065–4079, Sep. 2017.
[25] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.
[26] L. Chen, Q. Zhu, W. Meng, and Y. Hua, "Fast power allocation for secure communication with full-duplex radio," *IEEE Trans. Signal Process.*, vol. 65, no. 14, pp. 3846–3861, Jul. 2017.
[27] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.
[28] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
[29] J. Qiao, H. Zhang, D. Wu, and D. Yuan, "Secrecy rate analysis for jamming assisted relay communications systems," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, Apr. 2015, pp. 3143–3147.
[30] X. Tang, P. Ren, and Z. Han, "Combating full-duplex active eavesdropper: A game-theoretic perspective," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
[31] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in mimo wiretap channels: Construction and countermeasures," in *Proc. Conf. Rec. 45th Asilomar Conf. Signals, Syst. Comput. (ASILOMAR)*, Pacific Grove, CA, USA, Nov. 2011, pp. 265–269.
[32] L. Li, A. P. Petropulu, and Z. Chen, "MIMO secret communications against an active eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2387–2401, Oct. 2017.
[33] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 291–300, Feb. 2016.
[34] L. Sun, Q. Du, P. Ren, and Y. Wang, "Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8767–8774, Oct. 2016.
[35] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks*. New York, NY, USA: Cambridge Univ. Press, 2011.
[36] R. Lucchetti, F. Mignanego, and G. Pieri, "Existence theorems of equilibrium points in Stackelberg," *Optimization*, vol. 18, no. 6, pp. 857–866, 1987.
[37] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
[38] E. B. Vinberg, *A Course in Algebra*. Providence, RI, USA: AMS, 2003.
[39] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A Stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 4038–4047, Aug. 2013.
[40] V. Granville, M. Krivanek, and J.-P. Rasson, "Simulated annealing: A proof of convergence," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 6, pp. 652–656, Jun. 1994.

XIAO TANG (S'14) received the B.S. degree in information engineering (Elite Class Named after Tsien Hsue-shen) from Xi'an Jiaotong University, in 2011, where he is currently working toward the Ph.D. degree in information and communications engineering. From 2015 to 2016, he was a Visiting Student at the Department of Electrical and Computer Engineering, University of Houston. His research interests include wireless communications and networking, game theory, and physical layer security.

PINYI REN (M'10) received the B.S. degree in information and control engineering, the M.S. degree in information and communications engineering, and the Ph.D. degree in electronic and communications system from Xi'an Jiaotong University, China, in 1994, 1997, and 2001, respectively. He is currently a Professor at the Information and Communications Engineering Department, Xi'an Jiaotong University. He has published over 100 technical papers in international journals and conferences. He holds over 15 patents (first inventor) authorized by Chinese Government. He received the Best Letter Award from the IEICE Communications Society 2010. He has served as the General Chair of the ICST WICON 2011, and frequently serves as the Technical Program Committee members of the IEEE GLOBECOM, the IEEE ICC, and the IEEE CCNC. He serves as an Editor of the *Journal of Xi'an Jiaotong University*, and has served as the Leading Guest Editor of the Special Issue of Mobile Networks and Applications on Distributed Wireless Networks and Services and the special issues of the *Journal of Electronics on Cognitive Radio.*



ZHU HAN (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer at JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an Assistant Professor at Boise State University, Idaho, USA., He is currently a Professor at the Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several Best Paper Awards in the IEEE conferences. He is an IEEE Communications Society Distinguished Lecturer.