Jamming-assisted Eavesdropping over Parallel Fading Channels

Yitao Han, Lingjie Duan, *Senior Member, IEEE,* and Rui Zhang, *Fellow, IEEE*

Abstract—Unlike passive eavesdropping, proactive eavesdropping is recently proposed to use jamming to moderate a suspicious link's communication rate for facilitating simultaneous eavesdropping. This paper advances the proactive eavesdropping research by considering a practical half-duplex mode for the legitimate monitor (e.g., a government agency) and dealing with the challenging case that the suspicious link opportunistically communicates over parallel fading channels. To increase eavesdropping success probability, we propose cognitive jamming for the monitor to change the suspicious link's long-term belief on the parallel channels' distributions, and thereby induce it to transmit more likely over a smaller subset of unjammed channels with a lower transmission rate. As the half-duplex monitor cannot eavesdrop the channel that it is simultaneously jamming to, our jamming design should also control the probability of such "own goal" that occurs when the suspicious link chooses one of the jammed (uneavesdroppable) channels to transmit. We formulate the optimal jamming design problem as a mixed integer nonlinear programming (MINLP) and show that it is non-convex. Nevertheless, we prove that the monitor should optimally use the maximum jamming power if it decides to jam, for maximally reducing suspicious link's communication rate and driving the suspicious link out of the jammed channels. Then we manage to simplify the MINLP to integer programming and reveal a fundamental trade-off in deciding the number of jammed channels: jamming more channels helps reduce the suspicious link's communication rate for overhearing more clearly, but increases own goal probability and thus decreases eavesdropping success probability. Finally, we extend our study to the two-way suspicious communication scenario, and show there is another interesting trade-off in deciding the common jammed channels for balancing bidirectional eavesdropping performances. Numerical results show that our optimized jamming-assisted eavesdropping schemes greatly increase eavesdropping success probability as compared with the conventional passive eavesdropping.

Index Terms—Wireless surveillance, jamming-assisted eavesdropping, half-duplex monitor, parallel fading channels, eavesdropping success probability, bidirectional eavesdropping.

I. INTRODUCTION

Security issues in wireless communication have drawn increasingly more attentions from both academia and industry. Due to the broadcast nature of wireless communication, its physical layer is vulnerable to eavesdropping (interception of confidential information) and jamming (interruption of legitimate transmission) [1], and there are many works focusing on defence schemes against eavesdropping and jamming, such as secrecy beamforming [2]–[4], channel-based secret key [5],

Y. Han and L. Duan are with the Engineering Systems and Design Pillar, Singapore University of Technology and Design (e-mail: yitao_han@mymail.sutd.edu.sg, lingjie_duan@sutd.edu.sg).

R. Zhang is with the Department of Electrical and Computer Engineering, National University of Singapore (e-mail: elezhang@nus.edu.sg).

using cooperative networks to avoid eavesdropping [6] and using hopping to avoid jamming attacks [7]. These works view eavesdropping or jamming as malicious attacks and assume all the communication links are rightful (see [8]–[13]). However, they overlook the emerging case that wireless links or devices can be established and used by criminals or terrorists to present severe public security threats.

With the fast development of wireless technologies and devices, user-controlled or infrastructure-free communications (e.g., ad hoc network and short-range communication) now become popular. For examples, mobile applications such as MeshMe and FireChat can network users in the vicinity with reliable mutual connection, and drones can take nice photos or videos and send back to their users. While providing great convenience to normal users, these new technologies and devices can be misused to commit crimes. Terrorists can use them to facilitate their plotting and acts, and spies can use them to send out commercial or military secrets. Since the data do not go through any public infrastructure under internet service providers (ISPs), it is difficult to be monitored by government surveillance program. As a result, prior methods (e.g., deploying dedicated wiretapping devices in network infrastructure) for eavesdropping infrastructure-based communications (e.g., cellular networks) no longer work. There is thus a growing need for authorized parties to develop new approaches to legitimately eavesdrop these infrastructure-free suspicious wireless communications. For example, in the USA, the National Security Agency has launched Terrorist Surveillance Program and aims to intercept all wireless devices [14] to protect public security.

Traditionally, passive eavesdropping is used for such surveillance purpose but it does not provide good eavesdropping performance once the suspicious transmitter (ST) is far away from the monitor or hops to an undesirable channel. Recently, a novel approach called proactive eavesdropping via jamming is proposed in [15], [16], where the legitimate monitor, ideally operating in full-duplex mode, uses jamming to moderate the suspicious communication rate for facilitating simultaneous eavesdropping. [17] extends this work by assuming the legitimate monitor's knowledge of full channel state information (CSI) and designs adaptive jamming power in each fading block. [18] studies the case that the suspicious link adopts HARQ-based communication. [19] further considers that the monitor is equipped with multiple antennas to achieve more efficient jamming and better eavesdropping performance. [20] proposes another efficient eavesdropping method, where the monitor disguises as a fake relay to overhear the suspicious communication. These works largely assume that there is only

Fig. 1. System model of jamming-assisted eavesdropping over the suspicious link (suspicious transmitter to receiver).

one communication channel between the ST and suspicious receiver (SR), and they require the monitor to operate in interference-free full-duplex mode for enabling simultaneous jamming and eavesdropping. However in practice, full-duplex mode is difficult to implement, and self interference cancellation is hard to achieve as perfect [21] [22]. Rather, half-duplex mode is more widely used, and usually there is more than one channel for the suspicious link to communicate over.

In this paper, we study a practical wireless surveillance scenario: a half-duplex legitimate monitor eavesdrops from a suspicious communication link over parallel independent Rayleigh fading channels. As shown in Fig. 1, at the beginning of each fading block, based on the conditions of the parallel independently fading channels, the ST hops to the best one for transmission in this fading block.[1] Here we assume a typical delay-sensitive application (e.g., video talk) on the suspicious link, i.e., the transmitter adjusts its transmission rate by maintaining a certain target outage probability at the receiver [16]. Usually, the monitor is far away from the ST to stay undetected, which makes the traditional passive eavesdropping difficult or even infeasible. Under this challenging setup, the monitor can deliberately send jamming signals to the SR to induce the ST to transmit more likely over a smaller subset of unjammed channels with a lower transmission rate, so that the monitor can still eavesdrop effectively.

To avoid getting exposed, the monitor will not change its jamming power and jammed channels over time, it just disguises itself as a normal device-to-device (D2D) user in sharing the network, by sending randomly modulated messages over fixed channels with fixed power. The ST/SR is aware of its co-existence in the same network by updating the long-term belief of the parallel channels' distributions, but does not consider it as a jammer. If the monitor keeps changing its jammed channels or jamming power, then it is no longer like a normal user and will cause the ST/SR's suspicion to hop over channels to increase resilience in a game theoretic setting or directly stop transmitting any message as in [7] [23] [24].

The key novelty and main contributions of this paper are summarized as follows.

- *Novel jamming-assisted eavesdropping approach over parallel fading channels:* To our best knowledge, this is the first paper studying wireless surveillance of parallel fading channels via a half-duplex monitor. The monitor uses jamming to change the suspicious link's long-term belief on the parallel channels' distributions, and thereby induce it to transmit more likely in a smaller subset of unjammed channels with a lower transmission rate for higher eavesdropping success probability. For practical concern, we consider a challenging case that the monitor has no instantaneous CSI of any suspicious link channels, and the monitor in half-duplex mode cannot eavesdrop a channel that it is simultaneously jamming to.
- *Joint optimization of jamming power and number of jammed channels:* We formulate the problem for optimal jamming design over parallel fading channels as a mixed integer nonlinear programming (MINLP) and show it is non-convex. Nevertheless, we prove that the monitor should use the maximum jamming power if it decides to jam. Then we manage to simplify the MINLP to integer programming and further show that there is a fundamental trade-off in deciding the number of jammed channels: jamming more channels helps reduce the suspicious communication rate for overhearing more clearly, but at the risk that the ST is more likely to choose among the jammed channels to transmit and as a result cannot be overheard.
- *Jamming-assisted eavesdropping over two-way communications:* We extend the model to consider the two-way communications of the suspicious link. As the monitor cannot change its jamming strategy to avoid getting exposed, it needs to jam the same subset of channels for both communication directions. To decide the optimal number of jammed channels, we show there is another trade-off to balance the eavesdropping performances of the two-way communications.
- *Performance evaluation:* Numerical results show that our jamming-assisted eavesdropping schemes achieve great performance gain over conventional passive eavesdropping. We also show that the monitor will perform passive eavesdropping only when it is close to the ST, and will jam increasingly more channels when it is moving away from the ST to SR, due to deteriorating eavesdropping channels and improving jamming channels.

The rest of this paper is organized as follows. In Section II, we present the system model and formulate the legitimate monitor's proactive eavesdropping design problem. In Section III, we solve the eavesdropping optimization problem in the special two-channel case to gain useful insights. In Section IV, we extend to multi-channel case and show an interesting trade-off in deciding the number of jammed channels, for eavesdropping success probability maximization. In Section V, we further consider jamming-assisted eavesdropping over two-way communications. In Section VI, we provide more numerical results to evaluate our jamming-assisted eavesdropping approach. Finally, we conclude this paper in Section VII.

---

[1]This approach of channel hopping and selection is commonly used in the multi-channel scenario to enhance wireless security against eavesdropping and jamming (e.g., [7]). In the future work, we will further consider the case that the ST uses multiple channels to transmit, e.g., by deploying waterfilling-based power allocation over multiple channels, which will bring more challenges to legitimate eavesdropping.

TABLE I
SYMBOLS AND THEIR PHYSICAL MEANINGS

Symbols	Physical meanings
N	Total number of parallel channels.
n	Number of jammed channels.
g_{ai}, g_{bi}, g_{ci}	Channel power gain of the suspicious link with mean $1/\lambda_a$, eavesdropping link with mean $1/\lambda_b$, jamming link with mean $1/\lambda_c$, on channel i.
P	ST's transmitting power.
Q_i	Monitor's jamming power on channel i.
$Q_{\max}$	Jamming power budget of the monitor.
σ_a^2, σ_b^2, σ_c^2	Noise power level at the SR, the monitor, the ST.
R^I, R^{II}	Suspicious transmission rate of passive eavesdropping, jamming-assisted eavesdropping.
δ	Target outage probability at the SR.
ρ	Own goal probability (probability that one of the jammed channels is chosen by the ST for transmission).
φ^I, φ^{II}	Eavesdropping success probability of passive eavesdropping, jamming-assisted eavesdropping.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, the ST communicates with the SR over $N \geq 2$ parallel channels with independent Rayleigh fading, and there is a legitimate monitor aiming to eavesdrop their communications. We consider a quasi-stationary system model, where the monitor has sufficient time (before the ST and SR's movement to another locations) to learn the global channel distribution information (CDI) and launch jamming to eavesdrop from the suspicious link's transmission. The ST and SR are both equipped with one antenna, while the legitimate monitor is purposely equipped with two antennas, one for receiving (eavesdropping) and the other for transmitting (jamming). In order to characterize the fundamental performance limit of this jamming-assisted eavesdropping approach, we assume the encryption method used by the ST/SR is known to the monitor beforehand (e.g. via eavesdropping the related encryption codebook). Note that the focus of this work is on decoding the message instead of decrypting the message itself. The monitor disguises itself as a normal user in sharing the same set of channels with the suspicious link, and operates at half-duplex mode, which means it cannot eavesdrop the channel that it is jamming to. Thus, the monitor will not jam all N channels, otherwise, it overhears nothing. There are two eavesdropping schemes to investigate and compare:

- *Scheme I (passive eavesdropping):* The legitimate monitor performs passive eavesdropping over all N channels while jamming no channels. This is also a benchmark case for our proposed jamming-assisted eavesdropping to compare with.
- *Scheme II (jamming-assisted eavesdropping):* The legitimate monitor performs jamming-assisted eavesdropping by jamming n channels and eavesdropping from the rest $N - n$ channels, where $1 \leq n \leq N - 1$.

We consider a block fading model, where the channel stays unchanged in each fading block and may vary over different fading blocks. As shown in Fig. 1, we respectively denote the channel power gains of the suspicious communication link, eavesdropping link (from the ST to the monitor) and jamming link (from the monitor to the SR) on channel $i \in \{1, \cdots, N\}$ as g_{ai}, g_{bi} and g_{ci}. By considering independent Rayleigh

fading, g_{ai}, g_{bi} and g_{ci} are modelled as independent exponentially distributed random variables with mean $1/\lambda_a$, $1/\lambda_b$ and $1/\lambda_c$, respectively, with $i \in \{1, \cdots, N\}$. This suggests that all the suspicious link channels (g_{ai}, $\forall i$) are independent and identically distributed (i.i.d.), so are the eavesdropping channels (g_{bi}, $\forall i$) and the jamming channels (g_{ci}, $\forall i$). Hence in Scheme II, in statistical sense it does not matter which channels to jam given the jammed channel number by the monitor (who does not know the instantaneous CSI of any suspicions link channels). Thus, without loss of generality, we assume the half-duplex monitor picks the first n out of N channels to jam, and eavesdrops from the rest $N - n$ channels. We assume that the monitor only knows the global CDI ($1/\lambda_a$, $1/\lambda_b$ and $1/\lambda_c$), which can be obtained by the monitor through long-term observation as mentioned earlier.

On the other hand, we consider that the ST knows the CSI of all the suspicious communication channels (i.e., g_{ai}'s instantaneous values). The ST transmits at a fixed power P and keeps hopping to the best channel for transmission in each fading block. For ease of reading, Table I summarizes the main symbol notations used in this paper and their physical meanings.

A. Monitor's expected performance of the suspicious link without or with jamming

Both the signal sent by the ST and the jamming signal sent by the monitor are assumed to be circularly symmetric complex Gaussian (CSCG) random variables. This is because that CSCG message will achieve channel capacity given CSCG noise, and monitor's CSCG jamming signal will achieve the best jamming effect [8].

In Scheme I, the monitor does not jam, and the achievable rate of suspicious communication on channel $i \in \{1, \cdots, N\}$ is $\log_2(1 + \frac{g_{ai}P}{\sigma_a^2})$ in bits/second/Hertz (bps/Hz), where σ_a^2 denotes the noise power at the SR. The monitor expects the signal-to-noise ratio (SNR) $\frac{g_{ai}P}{\sigma_a^2}$ at the SR on the ith channel is a random variable, with cumulative distribution function (CDF) given by

$$\mathbb{P}\left(\frac{g_{ai}P}{\sigma_a^2} \leq \gamma\right) = 1 - e^{-\frac{\lambda_a \sigma_a^2}{P}\gamma}, \quad \gamma \geq 0. \quad (1)$$

In Scheme II, the monitor jams by allocating $Q_i \geq 0$ power to channel $i \in \{1, \cdots, N\}$, and thus the achievable rate of suspicious communication channel i is $\log_2(1 + \frac{g_{ai}P}{g_{ci}Q_i + \sigma_a^2})$. The monitor expects the signal-to-interference-plus-noise ratio (SINR) at the SR on the ith channel is a random variable, with CDF given by the following lemma.

Lemma 2.1: In Scheme II, the CDF of SINR $\frac{g_{ai}P}{g_{ci}Q_i + \sigma_a^2}$ at the SR under jamming is given by

$$\mathbb{P}\left(\frac{g_{ai}P}{g_{ci}Q_i + \sigma_a^2} \leq \gamma\right) = 1 - \frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P}\gamma}}{\lambda_c P + \lambda_a Q_i \gamma}, \quad \gamma \geq 0. \quad (2)$$

Proof: See Appendix A. ∎

Based on (1) and (2) under the two eavesdropping schemes, we are ready to formulate the monitor's design objective.

In Scheme I, the legitimate monitor performs passive eavesdropping. The ST will choose the best channel, i.e., the one with the highest SNR, in each fading block. From (1), the monitor's expected CDF of the maximum SNR γ^I at the SR among all the channels is

$$\mathbb{P}\left(\gamma^I = \max\left\{\frac{g_{a1}P}{\sigma_a^2}, \cdots, \frac{g_{aN}P}{\sigma_a^2}\right\} \leq \gamma\right)$$
$$= \left(1 - e^{-\frac{\lambda_a \sigma_a^2}{P}\gamma}\right)^N, \quad \gamma \geq 0. \quad (3)$$

We consider a typical delay-sensitive transmission model for the suspicious link, where the ST adjusts its transmission rate to keep a target outage probability δ at the SR. Only when the transmission rate R^I is no larger than the achievable rate of the best suspicious communication channel $r_a^I = \log_2(1+\gamma^I)$, the SR can successfully decode the delay-sensitive message. Thus we have

$$\mathbb{P}(r_a^I < R^I) = \delta, \quad (4)$$

which yields the suspicious transmission rate R^I as

$$R^I = \log_2\left(1 + \frac{P}{\lambda_a \sigma_a^2} \ln \frac{1}{1 - \delta^{\frac{1}{N}}}\right). \quad (5)$$

In Scheme II, the legitimate monitor performs jamming-assisted eavesdropping and jams $n \geq 1$ channels. Under jamming, the ST will choose the channel with the highest SINR among the n jammed channels or the channel with the highest SNR among the remaining $N-n$ channels without jamming in each fading block. Note that ST's chosen channel may still be a jammed channel by the monitor due to independent channel fading. From (1) and (2), the monitor's expected CDF of the maximum SINR or SNR γ^{II} at the SR among all the channels is

$$\mathbb{P}\left(\gamma^{II} = \max\left\{\frac{g_{a1}P}{g_{c1}Q_1 + \sigma_a^2}, \cdots, \frac{g_{an}P}{g_{cn}Q_n + \sigma_a^2}, \right.\right.$$
$$\left.\left. \frac{g_{a(n+1)}P}{\sigma_a^2}, \cdots, \frac{g_{aN}P}{\sigma_a^2}\right\} \leq \gamma\right)$$
$$= \left(1 - e^{-\frac{\lambda_a \sigma_a^2}{P}\gamma}\right)^{N-n} \prod_{i=1}^{n}\left(1 - \frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P}\gamma}}{\lambda_c P + \lambda_a Q_i \gamma}\right), \quad \gamma \geq 0. \quad (6)$$

To maintain target outage probability δ at the SR, the ST

sets the transmission rate R^{II} to ensure

$$\mathbb{P}(\log_2(1 + \gamma^{II}) < R^{II}) = \delta, \quad (7)$$

which yields

$$\left(1 - e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R^{II}}-1)}\right)^{N-n} \prod_{i=1}^{n}\left(1 - \frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R^{II}}-1)}}{\lambda_c P + \lambda_a Q_i (2^{R^{II}}-1)}\right) = \delta. \quad (8)$$

With its jamming power allocations $\{Q_i\}_{i=1}^{n}$, the monitor believes the ST will use rate R^{II} to transmit. Note that there is no closed-form solution R^{II} to equation (8).

B. Monitor's problem formulation for jamming-assisted eavesdropping

The legitimate monitor aims to maximize the eavesdropping success probability on the suspicious communication, which is the percentage of fading blocks it can successfully decode.

In Scheme I, assuming the suspicious communication is on the ith channel in a certain fading block, only when the achievable rate of the ith eavesdropping channel is no smaller than the suspicious transmission rate R^I in (5), the monitor can successfully eavesdrop in this fading block. Thus, the eavesdropping success probability φ^I under Scheme I (passive eavesdropping) is

$$\varphi^I = 1 - \mathbb{P}\left\{r_b = \log_2\left(1 + \frac{g_{bi}P}{\sigma_b^2}\right) < R^I\right\} = e^{-\frac{\lambda_b \sigma_b^2}{P}(2^{R^I}-1)}, \quad (9)$$

where σ_b^2 denotes the noise power at the legitimate monitor.

In Scheme II, since all the suspicious communication channels have independent fading, it is possible that a jammed channel is still chosen by the ST, and in this case the half-duplex monitor cannot eavesdrop anything. We define the probability that any jammed channel is chosen by the ST (i.e., own goal probability of the monitor's self-jamming) as $\rho \in [0, 1]$ and we will detail its analysis later in Sections III and IV.

Now, assuming the suspicious communication is on the ith channel in a certain fading block, only when none of the jammed channels is chosen by the ST, and the achievable rate of the ith eavesdropping channel is no smaller than the suspicious transmission rate R^{II} in (8), the monitor can successfully eavesdrop. Thus, the eavesdropping success probability φ^{II} under Scheme II (jamming-assisted eavesdropping) is

$$\varphi^{II}(n, Q_1, \cdots, Q_n) = (1 - \rho(n, Q_1, \cdots, Q_n))$$
$$\times \left(1 - \mathbb{P}\left\{r_b = \log_2\left(1 + \frac{g_{bi}P}{\sigma_b^2}\right) < R^{II}(n, Q_1, \cdots, Q_n)\right\}\right)$$
$$= (1 - \rho(n, Q_1, \cdots, Q_n))e^{-\frac{\lambda_b \sigma_b^2}{P}(2^{R^{II}(n,Q_1,\cdots,Q_n)}-1)}. \quad (10)$$

From (9) and (10), we can formulate the optimization problem for jamming design as a mixed integer nonlinear

programming (MINLP), given by

$$(\text{P1}): \max_{n,Q_1,\cdots,Q_n} \max\{\varphi^I, \varphi^{II}(n,Q_1,\cdots,Q_n)\}$$

$$\text{s.t. } 0 < \sum_{i=1}^{n} Q_i \le Q_{\max},$$

$$1 \le n \le N-1, n \in \mathbb{Z}.$$

Note that φ^I does not depend on n or Q_i and it is a constant. In other words, the monitor only jams if the optimized $\varphi^{II}(n,Q_1,\cdots,Q_n)$ is larger than φ^I.

The joint optimization of n and Q_i's in problem (P1) is difficult due to discrete n and non-concave objective $\varphi^{II}(n,Q_1,\cdots,Q_n)$. In the next section, we will first look into the two-channel case ($N=2$) to simplify this problem and provide tractable analysis and clean insights. We will generalize the results to the multi-channel case in Section IV.

III. OPTIMAL JAMMING-ASSISTED EAVESDROPPING OVER TWO CHANNELS

If there are only two parallel channels ($N=2$), in jamming-assisted eavesdropping approach, the half-duplex legitimate monitor will only jam one channel (i.e., $n=1$), otherwise, both channels are jammed and it cannot overhear anything due to own goal. Its eavesdropping success probability φ^{II} under our jamming-assisted eavesdropping in (10) now only depends on jamming power Q, i.e.,

$$\varphi^{II}(Q) = (1-\rho(Q))e^{-\frac{\lambda_b\sigma_b^2}{P}(2^{R^{II}(Q)}-1)}, \qquad (11)$$

and (P1) is simplified to

$$(\text{P2}): \max_Q \max\{\varphi^I, \varphi^{II}(Q)\}$$

$$\text{s.t. } 0 < Q \le Q_{\max}.$$

Proposition 3.1: In the two-channel case, the own goal probability $\rho(Q)$ in (11) due to self-jamming at the monitor is given by

$$\rho(Q) = -\frac{\lambda_c\sigma_a^2}{Q}e^{\frac{2\lambda_c\sigma_a^2}{Q}}\text{Ei}(-\frac{2\lambda_c\sigma_a^2}{Q}), \qquad (12)$$

where $\text{Ei}(\cdot)$ is the exponential integral function [25, Eq. 8.21]. As jamming power Q increases, $\rho(Q)$ decreases. This is because a higher jamming power helps drive the suspicious link to the other unjammed (eavesdropped) channel. More specifically, we have $\lim_{Q\to 0^+}\rho(Q) = 1/2$ due to trivial jamming effect on changing the ST's belief of channel distributions, and the suspicious link is equally likely to choose both i.i.d. channels to transmit. Moreover, $\lim_{Q\to\infty}\rho(Q) = 0$, since the jammed channel will never be chosen by the suspicious link under infinite jamming power.

Proof: See Appendix C, where we choose $N=2$ and $n=1$. By substituting $Q=0^+$ and $Q=\infty$ into (12), we can derive the two limits for $\rho(Q)$. ∎

Proof:

Next, we analyze the non-outage probability at the monitor $e^{-\lambda_b\sigma_b^2(2^{R^{II}(Q)}-1)/P}$, a part of (11), which is a function of $R^{II}(Q)$. By simplifying (8) under $N=2$ and $n=1$, we have the following results.

Fig. 2. Eavesdropping success probability versus jamming power at the monitor, where $N=2$, $\lambda_a=1$, $\lambda_b=\lambda_c=3$, $P=10$ dB, $\sigma_a^2=\sigma_b^2=1$ and $\delta=0.05$.

Proposition 3.2: In the two-channel case, the suspicious link's transmission rate $R^{II}(Q)$ in (11) is the unique solution to

$$\left(1-e^{-\frac{\lambda_a\sigma_a^2}{P}(2^{R^{II}(Q)}-1)}\right)\left(1-\frac{\lambda_c Pe^{-\frac{\lambda_a\sigma_a^2}{P}(2^{R^{II}(Q)}-1)}}{\lambda_c P+\lambda_a Q(2^{R^{II}(Q)}-1)}\right)=\delta. \qquad (13)$$

As jamming power Q increases, $R^{II}(Q)$ decreases. This is because the ST faces more noisy channel, and has to transmit at a lower rate in order to maintain target outage probability δ. More specifically, $\lim_{Q\to 0^+}R^{II}(Q) = \log_2\left(1+P\ln(1-\delta^{\frac{1}{2}})^{-1}/\lambda_a\sigma_a^2\right)$, which equals to R^I in (5) with $N=2$ under passive eavesdropping, due to trivial jamming effect on the suspicious communication. Moreover, $\lim_{Q\to\infty}R^{II}(Q) = \log_2\left(1+P\ln(1-\delta)^{-1}/\lambda_a\sigma_a^2\right)$, which equals to R^I in (5) with $N=1$ under the passive eavesdropping, since the jammed channel will never be chosen.

Proof: By substituting $N=2$ and $n=1$ into (8), we have (13). Denote the left-hand-side (LHS) of (13) to be $g(R^{II}(Q),Q)$. According to the implicit function theorem, we have

$$\frac{dR^{II}(Q)}{dQ} = -\frac{\partial g(R^{II}(Q),Q)/\partial Q}{\partial g(R^{II}(Q),Q)/\partial R^{II}(Q)} < 0,$$

thus $R^{II}(Q)$ monotonically decreases as Q increases. By substituting $Q=0^+$ and $Q=\infty$ into (13), we can derive the two limits for $R^{II}(Q)$. ∎

Theorem 3.1: We denote Q_{th} as the unique solution to

$$\left(1-\rho(Q_{\text{th}})\right)e^{-\frac{\lambda_b\sigma_b^2}{P}(2^{R^{II}(Q_{\text{th}})}-1)} = e^{-\frac{\lambda_b\sigma_b^2}{P}(2^{R^I}-1)}. \qquad (14)$$

If $Q_{\max} > Q_{\text{th}}$, the legitimate monitor will jam with the maximum power $Q_{\max}$, otherwise it will perform passive eavesdropping without jamming (as illustrated in Fig. 2).

According to Propositions 3.1 and 3.2, $\varphi^{II}(Q)$ in (11) monotonically increases with Q, thus the monitor will use the maximum jamming power $Q_{\max}$ if it decides to jam, while φ^I in (9) is a constant regardless of Q.

When jamming power Q is close to zero,

$$\lim_{Q\to 0^+} \varphi^{II}(Q) = \frac{1}{2}e^{-\frac{\lambda_b\sigma_b^2}{P}(2^{R^I}-1)} < \varphi^I.$$

On the other hand, when jamming power goes to infinity, $\lim_{Q\to\infty} R^{II}(Q) = R^I|_{(N=1)} < R^I$, hence

$$\lim_{Q\to\infty} \varphi^{II}(Q) = e^{-\frac{\lambda_b\sigma_b^2}{P}(2^{R^I|_{(N=1)}}-1)} > \varphi^I.$$

Given that when jamming power goes to zero, the performance of jamming-assisted eavesdropping is worse than passive eavesdropping, while the performance of jamming-assisted eavesdropping increases with jamming power, and eventually when jamming power goes to infinity, becomes better than passive eavesdropping, it follows that there exists a unique intersection point between φ^I and $\varphi^{II}(Q)$ at point $Q = Q_{\text{th}}$, which is given in (14). If $Q_{\max} > Q_{\text{th}}$, the monitor will jam with the maximum jamming power $Q_{\max}$, otherwise it will perform passive eavesdropping to obtain a greater φ^I than $\varphi^{II}(Q_{\max})$. ∎

As we can see from above, in jamming-assisted eavesdropping, jamming with a higher power helps reduce own goal probability $\rho(Q)$ and transmission rate $R^{II}(Q)$ at the same time. Thus, by using up jamming power budget $Q_{\max}$, the monitor can achieve the maximum eavesdropping success probability.

IV. OPTIMAL JAMMING-ASSISTED EAVESDROPPING OVER MULTIPLE CHANNELS

In this section, we consider the general case with multiple i.i.d. fading channels for the optimal jamming design, and need to further decide how many channels to jam. Similar to the $N = 2$ case in Theorem 3.1, we also expect to jam with the maximum power $Q_{\max}$ in the general case of $N \geq 2$ channels if the monitor decides to jam. More specifically, we have the following result.

Proposition 4.1: Given that $n \geq 1$ of N channels are jammed, the monitor should allocate all the jamming power over n jammed channels equally, i.e., $Q_i^* = Q_{\max}/n$, $\forall i \in \{1, \cdots, n\}$.

Proof: See Appendix B. ∎

Thanks to Proposition 4.1, we know that the monitor will evenly allocate all the jamming power over the jammed channels, as a result the eavesdropping success probability φ^{II} under jamming-assisted eavesdropping in (10) only depends on the number of jammed channels n, i.e.,

$$\varphi^{II}(n) = (1 - \rho(n))e^{-\frac{\lambda_b\sigma_b^2}{P}(2^{R^{II}(n)}-1)}. \quad (15)$$

Thus, we manage to simplify the non-convex MINLP in (P1) to the following single-variable problem:

$$(\text{P3}): \max_n \ \max\{\varphi^I, \varphi^{II}(n)\}$$
$$\text{s.t. } 1 \leq n \leq N-1, n \in \mathbb{Z}.$$

As n is an integer, problem (P3) is an integer programming problem and still difficult to solve analytically. Next, we will analyze the monotonic properties of own goal probability $\rho(n)$ and suspicious link's transmission rate $R^{II}(n)$ with respect to

Fig. 3. $\varphi^{II}(n)$, $1 - \rho(n)$ and non-outage probability at the monitor versus number of jammed channels n, where $N = 8$, $\lambda_a = \lambda_b = 1$, $\lambda_c = 3$, $P = 10$ dB, $Q_{\max} = 20$ dB, $\sigma_a^2 = \sigma_b^2 = 1$ and $\delta = 0.05$.

n in the objective, to understand the key insights and solve (P3).

Proposition 4.2: In the general multi-channel case, the own goal probability $\rho(n)$ at the monitor in (15) is given by

$$\rho(n) = \frac{(N-n)\lambda_a\sigma_a^2}{P} \sum_{i=0}^{N-n-1}\sum_{j=1}^{n}\binom{N-n-1}{i}\binom{n}{j}(-1)^{i+j+1}$$
$$\times \left(\frac{\lambda_a Q_{\max}}{n\lambda_c P}\right)^{-j}\left((1+i+j)\frac{\lambda_a\sigma_a^2}{P}\right)^{j-1}e^{\frac{(1+i+j)n\lambda_c\sigma_a^2}{Q_{\max}}}$$
$$\times \Gamma\left(1-j, \frac{(1+i+j)n\lambda_c\sigma_a^2}{Q_{\max}}\right), \quad (16)$$

where $\Gamma(\cdot, \cdot)$ is the upper incomplete gamma function [25, Eq. 8.35]. Further, $\rho(n)$ increases as n increases.

Proof: See Appendix C. ∎

Here, $\rho(n)$ increases with n due to two reasons. First, more channels are jammed and potentially they can be selected by the suspicious link for transmission. Second, the jamming power on each jammed channel weakens as n increases given the total jamming power budget, and thus each jammed channel is more likely to be chosen by the suspicious link. Thus, the suspicious link is more likely to transmit on the jammed channels and this increases the self-jamming (own goal) probability $\rho(n)$ for the monitor.

Next, we determine the non-outage probability $e^{-\lambda_b\sigma_b^2(2^{R^{II}(n)}-1)/P}$ at the monitor in (15), which is a function of $R^{II}(n)$. Similar to $\rho(n)$, here $R^{II}(n)$ only depends on n.

Proposition 4.3: In the general multi-channel case, the suspicious link's transmission rate $R^{II}(n)$ in (15) is the unique solution to

$$\left(1-e^{-\frac{\lambda_a\sigma_a^2}{P}(2^{R^{II}}-1)}\right)^{N-n}\left(1-\frac{\lambda_c Pe^{-\frac{\lambda_a\sigma_a^2}{P}(2^{R^{II}}-1)}}{\lambda_c P+\lambda_a\frac{Q_{\max}}{n}(2^{R^{II}}-1)}\right)^n = \delta. \quad (17)$$

Further, $R^{II}(n)$ monotonically decreases as n increases.

Proof: See Appendix D. ∎

Fig. 4. Jamming-assisted eavesdropping over two-way communications (user A and user B alternately communicate with each other over different time slots).

The reason why $R^{II}(n)$ decreases with n is because jamming more channels increases the chance that the ST chooses the jammed channels, and the ST will transmit at a lower rate to maintain target outage probability at the SR. A lower transmission rate $R^{II}(n)$ leads to a higher non-outage probability $e^{-\lambda_b \sigma_b^2 (2^{R^{II}(n)} - 1)/P}$ at the monitor, and thus the monitor can overhear more clearly.

Fig. 3 numerically illustrates $1 - \rho(n)$ in (16), non-outage probability in (17), and their product $\varphi^{II}(n)$ in (15). As n increases, it is observed that $1 - \rho(n)$ decreases and $e^{-\lambda_b \sigma_b^2 (2^{R^{II}(n)} - 1)/P}$ increases. To maximize $\varphi^{II}(n)$, there is thus a trade-off in deciding the optimal number of jammed channels n^* (here $n^* = 5$ in this numerical example).

It should be noted that it is still difficult to analytically solve n^* in (P3) even by relaxing n to be continuous for tractable analysis. This is because not only $R^{II}(n)$ in (17) is not in closed-form, but also it is difficult to approximate $\rho(n)$ in (16) to be a continuous function due to the combinatorial nature and the involved upper incomplete gamma function. Still, we can numerically obtain n^*, by a one-dimensional exhaustive search in the set $\{1, 2, \cdots, N-1\}$ with low computation complexity of $O(N)$.

Proposition 4.4: In jamming-assisted eavesdropping scheme, as the monitor's jamming power budget $Q_{\max}$ goes to zero, it is optimal for the monitor to jam as few channels as possible ($n^* = 1$), and the eavesdropping success probability is

$$\lim_{Q_{\max} \to 0^+} \varphi^{II}(n^* = 1) = \left(1 - \frac{1}{N}\right) e^{\frac{\lambda_b \sigma_b^2}{\lambda_a \sigma_a^2} \ln\left(1 - \delta^{\frac{1}{N}}\right)}. \quad (18)$$

On the other hand, as the monitor's jamming power budget $Q_{\max}$ goes to infinity, it is optimal for the monitor to maximally jam $n^* = N - 1$ channels and eavesdrop the remaining one with ideal zero own goal probability, and the eavesdropping success probability is

$$\lim_{Q_{\max} \to \infty} \varphi^{II}(n^* = N - 1) = e^{\frac{\lambda_b \sigma_b^2}{\lambda_a \sigma_a^2} \ln(1 - \delta)}. \quad (19)$$

Proof: When the monitor's jamming power budget goes to zero, the jammed channels and unjammed channels are the same in distribution, while the half-duplex monitor cannot eavesdrop the jammed channels, making the own goal proba-

bility proportional to n, i.e.,

$$\lim_{Q_{\max} \to 0^+} \rho(n) = \frac{n}{N}.$$

Meanwhile, the transmission rate $R^{II}(n)$ in (17) now becomes the same as constant transmission rate of passive eavesdropping in (5). Thus, the eavesdropping success probability in (15) becomes

$$\lim_{Q_{\max} \to 0^+} \varphi^{II}(n) = \left(1 - \frac{n}{N}\right) e^{\frac{\lambda_b \sigma_b^2}{\lambda_a \sigma_a^2} \ln\left(1 - \delta^{\frac{1}{N}}\right)}. \quad (20)$$

As we can see from (20), $\lim_{Q_{\max} \to 0^+} \varphi^{II}(n)$ monotonically decreases as n increases, thus it is optimal to only jam $n^* = 1$ channel when employing the jamming-assisted eavesdropping.

On the other hand, as jamming power budget goes to infinity, the own goal probability becomes $\lim_{Q_{\max} \to \infty} \rho(n) = 0$, as the severely jammed channel will never be chosen by the ST. Meanwhile, the transmission rate $R^{II}(n)$ becomes

$$\lim_{Q_{\max} \to \infty} R^{II}(n) = \log_2 \left(1 + \frac{P}{\lambda_a \sigma_a^2} \ln \frac{1}{1 - \delta^{\frac{1}{N-n}}}\right).$$

Thus, the eavesdropping success probability becomes

$$\lim_{Q_{\max} \to \infty} \varphi^{II}(n) = e^{\frac{\lambda_b \sigma_b^2}{\lambda_a \sigma_a^2} \ln\left(1 - \delta^{\frac{1}{N-n}}\right)}. \quad (21)$$

As we can see from (21), $\lim_{Q_{\max} \to \infty} \varphi^{II}(n)$ monotonically increases as n increases, thus it is optimal to jam $n^* = N - 1$ channels in this case. ∎

Note that under optimal n^*, if $\varphi^{II}(n^*) > \varphi^I$, the legitimate monitor will perform jamming-assisted eavesdropping, otherwise it will perform passive eavesdropping.

V. EXTENSION TO EAVESDROPPING TWO-WAY COMMUNICATIONS

So far, we have considered the one-way communication from the ST to the SR for the suspicious link, while in practice, the two users may need to alternately exchange information with each other over time periods or fading blocks (see Fig. 4). Our jamming-assisted eavesdropping approach in Section IV is designed for the one-way communication, and will be extended in this section for the two-way communications.

The distributions of channel power gains of the communication from user A to user B follow the same model defined in

Section II, i.e., $g_{ai} \sim \exp(\lambda_a)$, $g_{bi} \sim \exp(\lambda_b)$, $g_{ci} \sim \exp(\lambda_c)$. Due to the reciprocity of wireless channel, the suspicious communication channels are the same from user B to user A, i.e., $g'_{ai} \sim \exp(\lambda_a)$. However, the original jamming channels now become eavesdropping channels, i.e., $g'_{bi} \sim \exp(\lambda_c)$, and the original eavesdropping channels now become jamming channels, i.e., $g'_{ci} \sim \exp(\lambda_b)$. As we can see, the optimal number of jammed channels are in general different for user A to B communication (n^*_{AB} as computed in last section) and user B to A communication (n^*_{BA}), where subscript $(\cdot)_{AB}$ denotes the communication direction from user A to user B, and $(\cdot)_{BA}$ denotes the communication from user B to user A. But alternately jamming $n^*_{AB} \neq n^*_{BA}$ channels over time will easily arouse the suspicion of suspicious users by examining the channel statistics. Then the suspicious link can tell that the monitor is a jammer instead of a normal D2D user with time-division-duplex.

To intercept the two-way communications between user A and user B, we need to balance these two communication ways for maximizing the minimum eavesdropping success probability between both communication ways, keep the same jammed channels and jamming power in the long run. Without loss of generality, if n out of N i.i.d. fading channels are jammed in two-way communications, we consider the monitor picks the first n out of N channels to jam. Similar to Proposition 4.1 in the one-way communication, the monitor should also use up all the jamming power budget and evenly partition over the jammed channels in two-way communications. Thus, the max-min optimization problem can be reformulated as follows.[2]

$$(\text{P4}): \max_n \max\{\min\{\varphi^I_{AB}, \varphi^I_{BA}\}, \min\{\varphi^{II}_{AB}(n), \varphi^{II}_{BA}(n)\}\}$$
$$\text{s.t. } 1 \leq n \leq N-1, n \in \mathbb{Z}.$$

(P4) compares the performance of jamming-assisted eavesdropping $\min\{\varphi^{II}_{AB}(n), \varphi^{II}_{BA}(n)\}$ and the performance of passive eavesdropping $\min\{\varphi^I_{AB}, \varphi^I_{BA}\}$ in two-way communications. Since both φ^I_{AB} and φ^I_{BA} are constants, we can only focus on optimizing the performance of jamming-assisted eavesdropping $\min\{\varphi^{II}_{AB}(n), \varphi^{II}_{BA}(n)\}$. To numerically solve this integer programming, we can obtain the optimal number of jammed channels n^* in two-way communications, by efficiently performing one-dimensional exhaustive search in the set $\{1, 2, \cdots, N-1\}$ with low computation complexity of $O(N)$. Then we compare $\min\{\varphi^I_{AB}, \varphi^I_{BA}\}$ with $\min\{\varphi^{II}_{AB}(n^*), \varphi^{II}_{BA}(n^*)\}$: if the former is smaller, the monitor will perform jamming-assisted eavesdropping with n^* jammed channels, otherwise the monitor will perform passive eavesdropping.

We first use a numerical example to illustrate the eavesdropping success probability of jamming-assisted eavesdropping in two-way communications. Assuming there are $N = 8$ parallel channels, we set the mean channel power gains to be $1/\lambda_a = 1/5$, $1/\lambda_b = 1$ and $1/\lambda_c = 1/4$, additive white Gaussian noise (AWGN) power as $\sigma^2_a = \sigma^2_b = \sigma^2_c = 1$, target

---

[2]Our problem (P4) can further include different weights for the two communication ways. For example, if the monitor values the message from user A (e.g., a leader of a criminal gang) to user B (e.g., a follower) more important, it will assign a large weight to this way's eavesdropping success probability.

Fig. 5. Eavesdropping success probability in jamming-assisted eavesdropping of two-way communications, which is the minimum of the eavesdropping success probabilities from user A to B and from user B to A.

outage probability at user A/B as $\delta = 0.05$, transmitting power of user A/B as $P = 10$ dB and jamming power budget as $Q_{\max} = 20$ dB.

As Fig. 5 shows, the optimal number of jammed channels n^*_{AB} for suspicious user A's communication to user B is 2, while the optimal number of jammed channels n^*_{BA} for suspicious user B's communication to user A is 6; and we find the optimal number of jammed channels $n^* = 5$ to balance between the communications from user A to B and from user B to A.

It is difficult to analytically derive the optimal solution to (P4), due to the non-concave objective involving incomplete gamma function and the discrete nature of decision variable n. Despite of these, we still manage to derive some analytical results by assuming the one-way eavesdropping success probability $\varphi^{II}(n)$ (i.e., $\varphi^{II}_{AB}(n)$ for user A to B and $\varphi^{II}_{BA}(n)$ for user B to A) is unimodal (having only one peak) or monotonic in n as in Fig. 3. Actually, this is always the case in our extensive simulations though it is difficult to rigorously prove.

Proposition 5.1: Assuming the objective functions $\varphi^{II}_{AB}(n)$ and $\varphi^{II}_{BA}(n)$ in (P4) are unimodal or monotonic in n, the optimal jamming-assisted eavesdropping scheme is given as follows, depending on the jamming power budget $Q_{\max}$.

- If the monitor's jamming power budget $Q_{\max}$ is low (i.e., $Q_{\max} < \underline{Q}$), jamming more channels hurts the eavesdropping performances on both ways, where $\underline{Q} = \min\{Q_{\max}|\varphi^{II}_{AB}(1) \geq \varphi^{II}_{AB}(2), \varphi^{II}_{BA}(1) \geq \varphi^{II}_{BA}(2)\}$. In this case, it is optimal for the monitor to minimally jam $n^* = 1$ channel. As a special case, when $Q_{\max}$ goes to zero, $n^* = 1$ (as a two-way extension of Proposition 4.4).
- If the monitor's jamming power budget $Q_{\max}$ is high (i.e., $Q_{\max} > \bar{Q}$), jamming more channels improves the eavesdropping performances on both ways, where $\bar{Q} = \max\{Q_{\max}|\varphi^{II}_{AB}(N-2) \leq \varphi^{II}_{AB}(N-1), \varphi^{II}_{BA}(N-2) \leq \varphi^{II}_{BA}(N-1)\}$. In this case, it is optimal for the monitor to maximally jam $n^* = N-1$ channels. As a special case, when $Q_{\max}$ goes to infinity, $n^* = N-1$ (as a two-way extension of Proposition 4.4).

Fig. 6. Eavesdropping success probability φ^{II} versus number of jammed channels n under different power budget $Q_{\max}$'s.

Fig. 7. Eavesdropping success probability versus mean channel power gain of the eavesdropping and jamming links with different total numbers of channels N's.

- If the jamming power budget $Q_{\max}$ is medium (i.e., $\underline{Q} \leq Q_{\max} \leq \bar{Q}$), the optimal number of jammed channels n^* is between n^*_{AB} and n^*_{BA}, by balancing the eavesdropping performances of the two ways.

   Proof: See Appendix E. ∎

VI. NUMERICAL RESULTS

In this section, we provide more numerical results to validate our studies and designs. Assuming there are $N = 8$ parallel channels, we set the mean channel power gain of the suspicious communication link, eavesdropping link and jamming link in the one-way communication to be $1/\lambda_a = 1$, $1/\lambda_b = 1$ and $1/\lambda_c = 1/3$, respectively. We also set the AWGN power as $\sigma_a^2 = \sigma_b^2 = \sigma_c^2 = 1$, the target outage probability at the SR as $\delta = 0.05$ and transmitting power of the ST as $P = 10$ dB.

Fig. 6 shows the eavesdropping success probability φ^{II} as a function of n and $Q_{\max}$ for the case of one-way communication from suspicious user A to user B. When $Q_{\max}$ is small (e.g., $Q_{\max} = 4$ dB curve in Fig. 6), the monitor will perform passive eavesdropping. When $Q_{\max}$ is sufficiently large (starting from $Q_{\max} = 10$ dB), the monitor will jam to assist eavesdropping for a larger eavesdropping success probability. We can see that as $Q_{\max}$ increases, the monitor will jam more channels by optimally controlling the trade-off between own goal probability and transmission rate. When $Q_{\max}$ is further large (e.g., $Q_{\max} = 40$ dB), the monitor will optimally jam $N - 1$ channels to overhear the lowest-rate suspicious communication in the remaining single channel, without worrying about the own goal of self-jamming. This result is consistent with Proposition 4.4.

Then we consider the passive eavesdropping as a benchmark for performance comparison. We set the mean channel power gain of the suspicious communication link to be $1/\lambda_a = 1$ and jamming power budget to be $Q_{\max} = 30$ dB. Here we consider the monitor is far away from the ST and SR, thus the mean channel power gains of eavesdropping channels and jamming channels are nearly the same, i.e., $1/\lambda_b = 1/\lambda_c$.

Fig. 7 shows the eavesdropping success probability as a function of N and mean channel power gain of eavesdropping and jamming links. As their mean channel power gains increase, eavesdropping success probabilities of both jamming-assisted and passive eavesdropping increase. But jamming-assisted eavesdropping greatly outperforms passive eavesdropping. The performance of jamming-assisted eavesdropping is better when total number of channels is smaller (e.g., $N = 2$ in Fig. 7), as the monitor can more efficiently induce the suspicious link to use a smaller subset of unjammed channels and a lower transmission rate under the same jamming power budget. While the performance gain of jamming-assisted eavesdropping comparing with passive eavesdropping is greater when total number of channels is large (e.g., $N = 8$ in Fig. 7), as more channels provides more degrees of freedom for jamming.

Next, we study the effect of the monitor's location. To capture the effect of large-scale fading, we consider that for any two points with coordinates (x_1, y_1) and (x_2, y_2) in the two-dimensional (2D) ground plane, the mean channel power gain between the two points is inversely proportional to the square of their distance, i.e., $1/\lambda = 1/((x_1 - x_2)^2 + (y_1 - y_2)^2)$. The ST is located at $(3, 4.5)$, and the SR is located at $(7, 4.5)$. The distances are normalized with transmit power. The legitimate monitor is placed in different locations in this plane, and its jamming power budget is $Q_{\max} = 30$ dB.

Fig. 8(a) shows the optimal number of jammed channels n^* in different monitor's locations in the 2D ground plane. When the monitor is close to the ST, passive eavesdropping can already provide good eavesdropping performance. When the monitor is moving away from the ST, passive eavesdropping can no longer provide good eavesdropping performance, and the monitor will jam more channels to lower the suspicious link's transmission rate in order to overhear more clearly. When the monitor is close to the SR, which means now

(a) Optimal number of jammed channels n^* versus different monitor's locations in the 2D ground plane ($N = 8$ channels in total).

(b) Eavesdropping success probability of jamming-assisted eavesdropping versus different monitor's locations in the 2D ground plane.

(c) Eavesdropping success probability of passive eavesdropping versus different monitor's locations in the 2D ground plane.

Fig. 8. Effect of monitor's geometric locations on jamming strategy design, jamming-assisted eavesdropping performance, and passive eavesdropping performance.

Fig. 9. Eavesdropping success probability versus monitor's location in two-way communications.

the efficiency of jamming is high, the monitor will jam most channels (up to $N - 1$) for improving eavesdropping performance.

Fig. 8(b) and Fig. 8(c) compare the eavesdropping success probability of jamming-assisted eavesdropping and passive eavesdropping with different monitor's locations in the 2D ground plane. As we can see, the eavesdropping success probability of passive eavesdropping is fully determined by the distance between the monitor and the ST, and a good eavesdropping performance can only be guaranteed when the monitor is close to the ST. While our proposed jamming-assisted eavesdropping greatly outperforms passive eavesdropping even when the monitor is not close to the ST, because it can efficiently jam the SR and drive the ST to transmit in a smaller subset of channels with a lower transmission rate so that the monitor can eavesdrop more effectively. The performance gain of jamming-assisted eavesdropping is significant when the monitor is close to the SR, since now the efficiency of jamming is high. This clearly shows that passive eavesdropping is dramatically sensitive to the ST-monitor distance, while our

proposed jamming-assisted eavesdropping is no longer that sensitive even when the monitor is geometrically far away from the ST.

Finally, we examine the performance of jamming-assisted eavesdropping in two-way communications. Here we still assume the mean channel power gain between any two points is inversely proportional to the square of their distance, similar to the previous simulation. Suspicious user A is located at $(1, 1)$ and suspicious user B at $(3, 1)$. The legitimate monitor can be at any point between $(0, 0)$ and $(4, 0)$ to eavesdrop the two-way communications, and its jamming power budget is set to $Q_{\max} = 30$ dB. We provide two benchmark cases for performance comparison with our optimal solution. Benchmark n^*_{AB} tells that the monitor just focuses on the one-way communication from A to B, and jams n^*_{AB} channels according to the one-way surveillance problem in (P3). Meanwhile, benchmark n^*_{BA} focuses on the one-way communication from B to A, and jams n^*_{BA} channels.

Fig. 9(a) compares the optimal number of jammed channels n^* in (P4) with n^*_{AB} and n^*_{BA} when the monitor moves

horizontally between $(0,0)$ and $(4,0)$. Fig. 9(b) shows the eavesdropping success probability versus the monitor's location in two-way communications. We have the following observations.

- When the monitor is between $(0,0)$ and $(0.3,0)$, it is far away from user B and the overall eavesdropping performance is bottlenecked by user B as the ST, thus jamming n_{BA}^* channels will give the best eavesdropping performance as the optimal n^*. Note that n_{AB}^* is smaller than n_{BA}^* (n^*) in this case, since user A is much closer to the monitor than user B, which is consistent with Fig. 8(a) in the sense that the monitor will jam more channels when it is moving away from the ST.

- When the monitor is moving from $(0.3,0)$ to $(1.6,0)$, it is getting closer to user A than user B, thus the eavesdropping performance of benchmark n_{AB}^* improves more significantly than that of benchmark n_{BA}^*. Still, n^* outperforms benchmarks n_{AB}^* and n_{BA}^*. Note that n_{BA}^* is greater than n^* in this case, because now the monitor is very close to user A, and according to Fig. 8(a), the monitor will jam most channels when it is close to the SR.

- When the monitor is between $(1.6,0)$ and $(2,0)$, the monitor's distances to users A and B are close, thus both benchmarks n_{AB}^* and n_{BA}^* are symmetric and achieve the optimal eavesdropping performance as n^*. Note that in Fig. 9(b) the sharp performance increase of benchmarks n_{AB}^* and n_{BA}^* at point $(1.6,0)$ is caused by changing the number of jammed channels. Taking n_{AB}^* as an example, the monitor is moving closer to user B (SR in n_{AB}^*'s point of view), and at the point $(1.6,0)$, the monitor increases the number of jammed channels due to better jamming efficiency, which causes the obvious eavesdropping performance change.

Finally, the eavesdropping success probability reaches the maximum when the monitor is at $(2,0)$, since now the monitor's distances to user A and user B are the same. The eavesdropping performance analysis of the monitor moving from $(2,0)$ to $(4,0)$ is similar as above by symmetry.

VII. CONCLUSIONS

This paper proposes a new wireless security model, which is jamming-assisted legitimate eavesdropping over parallel independently fading channels. The legitimate monitor uses jamming in order to achieve better eavesdropping performance. Assuming Rayleigh fading, we formulate the optimization problem for jamming design as a mixed integer nonlinear programming (MINLP). Despite its non-convexity, we show that the legitimate monitor should use the maximum jamming power for the best eavesdropping performance if it decides to jam. Then we simplify the MINLP to integer programming and further show that there is a trade-off in deciding the number of jammed channels in the general multi-channel case, where jamming more channels helps reduce the suspicious communication rate for overhearing more clearly, but at the risk that the ST is more likely to choose jammed channels to transmit and as a result cannot be overheard. Finally, we extend

our study to two-way communications, and show another trade-off in deciding the common jammed channels for balancing the bidirectional eavesdropping performances. Numerical results show that our jamming-assisted eavesdropping schemes greatly improve eavesdropping success probability comparing with conventional passive eavesdropping.

This work can be extended in various directions. For example, the suspicious link can transmit at multiple channels and perform combining at the receiver, or there can be multiple suspicious link pairs, which will bring more challenges to legitimate eavesdropping. The more general case of parallel channels with correlated (non-independent) fading is also worth investigating in future work.

APPENDIX

A. Proof of Lemma 2.1

We aim to show the distribution of SINR $Y = \frac{g_{ai}P}{g_{ci}Q_i + \sigma_a^2}$ on jammed channel i. Denote its numerator and denominator as $Y_1 = g_{ai}P$ and $Y_2 = g_{ci}Q_i + \sigma_a^2$, respectively. As g_{ai} and g_{ci} follow independent exponential distributions with mean $1/\lambda_a$ and $1/\lambda_c$, respectively, we have

$$f_{Y_1}(y_1) = \frac{\lambda_a}{P} e^{-\frac{\lambda_a}{P} y_1}, \qquad y_1 \geq 0,$$

$$f_{Y_2}(y_2) = \frac{\lambda_c}{Q_i} e^{-\frac{\lambda_c}{Q_i}(y_2 - \sigma_a^2)}, \qquad y_2 \geq \sigma_a^2.$$

The probability density function (PDF) of $Y = Y_1/Y_2$ can be calculated as follows

$$f_Y(y) = \frac{\lambda_a \lambda_c}{PQ_i} e^{\frac{\lambda_c \sigma_a^2}{Q_i}} \int_{\sigma_a^2}^{\infty} y_2 e^{-(\frac{\lambda_c}{Q_i} + \frac{\lambda_a y}{P})y_2} \, dy_2.$$

With the help of [25, Eq. 3.351.2], we have

$$f_Y(y) = \frac{\lambda_a \lambda_c (\lambda_c P \sigma_a^2 + PQ_i + \lambda_a Q_i \sigma_a^2 y)}{(\lambda_c P + \lambda_a Q_i y)^2} e^{-\frac{\lambda_a \sigma_a^2 y}{P}}, \quad y \geq 0,$$

and the CDF of Y can be calculated as

$$\int_0^y f_Y(y) \, dy = 1 - \frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P} y}}{\lambda_c P + \lambda_a Q_i y}, \qquad y \geq 0.$$

B. Proof of Proposition 4.1

For certain jamming scheme S_1, the own goal probability can be expressed as

$$\rho_{S_1}(n) = \mathbb{P}\bigg(\max\bigg\{ \frac{g_{a1}P}{g_{c1}Q_1 + \sigma_a^2}, \cdots, \frac{g_{aj}P}{g_{cj}Q_j + \sigma_a^2}, \cdots, \frac{g_{an}P}{g_{cn}Q_n + \sigma_a^2} \bigg\} > \max\bigg\{ \frac{g_{a1}P}{\sigma_a^2}, \cdots, \frac{g_{a(N-n)}P}{\sigma_a^2} \bigg\} \bigg).$$

There exists a jamming scheme S_2, where the monitor reduces jamming power Q_j on channel j to $Q_j - \Delta$ with $\Delta > 0$, for which

$$\rho_{S_2}(n) = \mathbb{P}\bigg(\max\bigg\{ \frac{g_{a1}P}{g_{c1}Q_1 + \sigma_a^2}, \cdots, \frac{g_{aj}P}{g_{cj}(Q_j - \Delta) + \sigma_a^2}, \cdots, \frac{g_{an}P}{g_{cn}Q_n + \sigma_a^2} \bigg\} > \max\bigg\{ \frac{g_{a1}P}{\sigma_a^2}, \cdots, \frac{g_{a(N-n)}P}{\sigma_a^2} \bigg\} \bigg).$$

Clearly, $\rho_{S_2}(n)$ is larger than $\rho_{S_1}(n)$.

For certain jamming scheme S_1, the transmission rate of the ST satisfies

$$\left(1-e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R_{S_1}^{II}}-1)}\right)^{N-n}\prod_{i=1}^{n}\left(1-\frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R_{S_1}^{II}}-1)}}{\lambda_c P+\lambda_a Q_i(2^{R_{S_1}^{II}}-1)}\right)=\delta.$$

There exists a jamming scheme S_2, where the monitor reduces jamming power Q_j on channel j to $Q_j-\Delta$, for which

$$\left(1-e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R_{S_2}^{II}}-1)}\right)^{N-n}\left(1-\frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R_{S_2}^{II}}-1)}}{\lambda_c P+\lambda_a (Q_j-\Delta)(2^{R_{S_2}^{II}}-1)}\right)$$

$$\times\prod_{i=1,i\neq j}^{n}\left(1-\frac{\lambda_c P e^{-\frac{\lambda_a \sigma_a^2}{P}(2^{R_{S_2}^{II}}-1)}}{\lambda_c P+\lambda_a Q_i(2^{R_{S_2}^{II}}-1)}\right)=\delta.$$

Similar to the proof of Proposition 3.2, $R_{S_2}^{II}$ is larger than $R_{S_1}^{II}$, while maintaining the same target outage probability δ at the receiver, but the non-outage probability at the monitor will decrease due to the higher transmission rate $R_{S_2}^{II}$.

From above, if the jamming power on any jammed channel decreases, the product of non-outage probability and non-own-goal probability at the monitor, i.e. the eavesdropping success probability, will degenerate. So the monitor will always use up all the jamming power.

Further since all channels are i.i.d. fading, by symmetry it is optimal to allocate the same amount of jamming power over n jammed channels. Thus, if n of N channels are jammed, the monitor should evenly allocate all the jamming power over n jammed channels, i.e., $Q_{\max}/n$.

C. Proofs of Propositions 3.1 and 4.2

We first prove that the own goal probability $\rho(n)$ increases as the number of jammed channels n increases.

Assuming k out of N channels are jammed, the own goal probability can be expressed as

$$\rho(k)=\mathbb{P}\left(\max\left\{\frac{g_{a1}P}{g_{c1}\frac{Q_{\max}}{k}+\sigma_a^2},\cdots,\frac{g_{ak}P}{g_{ck}\frac{Q_{\max}}{k}+\sigma_a^2}\right\}>\right.$$
$$\left.\max\left\{\frac{g_{a1}P}{\sigma_a^2},\cdots,\frac{g_{a(N-k)}P}{\sigma_a^2}\right\}\right).$$

If now $k+1$ channels are jammed, then the own goal probability becomes

$$\rho(k+1)=\mathbb{P}\left(\max\left\{\frac{g_{a1}P}{g_{c1}\frac{Q_{\max}}{k+1}+\sigma_a^2},\cdots,\frac{g_{a(k+1)}P}{g_{c(k+1)}\frac{Q_{\max}}{k+1}+\sigma_a^2}\right\}>\right.$$
$$\left.\max\left\{\frac{g_{a1}P}{\sigma_a^2},\cdots,\frac{g_{a(N-k-1)}P}{\sigma_a^2}\right\}\right).$$

Since the number of jammed channels changes from k to $k+1$, the jamming power on each jammed channel gets smaller, which makes them easier to be chosen by the ST for transmission. Also, there are more jammed channels (from k to $k+1$) and less unjammed channels (from $N-k$ to $N-k-1$). Combining these two effects, clearly as the number of jammed channels n increases, the own goal probability $\rho(n)$ will also increase.

Note that Proposition 3.1 is a special case of Proposition 4.2 and it is sufficient to prove Proposition 4.2 here. Denote

$X_i=\frac{g_{ai}P}{\sigma_a^2}$ and $Y_i=\frac{g_{ai}P}{g_{ci}Q_i+\sigma_a^2}$, the CDFs of X_i and Y_i are given in (1) and (2), respectively. Then we have

$$\rho(n)=\int_0^{\infty}\mathbb{P}\{\max\{Y_{(1)},\cdots,Y_{(n)}\geq x\}\}$$
$$\times f_{\max\{X_{(1)},\cdots,X_{(N-n)}\}}(x)\,dx,$$

where $f_{\max\{X_{(1)},\cdots,X_{(N-n)}\}}(x)$ is the PDF of the maximum SNR of the $N-n$ unjammed channels. Thus we have

$$\rho(n)=\int_0^{\infty}\left(\int_x^{\infty}d[F_Y(y)]^n\right)d[F_X(x)]^{N-n}$$

$$=\frac{(N-n)\lambda_a\sigma_a^2}{P}\int_0^{\infty}\left(1-(1-\frac{e^{-\frac{\lambda_a\sigma_a^2}{P}x}}{1+\frac{\lambda_a Q_{\max}}{n\lambda_c P}x})^n\right)$$
$$\times e^{-\frac{\lambda_a\sigma_a^2}{P}x}(1-e^{-\frac{\lambda_a\sigma_a^2}{P}x})^{N-n-1}dx$$

$$\overset{(a)}{=}\frac{(N-n)\lambda_a\sigma_a^2}{P}\sum_{i=0}^{N-n-1}\sum_{j=1}^{n}\binom{N-n-1}{i}\binom{n}{j}(-1)^{i+j+1}$$
$$\times\int_0^{\infty}\frac{1}{(1+\frac{\lambda_a Q_{\max}}{n\lambda_c P}x)^j}e^{-(i+j+1)\frac{\lambda_a\sigma_a^2}{P}x}dx$$

$$\overset{(b)}{=}\frac{(N-n)\lambda_a\sigma_a^2}{P}\sum_{i=0}^{N-n-1}\sum_{j=1}^{n}\binom{N-n-1}{i}\binom{n}{j}(-1)^{i+j+1}$$
$$\times\left(\frac{\lambda_a Q_{\max}}{n\lambda_c P}\right)^{-j}\left((1+i+j)\frac{\lambda_a\sigma_a^2}{P}\right)^{j-1}e^{\frac{(1+i+j)n\lambda_c\sigma_a^2}{Q_{\max}}}$$
$$\times\Gamma\left(1-j,\frac{(1+i+j)n\lambda_c\sigma_a^2}{Q_{\max}}\right),$$

where equality $\overset{(a)}{=}$ comes from the fact that the total number of channels N and the number of jammed channels n are both integers, following the binomial expansion of the two polynomial terms; and equality $\overset{(b)}{=}$ comes from reference [25, Eq. 3.353.2], and $\Gamma(\cdot,\cdot)$ is the incomplete Gamma function. Note that $\Gamma(0,x)=-\text{Ei}(-x)$, which completes the proof of Proposition 3.1 with $N=2$ and $n=1$.

D. Proof of Proposition 4.3

Denote $u=2^{R^{II}}-1$. We define the LHS of (17) as $h(n,u)$, which is the outage probability at the SR. Then we have

$$h(n,u)-\delta=0.$$

By taking the first-order derivative of this implicit function over u and n, we have the relationship between u and n as follows

$$\frac{du}{dn}=-\frac{\partial h(n,u)/\partial n}{\partial h(n,u)/\partial u}.$$

We then can explicitly derive

$$\frac{\partial h(n,u)}{\partial n}=\left(\frac{-\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}e^{-\frac{\lambda_a\sigma_a^2}{P}u}}{(1+\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n})^2(1-\frac{e^{-\frac{\lambda_a\sigma_a^2}{P}u}}{1+\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}})}\right.$$
$$\left.+\ln\left(1+\frac{\frac{\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}}{1+\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}}e^{-\frac{\lambda_a\sigma_a^2}{P}u}}{1-e^{-\frac{\lambda_a\sigma_a^2}{P}u}}\right)\right),$$

and according to inequality $\ln(1+x) > \frac{x}{1+x}$ for any $x > 0$, we have

$$\frac{\partial h(n,u)}{\partial n} > \frac{\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}e^{-\frac{\lambda_a \sigma_a^2}{P}u}}{\left(1+\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}\right)\left(1-\frac{e^{-\frac{\lambda_a \sigma_a^2}{P}u}}{1+\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}}\right)}\left(1-\frac{1}{1+\frac{\lambda_a Q_{\max}}{\lambda_c P}\frac{u}{n}}\right)$$
$$> 0. \tag{22}$$

For $\frac{\partial h(n,u)}{\partial u}$, as the transmission rate R^{II} increases, outage probability at the SR $h(n,u)$ increases, thus

$$\frac{\partial h(n,u)}{\partial u} > 0. \tag{23}$$

Combining (22) and (23), we have

$$\frac{du}{dn} = -\frac{\partial h(n,u)/\partial n}{\partial h(n,u)/\partial u} < 0.$$

By substituting $R^{II} = \log_2(1+u)$ back, we have

$$\frac{dR^{II}}{dn} = \frac{du}{dn}\frac{dR^{II}}{du} < 0.$$

Thus, as the number of jammed channels n increases, the transmission rate $R^{II}(n)$ decreases.

E. Proof of Proposition 5.1

Consider the expression of eavesdropping success probability $\varphi^{II}(n)$ in (15), which is the product of non-own goal probability $1 - \rho(n)$ multiplied by non-outage probability at the monitor $e^{-\frac{\lambda_b \sigma_b^2}{P}(2^{R^{II}(n)}-1)}$.

For any fixed n, as jamming power budget $Q_{\max}$ increases, the first part, non-own goal probability, $1 - \rho(n)$ increases, since the jammed channels become less likely to be chosen by the suspicious link. The second part, non-outage probability at the monitor, $e^{-\frac{\lambda_b \sigma_b^2}{P}(2^{R^{II}(n)}-1)}$ also increases, since the suspicious link will transmit at a lower rate to maintain target outage probability and the monitor can eavesdrop more clearly. Thus $\varphi^{II}(n)$ monotonically increases with $Q_{\max}$ for any fixed n.

For $\varphi_{AB}^{II}(n)$, we can see from (20) that

$$\lim_{Q_{\max}\to 0^+} \varphi_{AB}^{II}(1) > \lim_{Q_{\max}\to 0^+} \varphi_{AB}^{II}(2),$$

and from (21), we can see that

$$\lim_{Q_{\max}\to\infty} \varphi_{AB}^{II}(1) < \lim_{Q_{\max}\to\infty} \varphi_{AB}^{II}(2).$$

Thus there exists a unique solution $Q_{\max}$, so that

$$\varphi_{AB}^{II}(1) = \varphi_{AB}^{II}(2),$$

and we call this solution as $\underline{Q}_{AB}$.

By assuming $\varphi_{AB}^{II}(n)$ is unimodal or monotonic in n, if $Q_{\max} < \underline{Q}_{AB}$, from $\varphi_{AB}^{II}(1) > \varphi_{AB}^{II}(2)$ we can conclude that $\varphi_{AB}^{II}(n)$ now monotonically decreases with n. For $\varphi_{BA}^{II}(n)$, we can derive $\underline{Q}_{BA}$ so that when $Q_{\max} < \underline{Q}_{BA}$, $\varphi_{BA}^{II}(n)$ decreases with n. Define $\underline{Q} = \min\{\underline{Q}_{AB}, \underline{Q}_{BA}\}$, when $Q_{\max} < \underline{Q}$, both $\varphi_{AB}^{II}(n)$ and $\varphi_{BA}^{II}(n)$ decrease with n, thus it is optimal for the monitor to jam $n^* = 1$ channel.

Similarly for $\varphi_{AB}^{II}(n)$, we can see from (20) that

$$\lim_{Q_{\max}\to 0^+} \varphi_{AB}^{II}(N-2) > \lim_{Q_{\max}\to 0^+} \varphi_{AB}^{II}(N-1),$$

and from (21), we can see that

$$\lim_{Q_{\max}\to\infty} \varphi_{AB}^{II}(N-2) < \lim_{Q_{\max}\to\infty} \varphi_{AB}^{II}(N-1).$$

There exists a unique solution $Q_{\max}$, so that

$$\varphi_{AB}^{II}(N-2) = \varphi_{AB}^{II}(N-1),$$

and we call this solution as $\bar{Q}_{AB}$.

By assuming $\varphi_{AB}^{II}(n)$ is unimodal or monotonic in n, if $Q_{\max} > \bar{Q}_{AB}$, from $\varphi_{AB}^{II}(N-2) < \varphi_{AB}^{II}(N-1)$ we can conclude that $\varphi_{AB}^{II}(n)$ now monotonically increases with n. Similarly for $\varphi_{BA}^{II}(n)$, we can derive $\bar{Q}_{BA}$ so that when $Q_{\max} > \bar{Q}_{BA}$, $\varphi_{BA}^{II}(n)$ increases with n. Define $\bar{Q} = \max\{\bar{Q}_{AB}, \bar{Q}_{BA}\}$, when $Q_{\max} < \bar{Q}$, both $\varphi_{AB}^{II}(n)$ and $\varphi_{BA}^{II}(n)$ increase with n, thus it is optimal for the monitor to jam $n^* = N - 1$ channels.

When $\underline{Q} \leq Q_{\max} \leq \bar{Q}$, at least one of $\varphi_{AB}^{II}(n)$ and $\varphi_{BA}^{II}(n)$ is unimodal. Without loss of generality, we assume $n_{AB}^* \leq n_{BA}^*$, clearly when $n < n_{AB}^*$, both $\varphi_{AB}^{II}(n)$ and $\varphi_{BA}^{II}(n)$ are monotonically increasing, and when $n > n_{BA}^*$, both $\varphi_{AB}^{II}(n)$ and $\varphi_{BA}^{II}(n)$ are monotonically decreasing. Thus n^* must lie between n_{AB}^* and n_{BA}^*, and can be numerically searched.

REFERENCES

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

[2] J. Li and A. P. Petropulu, "On beamforming solution for secrecy capacity of MIMO wiretap channels," in *Proc. IEEE GLOBECOM*, Dec. 2011, pp. 889–892.

[3] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: A block-markov Wyner secrecy encoding scheme," *IEEE Trans. Inform. Theory*, vol. 58, no. 7, pp. 4660–4677, Jul. 2012.

[4] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. ASILOMAR*, Nov. 2011, pp. 265–269.

[5] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Trans. Inform. Theory*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[6] K. Wang, L. Yuan, T. Miyazhaki, D. Zeng, S. Guo and Y. Sun, "Strategic antieavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9448–9457, May 2017.

[7] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proc. IEEE INFOCOM*, May 2007, pp. 2526–2530.

[8] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 2119–2123, Sept. 2004.

[9] Q. Liu, M. Li, X. Kong, and N. Zhao, "Disrupting MIMO communications with optimal jamming signal design," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5313–5325, Oct. 2015.

[10] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[11] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[12] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

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

[14] "Terrorist surveillance program." https://en.wikipedia.org/wiki/Terrorist_Surveillance_Program.

[15] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[16] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[17] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790–2806, May 2017.

[18] J. Xu, K. Li, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming over HARQ-based communications," in *Proc. IEEE GLOBECOM*, Dec. 2017, pp. 1–6.

[19] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.

[20] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[21] T. Riihonen, S. Werner, and R. Wichman, "Residual self-interference in full-duplex MIMO relays after null-space projection and cancellation," in *Proc. ASILOMAR*, Nov. 2010, pp. 653–657.

[22] A. Masmoudi and T. Le-Ngoc, "Self-interference cancellation limits in full-duplex communication systems," in *Proc. IEEE GLOBECOM*, Dec. 2016, pp. 1–6.

[23] H. Li and Z. Han, "Dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems, part I: known channel statistics," in *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3566–3577, Sep. 2010.

[24] H. Li and Z. Han, "Dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems, part II: unknown channel statistics," in *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274–283, Jan. 2011.

[25] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*. Academic Press, 2007.

Lingjie Duan (S'09-M'12-SM'16) received the Ph.D. degree from The Chinese University of Hong Kong in 2012. He is currently an Assistant Professor with the Engineering Systems and Design Pillar, Singapore University of Technology and Design, Singapore. His current research interests include network economics and game theory, cognitive and cooperative communications, energy harvesting wireless communications, mobile crowdsourcing, and wireless information surveillance. He was a recipient of the 2016 SUTD Excellence in Research Award, and the 10th IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2015. He was also the Finalist of the Hong Kong Young Scientist Award 2014 under Engineering Science track. He is now an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. In 2016, he was a Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Special Issue on Human-in-the-loop Mobile Networks, and was also a Guest Editor of the IEEE Wireless Communications Magazine for feature topic Sustainable Green Networking and Computing in 5G Systems. He is also a regular TPC member of a number of leading conferences on wireless communications and networking (e.g., IEEE INFOCOM, SECON, WiOPT, GLOBECOM, ICC and ACM MobiHoc).

Rui Zhang (S'00-M'07-SM'15-F'17) received the B.Eng. (first-class Hons.) and M.Eng. degrees from the National University of Singapore, Singapore, and the Ph.D. degree from the Stanford University, Stanford, CA, USA, all in electrical engineering.

From 2007 to 2010, he worked as a Research Scientist with the Institute for Infocomm Research, ASTAR, Singapore. Since 2010, he has joined the Department of Electrical and Computer Engineering, National University of Singapore, where he is now a Dean's Chair Associate Professor in the Faculty of Engineering. He has authored over 300 papers. He has been listed as a Highly Cited Researcher (also known as the World's Most Influential Scientific Minds), by Thomson Reuters (Clarivate Analytics) since 2015. His research interests include UAV/satellite communication, wireless information and power transfer, multiuser MIMO, smart and reconfigurable environment, and optimization methods.

He was the recipient of the 6th IEEE Communications Society Asia-Pacific Region Best Young Researcher Award in 2011, and the Young Researcher Award of National University of Singapore in 2015. He was the co-recipient of the IEEE Marconi Prize Paper Award in Wireless Communications in 2015, the IEEE Communications Society Asia-Pacific Region Best Paper Award in 2016, the IEEE Signal Processing Society Best Paper Award in 2016, the IEEE Communications Society Heinrich Hertz Prize Paper Award in 2017, the IEEE Signal Processing Society Donald G. Fink Overview Paper Award in 2017, and the IEEE Technical Committee on Green Communications & Computing (TCGCC) Best Journal Paper Award in 2017. His co-authored paper received the IEEE Signal Processing Society Young Author Best Paper Award in 2017. He served for over 30 international conferences as the TPC co-chair or an organizing committee member, and as the guest editor for 3 special issues in the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He was an elected member of the IEEE Signal Processing Society SPCOM Technical Committee from 2012 to 2017 and SAM Technical Committee from 2013 to 2015, and served as the Vice Chair of the IEEE Communications Society Asia-Pacific Board Technical Affairs Committee from 2014 to 2015. He served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2012 to 2016, the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS: Green Communications and Networking Series from 2015 to 2016, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING from 2013 to 2017. He is now an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING. He serves as a member of the Steering Committee of the IEEE Wireless Communications Letters. He is a Distinguished Lecturer of IEEE Signal Processing Society and IEEE Communications Society.

Yitao Han (S'19) received the B. Eng. degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 2015 and the M. Sc. degree in Department of Electrical and Computer Engineering from National University of Singapore, Singapore, in 2016. He is currently pursuing the Ph. D. degree in Engineering System and Design pillar, Singapore University of Technology and Design, Singapore, under SUTD-NUS joint Ph. D. programme with President's Graduate Fellowship.

His current research interests include physical layer security and UAV communications.