IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 8, 2019, accepted September 24, 2019, date of publication October 2, 2019, date of current version October 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2945060

Intelligent Secure Communication for Internet of Things With Statistical Channel State Information of Attacker

JUNJUAN XIA[1], YAN XU[1], DAN DENG[2], QINGFENG ZHOU[3], AND LISENG FAN[1]

[1]School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China
[2]School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou 511483, China
[3]School of Electrical Engineering and Intelligentization, Dongguan University of Technology, Dongguan 523808, China

Corresponding authors: Dan Deng (dengdan@ustc.edu), Qingfeng Zhou (enqfzhou@ieee.org), and Liseng Fan (lsfan2019@126.com)

This work was supported in part by the NSFC under Grant 61871139, in part by the Innovation Team Project of Guangdong Province University under Grant 2016KCXTD017, in part by the Science and Technology Program of Guangzhou under Grant 201807010103, and in part by the Natural Science Foundation of Guangdong Province under Grant 2017A030308006. The work of D. Deng was supported by the Natural Science Foundation of Guangdong Province (grant number 2018A030313736), Scientific Research Project of Education Department of Guangdong, China (grant number 2017GKTSCX045), and Science and Technology Program of Guangzhou, China (grant number 201707010389).

ABSTRACT In this paper, we investigate the power control strategy of intelligent secure communication with statistic channel state information (CSI) for Internet of Things (IoT) networks, where a transceiver and an attacker with several attack types, including silent, eavesdrop, jamming and spoofing, are considered. In order to solve the security problem that the transmitter only knows the statistical CSI of attacker, we propose a power control strategy based on Q-learning. In particular, Alice and Eve can choose their actions flexibly to maximize their reward under different system state and learn their best strategy according to the proposed strategy. In addition, the interactions between Alice and Eve are formulated as a zero-sum game, the Nash equilibrium and its existence conditions are deduced. Simulation results show that the impact of statistical CSI of attacker on system security performance can be reflected by the cost of attacker to launch attack and the average channel gain parameters. More importantly, the obtained results also show that the proposed power control strategy based on statistical CSI of attacker is worse than the scheme based on instantaneous CSI for statistical CSI leads a performance loss in terms of security.

INDEX TERMS Malicious attackers, statistical CSI, Q-learning, game theory.

I. INTRODUCTION

In recent years, there has been an increasing development in communication techniques [1]–[3], and the application scenarios can be fifth generation (5G) wireless communication [4]–[7] and Internet of Things (IoT) networks [8]–[11]. In the IoT networks, each element (node) can act as both the receiver and transmitter, and can flexibly communicate with other nodes in the network [12]. In particular, massive machine-type communications (mMTC) and ultra-reliable and low-latency communications (uRLLC) have been considered as two typical application scenarios [13]. Particularly, uRLLC needs a low-latency and high-reliability transmission. And mMTC supports massive connections of Internet of Things (IoT) devices with limited resource [14], [15]. Hence, the security problems of mMTC and uRLLC become very important due to their strict safety requirements of applications in smart traffic such as autonomous driving, smart health care, factory automation, etc [16], [17]. Otherwise, once a security accident occurs in these communication networks, it may cause communication obstacles among thousands of people, and bring unpredictable loss of social value and economic value [18]–[20].

In uRLLC or mMTC, the legitimate information transmitted in the channel is highly vulnerable to be attacked by malicious attackers for the openness of the wireless channel, which resulting in information leakage [16], [21]. To solve this problem, many researches have been studied with Q-learning and game theory [22]–[25]. For example, the authors in [22] extended the results of reliable and secure communication capacity requirements for eavesdropping attack to a more advanced chosen plain-text attack. The authors in [23] devised a generic security game, revealing the existence of several Nash equilibrium strategies. Moreover, a power control strategy based on Q-learning for the transmitter to suppress the attack motivation of smart

The associate editor coordinating the review of this manuscript and approving it for publication was Min Jia.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

attackers in a dynamic version of multiple-input multiple-output transmission game is proposed in [24]. However, most of these works are based on assumption that the transmitter knows the instantaneous perfect or inaccuracy estimated CSI of attacker, which is impractical due to the rapid change of channel [26]–[28]. In addition, the transmitter have to pay more costs to acquire the instantaneous CSI of the attacker. Hence, it is of vital importance to study an intelligent secure communication with statistical CSI of attacker, which motivates our research.

In this paper, we investigate the power control strategy of intelligent secure communication, which concludes a transceiver and an attacker, where the attacker can choose its attack mode from silent, eavesdropping, jamming and spoofing attacks. Different to [24], [25], [29], more attack modes with statistical CSI of attackers are considered here. To study the transmission security problem and the impact of statistical CSI of attacker, Q-learning and game theory are introduced. To be specific, according to attacker's attack mode, the transmit power of the transmitter can be adaptively adjusted through Q-learning to improve the network secrecy performance against attacks. Furthermore, we formulate the interactions between the transmitter and the attacker as a zero-sum game, and we deduce the Nash equilibrium (NE) and its existence conditions of this network. Finally, we disclose the impact on statistical CSI of attacker at the transmitter, compared with that with instantaneous CSI of attacker.

The main contributions of this work can be summarized as follows:

- The secrecy capacities of the secure communications attacked by four considered attack modes, including silent, eavesdropping, jamming and spoofing, with statistical CSI are derived in closed-form. With the aid of the developed secrecy capacities, we formulate an intelligent secure communication game with statistical CSI of attackers.
- Based on game theory, we derive the NE of the formulated secure game, and provide the existing conditions of the equilibrium. It reveals that an optimal secure transmission can be obtained according to the attack cost and transmission cost of legitimate transmitter.
- We propose a power control strategy for the secure communication with statistical CSI of attacker based on Q-learning technique, and analyse the impact on only the statistical CSI of attacker known at the transmitter.

We organize the remainder of this paper as follows. In Section II, we present the system model and formulate the secure problem with statistical CSI of attacker. In Section III, we formulate the intelligent secure communication game under statistical CSI of attacker, and investigate a power control strategy in Section IV. In Section V, we provide the simulation results and give some conclusions in Section VI.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. MODEL DESCRIPTION

Fig. 1 shows an intelligent secure communication network, which consists of a legitimate transmitter (Alice), an intended receiver (Bob) and an attacker (Eve). All of these users have a single-antenna. When Alice communicates with Bob through the main channel, Eve might correspondingly choose one of attack modes, including silent, eavesdrop, jamming and spoofing, as its action to attack main channel according to Alice's transmit power. On the other hand, Alice adjusts the transmit power to protect network against attacks from Eve by observing Eve's current attack mode. In this paper, we assume the transmit power of Alice is $p \in [0, P]$, where P denotes the maximum transmitter power. The attack modes of Eve are defined as $m = 1, 2, 3, 4$, which correspond to silent, eavesdrop, jamming and spoofing. It means that Eve might choose to keep silent, eavesdrop on Alice's signal, send a jamming signals to obstruct Alice's transmission or send a spoofing signal to deceive Bob, respectively.

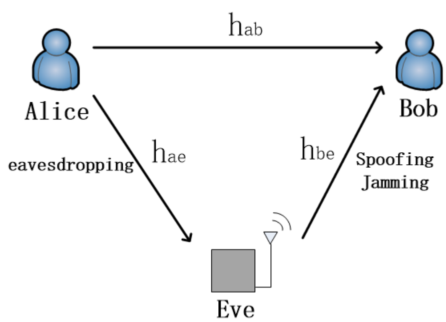


FIGURE 1. System model of an intelligent secure communication for Alice and Eve.

B. PROBLEM FORMULATION

In order to protect network against a possible attack from Eve, Alice has to adjust the transmit power based on the instantaneous CSI of Eve. However, acquiring instantaneous CSI is impractical due to the large feedback delay and the rapid change of wireless channel [30]. As a result, we consider a practical case that Alice knows the statistical CSI of Eve. To be specific, Eve might choose to keep silent, eavesdrop on Alice's signal when Alice sends a signal to Bob, send a jamming signals to obstruct Alice's transmission or send a spoofing signal to deceive Bob, respectively. In what follows, we introduce the secrecy capacities of these four attack modes with statistical CSI in detail.

Silent ($m = 1$): Alice sends a signal x_a to Bob and Eve chooses to keep silent, then the received signal at Bob is formulated as

$$y_1 = \sqrt{p} h_{ab} x_a + n_b, \tag{1}$$

where $h_{ab} \sim \mathcal{CN}(0, \sigma_{ab}^2)$ is the channel between Alice and Bob, $\sigma_{ab}^2 = 1/(1 + d_{ab}^{\zeta})$, d_{ab} is the distance between Alice and Bob, ζ denotes the path loss factor, and $n_b \sim \mathcal{CN}(0, \sigma_n^2)$ is the additive white Gaussian noise (AWGN) at Bob [10], [12], [14], [31]–[33]. Therefore, we write the secrecy capacity [34], as

$$C_1 = \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right). \tag{2}$$

Eavesdropping ($m = 2$): Eve chooses to eavesdrop on Alice's message when Alice sends a signal x_a to Bob. Bob receives a signal y_1 in (1) and Eve receives a signal y_2 given by

$$y_2 = \sqrt{p}h_{ae}x_a + n_e, \tag{3}$$

where $h_{ae} \sim \mathcal{CN}(0, \sigma_{ae}^2)$ is the channel of Alice-Eve link, $\sigma_{ae}^2 = \frac{1}{1+d_{ae}^{\zeta}}$, d_{ae} is the distance between Alice and Eve, and $n_e \sim \mathcal{CN}(0, \sigma_n^2)$ is the AWGN at Eve. Thus, the secrecy capacity is given by

$$C_2 = \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right) - \log_2\left(1+\frac{p|h_{ae}|^2}{\sigma_n^2}\right). \tag{4}$$

Note that the instantaneous CSI of Eve is unknown, we can't calculate the secrecy capacity C_2 directly. However, if the statistical CSI between Alice and Eve is known, we can rewrite the secrecy capacity C_2 in (4) as [35],

$$\begin{aligned} C_2' &= \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right) - \frac{1}{\sigma_{ae}^2}\int_0^{+\infty}\log_2\left(1+\frac{px_1}{\sigma_n^2}\right) \\ &\quad \times \exp\left(-\frac{x_1}{\sigma_{ae}^2}\right)dx_1 \\ &= \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right) + \frac{1}{\ln 2}\exp\left(\frac{\sigma_n^2}{\sigma_{ae}^2 p}\right)\mathrm{Ei}\left(-\frac{\sigma_n^2}{\sigma_{ae}^2 p}\right), \end{aligned} \tag{5}$$

where we use the fact that $x_1 = |h_{ae}|^2$ follows exponential distribution and $\mathrm{Ei}(x) = \int_{-x}^{+\infty}\frac{e^{-t}}{-t}dt$ is the exponential integral function [35].

Jamming ($m = 3$): Eve chooses to send a jamming signal x_J with power P_J to interfere Alice's transmission, the received signal at Bob can be given as follows,

$$y_3 = \sqrt{p}h_{ab}x_a + \sqrt{P_J}h_{be}x_J + n_b, \tag{6}$$

where $h_{be} \sim \mathcal{CN}(0, \sigma_{be}^2)$ is the channel parameter of Bob-Eve link, $\sigma_{be}^2 = \frac{1}{1+d_{be}^{\zeta}}$, d_{be} is the distance between Bob and Eve. Then the secrecy capacity can be written as

$$C_3 = \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2 + P_J|h_{be}|^2}\right). \tag{7}$$

Similarly, the secrecy capacity C_3 in (7) for the case that only the statistical CSI of Eve is known at Bob is rewritten as

$$\begin{aligned} C_3' &= \frac{1}{\sigma_{be}^2}\int_0^{+\infty}\log_2\left(\sigma_n^2 + ph_{ab}^2 + P_J x_2\right)\exp\left(-\frac{x_2}{\sigma_{be}^2}\right)dx_2 \\ &\quad - \frac{1}{\sigma_{be}^2}\int_0^{+\infty}\log_2\left(\sigma_n^2 + P_J x_2\right)\exp\left(-\frac{x_2}{\sigma_{be}^2}\right)dx_2 \\ &= \log_2\left(\sigma_n^2 + ph_{ab}^2\right) - \frac{1}{\ln 2}\exp\left(\frac{\sigma_n^2 + ph_{ab}^2}{P_J\sigma_{be}^2}\right)\cdot \\ &\quad \mathrm{Ei}\left(-\frac{\sigma_n^2 + ph_{ab}^2}{P_J\sigma_{be}^2}\right) + \frac{1}{\ln 2}\exp\left(\frac{\sigma_n^2}{P_J\sigma_{be}^2}\right)\mathrm{Ei}\left(-\frac{\sigma_n^2}{P_J\sigma_{be}^2}\right), \end{aligned} \tag{8}$$

where $x_2 = |h_{be}|^2$.

Spoofing ($m = 4$): Eve chooses to send a spoofing signal x_S with power P_S to deceive Bob. The received signal at Bob is given by

$$y_4 = \sqrt{p}h_{ab}x_a + \sqrt{P_S}h_{be}x_S + n_b. \tag{9}$$

Then the secrecy capacity can be written as

$$C_4 = \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right) - \gamma\log_2\left(1+\frac{P_S|h_{be}|^2}{\sigma_n^2}\right), \tag{10}$$

where γ reflects the impact of each unit size spoofing signal. Similar to the previous, the secrecy capacity with the statistical CSI of the spoofing link can be rewritten as

$$\begin{aligned} C_4' &= \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right) - \frac{1}{\sigma_{be}^2}\int_0^{+\infty}\gamma\log_2\left(1+\frac{P_S x_2}{\sigma_n^2}\right) \\ &\quad \times \exp\left(-\frac{x_2}{\sigma_{be}^2}\right)dx_2 \\ &= \log_2\left(1+\frac{p|h_{ab}|^2}{\sigma_n^2}\right) + \frac{\gamma}{\ln 2}\exp\left(\frac{\sigma_n^2}{P_S\sigma_{be}^2}\right)\mathrm{Ei}\left(-\frac{\sigma_n^2}{P_S\sigma_{be}^2}\right). \end{aligned} \tag{11}$$

For simplicity, we will replace the noise variance σ_n^2 by 1 directly in the remainder sections.

III. SECURE GAME WITH STATISTICAL INFORMATION OF ATTACKER

In intelligent secure communication, Alice aims at adjusting its transmit power to prevent Eve's attack when she only knows the statistical information of Eve. In this section, the interactions between Alice and Eve are formulated as a security game theory. In the game, Eve can correspondingly choose one of its attack modes as its action according to Alice's transmit power p. Similarly, Alice also can choose a transmit power as its next action by observing Eve's current attack mode m. The cost function of Eve's attack mode m is denoted as

$$f(m) = \begin{cases} 0, & m = 1, \\ \theta_E, & m = 2, \\ \theta_J, & m = 3, \\ \theta_S, & m = 4, \end{cases}$$

where θ_E, θ_J and θ_S are the cost of Eve to carry out eavesdropping, jamming, and spoofing, respectively.

Let R_a denote the reward of Alice, and

$$R_a(p, m) = \begin{cases} \ln 2C_1 - C_a p, & m = 1, \\ \ln 2C_m' - C_a p, & m = 2, 3, 4, \end{cases} \tag{12}$$

where C_a is the cost coefficient of Alice's transmit power. For the sake of derivatives and expressions, the secrecy capacity is multiplied by ln 2 in (12). Again, let R_e represent the reward of Eve, and it can be written as

$$R_e(p, m) = -\ln 2C_m - C_e f(m), \tag{13}$$

where C_e is the cost coefficient of Eve's attack mode. Further, let (p^*, m^*) denote the NE strategy of the security game, which can be written as

$$R_a(p^*, m^*) \geq R_a(p, m^*), \quad \forall 0 \leq p \leq P. \tag{14}$$

$$R_e(p^*, m^*) \geq R_e(p^*, m), \quad \forall m = 1, 2, 3, 4. \tag{15}$$

Eqs. (14) and (15) disclose that Alice and Eve can obtain the best reward at their NE strategy, namely, they can not obtain more rewards by altering their NE strategy. As a result, no one wants to upset the equilibrium. In addition, we can deduce an NE $(p^*, 1)$, which is given by the following *Lemma 1*.

Lemma 1: An NE $(p^*, 1)$ of security game with statistical CSI of attacker is given by

$$\begin{cases} \dfrac{|h_{ab}|^2}{1 + p^*|h_{ab}|^2} = C_a, & \text{(16a)} \\ 0 \leq p^* \leq P. & \text{(16b)} \end{cases}$$

If the following conditions are satisfied

$$\begin{cases} \theta_E \geq \dfrac{\ln(1 + p^*|h_{ae}|^2)}{C_e}, & \text{(17a)} \\ \theta_J \geq \dfrac{1}{C_e} \ln(1 + \dfrac{p^* P_J |h_{ab}|^2 |h_{be}|^2}{1 + P_J |h_{be}|^2 + p^*|h_{ab}|^2}), & \text{(17b)} \\ \theta_S \geq \dfrac{\gamma \ln(1 + P_S |h_{be}|^2)}{C_e}, & \text{(17c)} \\ \dfrac{|h_{ab}|^2}{1 + P|h_{ab}|^2} < C_a < |h_{ab}|^2. & \text{(17d)} \end{cases}$$

Proof: If (17a)-(17c) hold, from (15), we have

$$\begin{aligned} &R_e(p^*, 1) - R_e(p^*, 2) \\ &\quad = C_e\theta_E - \ln(1 + p^*|h_{ae}|^2)) \geq 0, \\ &R_e(p^*, 1) - R_e(p^*, 3) \\ &\quad = C_e\theta_J - \ln(1 + \frac{p^* P_J |h_{ab}|^2 |h_{be}|^2}{1 + P_J |h_{be}|^2 + p^*|h_{ab}|^2}) \geq 0, \\ &R_e(p^*, 1) - R_e(p^*, 4) \\ &\quad = C_e\theta_S - \gamma \ln(1 + P_S |h_{be}|^2) \geq 0. \end{aligned}$$

Thus, (15) holds for $(p^*, 1)$. From (14), we have

$$\frac{\partial R_a(p, 1)}{\partial p} = \frac{|h_{ab}|^2}{1 + p|h_{ab}|^2} - C_a, \tag{18}$$

$$\frac{\partial R_a^2(p, 1)}{\partial p^2} = -\frac{|h_{ab}|^4}{(1 + p|h_{ab}|^2)^2} \leq 0. \tag{19}$$

By (19), we know that $\partial R_a(p, 1)/\partial p$ a monotonically decreasing function with respect to (w.r.t) p. If (17d) holds, from (18), we have

$$\frac{\partial R_a(p, 1)}{\partial p}|_{p=0} = |h_{ab}|^2 - C_a > 0, \tag{20}$$

$$\frac{\partial R_a(p, 1)}{\partial p}|_{p=P} = \frac{|h_{ab}|^2}{1 + P|h_{ab}|^2} - C_a < 0. \tag{21}$$

Eqs. (19)-(21) show that $\partial R_a(p, 1)/\partial p = 0$ has a unique solution p^*, which is given by (16a). Moreover, it is obvious that $R_a(p, 1)$ increases in p if $0 \leq p \leq p^*$, while it decreases in p if $p^* \leq p \leq P$. Therefore, (14) holds for $(p^*, 1)$. At this point, we have completed the proof for *Lemma 1* by proving (14) and (15) hold for $(p^*, 1)$.

The results in *Lemma 1* reveal the security transmission conditions for Alice based on the NE. Furthermore, we can deduce an NE of the security game when Alice chooses the maximum transmit power in the following *Lemma 2*.

Lemma 2: This game has an NE $(P, 1)$, if

$$\begin{cases} \theta_E \geq \dfrac{\ln(1 + P|h_{ae}|^2)}{C_e}, & \text{(22a)} \\ \theta_J \geq \dfrac{1}{C_e} \ln(1 + \dfrac{P P_J |h_{ab}|^2 |h_{be}|^2}{1 + P_J |h_{be}|^2 + P|h_{ab}|^2}), & \text{(22b)} \\ \theta_S \geq \dfrac{\gamma \ln(1 + P_S |h_{be}|^2)}{C_e}, & \text{(22c)} \\ \dfrac{|h_{ab}|^2}{1 + P|h_{ab}|^2} \geq C_a. & \text{(22d)} \end{cases}$$

Proof: If (22a)-(22c) hold, from (15), we have

$$\begin{aligned} &R_e(P, 1) - R_e(P, 2) = C_e\theta_E - \ln(1 + P|h_{ae}|^2)) \geq 0, \\ &R_e(P, 1) - R_e(P, 3) = C_e\theta_J - \ln(1 + \frac{P P_J |h_{ab}|^2 |h_{be}|^2}{1 + P_J |h_{be}|^2 + P|h_{ab}|^2}) \geq 0, \\ &R_e(P, 1) - R_e(P, 4) = C_e\theta_S - \gamma \ln(1 + P_S |h_{be}|^2) \geq 0. \end{aligned}$$

Thus, (15) holds for $(P, 1)$. From (18), if (22d) hold, we have

$$\frac{\partial R_a(p, 1)}{\partial p}|_{p=P} = \frac{|h_{ab}|^2}{1 + P|h_{ab}|^2} - C_a \geq 0. \tag{23}$$

Since $\partial R_a(p, 1)/\partial p$ monotonically decreases in p, we can see that $\partial R_a(p, 1)/\partial p$ always greater than or equal to 0, for all $p \in [0, P]$. Thus, $R_a(p, 1)$ maximizes at P, namely (14) holds for $(P, 1)$. At this point, we have completed the proof for *Lemma 2* by proving (14) and (15) hold for $(P, 1)$.

TABLE 1. Main parameter setting for simulations.

Parameter	Value
Average channel gain	$\sigma^2_{ab} = 1.2, \sigma^2_{ae} = 0.5, \sigma^2_{be} = 2$
Jamming power	$P_J = 2$
Spoofing power	$P_S = 2.2$
Costs of considered attackers	$\theta_E = 2.4, \theta_J = 2, \theta_S = 2.2$
Cost of unit transmit power for Alice	$C_a = 0.1$
Cost coefficient for Eve	$C_e = 0.5$
Number of experiments	10^4

IV. A STATISTICAL CSI-BASED POWER CONTROL STRATEGY

In this section, we propose a power control strategy based on Q-learning under statistical CSI of Eve. With the aid of Q-learning, Alice and Eve can choose their actions flexibly to

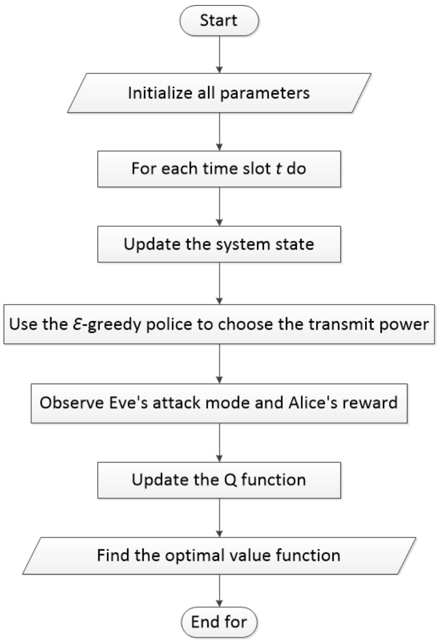


FIGURE 2. Algorithm flow diagram of power control strategy.

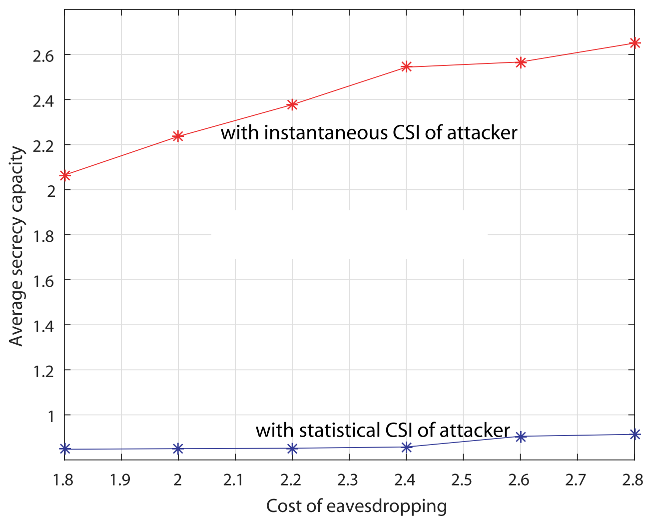
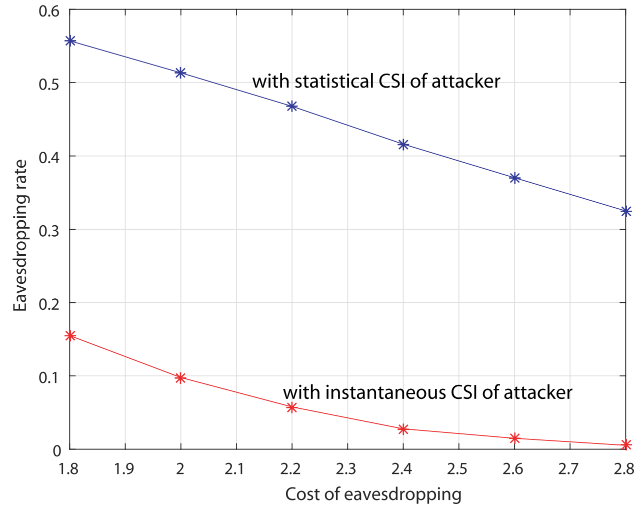


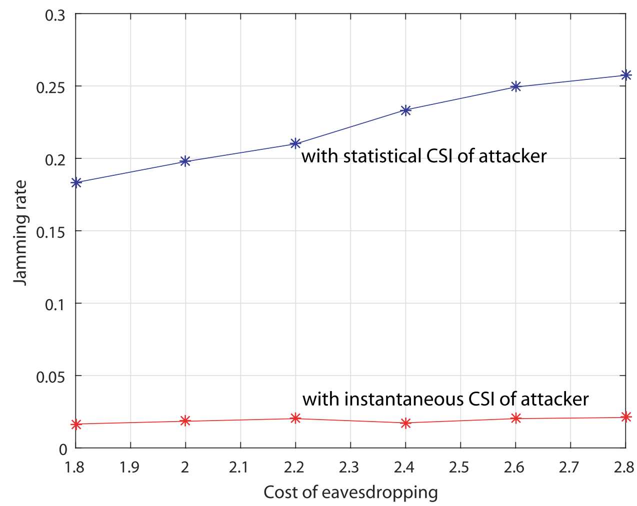
FIGURE 3. Average secrecy capacity of the considered network over the cost of eavesdropping.

maximize their reward under different system state and learn their best strategy. The statistical CSI-based power control algorithm flow diagram is given in Fig. 2. In this paper, we consider Alice can choose its action among $L+1$ levels at time t, namely $p_t \in \{lP/L\}_{0 \leq l \leq L}$. Before the game, we initialize all parameters and let the system state $s_t = m_{t-1}$ at time slot t. Firstly, Alice chooses the transmit power p_t using the ϵ-greedy police. Then, through observing the system state s_t and its reward under the statistical CSI of Eve, Alice updates its Q function $Q_a(s_t, p_t)$ and finds the optimal value function $V_a(s_t)$ by the following equations.

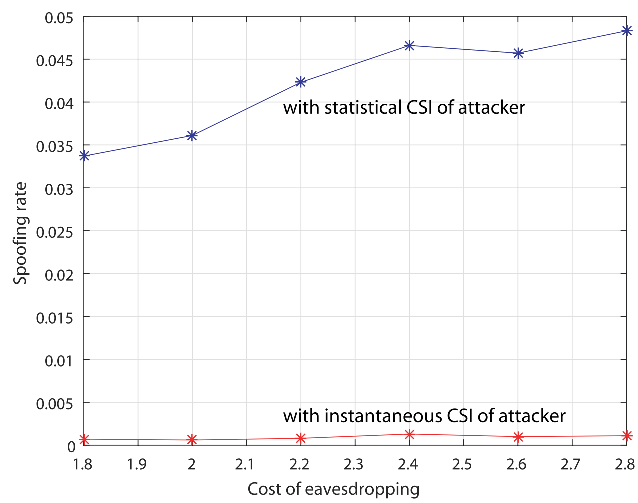
$$Q_a(s_t, p_t) = (1-\alpha)Q_a(s_t, p_t) + \alpha(R_a(s_t, p_t)) + \delta V_a(s_{t+1}), \tag{24}$$



(a) Eavesdropping rate



(b) Jamming rate



(c) Spoofing rate

FIGURE 4. Attack rate of Eve over the cost of eavesdropping.

$$V_a(s_t) = \max_{0 \leq p \leq P} Q_a(s_t, p), \tag{25}$$

where $\alpha \in [0, 1]$ is the learning rate, $\delta \in [0, 1]$ is the discount factor. Similarly, Eve updates its Q function by observing the

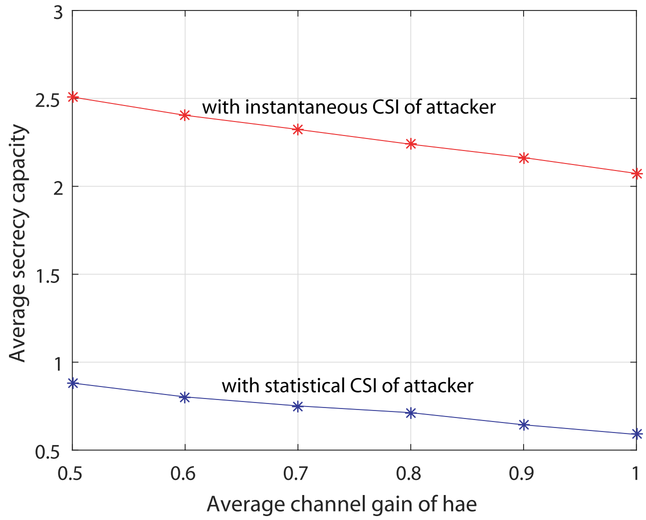


FIGURE 5. Average secrecy capacity of the considered network over the average channel gain of eavesdropping link.

action of Alice and the reward under the instantaneous CSI of itself, where the Q function of Eve is given by

$$Q_e(p_t, m_t) = (1-\alpha)Q_e(p_t, m_t) + \alpha(R_e(p_t, m_t)) + \delta V_e(p_{t+1}), \quad (26)$$

and Eve finds the optimal value function:

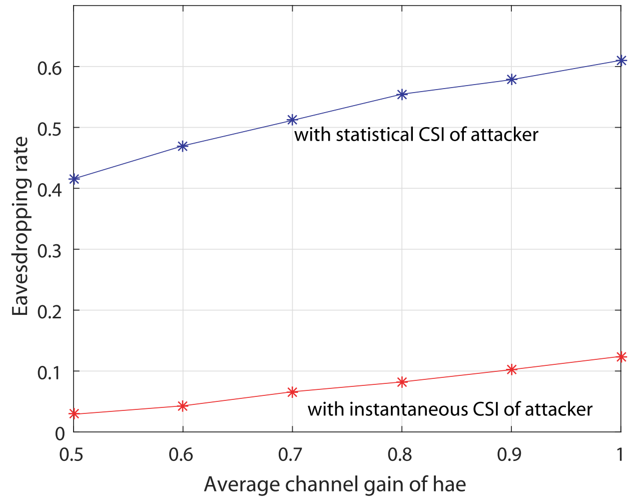
$$V_e(p_t) = \max_{m \in \{1,2,3,4\}} Q_e(p_t, m). \quad (27)$$

That is, Alice and Eve can learn their best strategy through the obtained value function in the game.

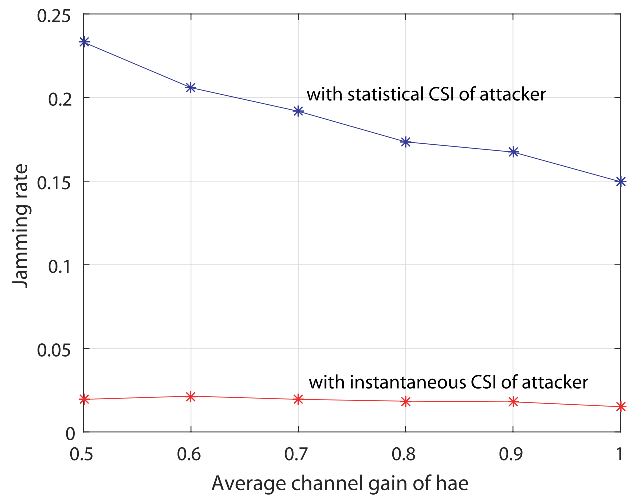
V. SIMULATION RESULTS

In this section, we will evaluate the system average secrecy capacities and the attack rates of different type attackers ($m = 1, 2, 3, 4$) from Eve with statistical CSI. The obtained results based on game theory are provided to disclose the impact on only statistical CSI of Eve known at Alice. The commonly-used parameters are listed in Table 1. Fig. 3 shows the average secrecy capacities for the cases that Alice knows instantaneous or statistical CSI of Eve, where the eavesdropping cost is range from 1.8 to 2.8, and the step size is 0.2. In addition, we use the average value at time slot 8000 to show in Fig. 3. Notice that the time slot is range from 0 to 8000 in our experiments, and we take the values of 8000 time slots for they have converged. As observed from Fig. 3, we can find that the average secrecy capacity with instantaneous CSI of attacker is increasing as the cost of eavesdropping increases, and it performs better than that with statistical CSI.

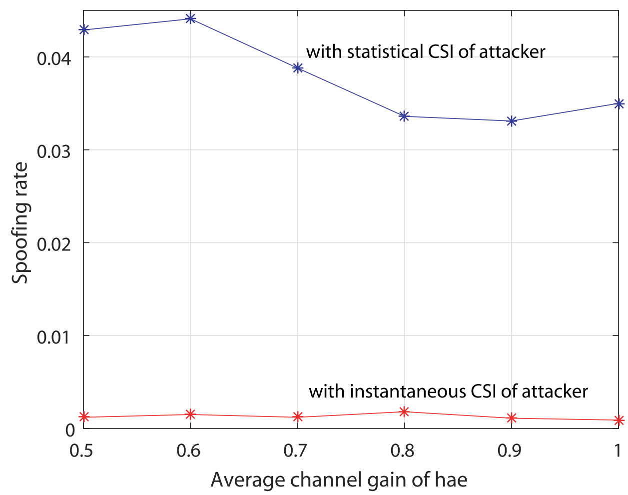
Fig. 4 presents the eavesdropping rate, jamming rate and spoofing rate of Eve. It is noted that, the attack rates of all attack modes ($m = 2, 3, 4$) with instantaneous CSI are smaller than that Alice only knows the statistical CSI of Eve. As shown in Fig. 4(a), we can find that the probability of Eve choosing to perform eavesdropping becomes



(a) Eavesdropping rate



(b) Jamming rate



(c) Spoofing rate

FIGURE 6. Attack rate of Eve over the average channel gain of eavesdropping link.

smaller with a larger eavesdropping cost, whether Alice knows Eve's instantaneous CSI or not. Similarly, Fig. 4(b) and Fig.4(c) show the jamming rate and the spoofing rate of Eve, respectively. It can be seen that the jamming rate and the spoofing rate with statistical information of attacker is increasing as the eavesdropping cost increases. In contrast with the statistical CSI of attacker, the jamming rate and the spoofing rate with instantaneous CSI of attacker is steady as the eavesdropping cost increases. The reason is that in the former case, Alice can't obtain Eve's instantaneous CSI accurately, so Eve is more inclined to choose to attack. But in the latter case, it is obvious that the eavesdropping cost with little influence of the jamming mode and spoofing mode.

Fig. 5 shows the average secrecy capacity with statistical CSI of Eve, where the average channel gain h_{ae} is range from 0.5 to 1, and the step size is 0.1. As observed from Fig. 5, we can find that the average secrecy capacity with instantaneous CSI of attacker is decreasing as the average channel gain of h_{ae} increases, and it performs better than that with statistical CSI.

The average channel gain versus the attack rate of Eve is shown in Fig. 6. It is obvious that the attack rates of all attack modes ($m = 2, 3, 4$) are higher when Alice only knows the statistical CSI of Eve than that when Alice knows the instantaneous CSI. As shown in Fig. 6(a), we can find that the probability of Eve choosing to perform eavesdropping becomes bigger with a larger average channel gain h_{ae}, whether Alice knows Eve's instantaneous CSI or not. Similarly, Fig. 6(b) and Fig. 6(c) show the jamming rate and the spoofing rate of Eve, respectively. We can find that the jamming rate and the spoofing rate with statistical CSI of attacker are decreasing as the average channel gain h_{ae} increases. In contrast, the jamming rate and the spoofing rate with instantaneous CSI of attacker are steady as the eavesdropping cost increases. This can be explained because Eve is more inclined to choose to overhear if it chooses to attack in the former case. But in the latter case, it is obvious that the eavesdropping link's average channel gain with little influence of the jamming mode and spoofing mode.

VI. CONCLUSION

In this paper, we investigated a statistical CSI-based power control strategy in an intelligent secure communication network, which concludes a transmitter, a receiver and an attacker, and the attacker has four attack types, including silent, eavesdropping, jamming and spoofing. With statistical CSI of Eve, we proposed a power control strategy based on Q-learning. In this control strategy, Alice and Eve could choose their actions flexibly to maximize their rewards under different system state and learn their best strategies. In addition, the interactions between Alice and Eve were formulated as a zero-sum game, the NE and its existence conditions of this network were deduced. Simulation results showed the impact on the statistical CSI of attacker known at the transmitter in secure communications. By comparing with that with instantaneous CSI of attacker, we find that the transmission performance with instantaneous CSI of attacker has better performance under same environment. In the future works, we're going to investigate some intelligent algorithms such as the deep learning based algorithm [36]–[38] for the considered system to improve the transmission performance with statistical CSI of attacker, and take this question: "How does Alice know whether Eve chooses eavesdropping" into consideration. Moreover, we will consider to incorporate wireless caching technique [39]–[43] into the considered system to enhance the transmission security.

REFERENCES

[1] X. Liu, F. Li, and Z. Na, "Optimal resource allocation in simultaneous cooperative spectrum sensing and energy harvesting for multichannel cognitive radio," *IEEE Access*, vol. 5, pp. 3801–3812, 2017.

[2] Z. Na, Y. Wang, X. Li, J. Xia, X. Liu, M. Xiong, and W. Lu, "Subcarrier allocation based simultaneous wireless information and power transfer algorithm in 5G cooperative OFDM communication systems," *Phys. Commun.*, vol. 29, pp. 164–170, Aug. 2018.

[3] F. Shi, J. Xia, Z. Na, X. Liu, Y. Ding, and Z. Wang, "Secure probabilistic caching in random multi-user multi-UAV relay networks," *Phys. Commun.*, vol. 32, pp. 31–40, Feb. 2019.

[4] X. Lai, W. Zou, D. Xie, X. Li, and L. Fan, "DF relaying networks with randomly distributed interferers," *IEEE Access*, vol. 5, pp. 18909–18917, 2017.

[5] X. Liu, M. Jia, Z. Na, W. Lu, and F. Li, "Multi-modal cooperative spectrum sensing based on dempster-shafer fusion in 5G-based cognitive radio," *IEEE Access*, vol. 6, pp. 199–208, 2018.

[6] Z. Na, J. Lv, M. Zhang, B. Peng, M. Guan, and M. Xiong, "GFDM based wireless powered communication for cooperative relay system," *IEEE Access*, vol. 7, pp. 50971–50979, 2019.

[7] M. Jia, Z. Gao, Q. Guo, Y. Lin, and X. Gu, "Sparse feature learning for correlation filter tracking toward 5G-enabled tactile Internet," *IEEE Trans. Ind. Informat.*, to be published.

[8] X. Lin, J. Xia, and Z. Wang, "Probabilistic caching placement in UAV-assisted heterogeneous wireless networks," *Phys. Commun.*, vol. 33, pp. 54–61, Apr. 2019.

[9] X. Lin, Y. Tang, X. Lei, J. Xia, Q. Zhou, H. Wu, and L. Fan, "MARL-based distributed cache placement for wireless networks," *IEEE Access*, vol. 7, pp. 62606–62615, 2019.

[10] M. Jia, X. Gu, Q. Guo, W. Xiang, and N. Zhang, "Broadband hybrid satellite-terrestrial communication systems based on cognitive radio toward 5G," *IEEE Wireless Commun.*, vol. 23, no. 6, pp. 96–106, Dec. 2016.

[11] X. Liu, X. Zhang, M. Jia, L. Fan, W. Lu, and X. Zhai, "5G-based green broadband communication system design with simultaneous wireless information and power transfer," *Phys. Commun.*, vol. 28, pp. 130–137, Jun. 2018.

[12] M. Jia, Z. Yin, D. Li, Q. Guo, and X. Gu, "Toward improved offloading efficiency of data transmission in the IoT-cloud by leveraging secure truncating OFDM," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4252–4261, Jun. 2019.

[13] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55765–55779, 2018.

[14] M. Jia, Z. Yin, Q. Guo, G. Liu, and X. Gu, "Downlink design for spectrum efficient IoT network," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3397–3404, Oct. 2018.

[15] J. Xia, "Cache-aided mobile edge computing for B5G wireless communication networks," *EURASIP J. Wireless Commun. Netw.*, to be published.

[16] X. Lai, L. Fan, X. Lei, J. Li, N. Yang, and G. K. Karagiannidis, "Distributed secure switch-and-stay combining over correlated fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2088–2101, Aug. 2019.

[17] K. He, "A MIMO detector with deep learning in the presence of correlated interference," *IEEE Trans. Veh. Technol.*, to be published.

[18] M. A. Stuchly, "Wireless communications and the safety of the user," *Int. J. Wireless Inf. Netw.*, vol. 1, no. 4, pp. 223–228, 1994.

[19] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE Commun. Mag.*, vol. 44, no. 1, pp. 74–82, Jan. 2006.

[20] N. Kapucu, B. Haupt, M. Yuksel, I. Guvenc, and W. Saad, "On the evolution of wireless communication technologies and spectrum sharing for public safety: Policies and practice," *Risk Hazards Crisis Public Policy*, vol. 7, no. 3, pp. 129–145, 2016.

[21] J. Yang, D. Ruan, J. Huang, X. Kang, and Y.-Q. Shi, "An embedding cost learning framework using GAN," *IEEE Trans. Inf. Forensics Security*, to be published.

[22] S. Liu, G. Bei, and H. Li, "Capacity analysis for secure communication under CPA attack in smart grid," in *Proc. IEEE Int. Conf. Electro/Inf. Technol.*, May 2013, pp. 1–5.

[23] M. Pilz, F. B. Naeini, K. Grammont, C. Smagghe, M. Davis, J.-C. Nebel, L. Al-Fagih, and E. Pfluegel, "Security attacks on smart grid scheduling and their defences: A game-theoretic approach," *Int. J. Inf. Secur.*, vol. 1, pp. 1–17, Aug. 2018.

[24] Y. Li, L. Xiao, H. Dai, and H. V. Poor, "Game theoretic study of protecting MIMO transmissions against smart attacks," in *Proc. IEEE Int. Conf. Commun.*, May 2017, pp. 1–6.

[25] Y. Xu, J. Xia, H. Wu, and L. Fan, "Q-learning based physical-layer secure game against multiagent attacks," *IEEE Access*, vol. 7, pp. 49212–49222, 2019.

[26] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "LDPC-based secure wireless communication with imperfect knowledge of the eavesdropper's channel," in *Proc. IEEE Inf. Theory Workshop (ITW) Chengdu*, Oct. 2006, pp. 155–159.

[27] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting secure communication under UAV smart attack with imperfect channel estimation," *IEEE Access*, vol. 6, pp. 76395–76401, 2018.

[28] C. Li, W. Zhou, K. Yu, L. Fan, and J. Xia, "Enhanced secure transmission against intelligent attacks," *IEEE Access*, vol. 7, pp. 53596–53602, 2019.

[29] X. Hu, C. Zhong, X. Chen, W. Xu, and Z. Zhang, "Cluster grouping and power control for angle-domain mmWave MIMO NOMA systems," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 5, pp. 1167–1180, Sep. 2019.

[30] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[31] B. Wang, F. Gao, S. Jin, H. Lin, and G. Y. Li, "Spatial- and frequency-wideband effects in millimeter-wave massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 66, no. 13, pp. 3393–3406, Jul. 2018.

[32] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3170–3184, Apr. 2017.

[33] X. Liu, M. Jia, X. Zhang, and W. Lu, "A novel multichannel Internet of things based on dynamic spectrum sharing in 5G communication," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5962–5970, Aug. 2019.

[34] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[35] I. S. Gradshteyn and I. M. Ryzhik, "Table of integrals, series, and products," *Math. Comput.*, vol. 20, no. 96, pp. 1157–1160, 2007.

[36] G. Liu, Y. Xu, Z. He, Y. Rao, J. Xia, and L. Fan, "Deep learning-based channel prediction for edge computing networks toward intelligent connected vehicles," *IEEE Access*, vol. 7, pp. 114487–114495, 2019.

[37] Z. Zhao, "A novel framework of three-hierarchical offloading optimization for mec in industrial IoT networks," *IEEE Trans. Ind. Informat.*, to be published.

[38] Z. Junhui, Y. Tao, G. Yi, W. Jiao, and F. Lei, "Power control algorithm of cognitive radio based on non-cooperative game theory," *China Commun.*, vol. 10, no. 11, pp. 143–154, 2013.

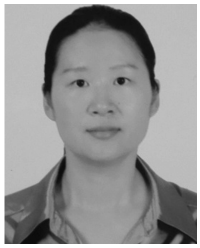
[39] L. Fan, N. Zhao, X. Lei, Q. Chen, N. Yang, and G. K. Karagiannidis, "Outage probability and optimal cache placement for multiple amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12373–12378, Dec. 2018.

[40] C. Li, "Cache-enabled physical-layer secure game against smart UAV-assisted attacks in B5G noma networks," *EURASIP J. Wireless Commun. Netw.*, to be published.

[41] M. Jia, X. Liu, Z. Yin, Q. Guo, and X. Gu, "Joint cooperative spectrum sensing and spectrum opportunity for satellite cluster communication networks," *Ad Hoc Netw.*, vol. 58, pp. 231–238, Apr. 2017.

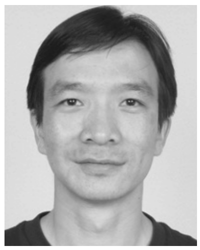
[42] J. Xia, L. Fan, W. Xu, X. Lei, X. Chen, G. K. Karagiannidis, and A. Nallanathan, "Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers," *IEEE Trans. Commun.*, to be published.

[43] J. Xia, "When distributed switch-and-stay combining meets buffer in IoT relaying networks," *Phys. Commun.*, to be published.



JUNJUAN XIA received the bachelor's degree from the Department of Computer Science from Tianjin University, in 2003, and the master's degree from the Department of Electronic Engineering from Shantou University, in 2015. She is currently a Laboratory Assistant with the School of Computer Science and Cyber Engineering, Guangzhou University. Her current research interests include wireless caching, physical-layer security, cooperative relaying, and interference modeling.

YAN XU received the bachelor's degree in electronic information science and technology from Hubei Normal University, in 2017. She is currently pursuing the master's degree with the School of Computer Science, Guangzhou University. Her research interests include wireless cooperative communications, physical-layer security, and multiagent machine learning algorithms.



DAN DENG received the bachelor's and Ph.D. degrees from the Department of Electronic Engineering and Information Science, University of Science and Technology of China, in 2003 and 2008, respectively. From 2008 to 2014, he was the Director of Comba Telecom Ltd., Guangzhou, China. He has been an Associate Professor with Guangzhou Panyu Polytechnic, since 2014. He has published 45 articles in international journals and conferences. He holds 19 patents. His research interests include MIMO communication and physical-layer security in next-generation wireless communication systems. He has served as a member of technical program committee for several conferences.

QINGFENG ZHOU received the B.Sc. degree from the University of Science and Technology of China (USTC), Hefei, China, the M.Sc. degree from Clemson University, SC, USA, and the Ph.D. degree in information engineering from The Hong Kong Polytechnic University, Hong Kong, in 2010. He is currently a Professor with the Dongguan University of Technology. His research interests include wireless communications, particularly focusing on interference alignment, distributive MIMO, sensor networks, and smart wearable devices.

LISENG FAN received the Ph.D. degree from the Tokyo Institute of Technology, Tokyo, in 2008. He is currently a Professor with the School of Computer Science and Cyber Engineering, Guangzhou University. He has published more than 40 articles in IEEE journals and conferences. His main research interests include information security, wireless networks, and artificial intelligence. His recent research interest includes applications of artificial intelligence into wireless networks.