IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 7, 2019, accepted October 24, 2019, date of publication November 1, 2019, date of current version November 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2950948

Cooperative Secondary Encryption for Primary Privacy Preserving in Cognitive Radio Networks

DAWEI WANG[1,2], (Member, IEEE), RUONAN ZHANG[1], (Member, IEEE), LIXIN LI[1], (Member, IEEE), SHAOYANG MEN[3], (Member, IEEE), DEYUN ZHOU[1], AND MOHSEN GUIZANI[4], (Fellow, IEEE)

[1]Department of Communication Engineering, Northwestern Polytechnical University, Xi'an 710072, China
[2]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
[3]School of Medical Information Engineering, Guangzhou University of Chinese Medicine, Guangzhou 510006, China
[4]Department of Computer Science and Engineering, Qatar University, 2713 Doha, Qatar

Corresponding authors: Ruonan Zhang (rzhang@nwpu.edu.cn) and Shaoyang Men (shaoyang.men@gzucm.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61901379, Grant 61901381, and Grant 61571370, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2019JQ-253, Grant 2019JQ-631, Grant 2018ZDCXL-GY-03-04, and Grant 2019ZDLGY07-10, in part by the Fundamental Research Funds for the Central Universities under Grant 31020180QD095, in part by the Open Research Fund of the National Mobile Communications Research Laboratory, Southeast University under Grant 2020D04, in part by the Advance Research Program on Common Information System Technologies under Grant 315075702, in part by the Medical Science and Technology Research Foundation of Guangdong under Grant B2018108, and in part by the Youth Creative Talent Project (Natural Science) of Guangdong under Grant 2017KQNCX041.

ABSTRACT Aiming at protecting primary privacy messages and supporting secondary quality-of-service (QoS), we propose a secondary encrypted secure strategy for cognitive radio networks. In this scheme, a primary system directly transmits privacy messages or employs pre-transmitted secure secondary messages to encrypt the primary privacy information, and the secondary system acquires a fraction of the interference-free licensed spectrum. Following this idea, we consider two secure communication scenarios: the non-buffer scenario and the buffer-aided scenario. For the non-buffer scenario, the primary system first evaluates the channel quality of the direct transmission link. Then, the primary transmitter adaptively chooses to directly transmit the privacy messages or employ the encryption of the secure secondary messages according to the evaluation results. For this scenario, we investigate the primary ergodic secrecy performance and the secondary average performance. For the buffer-aided scenario, the secure secondary messages can be stored in the buffers at both the primary transmitter and receivers. According to the buffer states and channel quality, the primary system adaptively chooses to directly transmit the primary privacy information, permit the secondary secure transmission, or utilize the encryption of the stored secure secondary information. For this scenario, we also investigate the performances of both the primary and secondary systems, and derive the closed-form expression of the primary information delay. Numerical results are given to prove that the proposed scheme can provide privacy preserving for the primary information and acquire high secondary average transmission rate.

INDEX TERMS Cognitive radio networks, primary information security, secondary transmission rate.

I. INTRODUCTION

Rapid proliferation of wireless devices and techniques enables anywhere and anytime communications which makes life comfortable and convenient. Much more privacy information, such as personal profiles, band account information, business secrets, and so on [1], [2] are contained in the large wireless information exchange processes. However, due to the openness propagation environment of wireless networks, the privacy information is almost defenseless for eavesdroppers' threat since eavesdroppers can also receive these privacy messages [3]–[5]. Besides the traditional high-layer encryption methods, physical-layer security, that benefits the physical features of the wireless link, is considered as a promising approach to protect the privacy information in the fifth generation mobile communication system [6]–[8].

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

The pioneering physical-layer security work was conducted by Wyner [9]. Then, the secrecy performances for broadcast [10] and Gaussian [11] channels were investigated. These pioneering works had verified the perfect information security of the physical-layer security when the quality of the legitimate link has an advantage over the wiretap link [12]–[14].

Cooperative relaying and/or cooperative jamming are two common approaches for the physical-layer security problems [12], [13], [15], [16]. In [17], the relay first harvested energy from the transmitted artificial noise signals and then it generated artificial noise to interfere the eavesdropper by utilizing the global channel state information or partial channel state information. In [18] and [19], the destination-aided secure transmission schemes were proposed where the destination transmitted artificial noise in the first scheduled time to prevent relays' eavesdropping, and the relays would forward the privacy signal and artificial noise to the destination in the following scheduling time. Assisted by multi-antennas, the authors in [20]–[22] designed optimal power allocation schemes for the artificial noise and privacy message to maximize the secrecy rate. In [23], [24], the authors studied the joint source and relay transmit power allocation to achieve the maximum secure energy-efficiency. Besides the information security, the crowd licensed spectrum also limits the performance improvement of the wireless networks.

To alleviate crowd licensed spectrum situation, the cognitive radio is proposed to improve the spectrum efficiency where the secondary network shares the primary licensed spectrum through the underlay or overlay strategies [25]. Besides, the secondary system can assist the primary transmission to acquire the licensed spectrum as a reward [26]. Due to the open spectrum sharing nature, the primary system also faces the eavesdropping threat, such as the eavesdropper can also access the licensed spectrum for eavesdropping [27]–[29]. Besides the secrecy policy of the primary system, the secondary system can employ the physical-layer security to assist the primary secure transmission through cooperative relaying and/or cooperative jamming and acquire some licensed spectrum as a reward. In [30], the secondary system utilized the full-duplex technique to securely relay the primary privacy information and transmit the secondary information. In [31], the authors investigated the tradeoff between the primary information security and secondary efficiency. In [32], the authors studied the time division multiple access based cooperation scheme where the secondary system provided cooperative jamming to interfere the eavesdropper and the remaining time slot was allocated for the secondary transmission. In [33], [34], the authors investigated the information security of the primary two-hop relay network assisted by the secondary jamming. In [35], the game theory was utilized to associate the primary secure transmission and the secondary transmission. In all the above works, the primary information security is preserved by the secondary relaying and/or jamming assistance, and the secondary system can acquire licensed spectrum to motivate the cooperation. However, the secondary relaying will consume the valuable secondary energy; the secondary jamming will not only consume the valuable secondary energy but also interfere both the primary and secondary transmissions. Therefore, it is a challenge to protect the primary information while eliminate the interference of the secondary jamming signals and improve the secondary energy efficiency.

Key queuing is another physical-layer security approach for the information security without affecting the secondary and primary transmissions. The pioneering work of key queuing was conducted by Khalil *et al.* [36] where the key packets would be transmitted when the channel could provide information security and the data queue was empty. In addition, the key packets would be stored in the key queue. When the network was insecure and there was data to be transmitted, the key packet would be employed to encrypt the privacy information. Assisted by the key queue, the secure transmission opportunities can be fully employed without cooperative jamming. Following this idea, the authors in [37]–[39] studied the key generation scheme, secrecy outage performance, and delay performance for the key aided secure transmission scheme. Moreover, we also investigated the power allocation and information delay performance for single-input single-output (SISO) and multiple-input single-output (MISO) networks in [40]. However, for the cognitive radio networks, the key assisted secure transmission for the primary privacy information is yet investigated which will be studied in this work.

In this paper, we propose a secondary encrypted secure transmission scheme for cognitive radio networks (which is partly published in [41]). In this work, the primary privacy information is adaptively transmitted through the direct communication link or by utilizing the pre-transmitted secure secondary packets to encrypt. Following this policy, we first consider the secondary encrypted secure transmission for the non-buffer scenario, and then we extend our work to the buffer-aided scenario. For the no buffer scenario, the secure transmission policy can be summarized as: (i) if the primary network can offer information security, the primary system directly transmits the privacy information; (ii) if the primary network cannot offer information security while the secondary information can be securely transmitted, the primary privacy information will be encrypted by the secure secondary information; (iii) when the primary privacy information cannot be securely transmitted even under the protection of the secondary system, the licensed spectrum will be allocated for the secondary transmission. For this proposed secrecy policy, we will investigate the primary ergodic secrecy and the secondary average transmission rate. Then, we consider the buffer-aided scenario where both the primary transmitter and receiver have data buffers to store the secure secondary messages. The stored secondary messages will be consumed to encrypt the following transmitted primary privacy messages. For this scenario, the secure transmission policy can be summarized as: (i) if the primary network can offer information security, the primary system will directly

transmit its information; (ii) if the primary network cannot offer information security, the secure secondary queue has no data, and the secondary information can be securely transmitted, the secondary system will occupy the channel for the secondary transmission and the primary system will store these secure secondary messages; (iii) if the primary network cannot offer information security while the secure secondary queue has data, the primary system will utilize the stored secure secondary messages to encrypt the primary privacy messages; (iv) when the primary privacy messages cannot be securely transmitted even under the assistance of the secondary network, the spectrum will be used for the secondary communication. For this policy, we also examine the primary secrecy performance and the secondary average performance. Moreover, we study the primary information delay and derive its closed-form expression. Numerical results have been presented to verify the improvement of both the secondary and the primary performances. The contribution of this work can be summarized as:

- We propose a secondary encrypted secure transmission scheme for cognitive radio networks. In the proposed scheme, the primary privacy information is encrypted by the secure secondary information and the secondary system acquires interference-free licensed spectrum as a reward. For the proposed scheme, the spectrum can be fully utilized and both the primary and secondary networks will benefit from the proposed scheme. According to the authors' best knowledge, this is the first work that employs the secure secondary information to assist the primary secure transmission.
- We propose two secure transmission policies for the non-buffer and buffer-aided scenarios. Specifically, we first clearly summarize the secure transmission policies for both scenarios. Following the above policies, we analyze the primary ergodic secrecy and the secondary average transmission rate for the non-buffer scenario, and we examine the primary secrecy rate and the secondary average transmission rate for the buffer-aided scenario. Besides, we study the primary information delay and derive its closed-form expression for the buffer-aided scenario.
- We implement Monte-Carlo simulation to evaluate the performance of the proposed scheme. Numerical results have been presented to verify the improvement of both the secondary and the primary performances.

The remaining sections are arranged as follows. Section II illustrates the network framework of the secondary encrypted secure strategy. In Section III, we first propose the secondary encrypted strategy for the non-buffer scenario and then, we analyze the primary ergodic secrecy rate and the secondary average transmission rate. In Section IV, we extend the secondary encrypted secure strategy for the buffer-aided scenario. We also analyze the primary average secrecy rate and secondary average rate. Moreover, the information delay of the primary system is studied. Extensive simulations are conducted in Section V, and we conclude this work in Section VI.

II. SYSTEM MODEL

Figure 1 presents the system diagram which consists a primary network and a secondary network. The primary network contains a primary transmitter (PT) and a primary receiver (PR); the secondary network contains a secondary transmitter (ST) and a secondary receiver (SR). Simultaneously, a passive eavesdropper (EV) threatens the primary information security. This system can capture the cognitive sensor network scenario, where PT is a macro base station that securely communications with a cellular user over the licensed spectrum while ST is a sensor node with none licensed spectrum and wants to acquire licensed spectrum for the uplink sensing data transmission. In order to securely transmit the primary privacy messages, the physical-layer security is adopted by the primary system to provide information security. When the information security of the primary network still cannot be satisfied by adopting physical-layer security, the primary system will request the secondary secure assistance and compensate the secondary network with licensed spectrum. Through secure cooperation, the primary system benefits with information security and the secondary system acquires some interference-free licensed spectrum which also can motive the secure cooperation.

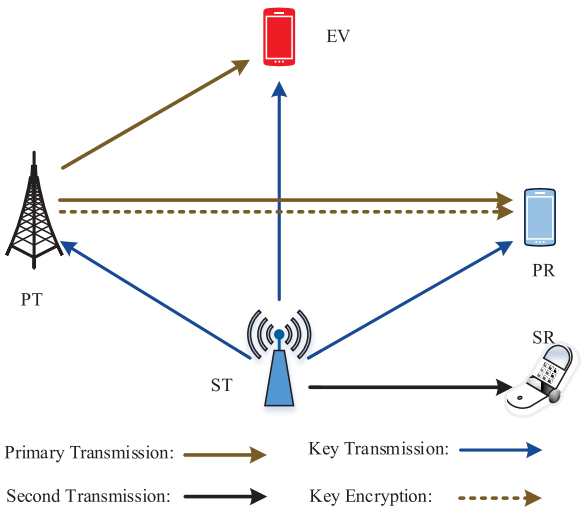

FIGURE 1. The system diagram of our proposed cooperative secure communication scheme.

In this network, both the primary and secondary networks experience quasistatic Rayleigh fading, which indicates that the network channel state is constant in one communication unit, while varies independently in different communication units [42]–[44]. Both the primary and secondary users are equipped with one antenna.[1] The channel variables of

[1]This work can be extended to multiple antenna scenario. However, to simply the analysis and clearly explain the proposed scheme, we consider the single antenna scenario and the multiple antenna will be investigated for the future work.

PT → PR, PT → EV, ST → PT, ST → PR, ST → EV, and ST → SR are denoted as h_{tr}, h_{te}, h_{st}, h_{sr}, h_{se}, and h_{ss}, respectively. Their channel power gains are $g_{tr} = |h_{tr}|^2$, $g_{te} = |h_{te}|^2$, $g_{st} = |h_{st}|^2$, $g_{sr} = |h_{sr}|^2$, $g_{se} = |h_{se}|^2$, and $g_{ss} = |h_{ss}|^2$ which follow exponential distributions with parameters λ_{tr}, λ_{te}, λ_{st}, λ_{sr}, λ_{se}, and λ_{ss}, respectively. In this system, we assume that the primary and secondary channel state information (CSI) can be obtained. This assumption can be realized in practice through the pilot estimation. Since EV is a passive user, the wiretap CSI is unavailable. For practical considering, we assume that the eavesdropping channel distribution information (CDI) is available.[2] The received noises in this system are assumed to follow Gaussian distribution with zero-mean and unit variance. PT and ST's transmit powers are expressed as p_p and p_s, respectively.

In order to securely transmit the primary privacy information, we adopt the wiretap codebook of $\mathcal{C}\left(2^{nR_b}, 2^{nR_s}, n\right)$ to encrypt the primary information, where R_b is the target primary transmission rate; R_s is the intended primary secrecy rate; the span of the codeword is denoted as n. The difference between R_b and R_s, denoted as $R_e \triangleq R_b - R_s$, will offer information redundancy for the primary privacy preserving. In each time slot, PT will adaptively transmit the primary privacy messages to PR or encrypt the primary information through the pre-transmitted secure secondary messages. When the primary network utilizes the secondary encryption, ST first securely transmits the secondary messages to PT and PR. Then, PT utilizes the secure secondary messages to encrypt the primary information through XOR operation[3] and PR will utilize the secure secondary messages to decode the primary information. Following this policy, we first study the secondary encrypted secure strategy for the no-buffer scenario and then, we study the buffer-aided scenario.

In the proposed scheme, when PT transmits the privacy messages to PR without the assistance from the secondary network, the received privacy information at PR is

$$y_{tr} = \sqrt{p_p} h_{tr} x_p + n_{pr} \tag{1}$$

where x_p is the primary privacy information and $\mathbb{E}\left\{|x_p|^2\right\} = 1$[4]; n_{pr} is PR's received noise. Due to the openness propagation nature, EV also receives this message as

$$y_{te} = \sqrt{p_p} h_{te} x_p + n_{ev} \tag{2}$$

where n_{ev} is the noise variable at EV. When the secondary system assists the primary secure transmission, there are two phases to complete the secure transmission. In the first phase, ST securely transmits the secondary information to PT and PR and the received signals at PT and PR are given by

$$\begin{cases} y_{st} = \sqrt{p_s} h_{st} x_s + n_{pt}, \\ y_{sr} = \sqrt{p_s} h_{sr} x_s + n'_{pr} \end{cases} \tag{3}$$

where x_s is the secondary message which has the same length as the primary message[5] and it is normalized to $\mathbb{E}\left\{|x_s|^2\right\} = 1$; n_{pt} and $'$ are the noise variables at PT and PR, respectively. Simultaneously, EV also receives this message as

$$y_{se} = \sqrt{p_s} h_{se} x_s + n'_{ev} \tag{4}$$

where n'_{ev} is the noise variable at EV. For the secondary system, SR can receive the secondary message as

$$y_{ss} = \sqrt{p_s} h_{ss} x_s + n_{sr} \tag{5}$$

where n_{sr} is the noise variable at SR. In the second phase, PT first implements the XOR operation between the primary privacy information and the secondary secure message and then, transmits the encrypted signal to PR. PR will utilize the secure secondary message to decode the encrypted primary information. If the secure cooperation still cannot defend the primary privacy message, the primary transmission will be suspended and the spectrum is occupied by the secondary transmission.

Remark: In this work, we only consider the information security for the primary network with the following three reasons [32], [48]–[50]. First, since the secondary system dynamically changes the sharing channels, it is challenging to monitor all the secondary transmission in all spectrum channels. Second, since the base stations are always built in the fixed places, it is easy to eavesdrop the primary information by just following the information transmissions of the base station. Third, due to shortage of the licensed spectrum, the important target of the secondary system is to acquire spectrum and the secondary information security can be separately considered in the future work.

III. SECONDARY ENCRYPTED SECURE TRANSMISSION FOR THE NON-BUFFER SCENARIO

In this section, we first design the secure transmission policy for both the primary and secondary systems. Following the proposed policy, we investigate the primary and secondary performances.

[2]We adopt the Rayleigh fading channel model which is a natural and reasonable model for the wiretap CDI in a rich scattering environment. Therefore, the channel power gains of the wiretap channels follow exponential distributions with parameters λ_{te} and λ_{se} where λ_{te} and λ_{se} represent the large-scale fading and are related to the distance between PT and Eve and between ST and Eve, respectively. These distance can be conservatively estimated based on the notion of secrecy protected zone, which is an eavesdropper-free area and can be constructed either inherently or intentional [45]–[47]

[3]Since the secondary information is secure, the primary system can encrypt the primary information through XOR operation with the secondary information. However, as the eavesdropper cannot decode the secondary information, it cannot decode the encrypted primary information. Therefore, the secondary encrypted primary information is secure.

[4]$\mathbb{E}\{\cdot\}$ denotes the expectation option.

[5]Since the secondary system can assist the primary secure transmission, the primary network is willing to inform the secondary system about the length of the primary privacy information. In order to acquire some licensed spectrum, the secondary system is willing to adopt the same length of the primary information. Therefore, both the primary and secondary systems can benefit from the same length information. In addition, the secondary users may be the same users with the primary users, such as, the secondary users may be cellular users that are willing to transmit information in the other cellulars' schedule unit. Moreover, since there are multiple secondary users, the primary network can select the secondary system which can support the same length information. Therefore, it is possible to transmit the same length information for the primary and secondary transmitters.

A. SECURE TRANSMISSION POLICY

When PT directly transmits the primary messages, the information rate at PR is given by

$$R_{tr} = \log_2\left(1 + p_p g_{tr}\right). \tag{6}$$

EV tries to eavesdrop the primary privacy messages and the eavesdropping rate is given by

$$R_{te} = \log_2\left(1 + p_p g_{te}\right). \tag{7}$$

Therefore, the primary secrecy rate for the primary direct transmission is derived as

$$R_{sec,d} = \left(\log_2\left(1 + p_p g_{tr}\right) - \log_2\left(1 + p_p g_{te}\right)\right)^+ \tag{8}$$

where $(a)^+ = \max(0, a)$. Since the instantaneous CSI associated with EV is unavailable, we utilize the secrecy outage probability to evaluate the secrecy performance. Therefore, the primary secrecy outage probability for the direct transmission is

$$\begin{aligned} P_{sec,d} &= \Pr\left\{\left(\log_2\left(1 + p_p g_{tr}\right) - \log_2\left(1 + p_p g_{te}\right)\right)^+ < R_s\right\} \\ &= 1 - \exp\left(-\frac{2^{-R_s}\left(1 + p_p g_{tr}\right) - 1}{p_p \lambda_{pe}}\right). \end{aligned} \tag{9}$$

Set the maximum permitted secrecy outage probability as $P_{s,out}$. When $P_{sec,d} \le P_{s,out}$, the primary information can be securely transmitted. Therefore, according to $P_{sec,d} \le P_{s,out}$, PT will directly transmit the primary privacy messages only when $g_{tr} \ge \tau_1$ where the parameter τ_1 is derived as

$$P_{sec,d} < P_{s,out}$$

$$\Rightarrow 1 - \exp\left(-\frac{2^{-R_s}\left(1 + p_p g_{tr}\right) - 1}{p_p \lambda_{pe}}\right) < P_{s,out} \tag{10a}$$

$$\Rightarrow g_{tr} > \tau_1 = \frac{2^{R_s}\left(1 - p_p \lambda_{pe} \ln\left(1 - P_{s,out}\right)\right) - 1}{p_p} \tag{10b}$$

If the primary direct transmission is insecure, the primary system needs the secure assistance from the secondary system. When ST assists the primary secure transmission, there are two phases to implement the cooperation. In the first phase, ST securely transmits the secondary messages to PT and PR with rates as

$$\begin{cases} R_{st} = \dfrac{1}{2}\log_2\left(1 + p_s g_{st}\right), \\ R_{sr} = \dfrac{1}{2}\log_2\left(1 + p_s g_{sr}\right). \end{cases} \tag{11}$$

In addition, EV also receives the secondary messages with rate as

$$R_{se} = \frac{1}{2}\log_2\left(1 + p_s g_{se}\right). \tag{12}$$

Therefore, the secrecy rate of the secondary information is derived as

$$R_{sec,a} = \frac{1}{2}\left(\min\left(R_{st}, R_{sr}\right) - R_{se}\right)^+. \tag{13}$$

Moreover, SR also receives the secondary messages with rate as

$$R_{ss} = \frac{1}{2}\log_2\left(1 + p_s g_{ss}\right). \tag{14}$$

In the second phase, PT implements XOR operation between the primary privacy information and the secure secondary messages and PR will decode the primary privacy information assisted by the secure secondary information. If the secure secondary message is eavesdropped, the primary privacy information will experience secrecy outage. This event occurs with probability as

$$\begin{aligned} P_{sec,a} &= \Pr\left\{R_{sec,a} < R_s\right\} \\ &= 1 - \exp\left(-\frac{2^{-R_s}\left(1 + p_s min\left(g_{st}, g_{sr}\right)\right) - 1}{p_p \lambda_{se}}\right). \end{aligned} \tag{15}$$

When $P_{sec,a} \le P_{s,out}$, the primary information can be securely transmitted with the maximum permitted secrecy outage probability $P_{s,out}$, and we can derive $\min\left(g_{st}, g_{sr}\right) > \tau_2$ where the parameter τ_2 is derived as

$$P_{sec,a} < P_{s,out}$$

$$\Rightarrow 1 - \exp\left(-\frac{2^{-R_s}\left(1 + p_s min\left(g_{st}, g_{sr}\right)\right) - 1}{p_p \lambda_{se}}\right) < P_{s,out} \tag{16a}$$

$$\Rightarrow \min\left(g_{st}, g_{sr}\right) > \tau_2 = \frac{2^{R_s}\left(1 - p_s \lambda_{se} \ln\left(1 - P_{s,out}\right)\right) - 1}{p_s}. \tag{16b}$$

Therefore, only when $\min\left(g_{st}, g_{sr}\right) > \tau_2$, ST can securely transmit the secondary information to PT and PR with the maximum permitted secrecy outage probability $P_{s,out}$.

If the direct transmission and secondary assistance cannot provide primary privacy preserving, the primary transmission will be suspended and the licensed spectrum is used for the secondary network.

According to the above discussion, the proposed cooperative secure transmission policy can be summarized as

- If $g_{tr} \ge \tau_1$, PT directly transmits the privacy messages to PR;
- If $g_{tr} < \tau_1$ and $\min\left(g_{st}, g_{sr}\right) \ge \tau_2$, ST first securely transmits secondary information and then, PT transmits the primary privacy information encrypted by the secure secondary messages;
- If $g_{tr} < \tau_1$ and $\min\left(g_{st}, g_{sr}\right) < \tau_2$, PT stops its transmission and ST accesses the licensed spectrum for the secondary transmission.

Remark: The proposed scheme is implemented as following. In each time slot, PT first transmits the pilot signal to PR. PR estimates the CSI between PT and PR according to received the pilot signal. If $g_{tr} \ge \tau_1$, PR responses with ACK to inform the link security between PT and PR. Otherwise, if $g_{tr} < \tau_1$, PR responses with NACK to inform the secrecy outage of the primary direct transmission. After received NACK, ST will transmit the pilot signal, and PT and PR will estimate their CSI according to the pilot signal. If $g_{st} \ge \tau_2$,

PT responses with ACK to confirm the link security between ST and PT. Otherwise, PT responses with NACK. If $g_{sr} \geq \tau_2$, PR responses with ACK to confirm the link security between ST and PR. Otherwise, PR will response with NACK. Therefore, the proposed scheme can be implemented according to the above processes.

B. PERFORMANCE ANALYSIS

For the primary network, PT transmits the privacy messages through the direct transmission or assisted from the secondary system. When $g_{tr} \geq \tau_1$, the primary system directly transmits the privacy messages with probability as

$$P_d = \Pr\{g_{tr} \geq \tau_1\} = \exp\left(-\frac{\tau_1}{\sigma_{tr}^2}\right). \tag{17}$$

Under this condition, the primary ergodic secrecy rate is derived as

$$\begin{aligned} R_{sec,d}^{ergodic} &= \mathbb{E}\left\{\log_2\left(1+p_p g_{tr}\right) - \log_2\left(1+p_p g_{te}\right)\right\} \\ &= -\frac{1}{\ln 2}\exp\left(\frac{1}{\sigma_{tr}^2 p_p}\right) Ei\left(-\frac{1}{\sigma_{tr}^2 p_p}\right) \\ &\quad + \frac{1}{\ln 2}\exp\left(\frac{1}{\sigma_{te}^2 p_p}\right) Ei\left(-\frac{1}{\sigma_{te}^2 p_p}\right) \end{aligned} \tag{18}$$

where $Ei(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t} dt$. When $g_{tr} < \tau_1$ and $\min(g_{st}, g_{sr}) \geq \tau_2$, the primary system will receive secure assistance from the secondary system with probability as

$$\begin{aligned} P_a &= \Pr\{g_{tr} < \tau_1, \min(g_{st}, g_{sr}) \geq \tau_2\} \\ &= \left(1 - \exp\left(-\frac{\tau_1}{\sigma_{st}^2}\right)\right) \exp\left(-\frac{\tau_2}{\sigma_{sr}^2} - \frac{\tau_2}{\sigma_{tr}^2}\right). \end{aligned} \tag{19}$$

For this case, ST first securely transmits the secondary messages to PT and PR. Then, PT utilizes the secondary messages to encode the primary privacy information. Therefore, the primary ergodic secrecy rate is derived as

$$\begin{aligned} R_{sec,a}^{ergodic} &= \mathbb{E}\left\{\frac{1}{2}\left(\min\left(R_{st}, R_{sr}\right) - R_{se}\right)\right\} \\ &= -\frac{1}{2\ln 2}\min\left(\exp\left(\frac{1}{\sigma_{st}^2 p_s}\right) Ei\left(-\frac{1}{\sigma_{st}^2 p_s}\right),\right. \\ &\quad \left.\exp\left(\frac{1}{\sigma_{sr}^2 p_s}\right) Ei\left(-\frac{1}{\sigma_{sr}^2 p_s}\right)\right) \\ &\quad + \frac{1}{2\ln 2}\exp\left(\frac{1}{\sigma_{se}^2 p_s}\right) Ei\left(-\frac{1}{\sigma_{se}^2 p_s}\right). \end{aligned} \tag{20}$$

Therefore, according to the above discussion, the primary ergodic secrecy rate for the proposed scheme can be derived as

$$R_p^{ergodic} = P_d R_{sec,d}^{ergodic} + P_a R_{sec,d}^{ergodic} \tag{21}$$

Submitting eqs. (17), (18), (19) and (20) into eq. (21), we can acquire the closed-form expression of the primary ergodic secrecy rate as

$$\begin{aligned} R_p^{ergodic} &= \frac{1}{\ln 2}\exp\left(\frac{1}{\sigma_{te}^2 p_p} - \frac{\tau_1}{\sigma_{tr}^2}\right) Ei\left(-\frac{1}{\sigma_{te}^2 p_p}\right) \\ &\quad - \frac{1}{\ln 2}\exp\left(\frac{1}{\sigma_{tr}^2 p_p} - \frac{\tau_1}{\sigma_{tr}^2}\right) Ei\left(-\frac{1}{\sigma_{tr}^2 p_p}\right) \\ &\quad + \left(1 - \exp\left(-\frac{\tau_1}{\sigma_{st}^2}\right)\right) \exp\left(-\frac{\tau_2}{\sigma_{sr}^2} - \frac{\tau_2}{\sigma_{tr}^2}\right) \\ &\quad - \frac{1}{2\ln 2}\min\left(\exp\left(\frac{1}{\sigma_{st}^2 p_s}\right)\right. \\ &\quad \left.\times\ Ei\left(-\frac{1}{\sigma_{st}^2 p_s}\right), \exp\left(\frac{1}{\sigma_{sr}^2 p_s}\right) Ei\left(-\frac{1}{\sigma_{sr}^2 p_s}\right)\right). \end{aligned} \tag{22}$$

For the secondary network, it will access the licensed spectrum when ST assists the primary secure transmission or ST assesses the licensed spectrum due to the secrecy outage of the primary system. When $g_{tr} < \tau_1$ and $\min(g_{st}, g_{sr}) < \tau_2$, PT stops its transmission and ST assesses the licensed spectrum with probability as

$$\begin{aligned} P_s &= \Pr\{g_{tr} < \tau_1, \min(g_{st}, g_{sr}) < \tau_2\} \\ &= \left(1 - \exp\left(-\frac{\tau_1}{\sigma_{st}^2}\right)\right)\left(1 - \exp\left(-\frac{\tau_2}{\sigma_{sr}^2} - \frac{\tau_2}{\sigma_{tr}^2}\right)\right). \end{aligned} \tag{23}$$

When the secondary system fully utilizes the licensed spectrum, the secondary transmission rate is derived as

$$R_{ss}^{s} = \log_2\left(1 + p_s g_{ss}\right). \tag{24}$$

Therefore, the secondary average transmission rate is derived as

$$\begin{aligned} R_{ss} &= P_a R_{ss} + P_s R_{ss}^{s} \\ &= \left(1 - \exp\left(-\frac{\tau_1}{\sigma_{st}^2}\right)\right)\left(1 - \frac{1}{2}\exp\left(-\frac{\tau_2}{\sigma_{sr}^2} - \frac{\tau_2}{\sigma_{tr}^2}\right)\right) \\ &\quad \times \log_2\left(1 + p_s g_{ss}\right). \end{aligned} \tag{25}$$

IV. SECONDARY ENCRYPTED SECURE TRANSMISSION WITH DATA BUFFER

In Section III, we consider the secondary encrypted secure transmission for the non-buffer scenario. When PT and PR are equipped with buffers, the secure secondary messages can be stored for some time slots that can encrypt the primary information in the following primary transmission. Therefore, in the section, we extend our work to the buffer-aided scenario. We first propose the secondary encrypted secure transmission policy for the buffer-aided scenario. Following, we investigate the performances of both the primary and secondary networks.

A. TRANSMISSION POLICY FOR DATA BUFFER-AIDED SCENARIO

For the buffer-aided scenario, PT has two buffers Q_p and Q_s to store the primary data packets and secure secondary packets, respectively. In addition, PR has a buffer to store the same secure secondary packets. We assume that all buffers have infinite capacities [38], [40]. For the data queue, we assume that $\lambda_p \in \{0, 1\}$, a Bernoulli distribution variable [51], is the probability of PT's data queue receiving a packet. Thus,

the primary privacy information arrival rate is λ_p. Considering the buffer states at PT and PR, the transmission policy for this scenario can be summarized as:

- If $g_{tr} \geq \tau_1$, PT directly transmits the privacy messages to PR;
- If $g_{tr} < \tau_1$, $Q_s = 0$, and $\min(g_{st}, g_{sr}) \geq \tau_2$, ST securely transmits the secondary packets, and PT and PR will store the secure secondary packets;
- If $g_{tr} < \tau_1$, and $Q_s \neq 0$, PT utilizes the secure secondary packet to encrypt the primary data packets;
- If $g_{tr} < \tau_1$, $Q_s = 0$ and $\min(g_{st}, g_{sr}) < \tau_2$, PT stops its transmission and ST accesses the licensed spectrum for the secondary transmission.

For the buffer-aided scenario, if $g_{tr} < \tau_1$, $Q_s = 0$ and $\min(g_{st}, g_{sr}) \geq \tau_2$, the secure secondary packets will be stored. Therefore, the arrive rate of the secondary buffer is given by

$$\begin{aligned}\lambda_s &= \Pr(g_{tr} < \tau_1)\Pr(Q_s = 0)\Pr(\min(g_{st}, g_{sr}) \geq \tau_2) \\ &= \left(1 - \exp\left(-\frac{\tau_1}{\lambda_{tr}}\right)\right)\left(1 - \frac{\lambda_s}{\mu_s}\right)\left(1 - \exp\left(-\frac{\tau_2}{\lambda_{st}}\right)\right) \\ &\quad \times \left(1 - \exp\left(-\frac{\tau_2}{\lambda_{sr}}\right)\right) \\ &= (1 - P_1) P_2 \left(1 - \frac{\lambda_s}{\mu_s}\right) \end{aligned} \tag{26}$$

where

$$\begin{cases} P_1 = \exp\left(-\dfrac{\tau_1}{\lambda_{tr}}\right), \\ P_2 = \left(1 - \exp\left(-\dfrac{\tau_2}{\lambda_{st}}\right)\right)\left(1 - \exp\left(-\dfrac{\tau_2}{\lambda_{sr}}\right)\right). \end{cases} \tag{27}$$

When $g_{tr} < \tau_1$, and $Q_s \neq 0$, PT will utilizes the stored secure secondary packets to encode the primary privacy information. Therefore, the departure rate of the stored secure secondary packets can be derived as

$$\begin{aligned}\mu_s &= \Pr(g_{tr} < \tau_1)\Pr(Q_s \neq 0) \\ &= \left(1 - \exp\left(-\frac{\tau_1}{\lambda_{tr}}\right)\right)\frac{\lambda_s}{\mu_s} \\ &= (1 - P_1)\frac{\lambda_s}{\mu_s} \end{aligned} \tag{28}$$

For the data queue, the arrival rate is λ_p. Through direct transmission and secondary assistance, the primary privacy information departure rate is derived as

$$\begin{aligned}\mu_p &= \Pr(g_{tr} \geq \tau_1) + \Pr(g_{tr} < \tau_1)\Pr(Q_s \neq 0) \\ &= \exp\left(-\frac{\tau_1}{\lambda_{tr}}\right) + \left(1 - \exp\left(-\frac{\tau_1}{\lambda_{tr}}\right)\right)\frac{\lambda_s}{\mu_s} \\ &= P_1 + (1 - P_1)\frac{\lambda_s}{\mu_s} \end{aligned} \tag{29}$$

From eqs. (26)-(29), we can observe that the primary data queue is coupled with the secure secondary data queue. However, since λ_p is given and there are three variables in eqs. (26)-(29), the average departure rate[6] of the primary privacy information is derived as [38], [40]

$$\mu_p = \frac{1}{2}\left(2P_1 + P_1P_2 - P_2 - (P_1 - 1)\sqrt{P_2(4 + P_2)}\right). \tag{30}$$

In addition, the arrival and departure rates of the secure secondary queue are respectively given by [38], [40]

$$\lambda_s = \frac{1}{2}\left(2P_2 - 2P_1P_2 + P_2^2 - P_1P_2^2 - (1 - P_1)P_2^{\frac{3}{2}}\sqrt{4 + P_2}\right) \tag{31}$$

and

$$\mu_s = \frac{1}{2}\left(-P_2 + P_1P_2 + (1 - P_1)\sqrt{P_2(4 + P_2)}\right). \tag{32}$$

For the secondary system, the secondary messages are transmitted when $g_{tr} < \tau_1$, $Q_s = 0$ and $\min(g_{st}, g_{sr}) \geq \tau_2$, or $g_{tr} < \tau_1$, $Q_s = 0$ and $\min(g_{st}, g_{sr}) < \tau_2$. Therefore, the secondary average transmission rate is derived as

$$\begin{aligned}C_s &= \Pr(g_{tr} < \tau_1)\Pr(Q_s = 0)\Pr(\min(g_{st}, g_{sr}) \geq \tau_2) \\ &\quad + \Pr(g_{tr} < \tau_1)\Pr(Q_s = 0)\Pr(\min(g_{st}, g_{sr}) < \tau_2) \\ &= \left(1 - \exp\left(-\frac{\tau_1}{\lambda_{tr}}\right)\right)\left(1 - \frac{\lambda_s}{\mu_s}\right). \end{aligned} \tag{33}$$

Submitting eqs. (31) and (32) into eq. (34), the closed-form expression of the secondary average transmission rate can be derived as

$$\begin{aligned}C_s = &\left(1 - \frac{2P_2 - 2P_1P_2 + P_2^2 - P_1P_2^2 - (1 - P_1)P_2^{\frac{3}{2}}\sqrt{4 + P_2}}{-P_2 + P_1P_2 + (1 - P_1)\sqrt{P_2(4 + P_2)}}\right) \\ &\times \left(1 - \exp\left(-\frac{\tau_1}{\lambda_{tr}}\right)\right). \end{aligned} \tag{34}$$

B. PRIMARY INFORMATION DELAY ANALYSIS

According to the queue theory, the primary average information delay can be derived as

$$D_p^s = \frac{N_p^s}{\lambda_p} \tag{35}$$

where N_p^s denotes the length of the primary data queue. Since the primary data and the stored secure secondary data are coupled, it is difficult to analyze the primary information delay. In this paper, we utilize the generation function method to analyze the length of the primary data queue.

We define the generation function of the primary data queue and secondary secure data queue as

$$\begin{aligned}G(x, y) &= \lim_{t \to \infty} \mathbb{E}\left\{x^{Q_p^t} y^{Q_s^t}\right\} \\ &= \lim_{t \to \infty} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} x^i y^j \Pr\left\{Q_p^t = i, Q_s^t = j\right\} \end{aligned} \tag{36}$$

where t denotes the time slot; Q_p^t denotes the queue state of the primary privacy messages at the tth slot; Q_s^t denotes

[6]Since the primary privacy information is securely transmitted, the primary average departure rate is the average secrecy rate.

the queue of the secure secondary messages at the tth slot; $\Pr\left\{Q_d^t = i, Q_k^t = j\right\}$ denotes the probability of $Q_p^t = i$ and $Q_s^t = j$ at the tth slot. We can obtain the first-order derivatives of x and y in eq. (36) as

$$G_x(x,y) = \lim_{t\to\infty} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} i x^{i-1} y^j \Pr\left\{Q_p^t = i, Q_s^t = j\right\} \quad (37)$$

and

$$G_y(x,y) = \lim_{t\to\infty} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} j x^{i} y^{j-1} \Pr\left\{Q_p^t = i, Q_s^t = j\right\}. \quad (38)$$

Submitting $(x, y) = (1, 1)$ into eqs. (37) and (38), the average length of the primary data and the secure secondary data queues are respectively derived as

$$\begin{aligned} G_x(1,1) &= \lim_{t\to\infty} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} i \Pr\left\{Q_d^t = i, Q_k^t = j\right\} \\ &= \lim_{t\to\infty} \sum_{i=0}^{\infty} i \Pr\left\{Q_d^t = i\right\} = N_p \end{aligned} \quad (39)$$

and

$$\begin{aligned} G_y(1,1) &= \lim_{t\to\infty} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} j \Pr\left\{Q_d^t = i, Q_k^t = j\right\} \\ &= \lim_{t\to\infty} \sum_{j=0}^{\infty} j \Pr\left\{Q_k^t = j\right\} = N_s. \end{aligned} \quad (40)$$

Therefore, if $G_x(1, 1)$ is derived, we can derive the primary average information delay.

In the proposed scheme, the information arrival process of the primary network is independent of the information arrival of the secondary network. Therefore, the expectation function in eq. (36) can be rewritten as

$$\begin{aligned} &\mathbb{E}\left\{x^{Q_p^{t+1}} y^{Q_s^{t+1}}\right\} \\ &= \mathbb{E}\left\{x^{Q_p^t + X_p^t - Y_p^t} y^{Q_s^t + X_s^t - Y_s^t}\right\} \\ &= \left(\lambda_p x + 1 - \lambda_p\right)\left(\lambda_s y + 1 - \lambda_s\right) \mathbb{E}\left\{x^{Q_p^t - Y_p^t} y^{Q_s^t - Y_s^t}\right\} \end{aligned} \quad (41)$$

where X_p^t and Y_p^T denote the primary arrival and departure rates, respectively; X_s^t and Y_s^T denote the secure secondary arrival and departure rates, respectively. In the proposed scheme, the primary data arrival and departure process has two cases:

- $Q_p^t > 0$ and $Q_s^t = 0$. For this case, there is no secure secondary message to encrypt the primary privacy information which indicates $Y_s^t = 0$. PT directly transmits the primary privacy messages and the primary information departure rate is given by

$$Y_p^t = \begin{cases} 1, & w.p.\ P_1, \\ 0, & w.p.\ 1 - P_1. \end{cases} \quad (42)$$

- $Q_d^t > 0$ and $Q_k^t > 0$. PT utilizes the primary direct transmission or acquires the secure assistance from the secondary system. Therefore, the departure rates of the primary privacy information and the secure secondary messages are respectively derived as

$$\begin{cases} Y_p^t = Y_s^t = 1, & w.p.\ (1 - P_1), \\ Y_p^t = 1, Y_s^t = 0, & w.p.\ P_1 \end{cases} \quad (43)$$

According to the above analysis, the expectation function of eq. (41) can be rewritten as

$$\begin{aligned} &\mathbb{E}\left\{x^{Q_p^{t+1}} y^{Q_s^{t+1}}\right\} \\ &= \left(\lambda_p x + 1 - \lambda_p\right)\left(\lambda_s y + 1 - \lambda_s\right) \\ &\quad \times \left(\left(\frac{P_1}{x} + 1 - P_1\right) \mathbb{E}\left\{x^{Q_p^t} \mathbf{I}\left\{Q_p^t > 0, Q_s^t = 0\right\}\right\}\right. \\ &\quad \left. + \left(\frac{(1-P_1)}{xy} + \frac{P_1}{x}\right) \mathbb{E}\left\{x^{Q_d^t} y^{Q_k^t} \mathbf{I}\left\{Q_d^t > 0, Q_k^t > 0\right\}\right\}\right) \end{aligned} \quad (44)$$

where the indicator function $\mathbf{I}\{X, Y\}$ is defined as

$$\mathbf{I}\{X,Y\} = \begin{cases} 1, & w.p.\ \Pr\{X = x, Y = y\}, \\ 0, & w.p.\ 1 - \Pr\{X = x, Y = y\}. \end{cases} \quad (45)$$

Substituting eq. (44) into eq. (36), we can derive

$$\begin{aligned} G(x,y) &= \left(\lambda_p x + 1 - \lambda_p\right)\left(\lambda_s y + 1 - \lambda_s\right) \\ &\quad \times \left(\left(\frac{P_1}{x} + 1 - P_1\right) G(x,0)\right. \\ &\quad \left. + \left(\frac{(1-P_1)}{xy} + \frac{P_1}{x}\right) G(x,y)\right) \end{aligned} \quad (46)$$

Then, the first derivative of eq. (46) with respect to x is derived as

$$G_x(x,y) = \frac{m(x,y) + n(x,y)}{1 - \left(\lambda_p x + 1 - \lambda_p\right)\left(\lambda_s y + 1 - \lambda_s\right)\left(\frac{(1-P_1)}{xy} + \frac{P_1}{x}\right)} \quad (47)$$

where

$$\begin{aligned} m(x,y) &= \left(\lambda_s y + 1 - \lambda_s\right)\lambda_p \left(\left(\frac{P_1}{x} + 1 - P_1\right) G(x,0)\right. \\ &\quad \left. + \left(\frac{(1-P_1)}{xy} + \frac{P_1}{x}\right) G(x,y)\right) \end{aligned} \quad (48)$$

and

$$\begin{aligned} n(x,y) &= \left(\lambda_p x + 1 - \lambda_p\right)\left(\lambda_s y + 1 - \lambda_s\right) \\ &\quad \times \left(-\frac{P_1}{x^2} G(x,0) + \left(\frac{P_1}{x} + 1 - P_1\right) G_x(x,0)\right. \\ &\quad \left. - \left(\frac{(1-P_1)}{x^2 y} + \frac{P_1}{x^2}\right) G(x,y)\right). \end{aligned} \quad (49)$$

Set $(x, y) \to (1, 1)$ and apply the L'Hopital's twice to eq. (47). Then, we can obtain

$$G_x(1,1) = \frac{g(1,1)}{(1-P_1) - \lambda_p - \lambda_s} \quad (50)$$

where $g(1, 1)$ is given by

$$g(1,1) = G(1,0)\left(-2\lambda_p P_1 + 2P_1 + \lambda_s \lambda_p - \lambda_s P_1\right)$$

$$+G_x(1,0)\left(2\lambda_p - P_1 + \lambda_s\right) + G_y(1,1)\left(\lambda_p + (1-P_1)\right) + G(1,1)\left(-2\lambda_p - 3 + \lambda_s\lambda_p + \lambda_p P_1 - \lambda_s\right). \quad (51)$$

When we set $y = x$ in eq. (36), the first-order derivative with respect to x is derived as

$$G_x(x,x) = \lim_{t\to\infty} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} ijx^{i-1}x^{j-1} \Pr\left\{Q_p^t = i, Q_s^t = j\right\}. \quad (52)$$

Since $G_x(1,1) = N_p + N_s$. Therefore, according to eq. (46), we can derive $G_x(1,1) + G_y(1,1)$ as shown in (53) at the bottom of this page. Then, N_p is derived as

$$N_p = \frac{m(1,1) + m(1,1)}{2(1-P_1) - \lambda_s} \quad (54)$$

where $m(1,1)$ is shown in (55) at the bottom of this page and $n(1,1)$ is given as

$$n(1,1) = G(1,0)\left(-2\lambda_p P_1 + 2P_1 + \lambda_s\lambda_p - \lambda_s P_1\right) + G_x(1,0)\left(2\lambda_p - P_1 + \lambda_s\right) + G(1,1)\left(-2\lambda_p - 3 + \lambda_s\lambda_p + \lambda_p P_1 - \lambda_s\right). \quad (56)$$

In addition, $G_x(1,0)$, $G(1,0)$ and $G(1,1)$ are given by

$$\begin{cases} G_x(1,0) = \left(1 - \dfrac{\lambda_s}{\mu_s}\right)\dfrac{\lambda_p}{\mu_p}, \\ G(1,0) = \lim\limits_{t\to\infty} \Pr\left\{Q_s^t = 0\right\} = 1 - \dfrac{\lambda_s}{\mu_s}, \\ G(1,1) = 1. \end{cases} \quad (57)$$

Therefore, the average information delay of the primary privacy information is derived as

$$D_p = \frac{G_x(1,1)}{\lambda_p}. \quad (58)$$

Submitting eq. (54) into eq. (58), we can acquire the closed-form expression of the primary privacy information delay.

V. NUMERICAL RESULTS

In this section, we will give some simulation results about our proposed secondary encrypted secure transmission scheme for the no-buffer and buffer-aided scenarios. The primary target transmission rate is set to 1.5 bit/s/Hz; the maximize permitted secrecy outage probability is set to 0.1. In addition, the traditional cooperative secure transmission scheme for cognitive radio networks in [34] is also simulated as the comparison scheme. In [34], the secondary system just transmits jamming signal to prevent the eavesdropping and transmits the secondary information concurrently with the primary transmission. Moreover, the underlay scheme is presented as a baseline scheme where the secondary system controls its interference to the primary system under a threshold.

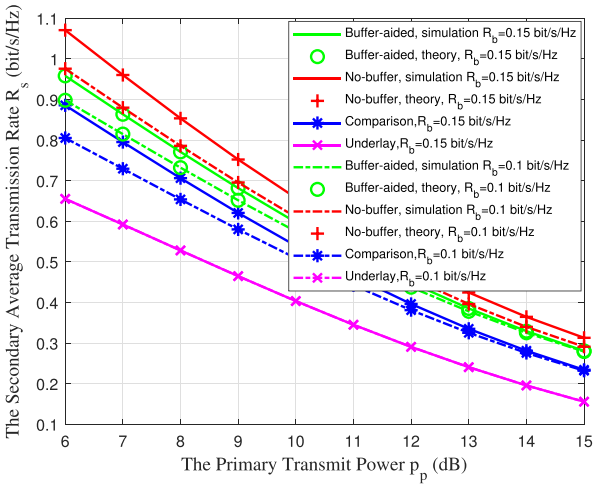

FIGURE 2. The secondary average transmission rate versus the primary transmit power p_p with different R_s.

Figure 2 presents the secondary average transmission rate versus the primary transmit power p_p with different target secrecy rate R_s. In Fig. 2, we can observe that the theoretical results are in excellent agreement with the simulation results. In addition, we can also observe that the secondary transmission rate is a decrease function of p_p. It is because that the increase of p_p supplies more power to provide the primary information security, and there will be few vacant licensed spectrum for the secondary transmission. When p_p is large enough, the primary direct transmission channel can provide more secure transmission opportunities. Therefore, there will be less secondary cooperation opportunities and the secondary transmission rate will decrease slowly. In addition, the increase of R_s indicates that it is difficult to successfully assist the primary secure transmission and there will be less secondary cooperative secure transmission opportunities. In the buffer-aided scheme, the secure secondary data queue can store the secure secondary packets for some time slots which indicates the primary network can fully utilize the secure transmission opportunities. In [34], a fraction of power is used for the interference signal which will interfere the secondary transmission and the secondary average transmission rate decreases. In the underlay scheme, since there is no

$$G_x(1,1) + G_y(1,1) = \frac{\left(\lambda_p + \lambda_s\right)G(1,0) - P_1 G(1,0) + G_x(1,0)}{2 - \left(\lambda_p + \lambda_s\right) - P_1} \quad (53)$$

$$m(1,1) = \frac{\left(\lambda_p + (1-P_1)\right)\left(\left(\lambda_p + \lambda_s\right)G(1,0) - P_1 G(1,0) + G_x(1,0)\right)}{2 - \left(\lambda_p + \lambda_s\right) - P_1} \quad (55)$$

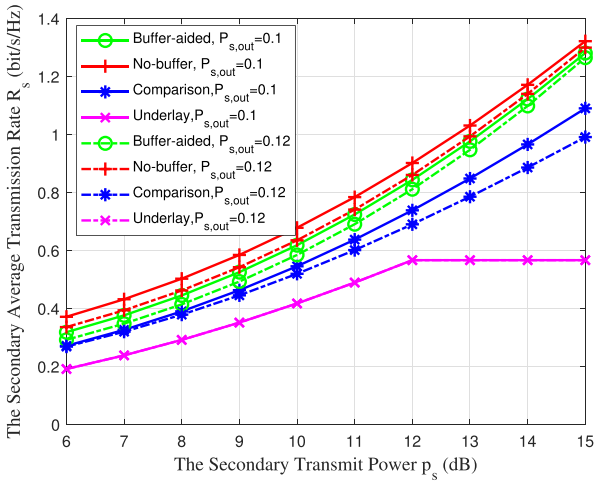

FIGURE 3. The secondary average transmission rate versus the secondary transmit power p_S with different $P_{s,out}$.

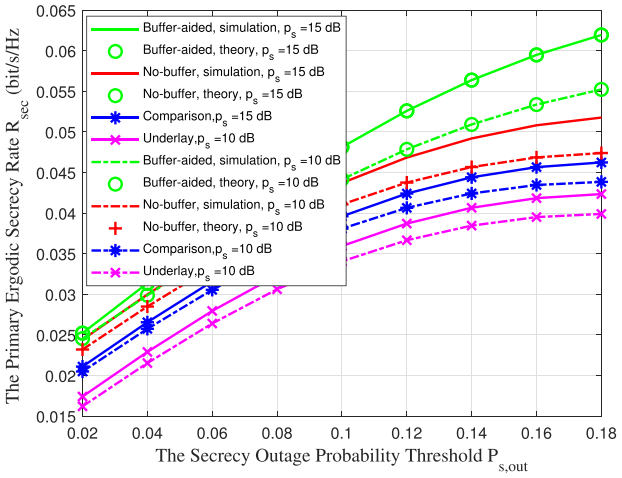

FIGURE 4. The primary ergodic secrecy rate versus the secrecy outage probability threshold $P_{s,out}$ with different p_S.

cooperation, the secondary average transmission rate is the lowest compared with the other schemes.

Figure 3 plots the secondary average transmission rate versus the secondary transmit power p_s with different $P_{s,out}$. From Fig. 3, we can observe that the secondary transmission rate is an increasing function of p_s. The increase of p_s indicates that there will more power to assist the primary secure transmission and there will be much more remaining power for the secondary transmission. Therefore, the secondary average transmission rate increases with p_s. The increase of $P_{s,out}$ indicates that the primary system can bear more secure transmission outage events. The primary network will directly transmit with high probability and there will be less cooperative transmission opportunities for the secondary network. In the buffer-aided scheme, the secure secondary data queue can store the secure secondary packets for some time slots which indicates that the primary network can fully utilize the secure transmission opportunities. In [34], a fraction of power is used for the interference signal which will interfere the secondary transmission and the secondary average transmission rate decreases. In the underlay scheme, since there is no cooperation, the secondary average transmission rate is the lowest compared with the other schemes.

Figure 4 plots the primary ergodic secrecy rate versus the secrecy outage probability threshold $P_{s,out}$ with different $P_{s,out}$. In Fig. 4, we can find that the theoretical results are in excellent agreement with the simulation results. In addition, we can also observe that the primary ergodic secrecy rate is an increase function of $P_{s,out}$. The increase of $P_{s,out}$ indicates that the secrecy constraint is loose and there will be more secure transmission opportunities for the primary secure transmission. When $P_{s,out}$ is large enough, the channel quality and the primary transmit power will limit the performance improvement. In addition, the increase of p_s provides more power for the cooperation and the primary ergodic secrecy rate will increase. For the under scheme, the increase of p_s will interfere the primary secure transmission which leads to the decease of R_{sec}. In the buffer-aided scheme, the secure secondary data queue can store the secure secondary packets for some time slots which indicates the primary network can fully utilize the secure transmission opportunities. In [34], a fraction of power is used for the interference signal which will interfere the secondary transmission and the secondary average transmission rate decreases. In the underlay scheme, since there is no cooperation, the secondary average transmission rate is the lowest compared with the other schemes.

Figure 5 plots the primary ergodic secrecy rate versus p_p with different $P_{s,out}$. In Fig. 5, we can observe that the primary ergodic secrecy rate is an increasing function of the primary transmit power p_p. The increase of p_p indicates that there will be more opportunities for the primary secure transmission and the primary ergodic secrecy rate will increase. However, when p_p is large enough, the primary direct

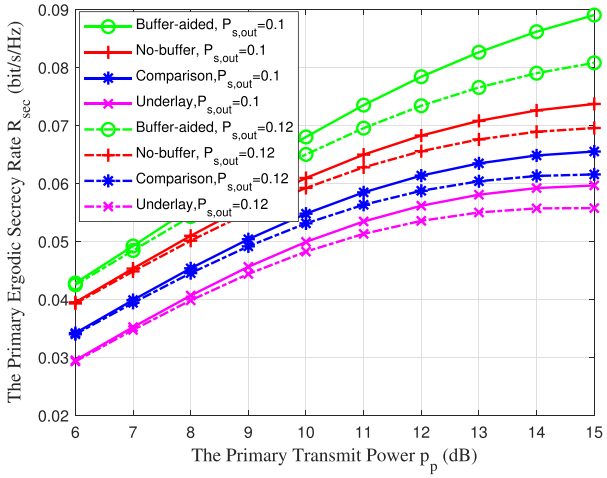

FIGURE 5. The primary ergodic secrecy rate versus the primary transmit power p_P with different $P_{s,out}$.

transmission channel quality will limit the improvement of the primary ergodic secrecy rate. In addition, the increase of $P_{s,out}$ means that the primary system can bear more secure transmission outage events. Therefore, the primary network can securely transmit with high rate and the ergodic secrecy rate of the primary system will increase. In the buffer-aided scheme, the secure secondary data queue can store the secure secondary packets for some time slots which indicates that the primary network can fully utilize the secure transmission opportunities. In [34], a fraction of power is used for the interference signal which will interfere the secondary transmission and the secondary average transmission rate decreases. In the underlay scheme, since there is no cooperation, the secondary average transmission rate is the lowest compared with the other schemes.

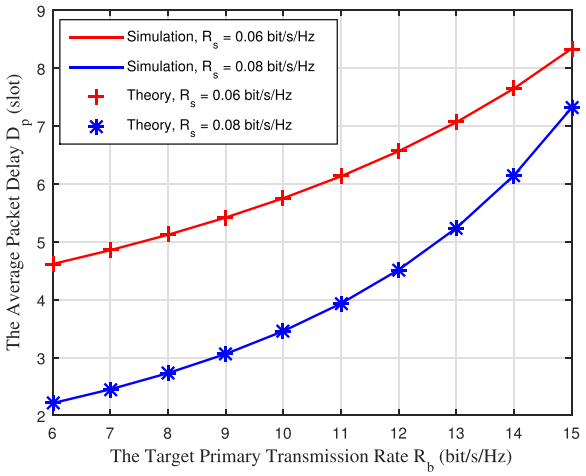

FIGURE 6. **The average packet delay versus the target primary transmission rate R_b.**

Figure 6 plots the primary privacy information delay versus the target primary transmission rate R_b. In Fig. 6, we can observe that the simulation results are almost the same with the theoretical results. The increase of R_b indicates that the primary privacy information can successfully transmit with low probability, and the primary privacy messages will wait for a long time. The increase of R_b means that there will be less secure transmission opportunities and the primary information delay will increase.

VI. CONCLUSION

In this paper, we proposed a novel secondary encrypted secure transmission scheme for the no-buffer and buffer-aided scenarios. In the proposed scheme, the primary network directly transmitted the privacy information or employed the pre-transmitted secure secondary messages to encrypt its privacy information, and the secondary system could acquire much more licensed spectrum for the secondary transmission. For the non-buffer scenario, we first proposed the secure transmission policy by considering the primary direct transmission or secondary assistance. Following this policy, we analyzed the primary ergodic secure rate and the secondary average transmission rate. Then, we considered the buffer-aided scenario where the secure secondary messages could be stored in the buffer for some time slots, and were employed to encrypt the primary privacy information in the following primary transmission. For this scenario, we also summarized the secure transmission policy and then, analyzed the primary average secrecy rate and the secondary average rate. Moreover, the primary information delay was investigated and its closed-form expression was derived. Numerical results demonstrate that the proposed strategies can provide primary secure preserving and verify the performance improvement of the secondary average transmission rate.

REFERENCES

[1] 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.

[2] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[3] Z. Ren, J. Goseling, J. H. Weber, and M. Gastpar, "Secure transmission on the two-hop relay channel with scaled compute-and-forward," *IEEE Trans. Inf. Theory*, vol. 63, no. 12, pp. 7753–7769, Dec. 2017.

[4] R. Fantacci, F. Gei, D. Marabissi, and L. Micciullo, "Public safety networks evolution toward broadband: Sharing infrastructures and spectrum with commercial systems," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 24–30, Apr. 2016.

[5] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[6] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[7] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[8] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[10] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[11] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[12] X. Chen, J. Chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8025–8035, Dec. 2016.

[13] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference- alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[14] T. Mekkawy, R. Yao, T. A. Tsiftsis, F. Xu, and Y. Lu, "Joint beamforming alignment with suboptimal power allocation for a two-way untrusted relay network," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2464–2474, Oct. 2018.

[15] Z. Wei and C. Masouros, "User-centric distributed antenna transmission: Secure precoding and antenna selection with interference exploitation," 2019, *arXiv:1812.05046*. [Online]. Available: https://arxiv.org/abs/1812.05046

[16] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

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

[18] L. Sun, T. Zhang, Y. Li, and N. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.
[19] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7274–7284, Sep. 2016.
[20] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.
[21] M. Vaezi, W. Shin, and H. V. Poor, "Optimal beamforming for Gaussian MIMO wiretap channels with two transmit antennas," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6726–6735, Oct. 2017.
[22] L. Li, Z. Chen, A. P. Petropulu, and J. Fang, "Linear precoder design for an MIMO Gaussian wiretap channel with full-duplex source and destination nodes," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 421–436, Feb. 2018.
[23] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861–1874, May 2016.
[24] E. R. Alotaibi and K. A. Hamdi, "Optimal cooperative relaying and jamming for secure communication," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 689–692, Dec. 2015.
[25] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.
[26] K.-Y. Hsieh, F.-S. Tseng, and M.-L. Ku, "A spectrum and energy cooperation strategy in hierarchical cognitive radio cellular networks," *IEEE Wireless Commun.*, vol. 5, no. 3, pp. 252–255, Jun. 2016.
[27] D. Li, J. Cheng, and V. C. M. Leung, "Adaptive spectrum sharing for half-duplex and full-duplex cognitive radios: From the energy efficiency perspective," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5067–5080, Nov. 2018.
[28] D. Li, D. Zhang, and J. Cheng, "Degrees of freedom for half-duplex and full-duplex cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2571–2584, Mar. 2019.
[29] F. Gabry, N. Li, N. Schrammar, M. Girnyk, L. K. Rasmussen, and M. Skoglund, "On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 451–463, Mar. 2014.
[30] G. Zheng, I. Krikidis, and B. Ottersten, "Full-duplex cooperative cognitive radio with transmit imperfections," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2498–2511, May 2013.
[31] M. Li, H. Yin, Y. Huang, Y. Wang, and R. Yu, "Physical layer security in overlay cognitive radio networks with energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11274–11279, Nov. 2018.
[32] M. R. Abedi, N. Mokari, M. R. Javan, and H. Yanikomeroglu, "Secure communication in OFDMA-based cognitive radio networks: An incentivized secondary network coexistence approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1171–1185, Feb. 2017.
[33] H. Zhang, T. Wang, L. Song, and Z. Han, "Interference improves PHY security for cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 609–620, Mar. 2016.
[34] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.
[35] A. Al-Talabani, Y. Deng, A. Nallanathan, and H. X. Nguyen, "Enhancing secrecy rate in cognitive radio networks via Stackelberg game," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4764–4775, Nov. 2016.
[36] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. El Gamal, "On the delay limited secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2009, pp. 2617–2621.
[37] A. El Shafie and N. Al-Dhahir, "On secure communications over a wiretap channel with fixed-rate transmission: Protocol design and queueing analysis," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 453–456, Aug. 2015.
[38] Z. Mao, C. E. Koksal, and N. B. Shroff, "Achieving full secrecy rate with low packet delays: An optimal control approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1944–1956, Sep. 2013.
[39] O. Güngör, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.
[40] D. Wang, P. Ren, J. Cheng, and Y. Wang, "Achieving full secrecy rate with energy-efficient transmission control," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5386–5400, Dec. 2017.
[41] D. Wang, P. Ren, Q. Xu, and Q. Du, "Secondary encrypted secure transmission in cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–5.
[42] R. Zhang, L. Cai, Z. Zhong, J. Zhao, and J. Zhou, "Cross-polarized three-dimensional channel measurement and modeling for small-cell street canyon scenario," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 7969–7983, Sep. 2018.
[43] D. Zhai, R. Zhang, L. Cai, B. Li, and Y. Jiang, "Energy-efficient user scheduling and power allocation for NOMA-based wireless networks with massive IoT devices," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1857–1868, Jun. 2018.
[44] Y. Yang, Z. Zeng, J. Cheng, C. Guo, and C. Feng, "A relay-assisted OFDM system for VLC uplink transmission," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6268–6281, Sep. 2019.
[45] Z. Wei, S. Sun, X. Zhu, Y. Huang, and J. Wang, "Energy-efficient hybrid duplexing strategy for bidirectional distributed antenna systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5096–5110, Jun. 2018.
[46] D. Wang, P. Ren, and J. Cheng, "Cooperative secure communication in two-hop buffer-aided networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 972–985, Mar. 2018.
[47] B. Wang and P. Mu, "Artificial noise-aided secure multicasting design under secrecy outage constraint," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5401–5414, Dec. 2017.
[48] M. Zhang and Y. Liu, "Secure beamforming for untrusted MISO cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4861–4872, Jul. 2018.
[49] A. H. A. El-Malek, A. M. Salhab, and S. A. Zummo, "New bandwidth efficient relaying schemes in cooperative cognitive two-way relay networks with physical layer security," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5372–5386, Jun. 2017.
[50] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.
[51] S. Kompella, G. Nguyen, C. Kam, J. E. Wieselthier, and A. Ephremides, "Cooperation in cognitive underlay networks: Stable throughput tradeoffs," *IEEE/ACM Trans. Netw.*, vol. 22, no. 6, pp. 1756–1768, Dec. 2014.

DAWEI WANG (S'14–M'18) received the B.S. degree from the University of Jinan, China, in 2011, and the Ph.D. degree from Xi'an Jiaotong University, China, in 2018. From 2016 to 2017, he was a Visiting Student with the School of Engineering, The University of British Columbia. He is currently an Associate Professor with the School of Electronics and Information, Northwestern Polythechnical University, Xi'an, China. His current research interests include physical-layer security, cognitive radio networks, cooperative communication, and resource allocation.

RUONAN ZHANG (S'09–M'10) received the B.S. and M.Sc. degrees from Xian Jiaotong University, Xian, China, in 2000 and 2003, respectively, and the Ph.D. degree from the University of Victoria, Victoria, BC, Canada, in 2010, all in electrical and electronics engineering. He was an IC Design Engineer with Motorola Inc., and Freescale Semiconductor Inc., Tianjin, China, from 2003 to 2006. Since 2010, he has been with the Department of Communication Engineering, Northwestern Polytechnical University, Xian, where he is currently a Professor. His current research interests include wireless channel measurement and modeling, architecture and protocol design of wireless networks, and satellite communications. Dr. Zhang was a recipient of the New Century Excellent Talent Grant from the Ministry of Education of China. He has served as a Local Arrangement Co-Chair for the IEEE/CIC International Conference on Communications, China, in 2013, and an Associate Editor for the *Journal of Communications and Networks*.

LIXIN LI (M'12) received the B.Sc. and M.Sc. degrees in communication engineering and the Ph.D. degree in control theory and its applications from Northwestern Polytechnical University (NPU), Xi'an, China, in 2001, 2004, and 2008, respectively. He was a Postdoctoral Fellow with NPU, from 2008 to 2010. In 2017, he was a Visiting Scholar with the University of Houston, Houston, TX, USA. He is currently an Associate Professor with the School of Electronics and Information, NPU. He has authored or coauthored over 100 technical articles in journals and international conferences. He holds ten patents. His current research interests include wireless communications, game theory, and machine learning. He has reviewed articles for many international journals. He received the 2016 NPU Outstanding Young Teacher Award, which is the highest research and education honors for young faculties in NPU.

SHAOYANG MEN (M'10) received the M.S. degree in electronics systems from Polytech'Nantes (Ecole Polytechnique de l'universite de Nantes), Nantes, France, in 2013, the M.S. degree in communication and information system from the South China University of Technology, Guangzhou, China, in 2014, and the Ph.D. degree in digital communications systems from the University of Nantes, Nantes, in 2016. He has been an Assistant Professor with the Guangzhou University of Chinese Medicine, China, since 2017. His current research interests include cognitive wireless sensor networks, signal detection, medical image processing, and medical text analysis.

DEYUN ZHOU received the B.S., M.S., and Ph.D. degrees from the Northwestern Polytechnical University, in 1985, 1988, and 1991, respectively. His current research interests include predictive control, adaptive control, intelligent control theory and its applications, complex system modeling and simulation, multi-objective optimization, information fusion, and complex network modeling and application.

MOHSEN GUIZANI (S'85–M'89–SM'99–F'09) received the bachelor's (Hons.) and master's degrees in electrical engineering, and the master's and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He served as the Associate Vice President of graduate studies, Qatar University, the Chair of the Computer Science Department, Western Michigan University, the Chair of the Computer Science Department, University of West Florida. He also served in academic positions with the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. He is currently a Professor with the Department of Computer Science and Engineering, Qatar University, Doha, Qatar. He is the author of nine books and more than 400 publications in refereed journals and conferences. His current research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. Dr. Guizani served as a member, a Chair, and the General Chair of a number of international conferences. He currently serves on the editorial boards of several international technical journals and the Founder and the Editor-in-Chief of the *Wireless Communications and Mobile Computing* journal (Wiley). He was selected as the Best Teaching Assistant for two consecutive years by Syracuse University. He received the Best Research Award from three institutions. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the TAOS Technical Committee. He guest edited a number of special issues in IEEE journals and magazines. He served as the IEEE Computer Society Distinguished Speaker, from 2003 to 2005.