IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 13, 2021, accepted February 7, 2021, date of publication February 10, 2021, date of current version February 18, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3058603

Adaptive Secure Transmission Strategy for Industrial Wireless Edge-Enabled CPS

HUANHUAN SONG[1], HONG WEN[1], (Senior Member, IEEE), QICONG YANG[2], JIE TANG[1], YI CHEN[3], (Graduate Student Member, IEEE), TENGYUE ZHANG[1], (Graduate Student Member, IEEE), FEIYI XIE[2], (Student Member, IEEE), AND SONGLIN CHEN[3]

[1]School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]Sichuan Jiuzhou Electric Group Company Ltd., Mianyang 621000, China
[3]National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding authors: Hong Wen (sunlike@uestc.edu.cn) and Jie Tang (cs.tan@uestc.edu.cn)

This work was supported in part by NSFC under Grant 61901089, and in part by the National Major Research and Development Program under Grant 2018YFB0904900 and Grant 2018YFB0904905.

ABSTRACT For real-time industrial wireless edge-enabled cyber-physical systems, this paper proposes an adaptive secure transmission mechanism under the large scale path loss to fight against randomly distributed illegal sensing devices. According to changes in the communication environment, the proposed scheme adaptively obtains the corresponding optimal power allocations and wiretap code rates. Specifically, by injecting artificial noise, an edge controller provides confidential control information for a legitimate wireless sensing device and achieves non-confidential data service for a service subscriber, simultaneously. Considering whether the secrecy and non-confidential service rate constraints are met, a dynamic secrecy transmission mechanism is introduced to minimize secrecy outage probability (SOP) based on random channel realizations. The optimal power allocation for minimizing the SOP is derived through the efficient alternating optimization algorithm with numerical methods. Numerical results show that the proposed adaptive secure transmission strategy can efficiently utilize transmit power to achieve non-confidential information traffic without compromising the secrecy performance.

INDEX TERMS Industrial wireless cyber physical security, adaptive secure transmission, secrecy outage probability.

I. INTRODUCTION

IN Industry 4.0, cyber-physical systems (CPS) are heavily utilized to intelligently sense, monitor, and control industrial processes, especially in harsh industrial environments such as high temperatures and rotating parts [1], [2]. CPS can be regarded as the key interconnecting entity to create solid ties between the virtual world and physical components such as sensors, actuators, and robotics while processing/exchanging important and confidential information as shown in Fig. 1 [3]. As replacement of aging wired industrial communication networks, industrial wireless CPS largely depend on distributed sensor networks and make industrial process more connected and open, which in turn poses serious security challenges. Malicious attackers are able to access sensors via the wireless channel easily. If illegal attackers issue malicious commands to critical infrastructure controllers, major industrial disasters may occur and security loss can be costly for manufacturing plants [4], [5].

All types of cryptographic algorithms such as hybrid homomorphic encryption [6] and RSA [7] constitute a universal security protection mechanism to resist any form of eavesdropping attacks. Nonetheless, attackers can launch various attacks such as differential cryptanalysis [8], boomerang attack [9], and zero-correlation linear cryptanalysis [10] to crack confidential information successfully. Equipped with low-power microcontrollers, most industrial devices such as sensors, actuators, and radio frequency identification chips

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

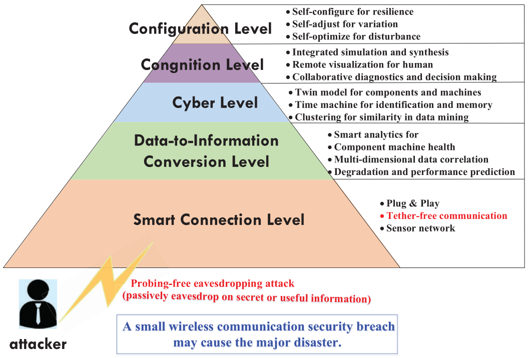

Configuration Level
• Self-configure for resilience
• Self-adjust for variation
• Self-optimize for disturbance
Congnition Level
• Integrated simulation and synthesis
• Remote visualization for human
• Collaborative diagnostics and decision making
Cyber Level
• Twin model for components and machines
• Time machine for identification and memory
• Clustering for similarity in data mining
Data-to-Information Conversion Level
• Smart analytics for
• Component machine health
• Multi-dimensional data correlation
• Degradation and performance prediction
Smart Connection Level
• Plug & Play
• Tether-free communication
• Sensor network
Probing-free eavesdropping attack
(passively eavesdrop on secret or useful information)
A small wireless communication security breach may cause the major disaster.
attacker

FIGURE 1. Layered architecture of CPS.

cannot support encryption methods based on complex calculation. By taking advantages of its light-weight computation, physical layer security (PLS) has recently become a key technology to safeguard data confidentiality against malicious eavesdroppers while ensuring the information reliability for many resource-constrained real-time industrial communication applications [11], [12]. An adaptive probabilistic MIMO transmission scheme under a noncollaborative game framework was proposed to cope with the smart attacker which can flexibly use programmable radio devices to launch various attacks like eavesdropping, jamming and spoofing in adverse channel conditions [13]. In the presence of a multiple-antenna-aided passive eavesdropper and a hostile jammer, authors in [14] investigated a light-weight artificial noise (AN) injection scheme with physical layer secret key generation to assure both information confidentiality and transmission resiliency. In [14], the communication system guarantees the secure transmission between a pair of single-antenna half-duplex devices, thus a more complicated synchronization process is required. Subsequently, the extension of [14] is investigated in [15]. The schemes of joint information theoretic secrecy and covert communication were presented in [16], [17] to achieve both secure and covert transmission. Different from the above literatures, this paper focuses on how to effectively resist passive eavesdropping attacks using physical layer security schemes due to the concealment of passive eavesdropping methods and potential destructive power in industrial environment.

AN was first presented in [18] to disrupt potential eavesdroppers' reception without affecting that of the legitimate user. Subsequently, multi-antenna AN-aided secure designs have gained much attention in recent studies [19]–[23]. However, these secure transmission schemes only focused on the confidential signal transmission. For achieving high spectral efficiency and meeting personalized service customization, physical layer service integration technology can wisely merge multiple services into an integrated service at the physical layer and achieve a variety of communication business under the same spectrum transmission [24]–[32]. The secrecy capacity region is achieved when the legitimate user performs successive interference cancellation to remove the multicast message [25]–[29], yet this is more suitable for the perfect or imperfect channel information scenarios that the system has obtained from unauthorized user. Based on instantaneous channel information of the secondary link, a simple adaptive secure transmission scheme was discussed in [31]. However, this secure scheme cannot cope with all communication conditions. In [32], authors considered that the transmitter simultaneously transmits confidential signal, AN, and non-confidential signal to provide secret and non-confidential data traffic. However, they assumed that the normal user's power approaches zero, which results in an inaccurate secrecy analysis result. This paper adopts exact numerical analysis methods to obtain the optimal transmit parameter design for the confidential and non-confidential service integration system. Another issue is that the above service integration schemes did not consider the large scale path loss and eavesdropping node location. To fill this gap, this paper presents an adaptive secure transmission mechanism by considering the large scale path loss as well as randomly located advesaries.

The traditional security application is limited in the terminal-to-cloud transmission with long-distance multi-route nodes. Edge computing (EC) in industrial wireless CPS makes communication transceiver directly connected or subject to a short-range connection with only one hop or two hops, while providing a powerful computing platform for physical layer security methods [33]–[35]. Motivated by the aforementioned studies, this paper presents that the industrial edge controller ensures the secure data transmission of a legitimate wireless sensing device via assisted AN, while providing data services for another service subscriber.

The main contributions of this paper are summarized as follows:

(1) Different from [25]–[29], this paper presents an adaptive secure transmission mechanism with the optimal power allocation and wiretap code rates to fight against any number of randomly located illegal sensing devices for industrial wireless edge-enabled CPS. Due to the complexity of security scenario, null-space constraint on the multicast message is imposed. The proposed scheme uses analytical analysis methods to obtain accurate transmission strategies, and the related mathematical analysis process is more challenging. Additionally, more sensing devices can subscribe to edge services if the proper scheduling policy is adopted at the industrial edge server.

(2) In this paper, the industrial edge controller (i.e., edge server) conveys both extremely important control instruction and broadcast message to different sensors. Meanwhile, AN is adopted at the edge controller to greatly resist eavesdropping attack. Our proposed adaptive security transmission mechanism can be applied to various industrial communication scenarios such as cooperative relay and multiple-antenna eavesdroppers.

(3) Secrecy outage probability (SOP) is adopted as the secrecy metric which effectively supports delay-sensitive industrial applications. An efficient alternating optimization algorithm with the numerical method is proposed to obtain exact optimal power parameters. Simulation results show that a higher number of transmit antennas, a shorter legal access distance, a smaller non-confidential service rate threshold, and a high-power area are conducive to reducing SOP and achieving confidential communication.

This paper is organized as follows. The industrial system model, secrecy performance metric, and adaptive secure transmission formulation are introduced in Section II. Section III and Section IV discuss multi-service and single-service secure transmission strategies, respectively. Numerical results are presented in Section V. Finally, Section VI concludes the paper.

Notation: Boldface upper (lower) case letters denote matrices (column vectors). Standard lowercase and uppercase letters denote scalars. $(\cdot)^H$, $|\cdot|$, and $\|\cdot\|$, represent conjugate transpose, absolute value, and Euclidean norm, respectively. Circularly symmetric complex Gaussian random vector submits to $\mathcal{CN}(\mu, \Lambda)$, with mean μ and covariance matrix Λ. null($\mathbf{X}$) denotes the null space of $\mathbf{X}$. $\Pr(\cdot)$ is the probability measure. $\mathbf{I}_N$ is the identity matrix of size $N \times N$. Exponential distribution with parameter λ is denoted as $\mathrm{E}(\lambda)$. $\Gamma(x)$ denotes the gamma function. Gamma distribution with shape parameter α and rate parameter β is denoted as $\Gamma(\alpha, \beta)$. The symbol $\Rightarrow$ denotes "implies".

II. SYSTEM MODEL AND PROBLEM DESCRIPTION

A. INDUSTRIAL SYSTEM MODEL

Sensing data and control commands are frequently exchanged over industrial wireless networks. Considering an industrial building, a local network is deployed to connect industrial wireless sensing devices and robot-controller. Since the network is utilized only for local control, it is isolated from external networks. The wireless channel is shared by all industrial devices within the signal radiation range and it is extremely difficult to prevent electromagnetic field leakage. Wireless sensing devices, whether in or outside the building, are very likely to become attackers. For example, an attacker can install an eavesdropping module on a mobile phone to steal key data in the manufacturing process. Generally, the passive eavesdropper configures single antenna [14] or multiple antennas [23], [24], [36], and its working mode can be colluding [17] or non-colluding [21]. In actual communication systems, especially in resource-constrained sensor networks, potential eavesdroppers are often randomly distributed and more willing to eavesdrop on secret messages by themselves to avoid the sophisticated process of information sharing. When the eavesdropper is equipped with multiple antennas, security optimization problems tend to be nonconvex polynomial-time hard or NP-hard problems which can be solved by a series of conservative convex approximation methods. Unfortunately, there is no general theory to prove the accuracy of the approximate solution and the corresponding computational complexity is relatively high. Therefore, this paper investigates how to resist randomly located non-colluding single-antenna eavesdroppers and obtain accurate analytical solutions of the corresponding security optimization problems.

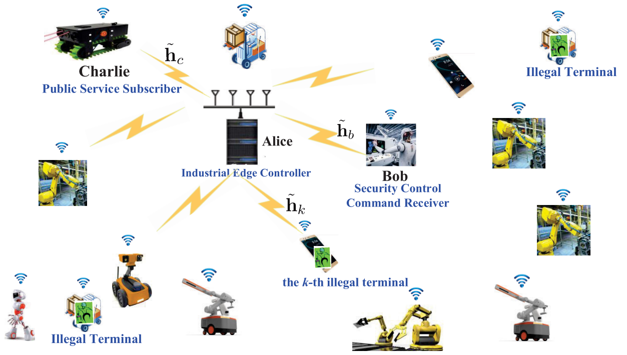


FIGURE 2. Industrial security communication model against eavesdropping.

As illustrated in Fig. 2, multiple wireless sensing devices communicate with the nearest edge controller, namely Alice. Specifically, Alice is located at the origin with N antennas and intends to transmit confidential control and non-confidential information to single-antenna end users Bob and Charlie (e.g., industrial inspection robot), respectively. Besides, the secure communication link is eavesdropped by multiple non-colluding adversaries Eves whose locations are distributed according to a two-dimensional homogeneous Poisson Point Process (PPP) Φ_E with density λ_E.

All wireless channels are characterized as independent and identically distributed (i.i.d.) flat Rayleigh fading. Large-scale path loss governed by a path loss exponent $\alpha(\alpha \geq 2)$. $(N \times 1)$-dimensional complex conjugate channel vectors from Alice to Bob, Charlie, and the k-th illegal terminal are represented as $\tilde{\mathbf{h}}_b = d_b^{-\frac{\alpha}{2}}\mathbf{h}_b$, $\tilde{\mathbf{h}}_c = d_c^{-\frac{\alpha}{2}}\mathbf{h}_c$, and $\tilde{\mathbf{h}}_k = d_k^{-\frac{\alpha}{2}}\mathbf{h}_k(k \in \Phi_E)$, respectively. Note that $\mathbf{h}_b$, $\mathbf{h}_c$, and $\mathbf{h}_k$ are mutually independent small scale fading channels and the entries of each channel are i.i.d. obeying $\mathcal{CN}(0, 1)$. d_b, d_c, and d_k respectively represent the distances from Alice to Bob, Charlie, and k-th illegal terminal. Assume that statistical channel state informations (CSIs) of adversaries and instantaneous CSIs of legitimate sensing devices are available at the edge server, which is widely-adopted in [31], [32], since adversaries can be the original service subscribers or other business subscribers.

Both the security control command receiver Bob and the non-confidential service subscriber Charlie request access to the edge side, simultaneously. Then, the edge controller Alice offers the corresponding service guarantee. For secure communication from Alice to Bob, the maximum ratio transmission (MRT) beamforming and null space based AN is adopted. The transmitted signal at Alice can be constructed as

$$\mathbf{x} = \sqrt{\phi_b P}\mathbf{w}_b x_b + \sqrt{\phi_c P}\mathbf{w}_c x_c + \sqrt{\phi_n P}\mathbf{Z}\mathbf{n}_a, \tag{1}$$

where P is the transmit power of Alice. $\phi_b \in [0, 1]$, $\phi_c \in [0, 1]$ and $\phi_n \in [0, 1]$ denote the power allocation coefficients of confidential signal, non-confidential signal, and the artificial noise, respectively. It can be easily seen that $\phi_b + \phi_c + \phi_n = 1$ due to energy conservation. $x_b \sim \mathcal{CN}(0, 1)$ is the secret information-bearing signal with the secrecy beamforming vector $\mathbf{w}_b = \mathbf{h}_b / \|\mathbf{h}_b\|_2$. $\mathbf{n}_a \sim \mathcal{CN}(\mathbf{0}, 1/(N-2)\mathbf{I}_{N-2})$ is the AN signal. To avoid affecting legitimate wireless sensing devices, the weighted matrix $\mathbf{Z} \in \mathbb{C}^{N\times(N-2)}$ is an orthonormal basis for null ($[\mathbf{h}_b, \mathbf{h}_c]$). The signal x_c is not required to be kept secret from other sensing devices. Besides, the system conveys non-confidential information as efficiently as possible to achieve high data rate. Meanwhile, the introduced signal must not interfere with Bob. Accordingly, the beamforming vector of the non-confidential signal can be obtained by the following optimization problem:

$$\max_{\mathbf{w}_c} \; P\left|\mathbf{h}_c^H \mathbf{w}_c\right|^2 \quad \text{s.t. } \mathbf{h}_b^H \mathbf{w}_c = 0. \tag{2}$$

The optimal beamforming vector is given by

$$\mathbf{w}_c = \frac{\left(\mathbf{I}_N - \mathbf{h}_b\left(\mathbf{h}_b^H \mathbf{h}_b\right)^{-1}\mathbf{h}_b^H\right)\mathbf{h}_c}{\left\|\left(\mathbf{I}_N - \mathbf{h}_b\left(\mathbf{h}_b^H \mathbf{h}_b\right)^{-1}\mathbf{h}_b^H\right)\mathbf{h}_c\right\|_2}. \tag{3}$$

The edge server transmits confidential, non-confidential, and interference signals in parallel. Accordingly, the received signals at Bob, Charlie, and the k-th illegal terminal are respectively expressed as

$$y_b = \sqrt{\phi_b P d_b^{-\frac{\alpha}{2}}} \|\mathbf{h}_b\|_2 x_b + n_b, \tag{4}$$

$$y_c = \sqrt{\phi_b P d_c^{-\frac{\alpha}{2}}} \mathbf{h}_c^H \mathbf{w}_b x_b + \sqrt{\phi_c P d_c^{-\frac{\alpha}{2}}} \mathbf{h}_c^H \mathbf{w}_c x_c + n_c, \tag{5}$$

$$y_k = \sqrt{\phi_b P d_k^{-\frac{\alpha}{2}}} \mathbf{h}_k^H \mathbf{w}_b x_b + \sqrt{\phi_c P d_k^{-\frac{\alpha}{2}}} \mathbf{h}_k^H \mathbf{w}_c x_c + \sqrt{\phi_n P d_k^{-\frac{\alpha}{2}}} \mathbf{h}_k^H \mathbf{Z}\mathbf{n}_a + n_k, \tag{6}$$

where $n_b \sim \mathcal{CN}(0, 1)$, $n_c \sim \mathcal{CN}(0, 1)$, and $n_k \sim \mathcal{CN}(0, 1)$ are the corresponding independent additive thermal noise.

Here, each sensing device only focuses on individual message of interest. Accordingly, the instantaneous received signal-to-interference-plus-noise ratios (SINRs) at Bob, Charlie, and the k-th illegal terminal are respectively given by

$$\rho_b = \phi_b r, \tag{7}$$

$$\rho_c = \frac{\phi_c P\left|\mathbf{h}_c^H \mathbf{w}_c\right|^2}{d_c^\alpha + \phi_b P\left|\mathbf{h}_c^H \mathbf{w}_b\right|^2}, \tag{8}$$

$$\rho_k = \frac{\phi_b P\left|\mathbf{h}_k^H \mathbf{w}_b\right|^2}{d_k^\alpha + \phi_c P\left|\mathbf{h}_k^H \mathbf{w}_c\right|^2 + \frac{\phi_n P}{N-2}\left\|\mathbf{h}_k^H \mathbf{Z}\right\|^2}, \tag{9}$$

where $r = P d_b^{-\alpha}\|\mathbf{h}_b\|_2^2$. Obviously, all SINRs are the monotonically decreasing function of communication distance and the monotonically increasing function of transmit power P. Intuitively, the short accessing distance of the sensing device is less affected by fading and can achieve high channel gain, which is benefit to realize the communication purpose of the transceiver. The instantaneous channel capacity from Alice to Bob and Charlie are calculated as $C_b = \log_2(1 + \rho_b)$ and $C_c = \log_2(1 + \rho_c)$. Suppose that non-colluding adversaries independently decode the secret message and the eavesdropping channel capacity depends on the illegal terminal with the best channel quality. As such, the eavesdropping channel capacity is denoted by $C_e = \log_2(1 + \rho_e)$, where $\rho_e = \max_{k\in\Phi_E} \rho_k$.

B. SECRECY OUTAGE PROBABILITY

In the following, we consider the widely-used wiretap code for secure information transmission [37]. Specifically, there are two rate parameters, namely, the transmitted codeword rate R_b and the secrecy rate R_s. Then, the redundant rate $R_e = R_b - R_s$ reflects the cost sacrificed to safeguard secret information against eavesdropping. If $R_b > C_b$, the undesirable transmission incurs capacity outage. If $C_e > R_e$, this will cause unacceptably secrecy outage. As such, edge controller sets R_b to C_b, since the instantaneous CSI of Bob is publicly known. The edge controller has no knowledge of Eves' instantaneous CSIs. Accordingly, the perfect secrecy cannot be always achievable. Notably, the physical layer security level is typically measured by SOP. In this paper, we adopt SOP as the secrecy performance metric, which is defined as

$$P_{so} = \Pr\left\{C_e > C_b - R_s\right\}, \forall C_b > R_s. \tag{10}$$

The secrecy outage probability implies the fraction of time for which the legitimate transceiver (i.e., Alice and Bob) cannot reach a non-zero secrecy rate.

C. ADAPTIVE SECURE TRANSMISSION FORMULATION

The secrecy demand between Alice and Bob is the prioritising design criterion since important industrial control instructions are extremely confidential. Once the control information is stolen illegally, it will cause serious economic losses to manufacturing plants. The edge controller should assign the highest priority to Bob with more stringent secrecy requirement. Considering rate constraints for both Bob and Charlie, the SOP minimization problem can be characterized by the following combinatorial optimization problem:

$$(P1) \quad \min_{R_s, \phi_b, \phi_c} \; P_{so} \tag{11a}$$

$$\text{s.t. } \log_2(1 + \rho_c) \geq \tau, \tag{11b}$$

$$R_{th} \leq R_s \leq C_b, \tag{11c}$$

$$0 \leq \phi_b + \phi_c \leq 1, 0 \leq \phi_b, \phi_c \leq 1, \tag{11d}$$

where R_{th} and τ are respectively represented as the minimum achievable secrecy rate and non-confidential service rate. The change of random channel may lead to the infeasible case of the secrecy optimization problem P1, which shall severely degrade the security performance. Charlie will be served in a more opportunistic manner. That is, the edge controller refuses to provide non-confidential service to Charlie if either of the following three situations is encountered: 1) the secrecy rate R_s is less than the threshold R_{th}; or 2) the secrecy rate R_s is greater than or equal to the main channel capacity C_b; or 3) the non-confidential service rate constraint (11b) is not fulfilled,

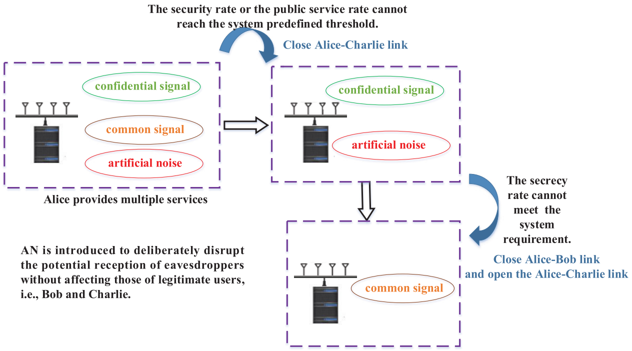

The security rate or the public service rate cannot reach the system predefined threshold.
Close Alice-Charlie link
confidential signal
common signal
artificial noise
Alice provides multiple services
confidential signal
artificial noise
The secrecy rate cannot meet the system requirement.
Close Alice-Bob link and open the Alice-Charlie link
AN is introduced to deliberately disrupt the potential reception of eavesdroppers without affecting those of legitimate users, i.e., Bob and Charlie.
common signal

FIGURE 3. **The proposed adaptive secure transmission strategy.**

i.e., $C_c < \tau$. When the stringent secrecy and non-confidential service constraints cannot hold, we prioritize the secrecy performance of the Alice-Bob pair. Consequently, only considering secure transmission, we propose the following secrecy scheme:

$$(P2)\ \min_{R_s,\phi_b}\ P_{so} \tag{12a}$$

$$\text{s.t. } R_{th} \le R_s \le C_b, \tag{12b}$$

$$\phi_b + \phi_n = 1, 0 \le \phi_b, \phi_n \le 1. \tag{12c}$$

In this case, the Alice-Charlie link stops communication, and Alice uses AN-assisted secure transmission method to enhance the quality of security service for Bob. If the security requirements of industrial wireless networks are still not met in this case, the edge server will use all its power to transmit broadcast data to Charlie. The proposed adaptive secure transmission strategy is demonstrated in Fig. 3. In the following two sections, the power allocation and rate parameters of the secrecy scheme P1 and the secrecy design P2 will be optimized.

III. MULTI-SERVICE SECURE TRANSMISSION SCHEME

In this section, we derive an optimal power allocation scheme to minimize SOP while satisfying the secrecy and non-confidential rate constraints.

Lemma 1: If $C_b > R_s$, the closed-form expression of the SOP is given by

$$P_{so}=1-\exp\left(-\mu\left(\frac{\phi_b}{\varepsilon_s}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_c\varepsilon_s}{\phi_b}\right)^{-1}\left(1+\frac{\phi_n\varepsilon_s}{\phi_b(N-2)}\right)^{2-N}\right), \tag{13}$$

where $\mu = \pi\lambda_E\Gamma\left(1+\frac{2}{\alpha}\right)P^{\frac{2}{\alpha}}$, $\varepsilon_s = (1+\phi_b r)2^{-R_s} - 1$.

Proof: The proof is provided in Appendix A. ■

It can be observed that the expression of SOP is a monotonically increasing function with λ_E, which means that increasing the number of adversaries per unit area will improve the risk of information leakage. That is to say, adversaries effectively utilize the growing spatial degrees of freedom to crack secret signals. Multiple-antenna technique in the edge controller is an efficient way to enhance the physical layer secrecy. Obviously, multiple antennas deployed at Alice are beneficial to reduce the SOP of the system.

An alternating optimization method is adopted to solve the security optimization problem P1. Taking the objective function (13) into account, we see that the SOP is a monotonically increasing function of the variable R_s on the other parameters being fixed. Thus, minimizing SOP is equivalent to minimizing secrecy rate. According to secrecy rate constraint (11c), we obtain the optimal value of the secrecy rate, i.e., $R_s^* = R_{th}$. Notably, as the variable ϕ_b increases, $C_b(\phi_b)$ gradually increases. That is, increasing the power allocation of the confidential signal improves the communication quality of the main channel. Next, we discuss four cases where a security interrupt event must occur.

Case 1). If $R_{th} = C_b(1)$, the edge controller uses all power to transmit the secret signal, and the optimal solution for power allocation is $\phi_b^* = 1$, which results in $P_{so} = 1$. This is mainly because the system security requirement is too high, triggering a security interrupt.

Case 2). If $R_{th} > C_b(1)$, the system cannot construct a wiretap code in this case, and the edge controller will close the security service. Based on the above two cases, the system cannot meet such high security requirement, so the edge controller can only transmit data service to Charlie.

Case 3). $R_{th} = C_b(\phi_b)$, $\phi_b \in (0, 1) \Rightarrow \phi_{b,min} = (2^{R_{th}} - 1)/r$. If $\phi_b = \phi_{b,min}$, the edge controller will stop transmitting the broadcast signal and resort to the secrecy scheme P2 for enhancing secrecy performance.

Case 4). We know that the edge controller transmits only when $\phi_b > \phi_{b,min}$. Note that the feasible region of $\phi_{b,min}$ is (0,1); otherwise, the edge controller shuts down confidential communication service and only provides data service to Charlie as a result of the poor main channel quality.

For a given variable ϕ_b, according to the service rate limit (11b), we derive $\phi_c \ge \frac{d_c^\alpha + \phi_b P|\mathbf{h}_c^H\mathbf{w}_b|^2}{P|\mathbf{h}_c^H\mathbf{w}_c|^2}(2^\tau - 1) = \phi_{c,min}$. Obviously, only when the rate threshold is $\tau = 0$, the minimum power alloction ratio of non-confidential signal is equal to zero, i.e., $\phi_{c,min} = 0$. The value range of $\phi_{c,min}$ is [0,1), otherwise the non-confidential broadcast service requirement cannot be met, and the server adopts the security optimization policy P2 for communication. It is observed from (13) that for any fixed ϕ_b, $P_{so}(\phi_c)$ is a gradually increasing function with ϕ_c. Therefore, minimizing the objective function is equivalent to the following optimization expression:

$$\max_{\phi_c} F(\phi_c) = \left(1+\frac{\phi_c\varepsilon_b}{\phi_b}\right)\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-2)}\right)^{N-2}, \tag{14}$$

where $\varepsilon_b = (1+\phi_b r)2^{-R_{th}} - 1$. The first derivative of $F(\phi_c)$ is calculated as

$$F'(\phi_c) = \frac{\varepsilon_b}{\phi_b}\left(1+\frac{1-\phi_b-\phi_c}{\phi_b(N-2)}\varepsilon_b\right)^{N-2} - \frac{\varepsilon_b(\phi_b+\phi_c\varepsilon_b)}{\phi_b^2}\left(1+\frac{1-\phi_b-\phi_c}{\phi_b(N-2)}\varepsilon_b\right)^{N-3}. \tag{15}$$

It shows that $F'(\phi_c)$ is a monotonically decreasing function on ϕ_c, which implies that the second-order derivative of $F(\phi_c)$ is negative, i.e., $F''(\phi_c) < 0$. We can conclude that $F(\phi_c)$ is a strictly concave function with respect to (w.r.t.) ϕ_c. The minimum SOP can be achieved at the extreme point $\phi_{c,0} = (1 - \phi_b)/(N - 1)$. Through the analysis above, the optimal power allocation of ϕ_c is given by

$$\phi_c^* = \max(\phi_{c,min}, \phi_{c,0}). \tag{16}$$

Finally, we analyze the variable ϕ_b. The SOP is nonlinearly coupled with variable ϕ_b. We find that the secrecy analysis process w.r.t. ϕ_b is very complicated and there is no accurate analytical solution of ϕ_b. Thus, we resort to one-dimensional unconstrained optimization algorithm including simulated annealing algorithm, genetic algorithm, and particle swarm optimization, to obtain the optimal power allocation ratio denoted by $\phi_{b,0}$. Accordingly, the optimal power allocation of ϕ_b can be expressed by

$$\phi_b^* = \min(\phi_{b,0}, 1 - \phi_c) \cap (\phi_{b,min}, 1]. \tag{17}$$

According to (16) and (17), it can be found that the optimal power allocation ϕ_c^* is a function of ϕ_b, and ϕ_b^* is a function of ϕ_c, hence there is no definitive closed-form solution for the secrecy optimization problem (11). In this paper, we propose an iterative optimization algorithm to iteratively optimize these two power allocation parameters. The specific process of solving the secrecy optimization problem (11) can be summarized in Algorithm 1.

IV. SINGLE-SERVICE SECURE TRANSMISSION STRATEGY

In this scheme, the edge controller adopts AN-aided beamforming strategy to enhance secrecy performance of the sensing device Bob, thus $\phi_c = 0$. The transmitted signal at the edge controller is designed in the form of

$$\mathbf{x} = \sqrt{\phi_b P}\mathbf{w}_b x_b + \sqrt{\frac{\phi_n P}{N-1}}\mathbf{W}\mathbf{n}_a, \tag{18}$$

where the AN signal is subject to $\mathbf{n}_a \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N-1})$ and the weighted matrix $\mathbf{W} \in \mathbb{C}^{N\times(N-1)}$ is an orthonormal basis for null $(\mathbf{h}_b)$ to avoid affecting Bob's received signal quality.

Lemma 2: If $C_b > R_s$, the closed-form expression of the SOP is given by

$$P_{so} = 1 - \exp\left(-\mu\left(\frac{\phi_b}{\varepsilon_s}\right)^{\frac{2}{\alpha}}\left(1 + \frac{\phi_n\varepsilon_s}{\phi_b(N-1)}\right)^{1-N}\right). \tag{19}$$

Proof: The proof is similar to the Lemma 1. Here, we omit the corresponding proof. ■

Likewise, the objective SOP (19) can get the minimum value only when $R_s^* = R_{th}$.

Theorem 1: The SOP is a quasi-convex function on ϕ_b.

Proof: The proof is provided in Appendix B. ■

Since the SOP in (19) is a quasi-convex function w.r.t. ϕ_b, the global optimal solution ϕ_b that minimizes the SOP can only be an extreme point or a boundary point of (19). Equation (36) can be rearranged as

$$\phi_b^3 + a\phi_b^2 + b\phi_b + c = 0, \tag{20}$$

Algorithm 1 The Iterative Optimization Algorithm for Solving Problem (11)

```
1) Initialize: Given $d_b, d_c, \lambda_E, N, P, \alpha, R_{th}, \tau, \mathbf{h}_b, \mathbf{h}_c$, and $\delta = 10^{-5}$;
2) Calculate: $C_b^{max} = \log_2(1 + r)$, $\phi_{b,min} = \frac{2^{R_{th}}-1}{r}$, $C_c^{max} = \log_2(1 + Pd_c^{-\alpha}\left|\mathbf{h}_c^H\mathbf{w}_c\right|^2)$, and $\phi_{c,min} = \frac{d_c^{\alpha}(2^{\tau}-1)}{P\left|\mathbf{h}_c^H\mathbf{w}_c\right|^2}$;
   1: if $R_{th} \geq C_b^{max}$ or $\phi_{b,min} \geq 1$, the edge controller closes the confidential communication and only provides public service for Charlie.
   2: elseif $C_c^{max} < \tau$ or $\phi_{c,min} > 1$, non-confidential service rate cannot be met and the edge controller adopts the P2 scheme.
   3: else the edge controller proceeds with the following steps:
3) Set: $\phi_b \in (\phi_{b,min}, 1]$,
   a) $n = 1$;
   b) calculate $\phi_c^*$ (Eq. (16));
   c) utilizing $\phi_c^*$, calculate $\phi_b^*$ (Eq. (17));
   d) calculate $P_{so}(n)$ in the $n$-th iteration (Eq. (13));
   e) $n=n+1$, $\phi_b = \phi_b^*$;
   f) repeat steps b) to e) until $|P_{so}(n+1)-P_{so}(n)| \leq \delta$;
4) Verify: If $R_{th} \geq C_b(\phi_b^*)$ or $\log_2(1 + \rho_c(\phi_b^*, \phi_c^*)) < \tau$ or $\phi_b^* + \phi_c^* \notin [0, 1]$, the edge controller adopts the P2 scheme.
```

where

$$a = \left(\frac{2}{(N-1)\alpha} - 1\right)\phi_{b,min}, \tag{21}$$

$$b = -\frac{2}{\alpha}\left(\frac{1}{1-2^{-R_{th}}} + \frac{1}{N-1}\right)\phi_{b,min}^2 - \left(1 + \frac{2}{(N-1)\alpha}\right)\phi_{b,min}, \tag{22}$$

$$c = \left(1 + \frac{2}{(N-1)\alpha}\right)\phi_{b,min}^2. \tag{23}$$

The extreme point of (19) is the unique root of the cubic equation (20), which is calculated as [38]

$$\vartheta = \sqrt[3]{\chi_1 + \chi_2} + \sqrt[3]{\chi_1 - \chi_2} - \frac{a}{3}, \tag{24}$$

where $\chi_1 = \sqrt{\left(\frac{b}{3} - \frac{a^2}{9}\right)^3 + \chi_2^2}$, and $\chi_2 = \frac{ab}{6} - \frac{c}{2} - \frac{2a^3}{54}$. Next, we analyze when the optimal value of ϕ_b takes the boundary point 1 or the extreme point ϑ. From (19), we can conclude that minimizing SOP is equivalent to minimizing the following function

$$\Omega(\phi_b) = \left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1 + \frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}. \tag{25}$$

The first derivative of $\Omega(\phi_b)$ is expressed as (26), as shown at the bottom of the next page. It is clear that the sign of $\Omega'(\phi_b)$ depends on the sign of $\rho(\phi_b) = \phi_b^3 + a\phi_b^2 + b\phi_b + c$.

The second derivative of $\rho(\phi_b)$ is given by

$$\rho''(\phi_b) = 2\left(3\phi_b + \phi_{b,min}\left(\frac{2}{(N-1)\alpha} - 1\right)\right). \tag{27}$$

Through the analysis of the previous system, we know that $\rho''(\phi_b) > 0$ due to $\phi_b > \phi_{b,min}$ and $-1 < \frac{2}{(N-1)\alpha} - 1 < 0$. Thus, we can conclude that $\rho(\phi_b) > 0$ is a convex function w.r.t. $\phi_b \in (\phi_{b,min}, 1]$. At the two boundary points of the variable interval, the function values of $\rho(\phi_b)$ are $\rho(\phi_{b,min}) = -\frac{2\phi_{b,min}^3}{\alpha(1-2^{-R_{th}})} < 0$ and $\rho(1) = (1-\phi_{b,min})^2 - \frac{2}{\alpha(1-2^{-R_{th}})}\phi_{b,min}^2$, respectively. If $\rho(1) < 0$, i.e., $\frac{1}{1+\sqrt{\frac{2}{\alpha}(1-2^{-R_{th}})}} < \phi_{b,min} < 1$, we infer that $\Omega'(\phi_b) < 0$ in this case. As such, $\phi_b^* = 1$ is the global optimal power allocation, which achieves the minimum SOP. The edge controller utilizes all the power to send secret information-bearing signal. If $\rho(1) \geq 0$, i.e., $0 < \phi_{b,min} \leq \frac{1}{1+\sqrt{\frac{2}{\alpha}(1-2^{-R_{th}})}}$, we obtain that $\Omega(\phi_b)$ first decreases and then increases w.r.t. ϕ_b. In this case, the extreme point ϑ is the global optimal power allocation parameter. In summary, the optimal power allocation ration of ϕ_b is given by

$$\phi_b^* = \begin{cases} 1, \frac{1}{1+\sqrt{\frac{2}{\alpha}(1-2^{-R_{th}})}} < \phi_{b,min} < 1 \\ \vartheta, 0 < \phi_{b,min} \leq \frac{1}{1+\sqrt{\frac{2}{\alpha}\left(1-2^{-R_{th}}\right)}} \end{cases} \tag{28}$$

V. NUMERICAL SIMULATIONS

In this section, we present several representative numerical results to evaluate the effectiveness of the proposed dynamic security mechanism. Moreover, to verify the effectiveness of the proposed adaptive security scheme, the solution that is obtained by the secrecy transmission strategy P2 is also provided for performance comparison. Note that one time random channel realization cannot reflect the effectiveness of the security scheme. In this section, the results are derived by averaging over 100 simulation trails and the related results reflect the overall security performance. The simulation settings are as follows unless otherwise specified: $d_b = 1$ m, $d_c = 2$ m, $\alpha = 2$, $\lambda_E = 2$ nodes/m^2, $N = 10$, $R_{th} = 2$ bps/Hz, and $\tau = 1.2$ bps/Hz.

Fig. 4 investigates the effect of the transmit power P. It is observed that the security performance of the proposed adaptive security scheme coincides well with that of the secure scheme P2 which only focuses on secure transmission. The optimal power allocation of Bob and the SOP first increase and then decrease with transmit power P. When the transmit power is less than -2.3 dB, the edge controller gradually increases the power allocation ratio of the secret signal to resist eavesdropping attack. Meanwhile, at low transmit power (i.e., P <= -1.2 dB), it is very likely that neither secure transmission nor non-confidential transmission meets the system requirements. That is, both multi-service secure transmission scheme P1 and single-service secure transmission scheme P2 are not established. Thus, the edge controller occasionally uses all the power only to transmit non-confidential broadcast service content, which is in line with the third strategy in the adaptive secure transmission mechanism as shown in Fig. 3. Moreover, when $P \leq 12$ dB, the system cannot fulfill the non-confidential service rate requirement. Thus, for enhancing security, the edge controller adopts secure scheme P2 to transmit only confidential signal and artificial noise. Under high power (e.g. 12 dB < P), compared with the single-service transmission scheme P2, the proposed adaptive scheme will provide service for Charlie without secrecy outage, which significantly boosts the energy efficiency and saves energy consumption of the system.

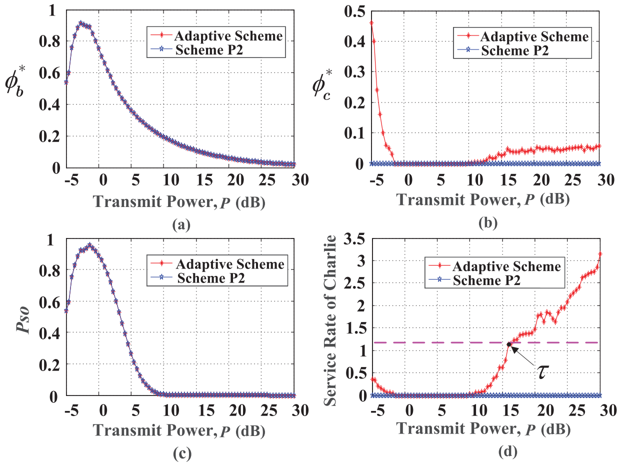


FIGURE 4. System performance and optimal power allocation versus the transmit power *P*.

Fig. 5 shows how the optimal system performance is influenced by the number of edge controller's antennas. It can be shown that the optimal power allocation of Bob and the SOP are both monotonically decreasing with the number of transmit antennas N, which reveals that using more antennas at the edge controller is beneficial for suppressing the array gains at the illegal terminal sides. In other words, more transmit antennas will provide greater array gain to resist passive eavesdropping attack. The service rate of Charlie increases with the number of transmit antennas. Obviously, the advantages of spatial freedom brought by the large antenna array can be used to resist eavesdropping attacks as well as can provide multi-service advantages.

$$\Omega'(\phi_b) = \frac{(1-2^{-R_{th}})\Omega(\phi_b)(\phi_b^3 + a\phi_b^2 + b\phi_b + c)}{\phi_b^2(\phi_b - \phi_{b,min})\left(\phi_{b,min} + (\phi_b - \phi_{b,min})(1-2^{-R_{th}})\frac{1-\phi_b}{\phi_b(N-1)}\right)}. \tag{26}$$

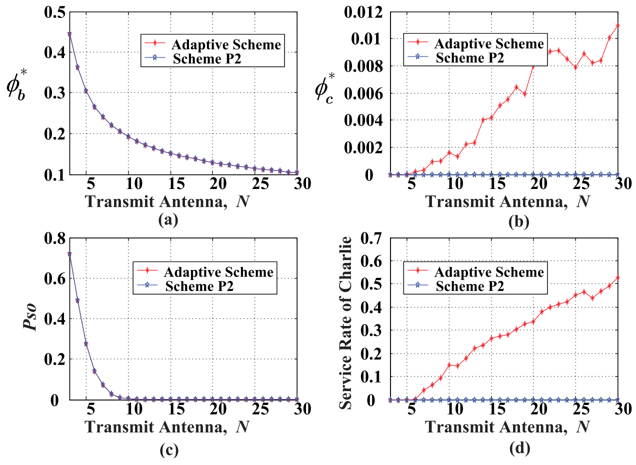


FIGURE 5. System performance and optimal power allocation versus the transmit antenna N, with $P = 10$ dB.

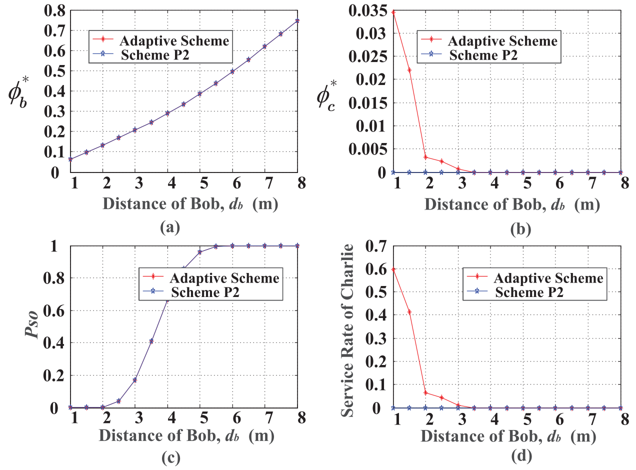


FIGURE 6. System performance and optimal power allocation versus Bob's distance d_b.

Fig. 6 depicts the numerical results on Bob's distance d_b. We find that as the path distance of the main channel increases, the non-confidential signal power allocation ratio and data traffic gradually decrease to zero. As expected, the SOP increases with d_b and the edge controller needs to increase power investment in confidential service to compensate for security losses caused by large-scale path. However, extremely poor main channel quality is not sufficient to ensure secure communication. Therefore, when the distance d_b reaches 5.5 m, security outage definitely occurs.

Fig. 7 describes the impact of the secrecy rate threshold R_{th} on power allocation and service rate. It is observed that with the increase of the security rate threshold R_{th}, the edge controller's power allocation to the confidential service subscriber Bob gradually increases, while the service subscriber Charlie needs to sacrifice his own data transmission, which reveals the inherent unsecure rate and secure trade-off between Bob and Charlie. The SOP decreases with the increase of security rate threshold, which also verifies the correctness of the previous security analysis process. Secrecy rate and secrecy outage probability need to be properly weighed in this case.

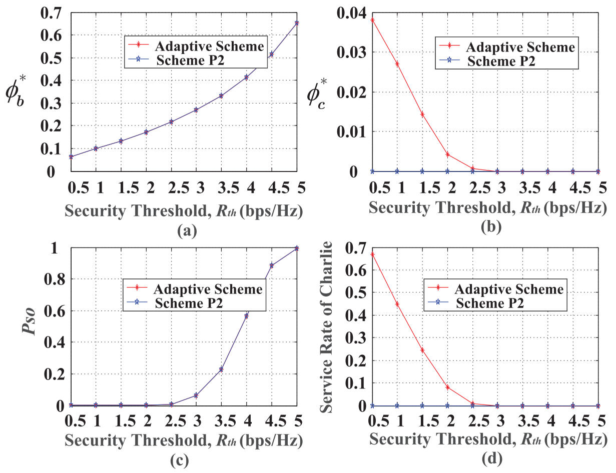


FIGURE 7. System performance and optimal power allocation versus security threshold R_{th}, with $\tau = 0.5$ bps/Hz, $N = 12$, and $P = 10$ dB.

VI. CONCLUSION

In this paper, we investigated an adaptive physical layer security protection mechanism for industrial wireless edge-enabled CPS to fight against randomly distributed malicious sensing devices under the large scale path loss. Introducing AN, we presented that the optimal power allocation and wiretap code rates adaptively adjust to meet various security and data service requirements as well as provided the explicit transmit design for SOP minimization under different cases. The simulation results verified that the proposed adaptive secrecy scheme provides data service for Charlie without increasing secrecy outage and greatly boosts the energy efficiency at high power transmission range, which caters to the concept of green and secure communication.

APPENDIX A
PROOF OF LEMMA 1

We obtain that $\mathbf{w}_b$ and $\mathbf{w}_c$ are mutually independent and uncorrelated, since the entries of $\mathbf{h}_b$ and $\mathbf{h}_c$ are i.i.d. complex random variables satisfying $\mathcal{CN}(\mathbf{0}, 1)$. We can conclude that $X1 = \phi_b P \left|\mathbf{h}_k^H \mathbf{w}_b\right|^2 \sim \mathrm{E}(\lambda_1)$, $X2 = \phi_c P \left|\mathbf{h}_k^H \mathbf{w}_c\right|^2 \sim \mathrm{E}(\lambda_2)$, and $X3 = \frac{\phi_n P}{N-2} \left\|\mathbf{h}_k^H \mathbf{Z}\right\|^2 \sim \Gamma(N-2, \lambda_3)$ where $\lambda_1 = \frac{1}{\phi_b P}$, $\lambda_2 = \frac{1}{\phi_c P}$, and $\lambda_3 = \frac{N-2}{\phi_n P}$. We define $Y = X_2 + X_3$. The probability density function (PDF) of the random variable Y can be derived as

$$
\begin{aligned}
&f_Y(y) \\
&= \int_{-\infty}^{\infty} f_{X_2}(y-x) f_{X_3}(x)\, dx \\
&= \frac{\lambda_2 \lambda_3^{N-2} e^{-\lambda_2 y}}{\Gamma(N-2)} \int_0^y x^{N-3} e^{-(\lambda_3-\lambda_2)x} dx \\
&= \begin{cases} \dfrac{\lambda_2 \lambda_3^{N-2} e^{-\lambda_2 y}}{\Gamma(N-1)} y^{N-2}, \lambda_2 = \lambda_3 \\ \dfrac{\lambda_2 \lambda_3^{N-2} e^{-\lambda_2 y}}{(\lambda_3-\lambda_2)^{N-2}} \left[1 - e^{(\lambda_2-\lambda_3)y} \sum_{k=0}^{N-3} \frac{y^k (\lambda_3-\lambda_2)^k}{k!}\right], \lambda_2 \neq \lambda_3 \end{cases}
\end{aligned} \tag{29}
$$

The cumulative distribution function (CDF) of the k-th illegal terminal is given by

$$\begin{aligned}&F_{\rho_k}(x)\\&=\Pr\left\{\frac{X_1}{d_k^\alpha+Y}<x\right\}\\&=\int_0^\infty\int_0^{x(d_k^\alpha+y)} f_{X_1}(x_1)f_Y(y)dx_1dy\\&=1-\left(1+\frac{\phi_c x}{\phi_b}\right)^{-1}\left(1+\frac{\phi_n x}{\phi_b(N-2)}\right)^{2-N} e^{-\frac{d_k^\alpha x}{\phi_b P}},\end{aligned}\tag{30}$$

where $\beta=\lambda_2\lambda_3^{N-2}(\lambda_3-\lambda_2)^{2-N}e^{-\lambda_1 d_k^\alpha x}$. The CDF of ρ_e is given by

$$\begin{aligned}&F_{\rho_e}(x)\\&=\Pr\left\{\max_{k\in\Phi_E}\rho_k<x\right\}\\&=\mathbb{E}_{\Phi_E}\left[\prod_{k\in\Phi_E}\Pr\{\rho_k<x\}\right]\\&\overset{(a)}{=}\exp\left(-\lambda_E\int_{\mathbb{R}^2}(1-\Pr\{\rho_k<x\})\right)\\&=\exp\left(-2\pi\lambda_E\left(1+\frac{\phi_c x}{\phi_b}\right)^{-1}\left(1+\frac{\phi_n x}{\phi_b(N-2)}\right)^{2-N}\right.\\&\qquad\left.\int_0^\infty re^{-\frac{xr^\alpha}{\phi_b P}}dr\right)\\&=\exp\left(-\mu\phi_b^{\frac{2}{\alpha}}x^{-\frac{2}{\alpha}}\left(1+\frac{\phi_c x}{\phi_b}\right)^{-1}\left(1+\frac{\phi_n x}{\phi_b(N-2)}\right)^{2-N}\right),\end{aligned}\tag{31}$$

where (a) holds for the probability generating functional lemma (PGFL) over PPP [39]. Through the above analysis, SOP is deduced as

$$P_{so}=\Pr\{C_e>C_b-R_s\}=\Pr\{\rho_e>\varepsilon_s\}.\tag{32}$$

Substituting (31) into (32), it is obtained that Lemma 1 is established.

APPENDIX B PROOF OF THEOREM 1

Lemma 3 [40]: The quadratic differentiable function $f(x)$ is a quasi-convex function on $\mathbb{R}$ if and only if

$$f'(x)=0\Rightarrow f''(x)>0.\tag{33}$$

According to (19), we have

$$P'_{so}(\phi_b)=\exp\left(-\mu\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}\right)T(\phi_b),\tag{34}$$

where

$$\begin{aligned}&T(\phi_b)\\&=\frac{2\mu}{\alpha}\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}-1}\frac{2^{-R_{th}}-1}{\varepsilon_b^2}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}\\&\quad-\mu\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{-N}\frac{-2^{-R_{th}}r\phi_b^2-2^{-R_{th}}+1}{\phi_b^2}.\end{aligned}\tag{35}$$

When $P'_{so}(\phi_b)=0$, we have $T(\phi_b)=0$. After some mathematical operations, $P'_{so}(\phi_b)=0$ can be rewritten as

$$\frac{-2^{-R_{th}}r\phi_b^2-2^{-R_{th}}+1}{\phi_b}=\frac{2}{\alpha}\frac{2^{-R_{th}}-1}{\varepsilon_b}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right).\tag{36}$$

The second derivative of the SOP is given by

$$\begin{aligned}P''_{so}(\phi_b)&=-\exp\left(-\mu\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}\right)T(\phi_b)^2\\&\quad+\exp\left(-\mu\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}\right)T'(\phi_b),\end{aligned}\tag{37}$$

where

$$\begin{aligned}&T'(\phi_b)\\&=\frac{2\mu}{\alpha}\left(\frac{2}{\alpha}-1\right)\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}-2}\frac{(2^{-R_{th}}-1)^2}{\varepsilon_b^4}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}\\&\quad-\frac{4\mu}{\alpha}\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}-1}\frac{2^{-R_{th}}-1}{\varepsilon_b^2}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{-N}\\&\quad\times\frac{-2^{-R_{th}}r\phi_b^2-2^{-R_{th}}+1}{\phi_b^2}\\&\quad+\frac{2\mu}{\alpha}\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}-1}\frac{2(1-2^{-R_{th}})2^{-R_{th}}r}{\varepsilon_b^3}\\&\quad\times\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}\\&\quad+\frac{\mu N}{N-1}\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{-1-N}\\&\quad\times\frac{(-2^{-R_{th}}r\phi_b^2-2^{-R_{th}}+1)^2}{\phi_b^4}\\&\quad+\mu\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{-N}\frac{2\phi_b(1-2^{-R_{th}})}{\phi_b^4}.\end{aligned}\tag{38}$$

It is easily verified that the first two terms on the right-hand side of (38) are negative and the remaining three terms are positive. Recalling (36), the first two terms on the right-hand side of the (38) can be organized into the following form:

$$\Xi=-\frac{2\mu}{\alpha}\left(\frac{2}{\alpha}+1\right)\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}-2}\frac{(2^{-R_{th}}-1)^2}{\varepsilon_b^4}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}.\tag{39}$$

According to (36), the fourth term on the right-hand side of (38) can be rewritten as

$$\Psi=\frac{4\mu N}{\alpha^2(N-1)}\left(\frac{\phi_b}{\varepsilon_b}\right)^{\frac{2}{\alpha}-2}\frac{(2^{-R_{th}}-1)^2}{\varepsilon_b^4}\left(1+\frac{\phi_n\varepsilon_b}{\phi_b(N-1)}\right)^{1-N}.\tag{40}$$

Through the above analysis, we can conclude that $P''_{so}(\phi_b)>0$ if $P'_{so}(\phi_b)=0$. Thus, the SOP in (19) is a quasi-convex function on ϕ_b.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their excellent suggestions.

REFERENCES

[1] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 389–425, 1st Quart., 2020.

[2] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018.

[3] B. Bagheri, S. Yang, H.-A. Kao, and J. Lee, "Cyber-physical systems architecture for self-aware machines in industry 4.0 environment," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 1622–1627, 2015.

[4] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-free physical layer authentication based on machine learning for industrial wireless CPS," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6481–6491, Dec. 2019.

[5] S. Rokka Chhetri and M. A. Al Faruque, "Side channels of cyber-physical systems: Case study in additive manufacturing," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 34, no. 4, pp. 18–25, Aug. 2017.

[6] J. Hee Cheon and J. Kim, "A hybrid scheme of public-key encryption and somewhat homomorphic encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 1052–1063, May 2015.

[7] H.-M. Sun, M.-E. Wu, W.-C. Ting, and M. J. Hinek, "Dual RSA and its security analysis," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2922–2933, Aug. 2007.

[8] M. Cao and W. Zhang, "Related-key differential cryptanalysis of the reduced-round block cipher GIFT," *IEEE Access*, vol. 7, pp. 175769–175778, Dec. 2019.

[9] J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, and N. Keller, "Related-key boomerang and rectangle attacks: Theory and experimental analysis," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4948–4966, Jul. 2012.

[10] Z. Liu, B. Sun, Q. Wang, K. Varici, and D. Gu, "Improved zero-correlation linear cryptanalysis of reduced-round camellia under weak keys," *IET Inf. Secur.*, vol. 10, no. 2, pp. 95–103, Mar. 2016.

[11] H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*. New York, NY, USA: Springer-Verlag, Feb. 2013.

[12] J. Tang, H. Wen, K. Zeng, R.-F. Liao, F. Pan, and L. Hu, "Light-weight physical layer enhanced security schemes for 5G wireless networks," *IEEE Netw.*, vol. 33, no. 5, pp. 126–133, Sep. 2019.

[13] X. Shen, Q. Chen, Y. Nie, and K. Gan, "Adaptive secure MIMO transmission mechanism against smart attacker," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–14, Feb. 2020.

[14] M. Letafati, A. Kuhestani, K.-K. Wong, and M. J. Piran, "A lightweight secure and resilient transmission scheme for the Internet-of-Things in the presence of a hostile jammer," *IEEE Internet Things J.*, early access, Sep. 24, 2020, doi: 10.1109/JIOT.2020.3026475.

[15] M. Letafati, A. Kuhestani, and H. Behroozi, "Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2856–2868, Mar. 2020.

[16] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet Things J.*, early access, Nov. 17, 2020, doi: 10.1109/JIOT.2020.3038682.

[17] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737–3749, Jun. 2020.

[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[19] H. Song, H. Wen, L. Hu, S. Chen, Z. Zhang, and R.-F. Liao, "Secure cooperative transmission with imperfect channel state information based on BPNN," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10482–10491, Nov. 2018.

[20] J. Tang, H. Wen, H. Song, T. Zhang, and K. Qin, "On the security–reliability and secrecy throughput of random mobile user in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10635–10649, Oct. 2020.

[21] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[22] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

[23] H. Song, H. Wen, R.-F. Liao, Y. Chen, and S. Chen, "Outage constrained secrecy rate maximization for MIMOME multicast wiretap channels," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 657–660, Jun. 2019.

[24] H. Song, H. Wen, J. Tang, Y. Chen, F. Xie, R.-F. Liao, and S. Chen, "PLS-based secrecy transmission for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7596–7608, Jul. 2020.

[25] W. Mei, Z. Chen, J. Fang, and S. Li, "Physical layer service integration in 5G: Potentials and challenges," *IEEE Access*, vol. 6, pp. 16563–16575, Feb. 2018.

[26] W. Mei, Z. Chen, and J. Fang, "GSVD-based precoding in MIMO systems with integrated services," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1528–1532, Nov. 2016.

[27] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, "On artificial-noise-aided transmit design for multiuser MISO systems with integrated services," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8179–8195, Sep. 2017.

[28] W. Mei, Z. Chen, and S. Li, "Confidential broadcasting and service integration in millimeter wave systems," *IEEE Syst. J.*, vol. 13, no. 1, pp. 147–158, Mar. 2019.

[29] M. Vaezi, Y. Qi, and X. Zhang, "A rotation-based precoding for MIMO broadcast channels with integrated services," *IEEE Signal Process. Lett.*, vol. 26, no. 11, pp. 1708–1712, Nov. 2019.

[30] H. Song, H. Wen, L. Hu, Y. Chen, and R.-F. Liao, "Optimal power allocation for secrecy rate maximization in broadcast wiretap channels," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 514–517, Aug. 2018.

[31] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[32] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505–515, Mar. 2017.

[33] X. Li, D. Li, J. Wan, C. Liu, and M. Imran, "Adaptive transmission optimization in SDN-based industrial Internet of Things with edge computing," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1351–1360, Jun. 2018.

[34] H. Lin, Y. Cao, Y. Zhong, and P. Liu, "Secure computation efficiency maximization in NOMA-enabled mobile edge computing networks," *IEEE Access*, vol. 7, pp. 87504–87512, Jul. 2019.

[35] X. He, R. Jin, and H. Dai, "Physical-layer assisted secure offloading in mobile-edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 4054–4066, Jun. 2020.

[36] M. Moradikia, H. Bastami, A. Kuhestani, H. Behroozi, and L. Hanzo, "Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments," *IEEE Access*, vol. 7, pp. 116942–116964, Aug. 2019.

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

[38] J. M. McNamee, *Numerical Methods for Roots of Polynomials*. Amsterdam, The Netherlands: Elsevier, 2007.

[39] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry Its Applications*. Hoboken, NJ, USA: Wiley, 1996.

[40] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

HUANHUAN SONG received the M.S. and Ph.D. degrees from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC), in 2015 and 2018, respectively. She is currently a Postdoctoral Fellow with the School of Aeronautics and Astronautics, UESTC. Her research interests include cooperation communication, wireless communication security, and artificial intelligence.

HONG WEN (Senior Member, IEEE) received the Ph.D. degree from the Communication and Computer Engineering Department, Southwest Jiaotong University, in 2004. Then, she worked as an Associate Professor with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC), China. From January 2008 to August 2009, she was a Visiting Scholar and a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. She is currently a Professor with UESTC. Her main research interests include wireless communication systems security, artificial intelligence, and edge computing.

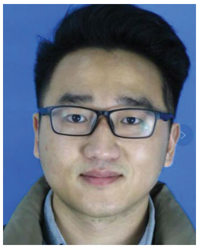
QICONG YANG received the B.S. degree from the Computer and Communication Engineering Department, Southwest Jiaotong University, in 2003. Before August 2016, he mainly engaged in the research of secondary radar (SSR) and tactical data link (TDL) technology. He currently serves as the Deputy Director for the Communication Technology Center and the Sichuan Jiuzhou Electric Group. He is also a Senior Engineer. His main research interests include satellite and wireless communication network technology, communication anti-interference, and secure communication systems.

JIE TANG received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China. He currently holds a postdoctoral position at George Mason University, Fairfax, VA, USA. His main research interests include wireless communications and physical layer security.

YI CHEN (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC), Chengdu, China. His main research interests include physical layer security and smart grid.

TENGYUE ZHANG (Graduate Student Member, IEEE) received the B.Eng. degree in electronic and information engineering from Xinjiang University, Xinjiang, China, in 2016. She is currently pursuing the Ph.D. degree with the School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu, China. Her research interests include wireless communication security, edge computing, and cooperation communication security.

FEIYI XIE (Student Member, IEEE) received the B.Eng. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2012. He is currently pursuing the Ph.D. degree with the University of Electronic Science and Technology of China (UESTC), Chengdu. He is currently engaged in the study of physical layer security and edge computing. His main research interest includes wireless and mobile communications.



SONGLIN CHEN is currently pursuing the Ph.D. degree in communication and information system with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC), Chengdu, China. His main research interests include physical security in wireless communication systems, edge computing, and smart grid.