Physical Layer Security in Large-Scale Random Multiple Access Wireless Sensor Networks: A Stochastic Geometry Approach

Tong-Xing Zheng, *Member, IEEE,* Xin Chen, Chao Wang, *Member, IEEE*, Kai-Kit Wong, *Fellow, IEEE*, and Jinhong Yuan, *Fellow, IEEE*

***Abstract*—This paper investigates physical layer security for a large-scale WSN with random multiple access, where each fusion center in the network randomly schedules a number of sensors to upload their sensed data subject to the overhearing of randomly distributed eavesdroppers. We propose an uncoordinated random jamming scheme in which those unscheduled sensors send jamming signals with a certain probability to defeat the eavesdroppers. With the aid of stochastic geometry theory and order statistics, we derive analytical expressions for the connection outage probability and secrecy outage probability to characterize transmission reliability and secrecy, respectively. Based on the obtained analytical results, we formulate an optimization problem for maximizing the sum secrecy throughput subject to both reliability and secrecy constraints, considering a joint design of the wiretap code rates for each scheduled sensor and the jamming probability for the unscheduled sensors. We provide both optimal and low-complexity sub-optimal algorithms to tackle the above problem, and further reveal various properties on the optimal parameters which are useful to guide practical designs. In particular, we demonstrate that the proposed random jamming scheme is beneficial for improving the sum secrecy throughput, and the optimal jamming probability is the result of trade-off between secrecy and throughput. We also show that the throughput performance of the sub-optimal scheme approaches that of the optimal one when facing a stringent reliability constraint or a loose secrecy constraint.**

***Index Terms*—Physical layer security, wireless sensor networks, random multiple access, outage probability, sum secrecy throughput, stochastic geometry.**

I. Introduction

Wireless sensor networks (WSNs) have drawn prominent research interests from both academia and industry in recent years and have been envisioned as key technologies for Internet-of-Things (IoTs) [1]. With a massive number of sensors deployed in a network, collecting and reporting diverse environmental data to fusion centers (FCs), WSNs show tremendous potential in a variety of applications, including security and battlefield surveillance, disaster alert, industrial automation, traffic management, smart healthcare and homes, etc [2]. However, delivering sensing data over the air is prone to eavesdropping attacks due to the openness of wireless channels. Moreover, it is challenging to employ key-based cryptographic techniques for WSNs, where the distribution, maintenance, and management of secret keys are expensive under dynamic and large-scale topologies. In general, sensors are incapable of implementing complicated cryptographic algorithms due to low energy and computing power [3]. In this context, *physical layer security* [4]–[7] has emerged as an appealing low-complexity paradigm to realize secure transmissions by exploiting wireless media characteristics, and it promises to be a powerful supplement or even alternative to the cryptographic mechanisms for WSNs.

A. Background and Motivations

The research of physical layer security dates back to as early as 1975 when Wyner postulated the information-theoretic foundation in his ground-breaking treatise [8]. Wyner introduced the degraded witetap channel model and showed that

Manuscript received XX XX, 2021; revised XX XX, 20XX; accepted XX XX, 2022. Date of publication XX XX, 2022; date of current version XX XX, 2022. The work of Tong-Xing Zheng and Xin Chen was supported in part by the National Natural Science Foundation of China under Grant 61701390, in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, under Grant 2021D07, in part by the China Postdoctoral Science Foundation under Grants 2021M702631, in part by the Natural Science Basic Research Plan of Shaanxi Province under Grant 2022JM-320, and in part by the Fundamental Research Funds for the Central Universities under Grant xzy012021033. The work of Chao Wang was supported in part by the National Natural Science Foundation of China under Grant 61801518, in part by the Key Research and Development Program of Shaanxi under Grant 2022KW-03, in part by the Defense Industrial Technology Development Program under Grant JCKY2021608B001, in part by the Zhejiang Lab's International Talent Fund for Young Professionals, in part by the China Postdoctoral Science Foundation under Grant 2020M683428, in part by the open research fund of the Ministry of Education Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, and in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, under Grant 2021D06. The work of Kai-Kit Wong was supported in part by the Engineering and Physical Sciences Research Council under Grant EP/T015985/1. The work of Jinhong Yuan was supported in part by the Australia Research Council Discovery Project under Grant DP220103596 and Linkage Project under Grant LP200301482. The associate editor coordinating the review of this paper and approving it for publication was Prof. Sonia Aissa. *(Corresponding authors: Tong-Xing Zheng and Chao Wang.)*

Tong-Xing Zheng and Xin Chen are with the School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China, also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, and also with the Ministry of Education Key Laboratory for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: zhengtx@mail.xjtu.edu.cn, cx0513@stu.xjtu.edu.cn).

Chao Wang is with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: drchaowang@126.com).

Kai-Kit Wong is with the Department of Electronic and Electrical Engineering, University College London, WC1E 6BT London, U.K. (e-mail: kai-kit.wong@ucl.ac.uk).

Jinhong Yuan is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: j.yuan@unsw.edu.au).

the reliability and secrecy of information delivery can be concurrently guaranteed with appropriate secrecy channel coding. This pioneering work has motivated substantial endeavors invested in developing physical layer security during the past decade, from the viewpoints of both information theory and signal processing.

Early research on physical layer security have been more concentrated on point-to-point communication links. Fundamental information-theoretic limits and optimal secrecy signaling schemes have been investigated by exploiting the channel state information (CSI) of both the main channel (spanning from transmitter to the intended receiver) and the wiretap channel (spanning from transmitter to the undesired receiver, or eavesdropper). When the eavesdropper's CSI is completely unavailable, Goel and Negi [9] proposed to radiate controllable artificial noise or jamming signals along with confidential information, through either centralized multiple antennas or distributed cooperative jammers, to degrade the wiretap channel while without impairing the main channel. With no need for the eavesdropper's CSI, the idea of artificial noise or cooperative jamming has opened a new avenue for enhancing physical layer security and has sparked a wave of innovation, e.g, see [10]–[16].

Different from the point-to-point scenarios, secure communications in large-scale wireless networks suffer from severe interference caused by a large amount of concurrent transmissions, and therefore the security performance depends heavily on the network geometry and the locations of nodes in the network. Against this background, stochastic geometry theory has offered powerful tools to study large-scale wireless networks from a statistical point of view by modeling node positions as some spatial distributions like Poisson point process (PPP) [17], and the research on physical layer security under a stochastic geometry framework has been extensively carried out recently. For example, for large-scale ad hoc networks, Zhou *et al.* [18] and Zhang *et al.* [19] respectively explored single- and multi-antenna secure transmissions and identified the tradeoff between reliability and secrecy against eavesdropping attacks. Zheng *et al.* [20], [21] explored the great benefit of full-duplex receiver jamming in enhancing the network-wide secrecy throughput and energy efficiency. For multi-cell cellular networks, Wang *et al.* [22] investigated the secure downlink transmissions and discussed the impact of cell association and the location information of mobile users. Geraci *et al.* [23] further evaluated the achievable secrecy rate with regularized channel inversion precoding under a massive multiple-input multiple-output (MIMO) system. Wang *et al.* [24] comprehensively analyzed the network-wide secrecy for a multi-tier heterogeneous cellular network, where a threshold-based mobile association policy was proposed to balance link quality and secrecy. Wang *et al.* [25] further applied the artificial noise aided physical layer security to the cellular vehicle-to-everything (C-V2X) networks. Interested readers are referred to [26] for a more thorough understanding of the physical layer security in random wireless networks under the stochastic geometry framework.

As mentioned previously, physical layer security is particularly important for WSNs, since employing traditional cryptographic mechanism is rather costly and difficult. Recently, physical layer security has been advocated to protect communications from eavesdropping for WSNs. The majority of existing literature on physical layer security in WSNs has been concentrated on deterministic network geometry, i.e., ignoring the uncertainty of nodes' locations or large-scale path loss [27]–[29]. Given that sensors are generally randomly scattered, Lee *et al.* [30] first introduced the concept of distributed network secrecy and quantified the secrecy throughput and energy consumption for a multilevel WSN using tools from stochastic geometry. Deng *et al.* [31] further analyzed the average secrecy rate for a three-tier WSN. However, these works only considered access technologies with orthogonal resource blocks (RBs).

Random multiple access has the virtue of being highly convenient and flexible without requiring a complicated control scheduling, which is well-suited for the large-scale WSNs particularly when the system load is overly heavy. Although studies of secure multiple access have been reported for various wiretap channel models, the results cannot be directly applied for large-scale WSNs with stochastic network geometry. In recent years, the physical layer security of non-orthogonal multiple access (NOMA) for large-scale networks has received considerable attention, e.g., [32]–[34], but unfortunately, at present researchers have mainly focused on two-user pairing sharing the same RB. In fact, random multiple access with non-orthogonal RBs will significantly hamper the analysis of channel statistics for large-scale WSNs, since we have to deal with the combined effect of channel fading, the random locations of external interfering sensors, as well as the uncertainty of the successive interference cancellation (SIC) based decoding order for internal sensors belong to the same FC. The intractability of analysis will in no doubt make it challenging to design schemes to optimize the network security performance in terms of e.g., sum secrecy throughput. Our research work aims to provide an analytical framework and design schemes to address the aforementioned problem.

B. *Our Work and Contributions*

In this paper, we study physical layer security for a large-scale WSN consisting of randomly deployed sensors and FCs, coexisting with randomly distributed eavesdroppers attempting to intercept the data broadcast by the sensors. We establish a joint analysis and design framework to evaluate the transmission reliability and secrecy and optimize the network-wide performance in terms of the sum secrecy throughput. Our main contributions care summarized as follows:

- We propose a random multiple access strategy which associates each sensor to its nearest FC, and each FC randomly selects a certain number of sensors for data acquisition. We then propose an uncoordinated jamming scheme to combat eavesdropping where those unscheduled sensors, who are not chosen for data collection at the current time slot, independently radiate jamming signals with a certain probability.
- We assume that each FC adopts zero-forcing SIC (ZF-SIC) to decode the multiple streams of the scheduled

sensors, where the decoding order is determined according to their distances to the associated FC. We derive new closed-form expressions for the connection outage probability of a typical FC, leveraging tools from the stochastic geometry theory and order statistics. We also provide analytical expressions for the secrecy outage probability of the typical FC, assuming that eavesdroppers employ the minimum mean square error (MMSE) receiver to demodulate signals and have a powerful multi-user detection capability.

- We formulate a problem of maximizing the sum secrecy throughput of the typical FC, imposing both reliability and secrecy constraints on each scheduled sensor. We jointly design the optimal parameters, including the code rates of the scheduled sensors and the jamming probability of the unscheduled sensors. We also provide a computational-convenient sub-optimal solution by forcing each scheduled sensor to attain a target high level of reliability. We derive closed-form expressions for the optimal code rates, and we prove that the sum secrecy throughput is a quasi-concave function of the jamming probability, where the optimal jamming probability can be efficiently calculated via the bisection method.

C. Organization and Notations

The remainder of this paper is organized as follows. Section II describes the random multiple access WSN and the optimization problem of interest. Section III analyzes the connection and secrecy outage probabilities of the secure transmission of the scheduled sensors. Section IV details the sum secrecy throughput maximization, with both optimal and sub-optimal solutions provided. Section V concludes this paper.

Notations: Bold uppercase (lowercase) letters denote matrices (column vectors). $|\cdot|$, $\|\cdot\|$, $(\cdot)^\dagger$, $(\cdot)^{\mathrm{T}}$, $\ln(\cdot)$, $\mathbb{P}\{\cdot\}$, and $\mathbb{E}_z[\cdot]$ denote the absolute value, Euclidean norm, conjugate, transpose, natural logarithm, probability, and the expectation over a random variable z, respectively. $f_z(\cdot)$ and $\mathcal{F}_z(\cdot)$ denote the probability density function (PDF) and cumulative distribution function (CDF) of z, respectively. $\mathcal{CN}(\mu, v)$, $\mathrm{Exp}(\lambda)$, and $\mathrm{Gamma}(N, \lambda)$ denote the circularly symmetric complex Gaussian distribution with mean μ and variance v, the exponential distribution with parameter λ, and the gamma distribution with parameters N and λ, respectively. $\mathbb{R}^{m\times n}$ and $\mathbb{C}^{m\times n}$ denote the $m \times n$ real and complex number domains, respectively. In addition, $\binom{n}{m} \triangleq \frac{n!}{m!(n-m)!}$ for integers $n > m \geq 0$.

II. Network Model and Problem Description

We consider the issue of secure wireless transmissions for a large-scale WSN as illustrated in Fig. 1, where a large number of sensor nodes continually monitor the surrounding environment and report their observations to the FCs which are responsible for decision making, whilst the ongoing data uploading is overheard by eavesdroppers hiding in the network. We assume that the sensors, FCs, and eavesdroppers are all spatially randomly positioned, and their locations are modeled as independent homogeneous PPPs Φ_s, Φ_c, and Φ_e in a two-dimensional plane $\mathbb{R}^2$, with spatial densities λ_s, λ_c, and λ_e, respectively.[1]

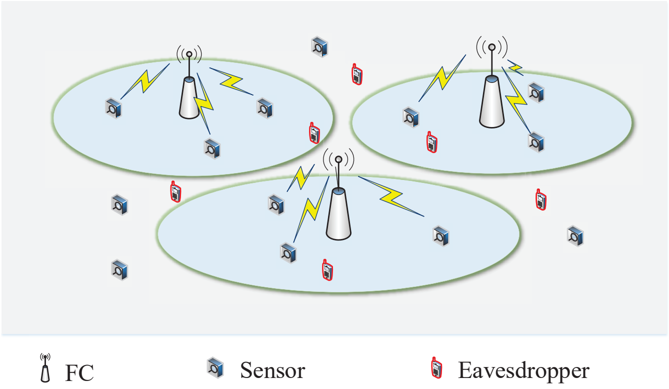


Fig. 1: Illustration of a large-scale security-oriented WSN. A great quantity of FCs are deployed in the network (three FCs in the figure), each of which collects different categories of environmental information from a certain number (three sensor nodes as a group for the same FC in the figure) of near sensors nodes in the presence of numerous randomly located eavesdroppers (six eavesdroppers in the figure).

A. Channel Model

We consider that the sensors are single-antenna devices due to hardware restrictions, and the FCs and eavesdroppers are equipped with M_c and M_e antennas, respectively, for achieving signal enhancement, interference suppression, etc. All the wireless channels are modeled by the combination of a frequency flat Rayleigh fading and a standard distance-based path loss. Hence, the channels from a sensor located at x to an FC located at y and to an eavesdropper located at z are respectively characterized as $\boldsymbol{h}_{y,x} r_{y,x}^{-\alpha/2}$ and $\boldsymbol{g}_{z,x} r_{z,x}^{-\alpha/2}$, respectively. To be specific, $\boldsymbol{h}_{y,x} \in \mathbb{C}^{M_c \times 1}$ and $\boldsymbol{g}_{z,x} \in \mathbb{C}^{M_e \times 1}$ represent the small-scale fading channel vector with independent and identically distributed (i.i.d.) entries obeying the distribution $\mathcal{CN}(0, 1)$, $r_{y,x}$ and $r_{z,x}$ denote the corresponding Euclidean distances, and $\alpha > 2$ is the path-loss exponent.

B. Random Multiple Access

We consider random multiple access scheduling, where each sensor is associated with its nearest FC, and each FC randomly chooses a set of $K < M_c$ sensors for data gathering at a given radio resource. Define $\mathcal{K} \triangleq \{1, 2, \cdots, K\}$. Note that due to the ultra-dense deployment of sensors, we consider a plausible scenario where the density of sensors is much higher than K times the density of FCs, i.e., $\lambda_s \gg K\lambda_c$, and there always exist more than K sensors assigned to the same FC. Under this circumstance, all the sensors in a specific time slot can be naturally divided into two thinned PPPs, namely, the scheduled sensors Φ_a with density $\lambda_a = K\lambda_c$ which are communicating with their associated FCs and the unscheduled sensors Φ_i with density $\lambda_i = \lambda_s - K\lambda_c$ which remain silent, respectively.

[1] Throughout this paper, we have a slight abuse with the notation Φ, which is used to represent the set of nodes' locations as well as the nodes themselves.

C. Uncoordinated Random Jamming

We assume that each FC knows perfectly the instantaneous CSI regarding its K scheduled sensors, whilst only has the statistical CSI of the other sensors and of the eavesdroppers.[2] In order to combat eavesdropping effectively while avoiding bringing severe interference to the FCs, an uncoordinated random jamming scheme is proposed, in which the unscheduled sensors radiate jamming signals at a probability $\rho \in [0,1]$. By doing this, the distribution of the jamming sensors follows a PPP Φ_j with density $\lambda_j = \rho\lambda_i$.

We emphasize that the proposed random jamming scheme is suitable for the energy-limited sensor networks owing to its low-level collaboration. This is fundamentally different from those higher-level collaboration schemes such as coordinated ZF jamming, which will cause high overhead and implementation complexity due to information sharing, beamformer design, and synchronization. Moreover, the jamming probability ρ is carefully designed off line for maximizing the network security performance, as will be discussed in Sec. IV, and hence our scheme can balance well between network performance and complexity.

D. Multi-Stream Decoding

At the FC side, the ZF-SIC method is employed to separate the multiple data streams received from its associated K sensors.[3] Theoretically, the SIC order should be sorted according to the instantaneous received signal strengths from the strongest to the weakest. However, given that the impact of large-scale path loss is generally more dominant on the channel impairment and is more stable compared with the small-scale channel fading, we schedule the SIC order based on the sensors' distances to the FC from the nearest to the farthest. To be more specific, the procedure of ZF-SIC can be described as follows: 1) first decode the signal received from the nearest sensor by removing the aggregated signals received from the $K-1$ farther sensors through projecting these signals on to the null space of the instantaneous channel of the nearest sensor, 2) then cancel the decoded signal from the composite received signals, and 3) successively decode the signal from the second nearest sensor in a similar way, and so on. After the ZF-SIC operation, when decoding the signal from any specific sensor, the FC can successfully eliminate the interfering signals generated by the other $K-1$ sensors.

E. Performance Metrics and Optimization Problem

In order to secure the data transmission, Wyner's secrecy-preserving channel code, generally known as the wiretap code, is employed. In the wiretap code, the rates of the transmitted codewords and the embedded confidential messages are represented by the codeword rate R_t and the secrecy rate R_s, respectively. The rate redundancy $R_e \triangleq R_t - R_s$ is intentionally introduced for guaranteeing secrecy against eavesdropping attacks. If the capacity of the main channel falls below the codeword rate R_t, the desired receiver cannot recover the codeword correctly, which is regarded as connection outage, and the probability that this event happens is termed *connection outage probability* (COP). If the capacity of the wiretap channel exceeds the rate redundancy R_e, perfect secrecy is not possible, which is considered to be secrecy outage, and the probability of this event occurring is referred to as *secrecy outage probability* (SOP).

Without loss of generality, we focus on a typical FC which is placed at the origin o of the polar coordinate, and denote its K scheduled sensors as $S_1, S_2, \cdots, S_K$ with an ascending sort order of their distances. The codeword rate and the secrecy rate of sensor S_k are denoted as $R_{t,k}$ and $R_{s,k}$, respectively, and the corresponding rate redundancy is given by $R_{e,k} = R_{t,k} - R_{s,k}$. The COP of S_k can be defined as

$$p_{co,k} \triangleq \mathbb{P}\{\mathrm{SINR}_{o,k} < \beta_{t,k}\}, \quad \forall k \in \mathcal{K}, \tag{1}$$

where $\mathrm{SINR}_{o,k}$ denotes the instantaneous signal-to-interference-plus-noise ratio (SINR) of the typical FC for resolving the signal from S_k, and $\beta_{t,k} \triangleq 2^{R_{t,k}} - 1$ is the threshold SINR for connection outage.

We consider the wiretap scenario in which the eavesdroppers do not collude with each other and decode messages individually. In this case, a secrecy outage event takes place if only confidential information is leaked to the most threatening eavesdropper of the highest SINR. Therefore, the SOP of S_k can be defined as

$$p_{so,k} \triangleq \mathbb{P}\left\{\max_{e\in\Phi_e} \mathrm{SINR}_{e,k} > \beta_{e,k}\right\}, \quad \forall k \in \mathcal{K}, \tag{2}$$

where $\mathrm{SINR}_{e,k}$ denotes the instantaneous SINR of the eavesdropper located at $e \in \Phi_e$ for intercepting the data from S_k, and $\beta_{e,k} \triangleq 2^{R_{e,k}} - 1$ is the threshold SINR for secrecy outage.

This paper uses the metric *sum secrecy throughput* to assess the capacity of multi-access secure transmissions from the viewpoint of secrecy outage, where the sum secrecy throughput of a typical FC is defined as the total average successfully received confidential information bits from its K scheduled sensors per second per Hertz per channel use subject to certain secrecy constraints. Formally, the sum secrecy throughput can be formulated as

$$\mathcal{T} = \sum_{k=1}^{K} R_{s,k}\left(1 - p_{co,k}\right), \ \text{s.t. } p_{so,k} \le \epsilon, \ \forall k \in \mathcal{K}, \tag{3}$$

where $\epsilon \in [0,1]$ is a prescribed threshold representing the maximal tolerable SOP.

In this paper, we aim to maximize the sum secrecy throughput $\mathcal{T}$ via jointly designing the wiretap code rates for each scheduled sensor (including the codeword rate $R_{t,k}$ and the secrecy rate $R_{s,k}$) and the jamming probability ρ for the unscheduled sensors. Before proceeding to the optimization problem, we will first derive analytical expressions for the COP $p_{co,k}$ and SOP $p_{so,k}$ for $k \in \mathcal{K}$ in the following section.

[2] Theoretically, an FC can obtain the perfect CSI of its scheduled sensors via channel estimation by letting them transmit orthogonal training sequences simultaneously.

[3] ZF is a typical linear filter for multi-user communication systems, and ZF-SIC is commonly used in an NOMA system to achieve SIC due to its ease of implementation and low computational complexity [35], [36]. In this sense, ZF-SIC is more subtable for the large-scale random multiple access WSN compared with more advanced but complicated methods, e.g., MMSE-SIC.

III. Analyses of COP and SOP

This section evaluates the reliability and secrecy performance of the large-scale WSN under investigation with random multiple access. Specifically, we will analyze in detail the COP $p_{co,k}$ and SOP $p_{so,k}$ of the secure transmission from the k-th nearest sensor S_k to the typical FC located at the origin o, utilizing the stochastic geometry theory and order statistics. For ease of notation, we define $\delta \triangleq 2/\alpha$ and $\phi \triangleq \pi\Gamma(1+\delta)\Gamma(1-\delta)$ throughout the paper.

A. General Results for COP

Denote the locations of the K sensors S_k scheduled by the typical FC as s_k for $k \in \mathcal{K}$, with an ascending order of their distances to the FC $L_1 \leq L_2, \cdots, \leq L_K$. Note that due to random multiple access and SIC order scheduling, the ordered distance L_k is a random variable, the statistics of which is characterized by the following lemma.

Lemma 1: The PDF of the ordered distance L_k from the typical FC to the k-th nearest sensor is given by

$$f_{L_k}(r) = 2k\binom{K}{k}\sum_{l=0}^{k-1}\binom{k-1}{l}(-1)^l \pi\lambda_c r e^{-\pi\lambda_c r^2(K-k+l+1)}, \tag{4}$$

Proof: The PDF of L_k follows from order statistics [37],

$$f_{L_k}(r) = k\binom{K}{k}\mathcal{F}_L(r)^{k-1}\left[1-\mathcal{F}_L(r)\right]^{K-k} f_L(r), \tag{5}$$

where $f_L(r) = 2\pi r\lambda_c e^{-\pi\lambda_c r^2}$ and $\mathcal{F}_L(r) = 1 - e^{-\pi\lambda_c r^2}$ are the PDF and CDF of the unordered distance L from a sensor to its nearest FC, respectively. ■

According to the ZF-SIC decoding described in Sec. II-B, the instantaneous SINR of S_k can be formulated as

$$\mathrm{SINR}_{o,k} = \frac{P_a|\boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}|^2 L_k^{-\alpha}}{I_a + I_j + \omega}, \tag{6}$$

where $I_a = \sum_{x\in\Phi_a\setminus o} P_a|\boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{h}_{o,x}|^2 r_{o,x}^{-\alpha}$ denotes the interference generated by those sensors scheduled by the FCs other than the typical FC, $I_j = \sum_{y\in\Phi_j} P_j|\boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{h}_{o,y}|^2 r_{o,y}^{-\alpha}$ denotes the power of the aggregated jamming signal from the unscheduled sensors, with P_a and P_j being the transmit power of the information-bearing signals and the jamming signals, respectively, and ω denotes the power of the receiver noise. Here, $\boldsymbol{w}_k = \frac{\boldsymbol{U}_k^{\dagger}\boldsymbol{U}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}^{\dagger}}{\|\boldsymbol{U}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}^{\dagger}\|}$ denotes the weight vector designed for the k-th sensor as per the ZF-MRC criterion, where $\boldsymbol{U}_k \in \mathbb{C}^{M_c\times M_k}$, with $M_k \triangleq M_c - K + k$, is the projection matrix onto the null space of the matrix $[\boldsymbol{h}_{o,s_{k+1}}, \cdots, \boldsymbol{h}_{o,s_K}]$ such that $\boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_j} = 0$ for $j > k$. Note that the columns of $\boldsymbol{U}_k$ constitute an orthogonal basis, and hence $|\boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}|^2 = \|\boldsymbol{U}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}^{\dagger}\|^2$ and $|\boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{h}_{o,x}|^2$ obey the gamma distribution $\mathrm{Gamma}(M_k, 1)$ and the exponential distribution $\mathrm{Exp}(1)$, respectively.

The COP of sensor S_k is defined in (1) with $\mathrm{SINR}_{o,k}$ given in (6). Note that the COP is affected by various uncertainties, including fading channels, node locations, as well as the decoding order. In the following proposition, we provide an expression for the exact COP.

Proposition 1: The COP of the secure transmission from the k-th nearest sensor S_k to the typical FC is given by

$$p_{co,k} = 1 - \pi\lambda_c k\binom{K}{k}\sum_{l=0}^{k-1}\binom{k-1}{l}\sum_{m=0}^{M_k-1}\sum_{p=0}^{m}\binom{m}{p}\frac{(-1)^l}{m!}\times \left(\frac{\omega\beta_{t,k}}{P_a}\right)^{m-p}\left[\mathbf{1}_{p=0}\Omega_{\frac{m\alpha}{2}} + \mathbf{1}_{p\neq 0}\sum_{n=1}^{p}\left(\delta\phi\lambda_o\beta_{t,k}^{\delta}\right)^n \Omega_\mu \Upsilon_{p,n}\right] \tag{7}$$

where $\mathbf{1}_{\mathcal{H}}$ is the indicator function with $\mathbf{1}_{\mathcal{H}} = 1$ when event $\mathcal{H}$ is true and $\mathbf{1}_{\mathcal{H}} = 0$ otherwise, $\lambda_o \triangleq \lambda_a + (P_j/P_a)^{\delta}\lambda_j$, $\mu = \frac{\alpha}{2}(m-p) + n$, $\Omega_\mu \triangleq \int_0^\infty x^\mu e^{-\tau_1 x^{\alpha/2} - \tau_2 x}dx$ with $\tau_1 = \omega\beta_{t,k}/P_a$ and $\tau_2 = \phi\lambda_o\beta_{t,k}^{\delta} + \pi\lambda_c(K-k+l+1)$, and $\Upsilon_{p,n} \triangleq \sum_{\psi_j\in\mathrm{comb}\binom{p-1}{p-n}}\prod_{\substack{q_{ij}\in\psi_j\\ i=1,\cdots,p-n}}[q_{ij} - \delta(q_{ij} - i + 1)]$, with the convention that $\Upsilon_{p,p} = 1$ for $p \geq 1$. The term $\mathrm{comb}\binom{p-1}{p-n}$ represents the set of all distinct subsets of the natural numbers $\{1, 2, \cdots, p-1\}$ with cardinality $p-n$. The elements in each subset ψ_j are sorted in an ascending order with q_{ij} being the i-th element of ψ_j.

Proof: Please refer to Appendix A. ■

Although (7) seems difficult to analyze due to the existence of the integral term Ω_μ, it provides a general and accurate expression for the COP without requiring time-consuming simulations. More importantly, it can be used as a baseline for comparison with other approximate results. For a special case with $\alpha = 4$, Ω_μ can be simplified by [40, Eq. (3.462.1)] as the following practically closed form,

$$\Omega_\mu^{\alpha=4} = (2\tau_1)^{-\frac{\mu+1}{2}}\Gamma(\mu+1)\exp\left(\frac{\tau_2^2}{8\tau_1}\right)\mathcal{D}_{-\mu-1}\left(\frac{\tau_2}{\sqrt{2\mu_1}}\right), \tag{8}$$

where $\mathcal{D}_{-\mu}(z)$ denotes the parabolic cylinder function [40, Eq. (9.241.2)]. Note that with (8), the new expression of the COP $p_{co,k}$ becomes rather computationally convenient which requires only the calculation or lookup of a $\mathcal{D}_{-\mu}(z)$ value.

B. Interference-Limited Case for COP

Owing to a large amount of uncoordinated concurrent transmissions in the network, the aggregate interference at a receiver generally dominates the thermal noise. Motivated by this fact, we turn to examine the interference-limited WSN by ignoring the receiver noise at the FC side.

The following corollary provides a closed-form expression for the COP $p_{co,k}$ considering the interference-limited case.

Corollary 1: For the interference-limited WSN, the COP of S_k is given by

$$p_{co,k} = 1 - \pi\lambda_c k\binom{K}{k}\sum_{l=0}^{k-1}\binom{k-1}{l}\frac{(-1)^l}{\tau_2}\times \left(1 + \sum_{m=1}^{M_k-1}\sum_{n=1}^{m}\frac{n!}{m!}\left(\frac{\delta\phi\lambda_o\beta_{t,k}^{\delta}}{\tau_2}\right)^n \Upsilon_{m,n}\right). \tag{9}$$

Proof: Please refer to Appendix B. ■

It should be noted that although (9) is in a closed form, the Diophantus equation therein still makes $p_{co,k}$ time-consuming to calculate when M_k goes large. More importantly, the coupling of various parameters, including the number of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2022.3167047, IEEE Transactions on Communications

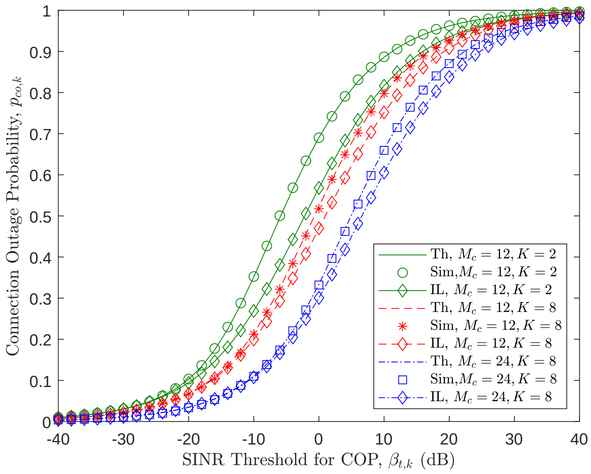


Fig. 2: COP $p_{co,k}$ at $k = 1$ v.s. SINR threshold $\beta_{t,k}$ for different M_c and K, with $P_j = 10$ dBm, $\lambda_c = 0.01$, and $\rho = 0.05$. Unless otherwise specified, we always set $P_a = 10$ dBm, $\omega = 0$ dBm, $\alpha = 4$, and $\lambda_s = 1$. The labels $\{\text{Th, Sim, IL}\}$ refer to the general theoretical result from (7), the Monte-Carlo simulated result, and the interference-limited result from (9), respectively.

scheduled sensors K, the SIC order index k, the number of receive antennas M_k, the COP threshold $\beta_{t,k}$, and the jamming probability ρ, makes $p_{co,k}$ complicated to analyze. In order to circumvent such a difficulty and facilitate the analysis, we focus on a practical requirement of high reliability and low latency. In particular, we examine the secure transmission in the ultra low COP regime for each sensor. Thereby, we obtain a much more compact expression for $p_{co,k}$ in the following corollary.

Corollary 2: In the low COP regime with $p_{co,k} \to 0$, the COP of S_k can be approximated by

$$p_{co,k} \approx \frac{\phi \lambda_o \beta_{t,k}^{\delta}}{\pi \lambda_c} \Lambda_k \Xi_{M_k}, \tag{10}$$

where $\Lambda_k = k\binom{K}{k} \sum_{l=0}^{k-1} \binom{k-1}{l} (-1)^l \frac{1}{(K-k+l+1)^2}$ and $\Xi_{M_k} = 1 + \sum_{m=1}^{M_k-1} \frac{1}{m!} \prod_{i=0}^{m-1} (i - \delta)$.

Proof: Please refer to Appendix C. ■

It is worth noting that by means of the approximation given above, key parameters such as K, k, M_k, $\beta_{t,k}$, and ρ are decoupled compared to (9), and various analytical relationships between the COP and the parameters can be extracted explicitly, some of which are particularly useful for the subsequent optimization of sum secrecy throughput. For example, it is clearly shown that $p_{co,k}$ increases as $\beta_{t,k}$ and ρ become larger, as λ_o is a monotonically increasing function of ρ. Meanwhile, it is as expected that $p_{co,k}$ decreases when M_k grows since $\Xi_{M_k} \in (0, 1)$ is monotonically decreasing with M_k.

Fig. 2 depicts the COP $p_{co,k}$ versus the SINR threshold $\beta_{t,k}$ for different values of the number M_c of FC antennas and the number K of sensor nodes associated with the same FC. Obviously, the Monte-Carlo simulation results are in good agreement with the exact theoretical values. It is expected that $p_{co,k}$ monotonically increases with $\beta_{s,k}$, and the interference-limited results are always smaller than the general ones whereas the gaps are relatively small and even can be negligible as M_c, K, or $\beta_{t,k}$ goes large enough. We can observe that $p_{co,k}$ decreases with a smaller K when M_c is fixed or with a larger M_c for a given K. This indicates that once additional sensor nodes are connected to an FC, the reliability for each sensor node will be degraded, which however can be ameliorated by equipping the FC with more antennas.

C. General Results for SOP

From a robust secure transmission perspective, we are inclined to consider a worst-case scenario by overestimating the wiretap capability of eavesdroppers. Specifically, we assume that the eavesdroppers have powerful multi-stream decoding capabilities such that they can distinguish multiple data streams received from the scheduled sensors through subtracting interference generated by the superposed signals from each other. In this case, the aggregate interference received at the eavesdroppers only consists of the signals emitted by the jamming sensors.

We further assume that the eavesdroppers employ the optimal linear receiver, i.e., the MMSE receiver, to improve the quality of the received signals. According to the MMSE criterion, the weight vector of the eavesdropper located at $e \in \Phi_e$ for decoding the signal from S_k can be devised in the form of [39]

$$\boldsymbol{w}_{e,k} = \left(\boldsymbol{\Psi}_e + \omega \boldsymbol{I}_{M_e}\right)^{-1} \boldsymbol{h}_{e,s_k}, \tag{11}$$

where $\boldsymbol{\Psi}_e \triangleq \sum_{z \in \Phi_j} P_j \boldsymbol{h}_{e,z} \boldsymbol{h}_{e,z}^H r_{e,z}^{-\alpha}$. The SINR of the eavesdropper at e can be given by

$$\mathrm{SINR}_{e,k} = P_a \boldsymbol{h}_{e,s_k}^H \left(\boldsymbol{\Psi}_e + \omega \boldsymbol{I}_{M_e}\right)^{-1} \boldsymbol{h}_{e,s_k} r_{e,s_k}^{-\alpha}. \tag{12}$$

The SOP $p_{so,k}$ of S_k is defined in (2) with $\mathrm{SINR}_{e,k}$ given above. The following proposition provides a general result for $p_{so,k}$.

Proposition 2: The SOP of the secure transmission from the k-th nearest sensor S_k to the typical FC is given by

$$p_{so,k} = 1 - \exp\left(-\pi \lambda_e \sum_{m=1}^{M_e} \sum_{n=0}^{M_e - m} \frac{\zeta_1^{m-1} \zeta_2^n}{(m-1)! n!} \Omega_u^{\circ}\right), \tag{13}$$

where Ω_u° has the same form as Ω_μ defined in Proposition 1 simply with $\mu = u = \frac{\alpha}{2}(m-1) + n$, $\tau_1 = \zeta_1 = \omega \beta_{e,k} / P_a$, and $\tau_2 = \zeta_2 = \phi \lambda_j \left(P_j \beta_{e,k} / P_a\right)^{\delta}$.

Proof: Please refer to Appendix D. ■

Proposition 2 clearly shows that the SOP $p_{so,k}$ exponentially increases with the eavesdropper density λ_e. That is to say, secrecy is severely compromised when facing dense eavesdroppers. Note that for the spacial case of $\alpha = 4$, Ω_u° in (13) can be recast into the same form of (8), which further leads to a practically closed-form expression for the SOP $p_{so,k}$.

D. Interference-Limited Case for SOP

Proposition 2 is not so straightforward for extracting key properties regarding the SOP, which motivates us to seek simplifications. To this end, we consider the interference-limited scenario, just as the discussion for the COP, where the receiver noise at eavesdroppers is ignored. Note that this is

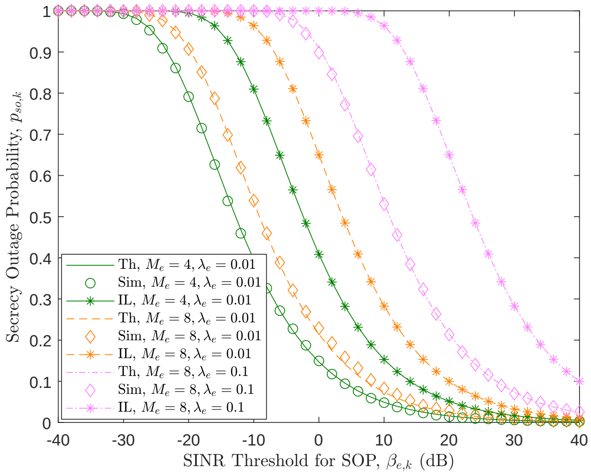


Fig. 3: SOP $p_{so,k}$ at $k = 1$ v.s. SINR threshold $\beta_{e,k}$ for different M_e and λ_e, with $P_j = 10$ dBm, $\lambda_c = 0.01$, $K = 3$, and $\rho = 0.05$. The labels {Th, Sim, IL} refer to the general theoretical result from (13), the Monte-Carlo simulated result, and the interference-limited result from (14), respectively.

reasonable since the noise power of eavesdroppers is typically unknown to the sensors.

In the following corollary, we provide an analytically tractable expression for the SOP.

Corollary 3: For the interference-limited WSN, the SOP of S_k is given by

$$p_{so,k} = 1 - \exp\left(-\frac{\pi\lambda_e M_e}{\phi\rho\lambda_i}\left(\frac{P_a}{P_j\beta_{e,k}}\right)^{\delta}\right). \tag{14}$$

Proof: The result follows easily by plugging $\omega = 0$ into (13) and leveraging some algebraic operations. ∎

Corollary 3 reveals that the SOP $p_{so,k}$ exponentially increases with M_e but decreases with ρ and $\beta_{e,k}$. This indicates that secrecy performance is dramatically degraded if eavesdroppers use a large number M_e of receiving antennas, whereas it can be significantly ameliorated by making a larger fraction ρ of sensors send jamming signals and choosing a larger rate redundancy $R_{e,k}$ for channel coding. Note that this is fundamentally different from the case of COP where increasing the jammer fraction ρ becomes harmful, which reflects an intrinsic trade-off between reliability and secrecy when introducing jamming signals.

The monotonicity of the SOP $p_{so,k}$ w.r.t. the SINR threshold $\beta_{e,k}$, the number M_e of eavesdropping antennas, and the density λ_e of eavesdroppers is validated by both numerical and simulated results as shown in Fig. 3. Different from the situation of COP, the interference-limited SOP is apparently larger than the general one. This implies that the interference-limited SOP embodies an overestimation of eavesdropping capability, which is generally preferred when investigating physical layer security for the purpose of robustness designs.

IV. Maximization of Sum Secrecy Throughput

This section maximizes the sum secrecy throughput for a typical FC in the large-scale WSN with random multiple access, by jointly determining the optimal parameters, including the codeword rate $R_{t,k}$ and the secrecy rate $R_{s,k}$ of the wiretap code for the K scheduled sensors, and the jamming probability ρ of the proposed random jamming scheme. Recalling the definition of sum secrecy throughput in (3), the optimization problem can be formulated as

$$\max_{R_{t,k},R_{s,k},\forall k\in\mathcal{K},\rho} \quad \mathcal{T} = \sum_{k=1}^{K} R_{s,k}\left(1 - p_{co,k}\right) \tag{15a}$$

$$\text{s.t.}\quad p_{co,k} \le \sigma,\ \forall k \in \mathcal{K}, \tag{15b}$$

$$p_{so,k} \le \epsilon,\ \forall k \in \mathcal{K}, \tag{15c}$$

$$0 \le R_{e,k} = R_{t,k} - R_{s,k},\ \forall k \in \mathcal{K}, \tag{15d}$$

$$0 \le \rho \le 1. \tag{15e}$$

Note that constraints (15b) and (15c) describe the reliability and secrecy requirements, respectively; constraints (15d) and (15e) are imposed by the wiretap code scheme and the random jamming scheme, respectively.

The original problem (15) can be decomposed into the following two subproblems.

1) We first design the optimal $R_{s,k}$ and $R_{e,k}$ (or $R_{t,k}$) for the k-th scheduled sensor to maximize its secrecy throughput $\mathcal{T}_k \triangleq R_{s,k}\left(1 - p_{co,k}\right)$ conditioned on a fixed ρ, as

$$\max_{R_{s,k},R_{e,k}} \mathcal{T}_k,\ \forall k \in \mathcal{K},\quad \text{s.t.}\ \ (15\text{b}) - (15\text{d}). \tag{16}$$

2) With the resultant maximal $\mathcal{T}_k$ for $k \in \mathcal{K}$, we then design the optimal ρ to maximize $\mathcal{T}$ expressed in (15), i.e.,

$$\max_{\rho}\ \mathcal{T},\quad \text{s.t.}\ \ (15\text{e}). \tag{17}$$

In the following two subsections, we first discuss an optimal design scheme in which the optimal $R_{s,k}$ and $R_{e,k}$ can be efficiently calculated by the bisection method while the optimal ρ can only be obtained by one-dimensional search. We then examine a sub-optimal scheme for the purpose of a low computational complexity, where closed-form expressions are derived for the optimal $R_{s,k}$ and $R_{e,k}$, and $\mathcal{T}$ is proved to be quasi-concave w.r.t. ρ such that the optimal ρ can be computed using the bisection method.

A. Optimal Design

Based on the above discussion, we first examine the subproblem (16) and design the optimal $R_{e,k}$ and $R_{s,k}$ successively. Consider a fixed $R_{s,k}$, it is apparent from (1) that the COP $p_{co,k}$ monotonically decreases with $R_{e,k}$ as $R_{t,k} = R_{s,k} + R_{e,k}$. This suggests that the optimal $R_{e,k}$ for maximizing $\mathcal{T}_k$ should be the minimal $R_{e,k}$ while satisfying the secrecy constraint $p_{so,k} \le \epsilon$. Note that $p_{so,k}$ decreases with $R_{e,k}$ (since $\beta_{e,k} = 2^{R_{e,k}} - 1$ shown in (2)), the optimal $R_{e,k}$ is given as the inverse of $p_{so,k}(R_{e,k})$ at ϵ, which is

$$R_{e,k}^{*} = p_{so,k}^{-1}(\epsilon). \tag{18}$$

Obviously, $R_{e,k}^{*}$ monotonically decreases with ϵ, which means that a larger rate redundancy is required to combat the eavesdropper in order to meet a more rigorous secrecy constraint. Although it is intractable to express $R_{e,k}^{*}$ in an explicit form due to the complicated expression of $p_{so,k}$, the value of $R_{e,k}^{*}$

can be efficiently obtained through bisection search with the equation $p_{so,k}(R_{e,k}) = \epsilon$.

For designing the optimal $R_{s,k}$, we focus on the low COP regime and substitute the approximate COP $p_{co,k}$ given in (10) into problem (16). Moreover, since $R_{t,k} = R^*_{e,k} + R_{s,k} \Rightarrow \beta_{t,k} = \beta^*_{e,k} + (1+\beta^*_{e,k})\beta_{s,k}$ with $\beta_{s,k} \triangleq 2^{R_{s,k}} - 1$, problem (16) can be equivalently translated into

$$\max_{0\le\beta_{s,k}\le\beta_{s,k}^{\max}} \mathcal{T}_k = \left(1 - A_k\left(\beta_{s,k}+B_k\right)^{\delta}\right)\log_2(1+\beta_{s,k}), \tag{19}$$

where $A_k \triangleq \frac{\phi\lambda_o}{\pi\lambda_c}\Lambda_k\Xi_{M_k}$ with Λ_k and Ξ_{M_k} defined in Corollary 2, $B_k \triangleq \frac{\beta^*_{e,k}}{1+\beta^*_{e,k}}$, and $\beta^{\max}_{s,k} \triangleq A_k^{-\alpha/2} - B_k$. It is noteworthy that $\beta^{\max}_{s,k}$ is introduced to guarantee a non-negative value of $\mathcal{T}_k$. The solution to the above problem is provided by the following proposition.

Proposition 3: The secrecy throughput $\mathcal{T}_k$ given in (19) is a concave function of $\beta_{s,k}$, and the optimal $\beta^*_{s,k}$ maximizing $\mathcal{T}_k$ satisfies the following equation,

$$\frac{d\mathcal{T}_k}{d\beta_{s,k}}\Big|_{\beta_{s,k}=\beta^*_{s,k}} = 0, \tag{20}$$

i.e., it is the unique zero-crossing point $\beta_{s,k}$ of the derivative $\frac{d\mathcal{T}_k}{d\beta_{s,k}}$ given below

$$\frac{d\mathcal{T}_k}{d\beta_{s,k}} = \frac{1 - A_k(\beta_{s,k}+B_k)^{\delta}}{(1+\beta_{s,k})\ln 2} - \frac{A_k\delta\log_2(1+\beta_{s,k})}{(\beta_{s,k}+B_k)^{1-\delta}}. \tag{21}$$

Proof: For brevity, the subscripts of $\beta_{s,k}$, A_k, and B_k are omitted. It is intractable to prove the concavity of $\mathcal{T}_k$ on β by determining the sign of the second-order derivative $\frac{d^2\mathcal{T}_k}{d\beta^2}$. Instead, it can be easily confirmed that the two boundary values of β yield $\frac{d\mathcal{T}_k}{d\beta}|_{\beta=0} > 0$ and $\frac{d\mathcal{T}_k}{d\beta}|_{\beta=\beta^{\max}_{s,k}} < 0$. Combined with the fact that $\mathcal{T}_k$ is continuously differentiable on β, there at least exists one zero-crossing point of $\frac{d\mathcal{T}_k}{d\beta}$. Let β° denote an arbitrary one such that $\frac{d\mathcal{T}_k}{d\beta}|_{\beta=\beta^\circ} = 0$, and then the second-order derivative $\frac{d^2\mathcal{T}_k}{d\beta^2}$ at $\beta = \beta^\circ$ can be calculated as

$$\begin{aligned}
\frac{d^2\mathcal{T}_k}{d\beta^2}\Big|_{\beta=\beta^\circ} &= -\frac{2A\delta(\beta^\circ+B)^{\delta-1}}{(1+\beta^\circ)\ln 2} - \frac{1-A(\beta^\circ+B)^{\delta}}{(1+\beta^\circ)^2\ln 2} + \\
&\qquad A\delta(1-\delta)(\beta^\circ+B)^{\delta-2}\log_2(1+\beta^\circ) \\
&\overset{(a)}{=} \frac{A\delta(\beta^\circ+B)^{\delta-2}}{\ln 2}\Bigg((1-\delta)\ln(1+\beta^\circ) - \\
&\qquad \frac{(\beta^\circ+B)\left[2+\ln(1+\beta^\circ)\right]}{1+\beta^\circ}\Bigg) \\
&\overset{(b)}{<} \frac{A\delta(\beta^\circ+B)^{\delta-2}}{\ln 2}\left(\ln(1+\beta^\circ) - \frac{\beta^\circ\left[1+\ln(1+\beta^\circ)\right]}{1+\beta^\circ}\right) \\
&= \frac{A\delta(\beta^\circ+B)^{\delta-2}}{(1+\beta^\circ)\ln 2}\left[\ln(1+\beta^\circ) - \beta^\circ\right] \\
&\overset{(c)}{\le} 0,
\end{aligned} \tag{22}$$

where (a) holds by noting that $\frac{d\mathcal{T}_k}{d\beta}|_{\beta=\beta^\circ} = 0 \Rightarrow \frac{1-A(\beta^\circ+B)^{\delta}}{(1+\beta^\circ)^2} = A\delta(\beta^\circ+B)^{\delta-1}\ln(1+\beta^\circ)$ in (21), (b) gives an upper bound, and (c) follows from the fact $\ln(1+\beta^\circ) \le \beta^\circ$. The above result indicates that $\mathcal{T}_k$ is a quasi-concave function of β [42], and β° is the unique zero-crossing point of $\frac{d\mathcal{T}_k}{d\beta}$ and is also the solution to problem (19). ■

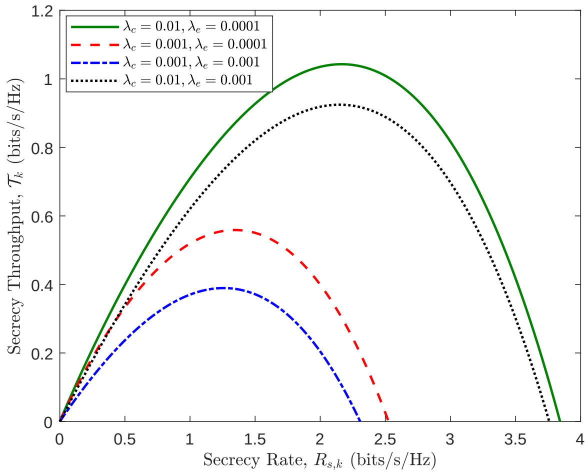


Fig. 4: Secrecy throughput $\mathcal{T}_k$ at $k = 1$ v.s. secrecy rate $R_{s,k}$ for different λ_c and λ_e, with $P_j = 0$ dBm, $\rho = 0.01$, $M_c = 16$, $M_e = 2$, $K = 4$, $\epsilon = 0.1$, and $\sigma = 0.1$.

Due to the quasi-concavity of $\mathcal{T}_k$ on $\beta_{s,k}$, the value of the optimal $\beta^*_{s,k}$ can be efficiently calculated using the bisection method with (20). After that, by substituting the obtained optimal $R^*_{e,k}$ and $R^*_{s,k}$ for $k \in \mathcal{K}$ into (15), the optimal jamming probability ρ^* can be numerically searched by solving problem (17).

Fig. 4 depicts the secrecy throughput $\mathcal{T}_k$ as a function of the secrecy rate $R_{s,k}$. Just as analyzed in Proposition 3, we see that $\mathcal{T}_k$ indeed initially increases and then decreases with $R_{s,k}$, and there is a unique $R_{s,k}$ for maximizing $\mathcal{T}_k$. It is expected that increasing the density λ_e of eavesdroppers is harmful to the improvement of secrecy throughput. We also observe that, with our proposed random access scheme, the secrecy throughput can be dramatically increased with the increase of FC density λ_c. This seemingly counter-intuitive result can be understood if one can realize that although deploying more FCs will accommodate more sensor nodes resulting in more severe network interference, it will reduce the distances between the FC and its associated sensor nodes making transmission reliability significantly enhanced.

B. Sub-optimal Design

Note that the optimal code rates and optimal jamming probability for the optimal design scheme can only be obtained numerically via bisection search or exhaustive search, which not only results in high computational complexity but also makes it difficult to develop useful insights into practical system designs. To this end, this subsection examines a sub-optimal solution to problem (15) by focusing on the sum secrecy throughput with COP constraints $p_{co,k} = \sigma$ and SOP constraints $p_{so,k} = \epsilon$ for $k \in \mathcal{K}$. The corresponding sum secrecy throughput can be written as

$$\mathcal{T} = (1-\sigma)\sum_{k=1}^{K}\log_2\frac{1+\beta^*_{t,k}}{1+\beta^*_{e,k}}, \tag{23}$$

where $\beta_{t,k}^*$ and $\beta_{e,k}^*$ are the unique roots of $\beta_{t,k}$ and $\beta_{e,k}$ of the equations $p_{co,k}(\beta_{t,k}) = \sigma$ and $p_{so,k}(\beta_{e,k}) = \epsilon$, respectively. The rationality of devising the sub-optimal design is that the values of σ and ϵ are generally set small enough to guarantee a high level of reliability and secrecy. Moreover, when the COP and SOP constraints can be controlled, we are able to maximize $\mathcal{T}$ by finding the optimal values of σ and ϵ in (23).

By solving the equations $p_{co,k}(\beta_{t,k}^*) = \sigma$ and $p_{so,k}(\beta_{e,k}^*) = \epsilon$ recalling $p_{co,k}$ in (10) and $p_{so,k}$ in (14), we can provide closed-form expressions for $\beta_{t,k}^*$ and $\beta_{e,k}^*$ (also $R_{t,k}^*$ and $R_{e,k}^*$) by the following proposition.

Proposition 4: The values of $\beta_{t,k}^*$ and $\beta_{e,k}^*$ for $k \in \mathcal{K}$ that satisfy $p_{co,k}(\beta_{t,k}^*) = \sigma$ and $p_{so,k}(\beta_{e,k}^*) = \epsilon$ can be respectively given by

$$\beta_{t,k}^* = \left(\frac{\sigma\pi\lambda_c}{\lambda_a\phi\Lambda_k\Xi_{M_k}}\right)^{\frac{\alpha}{2}}\left[1 + \frac{\lambda_i P_j^\delta}{\lambda_a P_a^\delta}\rho\right]^{-\frac{\alpha}{2}}, \tag{24}$$

$$\beta_{e,k}^* = \frac{P_a\rho^{-\frac{\alpha}{2}}}{P_j}\left(\frac{\pi\lambda_e M_e}{\phi\lambda_i\ln\frac{1}{1-\epsilon}}\right)^{\frac{\alpha}{2}}. \tag{25}$$

The next step is to design the optimal jamming probability ρ to maximize the sum secrecy throughput $\mathcal{T}$. Before proceeding to the optimization procedure, we introduce three auxiliary variables $X_k \triangleq \left(\frac{\sigma\pi\lambda_c}{\lambda_a\phi\Lambda_k\Xi_{M_k}}\right)^{\frac{\alpha}{2}}$, $Y \triangleq \frac{\lambda_i P_j^\delta}{\lambda_a P_a^\delta}$, and $Z \triangleq \frac{P_a}{P_j}\left(\frac{\pi\lambda_e M_e}{\phi\lambda_i\ln\frac{1}{1-\epsilon}}\right)^{\frac{\alpha}{2}}$ for (24) and (25), with which $\mathcal{T}$ in (23) can be recast as a function of a single variable ρ as given below:

$$\mathcal{T} = \sum_{k=1}^K \mathcal{T}_k = (1-\sigma)\sum_{k=1}^K \log_2\frac{1 + X_k(1+Y\rho)^{-\frac{\alpha}{2}}}{1 + Z\rho^{-\frac{\alpha}{2}}}. \tag{26}$$

Remarkably, X_k, Y, and Z have clear physical significance. Specifically, X_k can be interpreted as the ability of boosting the achievable rate for the legitimate channel. For example, a looser COP constraint (a larger σ) and a larger number of receive antennas at the FC side (a smaller Ξ_{M_k}) will increase X_k and are beneficial for improving transmission reliability. Similarly, Z can be translated as the wiretapping capability and Y reflects the jamming power level a sensor can afford.

It is obvious that in order to guarantee a non-negative secrecy throughput for each sensor, i.e., $\mathcal{T}_k \geq 0$ for $k \in \mathcal{K}$, $X_k(1+Y\rho)^{-\frac{\alpha}{2}} > Z\rho^{-\frac{\alpha}{2}}$ must be satisfied from (26), which produces $\rho \geq \left(\left(\frac{X_k}{Z}\right)^\delta - Y\right)^{-1}$. In other words, we should ensure $\rho \geq \rho_{\min} \triangleq \max_{k\in\mathcal{K}}\left(\left(\frac{X_k}{Z}\right)^\delta - Y\right)^{-1}$. Hence, the optimal ρ^* maximizing $\mathcal{T}$ can be obtained by solving the following equivalent problem.

$$\max_{\rho_{\min}\leq\rho\leq 1} T(\rho) \triangleq \sum_{k=1}^K \ln\frac{1 + X_k(1+Y\rho)^{-\frac{\alpha}{2}}}{1 + Z\rho^{-\frac{\alpha}{2}}}. \tag{27}$$

Although the above problem is not convex, in the following proposition we introduce a derivative reconstruction method to prove that $T(\rho)$ is actually first-increasing-then-decreasing w.r.t. ρ such that the optimal ρ^* maximizing $T(\rho)$ must be unique.

Proposition 5: The objective function $T(\rho)$ in (27) initially increases and then decreases with an increasing ρ, and the optimal ρ^* that maximizes $T(\rho)$ is provided as

$$\rho^* = \begin{cases} \rho_{\min}, & Z < \frac{Y\rho_{\min}^{\alpha/2+1}(1-\kappa(\rho_{\min}))}{1+Y\rho_{\min}\kappa(\rho_{\min})} \\ 1, & Z \geq \frac{Y(1-\kappa(1))}{1+Y\kappa(1)} \\ \rho^\circ, & \text{otherwise} \end{cases} \tag{28}$$

where $\kappa(\rho) \triangleq \frac{1}{K}\sum_{k=1}^K \frac{1}{X_k(1+Y\rho)^{-\alpha/2}+1} < 1$, and ρ° is the unique root ρ of the equation $G(\rho) = 0$ with $G(\rho)$ being a monotonically decreasing function of ρ given by

$$G(\rho) = 1 + Y\rho\kappa(\rho) - \frac{Y\rho^{\alpha/2+1}}{Z}(1 - \kappa(\rho)). \tag{29}$$

Proof: Please refer to Appendix E. ■

Some observations regarding the design of the optimal jamming probability ρ^* can be obtained from Proposition 5:

1) As previously explained, the variable Z actually embodies the advantage that eavesdroppers can perform attacks. When such advantage is marginal, i.e., $Z < \frac{Y\rho_{\min}^{\alpha/2+1}(1-\kappa(\rho_{\min}))}{1+Y\rho_{\min}\kappa(\rho_{\min})}$, it is not necessary to activate too many sensors to radiate jamming signals to confuse the eavesdroppers. In this case, we can simply set the optimal ρ^* to its minimal achievable value $\rho_{\min}$. Nevertheless, the maximization of sum secrecy throughput comes at the expense of unfairness, since there exists at least one sensor whose secrecy throughput would be reduced to zero, i.e., the sensor with index $k^\circ = \arg\max_{k\in\mathcal{K}}\left(\left(\frac{X_k}{Z}\right)^\delta - Y\right)^{-1}$.

2) If the eavesdroppers' superiority exceeds a certain level, i.e., $Z \geq \frac{Y(1-\kappa(1))}{1+Y\kappa(1)}$, all the idle sensors have to be mobilized for anti-eavesdropping. Hence, $\rho^* = 1$ is optimal for the sum secrecy throughput maximization.

3) Beyond the above two situations, we should properly set the jamming probability ρ to strike a good balance between throughput and secrecy. Although an explicit form of ρ° cannot be derived, we can still develop some useful properties on ρ° to guideline practical designs, as summarized in the following corollary.

Corollary 4: The optimal jamming probability ρ° decreases with the maximal endurable COP σ and SOP ϵ, the number M_c of antennas at the FC side, the sensor density λ_s, and the ratio P_j/P_a of jamming power to transmit power of a sensor, while increases with the FC density λ_c, the number K of sensors associated with each FC, the eavesdropper density λ_e, and the number M_e of antennas at the eavesdropper side.

Proof: Please refer to Appendix F. ■

Fig. 5 illustrates the secrecy throughput $\mathcal{T}$ as a function of jamming probability ρ for both the optimal and sub-optimal schemes. As proved previously, $\mathcal{T}$ first increases and then decreases as ρ increases, and there exists a unique optimal ρ that maximizes $\mathcal{T}$. We show that as either ϵ or σ becomes larger, the optimal ρ becomes smaller producing a higher $\mathcal{T}$ for both the optimal and sub-optimal schemes, which validates Corollary 4. The reason behind is that facing a looser SOP constraint (a larger ϵ), fewer sensor nodes are required to send jamming signals against eavesdropping; meanwhile, when a

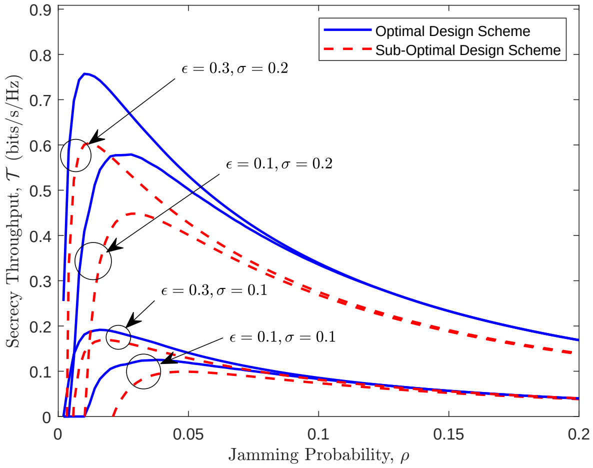


Fig. 5: Secrecy throughput $\mathcal{T}$ v.s. jamming probability ρ for different ϵ and σ, with $P_j = 1$ dBm, $\lambda_c = 0.01$, $M_c = 16$, $K = 4$, $M_e = 2$, and $\lambda_e = 0.0001$.

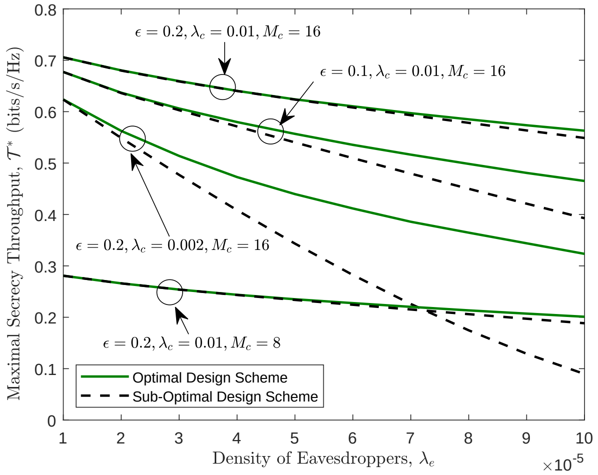


Fig. 6: Maximal secrecy throughput $\mathcal{T}^*$ v.s. eavesdropper density λ_e for different ϵ, λ_c, and M_c, with $P_j = 1$ dBm, $K = 4$, $M_e = 2$, and $\sigma = 0.2$.

larger COP σ can be tolerable, activating less jammers significantly benefits secrecy throughput via supporting a much larger secrecy rate. We find that as ρ increases, the two curves with different ϵ's but identical σ merge. This implies that the jamming probability is sufficiently large to defeat eavesdroppers such that the secrecy throughput performance is less sensitive to the variation of the SOP constraints. It is interesting to observe that the gap between optimal and sub-optimal schemes decreases obviously as the COP threshold σ reduces. This is because for a more stringent COP constraint, the feasible region of the secrecy rate for the optimal scheme shrinks such that the optimal secrecy rate maximizing secrecy throughput approaches that of the sub-optimal scheme.

Fig. 6 plots the maximal secrecy throughput $\mathcal{T}^*$ of both optimal and sub-optimal schemes. It is easy to understand that $\mathcal{T}^*$ decreases with increasing density λ_e of eavesdroppers and grows with increasing SOP threshold ϵ, density λ_c of FCs, and number M_c of antennas at the FC side. We also show that the gap between the optimal and sub-optimal schemes decreases as ϵ or λ_c increases or as λ_e decreases. The underlying reason is that for these situations, adopting a larger secrecy rate can be more beneficial for maximizing secrecy throughput even sacrificing the reliability. This would make the resultant COP for the optimal scheme approach the COP threshold σ which is the COP for the sub-optimal case, and hence the secrecy throughput performance for the two schemes becomes similar.

V. Conclusions

Physical layer security was investigated for a large-scale WSN with random multiple access under a stochastic geometry framework. An uncoordinated jamming scheme was devised to thwart the randomly distributed eavesdroppers. Analytical expressions were derived for both the COP and SOP of the secure data delivery from sensors to a typical FC against eavesdropping. Afterwards, the optimal wiretap code rates and the jamming probability were jointly designed to maximize the sum secrecy throughput subject to both COP and SOP constraints, with both optimal and sub-optimal algorithms examined. Furthermore, some insights into how the optimal parameters should be adjusted to the communication environment and performance requirements were provided. Numerical results were presented to validate the theoretical fundings. In particular, it was shown that for a stringent COP constraint or a loose SOP constraint, the performance gap between optimal and sub-optimal schemes becomes insignificant meaning that the sub-optimal scheme can be adopted as a low-complexity alternative to the optimal one.

Appendix

A. Proof of Proposition 1

Let $s \triangleq \frac{\beta_{t,k} L_k^\alpha}{P_a}$ and $I = I_a + I_j$, the COP $p_{co,k}$ can be computed by substituting (6) into (1),

$$\begin{aligned} p_{co,k} &= 1 - \mathbb{E}_{L_k}\mathbb{E}_I\left[\mathbb{P}\left\{\|\boldsymbol{U}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}^{\dagger}\|^2 \geq s(I+\omega)\right\}\right] \\ &\overset{\text{(a)}}{=} 1 - \mathbb{E}_{L_k}\mathbb{E}_I\left[e^{-s(I+\omega)}\sum_{m=0}^{M_k-1}\frac{s^m(I+\omega)^m}{m!}\right] \\ &= 1 - \mathbb{E}_{L_k}\left[e^{-s\omega}\sum_{m=0}^{M_k-1}\sum_{p=0}^{m}\binom{m}{p}\frac{\omega^{m-p}s^m}{m!}\mathbb{E}_I\left[I^p e^{-sI}\right]\right] \\ &\overset{\text{(b)}}{=} 1 - \mathbb{E}_{L_k}\left[e^{-s\omega}\sum_{m=0}^{M_k-1}\sum_{p=0}^{m}\binom{m}{p}\frac{\omega^{m-p}s^m}{(-1)^p m!}\frac{d^p}{ds^p}\mathcal{L}_I(s)\right], \end{aligned} \tag{30}$$

where (a) is due to $\|\boldsymbol{U}_k^{\mathrm{T}}\boldsymbol{h}_{o,s_k}^{\dagger}\|^2 \sim \mathrm{Gamma}(M_k, 1)$, and (b) follows from the Laplace transform property $t^n f(t) \overset{\mathcal{L}}{\leftrightarrow} (-1)^n \frac{d^n}{ds^n}\mathcal{L}_{f(t)}(s)$. Due to the independence of I_a and I_j, the Laplace transform $\mathcal{L}_I(s)$ can be expressed as [17, eqn. (8)]

$$\begin{aligned} \mathcal{L}_I(s) &= \mathbb{E}_{I_a+I_j}\left[e^{-s(I_a+I_j)}\right] = \mathcal{L}_{I_a}(s)\mathcal{L}_{I_j}(s) \\ &= e^{-\phi\left(\lambda_a P_a^\delta + \lambda_j P_j^\delta\right)s^\delta} = e^{-\phi\lambda_o(P_a s)^\delta}, \end{aligned} \tag{31}$$

where $\lambda_o = \lambda_a + (P_j/P_a)^{\delta}\lambda_j$. The p-order derivative $\frac{d^p}{ds^p}\mathcal{L}_I(s)$ can be obtained by [38, Eq. (51)]

$$\frac{d^p}{ds^p}\mathcal{L}_I(s) = \frac{e^{-\phi\lambda_o(P_a s)^{\delta}}}{(-s)^p}\sum_{n=1}^{p}\left[\delta\phi\lambda_o(P_a s)^{\delta}\right]^n \Upsilon_{p,n}. \quad (32)$$

Substituting (32) into (30) with $s = \beta_{t,k}L_k^{\alpha}/P_a$ yields

$$\begin{aligned} p_{co,k} =& 1 - \sum_{m=0}^{M_k-1}\sum_{p=0}^{m}\binom{m}{p}\left(\frac{\omega\beta_{t,k}}{P_a}\right)^{m-p}\sum_{n=1}^{p}\frac{\left(\delta\phi\lambda_o\beta_{t,k}^{\delta}\right)^n}{m!} \\ & \Upsilon_{p,n}\underbrace{\mathbb{E}_{L_k}\left[L_k^{\alpha(m-p)+2n}e^{-\frac{\omega\beta_{t,k}}{P_a}L_k^{\alpha}-\phi\lambda_o\beta_{t,k}^{\delta}L_k^2}\right]}_{\mathcal{I}_k}. \quad (33) \end{aligned}$$

The term $\mathcal{I}_k$ in (33) can be calculated as

$$\begin{aligned} \mathcal{I}_k =& \int_0^{\infty} r^{\alpha(m-p)+2n}e^{-\frac{\omega\beta_{t,k}}{P_a}r^{\alpha}-\phi\lambda_o\beta_{t,k}^{\delta}r^2}f_{L_k}(r)dr \\ \overset{(a)}{=}& \pi\lambda_c k\binom{K}{k}\sum_{l=0}^{k-1}\binom{k-1}{l}(-1)^l\underbrace{\int_0^{\infty}x^{\mu}e^{-\tau_1 x^{\alpha/2}-\tau_2 x}dx}_{\Omega_{\mu}}, \end{aligned} \quad (34)$$

where (a) follows from invoking the PDF $f_{L_k}(r)$ of L_k given in (4) along with the substitution $r^2 \to x$. The proof can be completed after discussing the cases $p = 0$ and $p \neq 0$.

B. Proof of Corollary 1

Plugging $\omega = 0$ into (7) yields

$$\begin{aligned} p_{co,k} =& 1 - \pi\lambda_c k\binom{K}{k}\sum_{l=0}^{k-1}\binom{k-1}{l}\sum_{m=0}^{M_k-1}\frac{(-1)^l}{m!}\times \\ & \left[\mathbf{1}_{m=0}\Omega_0 + \mathbf{1}_{m\neq 0}\sum_{n=1}^{m}\left(\delta\phi\lambda_o\beta_{t,k}^{\delta}\right)^n\Omega_n\Upsilon_{m,n}\right]. \quad (35) \end{aligned}$$

Recalling Ω_{μ} defined in Proposition 1, it is easy to obtain that $\Omega_0 = 1/\tau_2$ and $\Omega_n = n!/\tau_2^{n+1}$. Then, the proof is completed.

C. Proof of Corollary 2

To begin with, let us revisit $p_{co,k}$ in (30) and plug (32) with $s = \beta_{t,k}L_k^{\alpha}/P_a$ and $\omega = 0$ into (30). Then we obtain

$$\begin{aligned} p_{co,k} =& 1 - \mathbb{E}_{L_k}\left[\sum_{m=0}^{M_k-1}\frac{(-s)^m}{m!}\frac{d^m}{ds^m}\mathcal{L}_I(s)\right] = 1- \\ & \mathbb{E}_{L_k}\left[\underbrace{e^{-\psi_k\beta_{t,k}^{\delta}}\left(1+\sum_{m=1}^{M_k-1}\sum_{n=1}^{m}\frac{\left(\delta\psi_k\beta_{t,k}^{\delta}\right)^n}{m!}\Upsilon_{m,n}\right)}_{\mathcal{Q}_k}\right], \quad (36) \end{aligned}$$

where $\psi_k = \phi\lambda_o L_k^2$. We observe that as $\psi_k \to 0$, the term $\mathcal{Q}_k \to 1$ for any L_k, which finally leads to $p_{co,k} \to 0$. Note that the asymptotic region $\psi_k \to 0$ reflects all possible situations where parameters including but not limited to λ_c, λ_j, P_j, and L_k may produce a sufficiently small COP $p_{co,k}$. Invoking the first-order Taylor expansion with $e^{-\psi_k\beta_{t,k}^{\delta}}$ in (36) around $\psi_k = 0$ and discarding the high order terms $\mathcal{O}\left(\psi_k^2\right)$, $p_{co,k}$ is simplified as

$$\begin{aligned} p_{co,k} &\approx 1 - \mathbb{E}_{L_k}\left[1 - \psi_k\beta_{t,k}^{\delta}\Xi_{M_k}\right] \\ &= \mathbb{E}_{L_k}\left[\phi\lambda_o L_k^2\beta_{t,k}^{\delta}\Xi_{M_k}\right], \quad (37) \end{aligned}$$

with Ξ_{M_k} defined in Corollary 2. Computing the above expectation by invoking (4) gives the result in (10).

D. Proof of Proposition 2

The SOP defined in (2) can be rewritten cas

$$\begin{aligned} p_{so,k} =& 1 - \mathbb{E}_{\Phi_e}\left[\prod_{e\in\Phi_e}\mathbb{P}\left\{\mathrm{SINR}_{e,k} < \beta_{e,k}|\Phi_e\right\}\right] \\ \overset{(a)}{=}& 1 - \exp\left(-\lambda_e\int_0^{\infty}\int_0^{2\pi}\mathbb{P}\left\{\mathrm{SINR}_{e,k} \geq \beta_{e,k}\right\}rd\theta dr\right), \end{aligned} \quad (38)$$

where $\mathrm{SINR}_{e,k}$ is given by (12) with $r \triangleq r_{e,s_k}$, and (a) follows from the probability generating functional (PGFL) over a PPP [41].

Defining $v \triangleq r^{\alpha}\beta_{e,k}/P_a$, then $\mathbb{P}\left\{\mathrm{SINR}_{e,k} \geq \beta_{e,k}\right\}$ in (38) can be calculated by invoking [39, Eq. (11)], i.e.,

$$\mathbb{P}\left\{\mathrm{SINR}_{e,k} \geq \beta_{e,k}\right\} = e^{-\omega v}\sum_{m=1}^{M_e}\frac{(\omega v)^{m-1}}{(m-1)!}\mathbb{E}_{\Phi_j}\left[A_m(v)\right], \quad (39)$$

where $A_m(v) = \frac{\sum_{n=0}^{M_e-m}c_n v^n}{\prod_{z\in\Phi_j}\left(1+P_j r_{e,z}^{-\alpha}v\right)}$ with c_n being the coefficient of v^n in $\prod_{z\in\Phi_j}\left(1+P_j r_{e,z}^{-\alpha}v\right)$, which is

$$c_n = \frac{1}{n!}\sum_{\mathcal{Z}_n\subset\Phi_j}\prod_{i=1}^{n}\frac{P_j}{r_{e,z_i}^{\alpha}}, \quad (40)$$

where $\mathcal{Z}_n \triangleq \{z_1, \cdots, z_n\}$ denotes an arbitrary subset of n points selected from Φ_j. Substituting (40) into $A_m(v)$ yields

$$\mathbb{E}_{\Phi_j}\left[A_m(v)\right] = \sum_{n=0}^{M_e-m}\frac{1}{n!}\underbrace{\mathbb{E}_{\Phi_j}\left[\sum_{\mathcal{Z}_n\in\Phi_j}\frac{P_j^n v^n\prod_{i=1}^{n}r_{e,z_i}^{-\alpha}}{\prod_{z\in\Phi_j}\left(1+P_j r_{e,z}^{-\alpha}v\right)}\right]}_{\mathcal{C}}. \quad (41)$$

Invoking Campbell-Mecke theorem [41, Theorem 4.2] with the term $\mathcal{C}$ in (41) gives

$$\begin{aligned} \mathcal{C} =& \left(2\pi\lambda_j\int_0^{\infty}\frac{\vartheta}{1+\vartheta}tdt\right)^n\exp\left(-2\pi\lambda_j\int_0^{\infty}\frac{\vartheta}{1+\vartheta}tdt\right) \\ \overset{(a)}{=}& \left(\phi\lambda_j P_j^{\delta}v^{\delta}\right)^n\exp\left(-\phi\lambda_j P_j^{\delta}v^{\delta}\right), \quad (42) \end{aligned}$$

where $\vartheta \triangleq P_j v t^{-\alpha}$, and (a) stems from [40, Eq. (3.241.2)]. Substituting (41) with (42) into (39) and plugging the result into (38), the proof can be completed after some algebraic operations.

E. Proof of Proposition 5

We begin with re-expressing the objective function $T(\rho)$ in (27) as $T(\rho) = \sum_{k=1}^{K} T_k(\rho) = \sum_{k=1}^{K} \ln \frac{W_k(\rho)}{Q(\rho)}$, where $W_k(\rho) = 1 + X_k(1+Y\rho)^{-\frac{\alpha}{2}}$ and $Q(\rho) = 1 + Z\rho^{-\frac{\alpha}{2}}$. For simplicity, we use the notations T, T_k, W_k, and Q, which are functions of ρ by default. The derivative $\frac{dT}{d\rho}$ can be calculated as

$$\begin{aligned}\frac{dT}{d\rho} &= \sum_{k=1}^{K} \frac{1}{W_k Q}\left(Q\frac{dW_k}{d\rho} - W_k\frac{dQ}{d\rho}\right)\\ &\overset{\text{(a)}}{=} \sum_{k=1}^{K} \frac{1}{W_k Q}\left(-\frac{\alpha Y(W_k-1)Q}{2(1+Y\rho)} + \frac{\alpha(Q-1)W_k}{2\rho}\right)\\ &= \frac{\alpha}{2}\left(\frac{K(Q-1)}{\rho Q(1+Y\rho)} - \sum_{k=1}^{K}\frac{Y(W_k-Q)}{QW_k(1+Y\rho)}\right), \end{aligned} \tag{43}$$

where (a) follows from the following two derivatives

$$\frac{dW_k}{d\rho} = -\frac{\alpha}{2}X_k(1+Y\rho)^{-\alpha/2-1}Y = -\frac{\alpha}{2}\frac{Y(W_k-1)}{1+Y\rho}, \tag{44}$$

$$\frac{dQ}{d\rho} = -\frac{\alpha}{2}Z\rho^{-\alpha/2-1} = -\frac{\alpha(Q-1)}{2\rho}. \tag{45}$$

It is difficult to prove the concavity of T w.r.t. ρ by directly judging the monotonicity of $\frac{dT}{d\rho}$ from (43). In order to circumvent this issue, we reconstruct $\frac{dT}{d\rho}$ as below and resort to exploring the properties of its sign,

$$\frac{dT}{d\rho} = \frac{\alpha K(Q-1)}{2\rho Q(1+Y\rho)}\left(\underbrace{1 - \sum_{k=1}^{K}\frac{Y\rho(W_k-Q)}{KW_k(Q-1)}}_{G(\rho)}\right). \tag{46}$$

Clearly, the first term $\frac{\alpha K(Q-1)}{2\rho Q(1+Y\rho)}$ in (46) is constantly positive, and therefore the sign of $\frac{dT}{d\rho}$ is solely determined by that of the second term $G(\rho)$ which unfortunately is intuitively elusive. To this end, we turn to examine the monotonicity of $G(\rho)$ on ρ before determining its sign. Specifically, we rewrite $G(\rho)$ as $G(\rho) = 1 - \sum_{k=1}^{K} G_{1,k}(\rho)G_{2,k}(\rho)$ with $G_{1,k}(\rho) \triangleq \frac{Y\rho}{KW_k}$ and $G_{2,k}(\rho) \triangleq \frac{W_k - Q}{Q-1}$. Since both W_k and Q are decreasing functions of ρ, we can easily prove that $G_{1,k}(\rho)$ increases with ρ. Substituting W_k and Q into $G_{2,k}(\rho)$ yields $G_{2,k}(\rho) = \frac{X_k}{Z}\left(\rho^{-1}+Y\right)^{-\alpha/2} - 1$, which also increases with ρ. Consequently, $G(\rho)$ is a monotonically decreasing function of ρ. This result significantly facilitates the derivation of the optimal ρ^* that maximizes T by differentiating the following cases.

1) Case $G(\rho_{\min}) < 0$: Since $G(\rho)$ monotonically decreases with ρ, in this case $G(\rho)$ or $\frac{dT}{d\rho}$ keeps negative within $\rho \in [\rho_{\min}, 1]$. This indicates that T is a decreasing function of ρ, and the optimal ρ^* reaching the maximal T is $\rho^* = \rho_{\min}$. The condition $G(\rho_{\min}) < 0$ can be equivalently transformed as below by plugging $\rho = \rho_{\min}$ into $G(\rho)$,

$$\begin{aligned} G(\rho_{\min}) = 1 - \sum_{k=1}^{K}\frac{Y\rho_{\min}}{KZ}\frac{X_k\left(Y+1/\rho_{\min}\right)^{-\alpha/2} - Z}{X_k\left(1+Y\rho_{\min}\right)^{-\alpha/2}+1} < 0\\ \Leftrightarrow Z < \frac{Y\rho_{\min}^{\alpha/2+1}\left(1-\kappa(\rho_{\min})\right)}{1+Y\rho_{\min}\kappa(\rho_{\min})}. \end{aligned} \tag{47}$$

2) Case $G(1) \geq 0$: Again, due to the monotonically-decreasing feature of $G(\rho)$ on ρ, in this case $G(\rho)$ or $\frac{dT}{d\rho}$ maintains positive within $\rho \in [\rho_{\min}, 1]$. In other words, T monotonically increases with ρ and is maximized at $\rho = 1$. Following (47), the condition $G(1) \geq 0$ is equivalent to $Z \geq \frac{Y(1-\kappa(1))}{1+Y\kappa(1)}$.

3) Case $G(1) < 0 \leq G(\rho_{\min})$: In this case, as ρ increases from $\rho_{\min}$ to 1, $G(\rho)$ or $\frac{dT}{d\rho}$ is initially positive and then becomes negative, which implies T first increases and then decreases with an increasing ρ, and there exists a unique peak value of T. Obviously, the maximal T is obtained when ρ arrives at the zero-crossing point of $G(\rho)$ or $\frac{dT}{d\rho}$.

By now, the proof is completed.

F. Proof of Corollary 4

The results provided by Corollary 4 can be obtained by examining the derivatives of ρ° on the variables X_k, Y, and Z, respectively, invoking the derivative rule for implicit functions with the equation $G(\rho^\circ) = 0$ with $G(\rho)$ defined in (29) [10].

To begin with, the derivative $\frac{d\rho^\circ}{dX_k}$ can be calculated as

$$\frac{d\rho^\circ}{dX_k} = -\frac{\partial G(\rho^\circ)/\partial X_k}{\partial G(\rho^\circ)/\partial \rho^\circ}. \tag{48}$$

It is easy to see that $\frac{\partial G(\rho^\circ)}{\partial \rho^\circ} < 0$ since $G(\rho)$ is a decreasing function of ρ. Besides, as $\kappa(\rho^\circ)$ is a decreasing function of X_k and at the same time $G(\rho^\circ)$ increases with $\kappa(\rho^\circ)$, we have $\frac{\partial G(\rho^\circ)}{\partial X_k} < 0$, which yields $\frac{d\rho^\circ}{dX_k} < 0$. Similarly, we can readily show $\frac{d\rho^\circ}{dZ} > 0$. We can also prove that $\frac{d\rho^\circ}{dY} < 0$ by noting that

$$\frac{\partial G(\rho^\circ)}{\partial Y} = \rho^\circ\kappa(\rho^\circ) - \frac{(\rho^\circ)^{\alpha/2+1}\left(1-\kappa(\rho^\circ)\right)}{Z} \overset{\text{(a)}}{=} -\frac{1}{Y} < 0, \tag{49}$$

where (a) follows from $G(\rho^\circ) = 0$. After obtaining the above results, the proof can be completed by simply determining the relationships between the key parameters $\{\sigma, \epsilon, M_c, \lambda_s, P_j/P_a, \lambda_c, K, \lambda_e, M_e\}$ and the auxiliary variables $\{X_k, Y, Z\}$. Due to space limitation, we just take the SOP threshold ϵ as an example, where we observe that Z decreases with ϵ and meanwhile $\frac{d\rho^\circ}{dZ} > 0$ such that $\frac{d\rho^\circ}{d\epsilon} < 0$.

References

[1] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Int. Things J.*, vol. 3, no. 1, pp. 70–95, Feb. 2016.

[2] N.-S. Vo, T. Q. Duong, M. Guizani, and A. Kortun, "5G optimized caching and downlink resource sharing for smart cities," *IEEE Access*, vol. 6, pp. 31457–31468, May 2018.

[3] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, Second Quarter 2009.

[4] K. N. Le (ed.), *Physical Layer Security*. Cham, Switzerland: Springer, Jan. 2021.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2022.3167047, IEEE Transactions on Communications

[5] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

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

[10] 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.

[11] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[12] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4457–4462, May 2017.

[13] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

[14] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, "Three artificial noise-aided secure transmission schemes in wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3669–3673, Apr. 2018.

[15] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, "Secure cooperative communications with an untrusted relay: A NOMA-inspired jamming and relaying approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3191–3205, Dec. 2019.

[16] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. K. Ng, G. Zhang, J. Tang, and O. A. Dobre, "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476–4489, Jul. 2020.

[17] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[18] X. Zhou, R. Ganti, J. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[19] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[20] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017

[21] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[22] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[23] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[24] 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.

[25] C. Wang, Z. Li, X.-G. Xia, J. Shi, J. Si, and Y. Zou, "Physical layer security enhancement using artificial noise in cellular vehicle-to-everything (C-V2X) networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15253–15268, Dec. 2020.

[26] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, Oct. 2016.

[27] S. Marano, V. Matta, and P. K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 1976–1986, May 2009.

[28] R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-layer security for distributed detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1118–1126, Aug. 2012.

[29] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 839–850, May 2014.

[30] J. Lee, A. Conti, A. Rabbachin, and M. Z. Win, "Distributed network secrecy," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1889–1900, Sep. 2013.

[31] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

[32] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[33] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan. "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70422–70435, 2019.

[34] S. Zhang, X. Xu, H.-M. Wang, J. Peng, D. Zhang, and K. Huang, "Enhancing the physical layer security of uplink non-orthogonal multiple access in cellular Internet of Things," *IEEE Access*, vol. 6, pp. 58405–58417, 2018.

[35] K. Jiang, T. Jing, F. Zhang, Y. Huo, and Z. Li, "ZF-SIC based individual secrecy in SIMO multiple access wiretap channel," *IEEE Access*, vol. 5, pp. 7244–7253, 2017.

[36] K. Jiang, T. Jing, Y. Huo, F. Zhang, and Z. Li, "SIC-based secrecy performance in uplink NOMA multi-eavesdropper wiretap channels," *IEEE Access*, vol. 6, pp. 19664–19680, 2018.

[37] H. A. David and H. N. Nagaraja, *Order Statistics, 3rd ed*. Hoboken, NJ, USA: Wiley, 2003.

[38] A. M. Hunter, J. G. Andrews, and S. Weber, "Transmission capacity of ad hoc networks with spatial diversity," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5058–5071, Dec. 2008.

[39] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

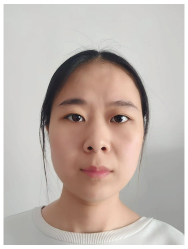
[40] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, *Table of Integrals, Series, and Products, 7th ed*. New York: Academic Press, 2007.

[41] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications, 3rd ed*. New York: John Wiley and Sons, 2013.

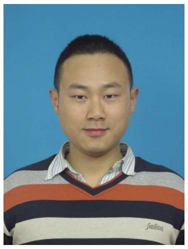
[42] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2022.3167047, IEEE Transactions on Communications

Tong-Xing Zheng (Member, IEEE) received the B.S. degree in information engineering and Ph.D. degree in information and communications engineering from Xi'an Jiaotong University, Xi'an, China, in 2010 and 2016, respectively. From 2017 to 2018, he was a Visiting Scholar with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. He is currently an Associate Professor with Xi'an Jiaotong University. His current research interests include 5G&6G wireless networks and key technologies, physical layer security, and covert communications. He has co-authored the book *Physical Layer Security in Random Cellular Networks* (Springer, 2016), one book chapter, and has authored or co-authored over 60 papers in telecommunications journals and conference proceedings. He was a recipient of the Excellent Doctoral Dissertation Award of Shaanxi Province in 2019 and the First Prize of Science and Technology Award in Higher Institution of Shaanxi Province in 2019. He was honored as an Exemplary Reviewer of IEEE TRANSACTIONS ON COMMUNICATIONS in 2017, 2018, and 2021, respectively. He was a Leading Guest Editor of FRONTIERS IN COMMUNICATIONS AND NETWORKS for the Special Issue on Covert Communications for Next-Generation Wireless Networks in 2021 and a Guest Editor of WIRELESS COMMUNICATIONS AND MOBILE COMPUTING for the Special Issue on Physical Layer Security for Internet of Things in 2018. He is currently serving as an Associate Editor of IET ELECTRONIC LETTERS and a Review Editor of FRONTIERS IN COMMUNICATIONS AND NETWORKS.



Xin Chen received the B.S. degree in information engineering from Xi'an Jiaotong University, Xi'an, China, in 2021, where she is pursuing the M.S. degree. Her current research interests include wireless physical layer security, covert communications, intelligent reflecting surface, and integrated sensing and communications.



Chao Wang (Senior Member, IEEE) received the B.S., M. S., and Ph.D. degrees in information and communications engineering from Xi'an Jiaotong University, Xian, China, in 2008, 2013, and 2016, respectively. He is currently a Lecturer with the State Key Laboratory of Integrated Services Networks, School of Telecommunications Engineering, Xidian University. His current research interests include 5G&6G wireless networks and key technologies, physical-layer security, covert communications, and deep learning and its application in the optimization of wireless communications. He was a recipient of the Excellent Doctoral Dissertation Award of Shaanxi Province in 2018 and China Institute of Communications in 2016, the Best Paper Awards at the IEEE ICCC 2014 and IEEE SAGC 2020, respectively.

Kai-Kit Wong (Fellow, IEEE) received the BEng, the MPhil, and the PhD degrees, all in Electrical and Electronic Engineering, from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions at the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, UK. He is Chair in Wireless Communications at the Department of Electronic and Electrical Engineering, University College London, UK. His current research centers around 5G and beyond mobile communications. He is a co-recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award at the IEEE Vehicular Technology Conference in Japan in 2000, and a few other international best paper awards. He is Fellow of IEEE and IET and is also on the editorial board of several international journals. He is the Editor-in-Chief for IEEE WIRELESS COMMUNICATIONS LETTERS since 2020.

Jinhong Yuan (Fellow, IEEE) received the B.E. and Ph.D. degrees in electronics engineering from the Beijing Institute of Technology, Beijing, China, in 1991 and 1997, respectively. From 1997 to 1999, he was a Research Fellow with the School of Electrical Engineering, The University of Sydney, Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia, where he is currently a Professor and the Head of Telecommunication Group with the School. He has published two books, six book chapters, over 300 papers in telecommunications journals and conference proceedings, and 50 industrial reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density-parity-check codes. His current research interests include error control coding and information theory, communication theory, and wireless communications. He has co-authored four Best Paper Awards and one Best Poster Award, including the Best Paper Award from the IEEE International Conference on Communications, Kansas City, USA, in 2018, the Best Paper Award from IEEE Wireless Communications and Networking Conference, Cancun, Mexico, in 2011, and the Best Paper Award from the IEEE International Symposium on Wireless Communications Systems, Trondheim, Norway, in 2007. He served as the IEEE NSW Chapter Chair of Joint Communications/Signal Processions/Ocean Engineering Chapter during 2011-2014. He has served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS during 2012-2017. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.