Wiretap TDMA Networks with Energy-Harvesting Rechargeable-Battery Buffered Sources

Citation:

El Shafie, Ahmed, Naofal Al-Dhahir, Zhiguo Ding, Trung Q. Duong, et al. 2019. "Wiretap TDMA Networks With Energy-Harvesting Rechargeable-Battery Buffered Sourced." IEEE Access 7: 17215-17229, doi: 10.1109/ACCESS.2019.2895246

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 6, 2019, accepted January 14, 2019, date of publication January 25, 2019, date of current version February 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2895246

Wiretap TDMA Networks With Energy-Harvesting Rechargeable-Battery Buffered Sources

AHMED EL SHAFIE[1], (Senior Member, IEEE), NAOFAL AL-DHAHIR[2], (Fellow, IEEE), ZHIGUO DING[3], (Senior Member, IEEE), TRUNG Q. DUONG[4], (Senior Member, IEEE), AND RIDHA HAMILA[5], (Senior Member, IEEE)

[1]Qualcomm Technologies, Inc., San Diego, CA 92121, USA
[2]The University of Texas at Dallas, Richardson, TX 75080, USA
[3]School of Electrical and Electronic Engineering, The University of Manchester, Manchester M13 9PL, U.K.
[4]Queen's University Belfast, Belfast BT7 1NN, U.K.
[5]Department of Electrical Engineering, Qatar University, Doha, Qatar

Corresponding author: Ahmed El Shafie (aelshafi@qti.qualcomm.com)

This publication was made possible by NPRP grant # NPRP 8-627-2-260 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

ABSTRACT We investigate the physical-layer security of an uplink wireless time-division multiple-access channel with energy-harvesting source nodes. We consider a set of source nodes equipped with rechargeable batteries and information buffers communicating confidentially with a base station, Bob, in the presence of a passive eavesdropper, Eve. An energy-harvesting rechargeable-battery cooperative jammer is assumed to assist the source nodes to confidentially send their information messages. We propose a two-level optimization formulation to improve the system's security performance. At the first optimization level, we propose a jamming scheme under energy constraints at different nodes to reduce the secrecy outage probabilities without relying on the eavesdropper's instantaneous channel state information. At the second optimization level, we optimize the number of energy packets used at the source nodes and the cooperative jammer as well as the time-slot allocation probabilities to maximize the secure throughput under the network's queues stability constraints and an application-specific secure throughput for each legitimate source node. The numerical results show the significant performance gains of our proposed optimization relative to two important benchmarks. We verify our theoretical findings through simulations and quantify the impact of key system design parameters on the security performance.

INDEX TERMS Energy harvesting, physical-layer security, information and energy queues, secrecy rates, secure throughput.

I. INTRODUCTION

Confidentiality of legitimate users data from eavesdropping is very critical in wireless communications systems due to the broadcast nature of the medium. Internet-of-things (IoT) applications [1], [2] and 5G ultra-dense networks [3] are growing significantly and, at the same time, introducing new and significant security challenges [1], [2]. Confidential information transmissions in a shared medium, from a provable and quantifiable information-theoretic sense, was first introduced in the seminal work of Wyner [4] which is currently well-known as the physical (PHY) layer security. In PHY-layer security, a legitimate transmitter, referred to as Alice, can confidentially send her information to a legitimate receiver, referred to as Bob, in the presence of an eavesdropper, referred to as Eve. The difference between the rate of the Alice-Bob link and the rate of the Alice-Eve link is defined as the system's instantaneous secrecy rate.

The instantaneous secrecy rate can be increased by (1) increasing the signal-to-noise ratio (SNR) of the received signal at Bob and/or (2) decreasing the SNR of the received signal at Eve (e.g., by injecting artificial noise (AN) signals into the transmitted information signal). The AN-aided scheme was first proposed by Goel and Negi [5] and then extended in [6]–[8]. Yang *et al.* [6], [7] studied secure communications with multi-antenna transmissions in fading channels.

A. RELATED WORK

Cooperative jammers (also referred to as friendly jammers) have been investigated to degrade Eve's SNR (see, e.g., [9] and [10]). Several jamming schemes were suggested in [9]

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

subject to the ability of the legitimate nodes to access the channel state information (CSI) of various links. The work in [10] proposed a distributed jamming scheme to simultaneously secure legitimate transmissions and power a wireless legitimate receiving node equipped with a non-linear energy-harvesting circuits. Dong *et al.* [11] and Shafie *et al.* [12] investigated a wireless system in the presence of a multi-antenna friendly jamming node which injects AN signals to increase the system's instantaneous secrecy rate. Dong *et al.* [11] and Shafie *et al.* [12] assumed that Eve's instantaneous CSI is known at the transmitters and they designed the beamformer vectors and the power allocation scheme at the friendly jammer to enhance the system's security. Following the same jamming techniques as in [11], Wang *et al.* [13] investigated the impact of having a group of amplify-and-forward wireless relaying nodes which aid in delivering the source node's information packets in addition to cooperatively jamming the eavesdropping channels.

In [14], a security-enhanced slotted-ALOHA scheme was introduced where each transmitting node either sends its own information signal or helps in enhancing the transmission security of the other nodes by probabilistically acting as a friendly jammer. Wang *et al.* [15] investigated the simple scenario of a single-input multiple-output multi-eavesdropper wiretap channel with multiple single-antenna friendly jamming nodes. The wireless nodes in the networks were assumed to be randomly distributed where the distribution of the friendly jamming nodes and the eavesdropping nodes were considered to follow an independent two-dimensional homogeneous Poisson point processes (PPP). To confuse the eavesdropping nodes by degrading their received information signals, an opportunistic friendly jammer selection scheme was introduced in [15], where the friendly jamming nodes, whose wireless channels are almost orthogonal to the legitimate receiver channel, were selected to jam the eavesdropping nodes using independent and identically distributed (i.i.d.) Gaussian random signals. Zhang *et al.* [16] studied the secrecy throughput subject to a certain secrecy outage constraint for a multiple-input single-output (MISO) slowly-fading wireless channel.

Zhong *et al.* [17] studied the tradeoff between delay and PHY-layer security in wireless networks. Yang *et al.* [18] investigated several promising technologies for the PHY-layer security of 5G systems, including heterogeneous networks, massive multiple-input multiple-output (MIMO), and millimeter wave (mmW). Zhou and McKay [19] studied the secure communication problem of multiple-antenna transmissions in wireless fading channels with single-antenna legitimate receivers and in the presence of multiple single-antenna eavesdroppers. The transmitter was assumed to simultaneously send an information signal to the legitimate receiving node and inject a jamming signal to degrade the eavesdroppers' channels. Hu *et al.* [20] proposed an on-off information transmission scheme for wireless wiretap channels when the CSI is outdated. The authors investigated two scenarios for the legitimate receiver's outdated CSI, depending on the knowledge of the eavesdropper's outdated CSI at the transmitter. Secure information transmission under channel estimation errors at the legitimate receiving node was considered in [21].

To secure the transmissions in a multiple-input multiple-output multiple-eavesdropper (MIMOME) wiretap channel, Hu *et al.* [22] proposed new AN-based schemes where the legitimate transmitting node adopts transmit antenna selection (TAS) to select the antenna that maximizes the instantaneous SNR at the legitimate receiving node. All receivers use the maximal-ratio combining (MRC) scheme to combine the received signals. During the TAS process, the authors considered the outdated-CSI scenario. Hence, they proposed a scheme to reduce the impact of the outdated CSI on the legitimate system. In addition, the authors studied the effect of the spatial correlation between the antennas at the receiving nodes. It was shown that, in the low-SNR regime, the antenna correlation can improve the legitimate transmission secrecy. Nevertheless, in the moderate- and high-SNR regimes, antenna correlation can degrade the legitimate transmission secrecy.

The preliminary results in [23] showed the gain of joint medium-access control and PHY layer designs on enhancing the security of buffered information source nodes, when those nodes help in jamming whenever they are not scheduled for information transmission. In this paper, unlike [23], we do not assume knowledge of Eve's instantaneous CSI at the legitimate nodes. Furthermore, we assume the presence of a battery-powered cooperative jammer that helps in securing the transmissions and achieving the quality-of-service (QoS) requirements of the multiple-access system when the source nodes are equipped with rechargeable batteries and harvest energy from the ambient energy sources. In addition, we show the impact of the batteries and energy-harvesting parameters on the system's security. More specifically, in this work, we propose an AN-aided secure scheme for energy-harvesting based time-division multiple-access (TDMA) networks where the transmitting nodes are assumed to be energy-limited with rechargeable batteries. The time is discretized into equal-size time slots and one legitimate user, Alice, is assumed to be selected for information transmission in a slot. If a legitimate user is not assigned for information transmission, then this user should remain idle to save its battery's energy. We assume different QoS requirements measured by the queue stability of the legitimate source nodes and a certain secure throughput requirement for each user. To achieve our optimization goals, the time-slot allocation probabilities are optimized based on the system's energy constraints. It is noteworthy that our assumption of TDMA transmissions is practical since our model applies to the uplink scenario of many systems including GSM cellular networks [24], [25], Bluetooth personal area networks, IEEE 802.16a WiMAX broadband wireless access networks, and emerging wireless networks that will be part of the IoT.

TABLE 1. List of key variables.

Symbol	Description	Symbol	Description
$\mathcal{M}$	Number of Alices (source nodes)	Q_J	Energy queue (battery) at Jim
$Q_{e,k}$	Energy queue (battery) at the k-th Alice	T and W	Slot duration and channel bandwidth
$\mathcal{R}$	Target secrecy rate	$\mathcal{E}_{\max}$	Maximum capacity of an energy battery/queue
γ_k	k-th Alice's input SNR	γ_J	Jim's input SNR
κ	Thermal noise power spectral density	ω_k	Probability of assigning the k-th Alice to a time slot
$Q_{\mathrm{d},k}$	Data (information) buffer at the k-th Alice	$\mu_{\mathrm{d},k}/\mu_{\mathrm{e},k}$	Average service rate of the k-th Alice data/energy queue
$\lambda_{\mathrm{d},k}$	Mean arrival rate at information queue $Q_{\mathrm{d},k}$	$\mathcal{N}$	Number of transmit antennas at Jim
$\mathbb{R}_{n_1,n_2}$	Instantaneous rate of the n_1-n_2 link	$R_{\mathrm{sec},k}$	Instantaneous secrecy rate of the k-th Alice
h_{n_1,n_2}	Channel coefficient between node n_1 and node n_2	$\beta_{n_1,n_2}=\lvert h_{n_1,n_2}\rvert^2$	Channel gain between node n_1 and node n_2
$\mathcal{P}^{\mathrm{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}/\mathcal{P}^{\mathrm{nojam}}_{k,\hat{\mathcal{L}}_A}$	Probability of secrecy outage of the k-th Alice transmission when Jim is active/inactive	$\mathcal{P}^{\mathrm{noEve}}_{k,\mathrm{B}}$	Probability of secrecy outage of the k-th Alice transmission when there is no Eve
$\mu_{\mathrm{req},k}$	QoS requirement (required secure throughput) for the k-th Alice	$\mu_{\mathrm{sec},k}$	Secure throughput of the k-th Alice

B. CONTRIBUTIONS

Our contributions can be summarized as follows

- We propose a new scheme to improve the information-theoretic security of TDMA systems under energy-limited battery-powered transmitting wireless nodes. We investigate the presence of an energy-limited rechargeable-battery friendly cooperative jammer to help in securing the legitimate transmissions.
- We optimize the time-slot allocation parameters as well as the beamforming coefficients vector at a helper, Jim. The dynamics of the energy arrivals at different nodes are taken into consideration and the system's design parameters are selected to satisfy the QoS requirements of the buffered legitimate users.
- Without a global CSI of the legitimate wireless links or the availability of the Eve's instantaneous CSI at the legitimate transmitting nodes, we design an AN-aided scheme and derive closed-form expressions for the beamformer at the cooperative jammer as well as the secrecy outage probabilities SOPs) of the wireless links. We quantify the impact of our proposed system and the energy-harvesting parameters on the SOP formulas.
- We quantify the impact of the energy-harvesting parameters of various nodes on the time-slot allocation probabilities and the achievable secure throughput. In addition, we model the energy and information arrival and departure as queueing systems and analyze their Markov chains. Furthermore, we derive closed-form expressions for all the steady-state distributions of all queues in the system.

Notation: $(\cdot)^*$ denotes the complex-conjugate operation. $(\cdot)^\top$ denotes the vector transpose. $\|\cdot\|$ denotes the Euclidean norm of a vector. $|\cdot|$ denotes either absolute value or set cardinality depending on the context in which it is used. $\mathbb{E}\{\cdot\}$ denotes statistical expectation. $\mathbf{0}$ denotes the all-zero matrix/vector and its size is understood from the context. $\lceil\cdot\rceil$ is the ceil of the argument. The factorial of a non-negative integer n is denoted by $n!$. $\Gamma(\cdot)$ is the Gamma function. $\mathrm{Ei}(\cdot)$ is the exponential integral function, $[\cdot]^+=\max(\cdot,0)$ denotes the maximum between the enclosed values in brackets and **zero**, and $\overline{X}=1-X$. A list of the key variables is given in Table 1.

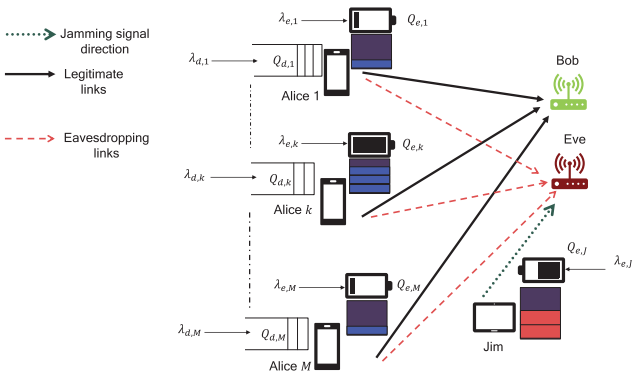


FIGURE 1. The considered network model. Each Alice is assumed to be equipped with an information buffer to store its own traffic and a rechargeable-battery to store energy. The number of potential source nodes, Alices, is $\mathcal{M}$. Jim is the energy-harvesting cooperative jamming node. Furthermore, Eve is the eavesdropping node.

II. SYSTEM MODEL AND ASSUMPTIONS

We consider a wireless network composed of a set of energy-harvesting source nodes (Alices), with cardinality $\mathcal{M}$, sharing the same channel resources and communicating confidentially with a base-station (Bob) in the presence of an eavesdropping node (Eve) as shown in Fig. 1. The Alices are labeled $1,2,\ldots,\mathcal{M}$. The k-th Alice, Bob, and Eve

are denoted by k, B, and E, respectively. To protect the legitimate wireless transmissions from the eavesdropping attacks, a multi-antenna energy-harvesting cooperative jamming node, Jim, is assumed to jam the eavesdropping channels. The Alices, Bob, and Eve are assumed to be equipped with one antenna. In addition, we assume that the Alices and Jim are energy harvesters with average energy arrival rates of $\lambda_{e,k}$ and $\lambda_{J,k}$ at the energy queue of the k-th Alice and at the energy queue of Jim, respectively.[1]

We assume quasi-static flat Rayleigh-fading channels. Let h_{n_1,n_2} denote the channel coefficient between node $n_1 \in \{1, 2, \ldots, \mathcal{M}, \mathrm{B}, E\}$ and node $n_2 \in \{1, 2, \ldots, \mathcal{M}, \mathrm{B}, E\}$. According to the quasi-static flat-fading channel model, h_{n_1,n_2} remains fixed during the coherence time duration (i.e., time slot duration). However, it changes identically and independently from one time slot duration to another. Since the channel is Rayleigh fading, the channel coefficient of each wireless link is modeled as a zero-mean circularly-symmetric Gaussian random variable with unit variance. The thermal noise effect at a receiver is assumed to be modeled as a zero-mean additive white Gaussian noise (AWGN) with power spectral density κ. Assuming a channel bandwidth of W, the noise power is κW. The communication time is assumed to be partitioned into discrete time slots each of which has a duration of T and is equal to the channel coherence time [24], [25]. Since we assume a TDMA scheme, in a given time slot, only one Alice is scheduled for information transmission. The k-th Alice ($k \in \{1, 2, \ldots, \mathcal{M}\}$) is assigned to a time slot for information transmission with probability $0 \leq \omega_k \leq 1$. Hence, we have the constraint that $\sum_{k=1}^{\mathcal{M}} \omega_k = 1$ [24], [25]. Note that ω_k can be interpreted as the fraction of time slots assigned/allocated to the k-th Alice from the total communication time slots of the network. In our design, the time-slot allocation probabilities $(\omega_1, \omega_2, \ldots, \omega_{\mathcal{M}})$ are adjusted to satisfy the QoS requirements of the Alices.

A. ENERGY AND INFORMATION QUEUES MODEL

We assume that the k-th Alice maintains an information buffer/queue, denoted by $Q_{\mathrm{d},k}$, to store her incoming information traffic and an energy queue $Q_{\mathrm{e},k}$ to store the energy packet arrivals at the k-th Alice queue. The information and energy arrivals at the k-Alice are assumed to be Bernoulli random variables [24], [26] with mean $0 \leq \lambda_{\mathrm{d},k} \leq 1$ packets/slot for her information queue and $0 \leq \lambda_{e,k} \leq 1$ energy packets/slot for her energy queue. The Bernoulli arrival model is a simple yet efficient model to capture the random and sporadic nature of energy and information packet arrivals [24], [26] at the batteries and the information queues, respectively. If $\lambda_{\mathrm{d},k} = 0$, the k-th Alice has no information to send. If $\lambda_{e,k} = 0$, the k-th Alice is completely inactive in the network or does not harvest energy from ambient energy sources. Jim's battery (energy queue) is denoted by Q_J.[2] We assume that Jim starts jamming whenever his battery has $\mathcal{L}_J \geq 1$ energy packets which will allow him to create stronger interference at Eve since more energy is used in jamming. Moreover, the parameter $\mathcal{L}_J$ is optimized to enhance the system's security performance. The maximum capacity of a battery (i.e., energy queue) is $\mathcal{E}_{\max}$ energy packets. Hence, $\mathcal{L}_J \in \{1, 2, \ldots, \mathcal{E}_{\max}\}$.

In wireless communications systems, the time slot is composed of three time durations: 1) channel estimation duration which consumes $\tau < T$ of the time slot duration T; 2) information decodability status reporting duration (acknowledgement (ACK) or negative-acknowledgement (NACK)) which consumes $\tau_f < T$; 3) information transmission duration which consumes the remaining slot duration fraction of $(T - \tau - \tau_f)$. When Alice's energy queue contains $\hat{\mathcal{L}}_A \geq \mathcal{L}_A \in \{1, 2, \ldots, \mathcal{E}_{\max}\}$ energy packets used for information transmissions, the k-th Alice's transmit power level is given by

$$P_k = \frac{\hat{\mathcal{L}}_A \mathrm{e}_k}{T - \tau - \tau_f} \stackrel{def}{=} \hat{\mathcal{L}}_A P_{\circ,k} \tag{1}$$

where $k \in \{1, 2, \ldots, \mathcal{M}\}$, e_k is the energy in one energy packet at the k-th Alice, and $P_{\circ,k}$ is the transmit power when $\hat{\mathcal{L}}_A = 1$. Similarly, when Jim's energy queue has $\hat{\mathcal{L}}_J \geq \mathcal{L}_J$ energy packets, Jim's transmit power level is given by

$$P_J = \frac{\hat{\mathcal{L}}_J \mathrm{e}_J}{T - \tau - \tau_f} \stackrel{def}{=} \hat{\mathcal{L}}_J P_{\circ,J} \tag{2}$$

where e_J is the energy in one energy packet at Jim. As shown in Eqns. (1) and (2), the more energy packets are used in transmissions, the higher the transmit power will be.

B. INFORMATION AND ENERGY QUEUES SERVICE RATES

We assume that the transmitting node uses $\hat{\mathcal{L}} \geq \mathcal{L}_{\mathcal{A}}$ energy packets for the information/AN packet transmission and can adjust the parameter $\mathcal{L}_{\mathcal{A}}$ based on the required performance. This scheme is motivated by the fact that increasing the information/AN packets transmission powers increases the instantaneous secrecy rates. Also, it is motivated by reducing the information packets retransmissions to avoid information combining at the eavesdroppers. In other words, the Alices transmit their information packets whenever Bob is able to decode them.

A packet at the head of the k-th Alice information queue, $Q_{\mathrm{d},k}$, departs to Bob when the user is scheduled for information transmission, which occurs with probability ω_k, and the channel between Alice and Bob is not in connection outage. Hence, the mean service rate of $Q_{\mathrm{d},k}$ is given by

$$\mu_{\mathrm{d},k} = \omega_k \sum_{\hat{\mathcal{L}}_A = \mathcal{L}_A}^{\mathcal{E}_{\max}} |\pi^k_{\hat{\mathcal{L}}_A} \exp\left(-\frac{2^{\mathcal{R}} - 1}{\hat{\mathcal{L}}_A \gamma_k}\right) \tag{3}$$

[1] The energy harvested can be from any ambient energy-harvesting sources such as radio-frequency (RF) transmissions from a dedicated energy channel, wind, solar, vibration, etc.

[2] Throughout this paper, we denote both a queue and its state/size (number of packets inside the queue) using the same notation. That is, the number of packets at Q_x is also denoted by Q_x.

where $\gamma_k = P_{\circ,k}/(\kappa W)$ is the k-th Alice's input SNR and $\pi^k_{\hat{\mathcal{L}}_A}$ is the probability that the k-th Alice's energy queue has $\hat{\mathcal{L}}_A$ energy packets.

When the k-th Alice is selected for information transmission and she has enough energy in her battery according to the proposed scheme, a packet at her information queue, $Q_{\mathrm{d},k}$, is transmitted *securely* to Bob if i) the transmission is perfectly secured, which occurs with probability $\overline{\mathcal{P}^{\mathrm{nojam}}_{k,s}}$, when Jim has energy packets less than $\mathcal{L}_\mathrm{J}$, or ii) Jim has enough energy (i.e., energy packets greater than or equal to $\mathcal{L}_J$) and the transmission is perfectly secured, which occurs with probability $\overline{\mathcal{P}^{\mathrm{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}}$ when Jim has $\hat{\mathcal{L}}_J \geq \mathcal{L}_\mathrm{J}$ energy packets. Hence, the k-th Alice's secure throughput, given a data packet, is given by

$$\mu_{\mathrm{sec},k} = \omega_k \sum_{s=\mathcal{L}_\mathrm{A}}^{\mathcal{E}_{\max}} \pi^k_s \left[\Pr\{Q_J < \mathcal{L}_\mathrm{J}\} \overline{\mathcal{P}^{\mathrm{nojam}}_{k,s}} + \sum_{j=\mathcal{L}_\mathrm{J}}^{\mathcal{E}_{\max}} \pi^J_j \overline{\mathcal{P}^{\mathrm{jam}}_{k,s,j}} \right] \tag{4}$$

where $\Pr\{Q_J < \mathcal{L}_\mathrm{J}\} = \sum_{j=0}^{\mathcal{L}_\mathrm{J}-1} \pi^J_j$ with π^J_j denoting the probability that Jim's energy queue has j energy packets. Therefore, controlling the SOPs can effectively control the mean service rate of the queues given by (3) and the secure throughput given by (4). Hence, for given time slot allocation probabilities $(\omega_1, \ldots, \omega_{\mathcal{M}})$, to increase the service rate of information queue $Q_{\mathrm{d},k}$ (which also increases the secure throughput of the k-th Alice), the SOPs should be reduced. The SOPs can be efficiently controlled by managing the secrecy rate of the transmission and the PHY layer parameters. Moreover, the status of the energy queues affects the SOPs. From the rate expression in (10), which will be discussed shortly, by decreasing Eve's rate, the Alice's transmission secrecy rate increases. Therefore, in the following section, we propose an AN zero-forcing (AN-ZF) jamming scheme where Jim designs his transmit antennas' beamformer weights to degrade Eve's instantaneous signal-to-interference-plus-noise ratio (SINR) while cancelling the interference at Bob's receiver.

The mean service rate of $Q_{\mathrm{e},k}$, when the battery has $\hat{\mathcal{L}}_A \geq \mathcal{L}_A$ energy packets, is given by

$$\mu_{\mathrm{e},k} = \omega_k \Pr\{Q_{\mathrm{d},k} \neq 0\} \tag{5}$$

In other words, this is the probability that the energy queue expends $\hat{\mathcal{L}}_A$ energy packet in a given time slot.

Since the information and energy queues at each Alice interact with each other as shown from Eqns. (3) and (5), the exact analysis cannot be done directly. Hence, we assume that the Markov chains that model the energy queues' dynamics are computed when the information queues at the Alices are always non-empty. Specifically, we let $\Pr\{Q_{\mathrm{d},k} = 1\} = 1$ in the state-transition probabilities of the Markov chains. This implies that $\mathcal{L}$ energy packets (where $\mathcal{L} = \mathcal{L}_A$ for Alice's energy queues and $\mathcal{L} = \mathcal{L}_J$ for Jim's energy queue) will be consumed from the energy queue once they are available at the queue. Hence, the probability of the event that the time slot is assigned to the k-th Alice and her energy queue has $\mathcal{L}_A$ packets is reduced. Moreover, the ability of Jim to help whenever there is information at Alice's queue will be reduced. Accordingly, this approximation may result in *under-estimation* of Alice's secure throughput. The Markov chain modeling the energy queue in this case is analyzed in Appendix -A.

At high input SNR at Alices, which is assumed in the sequel of this paper, the connection probability of the Alice-Bob link is almost 1. Hence, the energy queues' Markov chains follow the Markov chain in Fig. 2. In this new system of queues, for states (number of energy packets) less than $\mathcal{L}$, the energy departure rate (i.e., number of energy packets departing from the energy queue) is zero. Hence, the probability that an energy queue stores $\ell > \mathcal{L}$ is zero.[3]

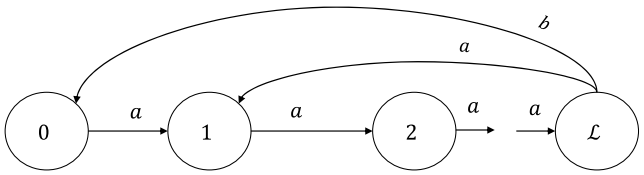


FIGURE 2. The Markov chain that models an energy queue. For visual clarity, the state-self transitions are eliminated from the graph. The transition probability from $\mathcal{L}$ to $\mathcal{L}+r$, $r \in \{1, 2, \ldots, \mathcal{E}_{\max} - \mathcal{L}\}$, is zero. In the figure, $a = \lambda_{\mathrm{e},k}$ and $b = 1 - \lambda_{\mathrm{e},k}$.

Let π^k_ℓ denote the probability of the k-th Alice energy queue having ℓ energy packets. Using the Markov chain analysis in Appendix -A, the steady state probabilities are given by

$$\begin{aligned} \pi^k_0 &= \frac{\overline{\lambda_{\mathrm{e},k}}}{\mathcal{L}_A}, \quad \pi^k_\ell = \frac{1}{\mathcal{L}_A} \forall \ell \in \Theta_A, \\ \pi_{\mathcal{L}_A} &= \frac{\lambda_{\mathrm{e},k}}{\mathcal{L}_A}, \quad \pi^k_\ell = 0 \; \forall \ell > \mathcal{L}_A \end{aligned} \tag{6}$$

where $\Theta_A = \{1, 2, \ldots, \mathcal{L}_A - 1\}$. Although the steady-state probabilities in (6) decrease with $\mathcal{L}_A$, the no-secrecy outage probability (NSOP) increases with $\mathcal{L}_A$ which increases the system's secure throughput. This represents a tradeoff in selecting the best value of $\mathcal{L}_A \in \{1, 2, \ldots, \mathcal{E}_{\max}\}$.

The steady-state probabilities for Jim's energy queue are given by

$$\begin{aligned} \pi^\mathrm{J}_0 &= \frac{\overline{\lambda_\mathrm{J}}}{\mathcal{L}_J}, \quad \pi^\mathrm{J}_\ell = \frac{1}{\mathcal{L}_J} \forall \ell \in \Theta_J, \\ \pi^\mathrm{J}_{\mathcal{L}_J} &= \frac{\lambda_J}{\mathcal{L}_J}, \quad \pi^\mathrm{J}_\ell = 0 \; \forall \ell > \mathcal{L}_J \end{aligned} \tag{7}$$

where $\Theta_J = \{1, 2, \ldots, \mathcal{L}_J - 1\}$.

The mean service rate of the k-th Alice information queue $Q_{\mathrm{d},k}$ is given by

$$\mu_{\mathrm{d},k} = \omega_k \frac{\lambda_{\mathrm{e},k}}{\mathcal{L}_A} \exp\left(-\frac{2^{\mathcal{R}} - 1}{\mathcal{L}_A \gamma_k} \right) \tag{8}$$

[3]It is noteworthy that the energy queues, under the given assumptions, can be viewed as decoupled M/D/1 queues with service rates equal to $\mathcal{L}$ packets.

Furthermore, the secure throughput of the k-th Alice is given by

$$\mu_{\text{sec},k} = \omega_k \frac{\lambda_{\text{e},k}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\text{nojam}}_{k,\mathcal{L}_A}} + \frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\text{jam}}_{k,\mathcal{L}_A,\mathcal{L}_J}}\right] \quad (9)$$

where $\overline{\mathcal{P}^{\text{nojam}}_{k,\mathcal{L}_A}}$ and $\overline{\mathcal{P}^{\text{jam}}_{k,\mathcal{L}_A,\mathcal{L}_J}}$ are the outage probabilities without and with jamming from Jim, respectively.

C. OPTIMIZATION METHODOLOGY

Our proposed optimization approach is performed at two levels. At the first optimization level, we optimize the instantaneous secrecy rates by injecting the AN and optimizing its precoding matrix. This is realized without the need for Eve's instantaneous CSI or even global CSI of the legitimate links, as it will be discussed in Section III-E. At the second optimization level, we use the resultant SOPs from the first optimization level and, in addition to optimizing the number of energy packets used at the Alices and Jim per transmission, we optimize the time-slot allocation probabilities. Our goal is to maximize the secure throughput of the legitimate users under the network's queues stability and an application-specific secure throughput requirement for each Alice. We emphasize here that the optimization of the number of energy packets used at the Alices and Jim is motivated by the fact that the number of energy packets changes the steady-state probabilities of the energy queues, the SOPs, and the ability of nodes to transmit information and AN signals. Hence, optimizing those parameters can improve the system's performance. This will be verified in our analysis and our numerical simulations section.

III. SOP WITHOUT AND WITH COOPERATIVE JAMMING

As explained in the previous section, to improve the users' security and enhance their QoS, we need to reduce the SOPs which, in turn, increases the users' throughput. Hence, we propose an AN-ZF jamming scheme to reduce the SOPs of the wireless links. Our proposed scheme does not depend on Eve's instantaneous CSI or the instantaneous CSI of the Alices. Instead, it only relies on the CSI of the Jim-Bob link.

A. INFORMATION AND SECRECY RATES

Assume that an information packet contains K_b bits. Letting W denote the channel bandwidth, the information rate (i.e., target secrecy rate) of an Alice is given by $\mathcal{R} = \frac{K_b}{(T-\tau-\tau_f)W}$. As explained in [9], [11], [13], and [27], a secrecy outage event occurs when the target secrecy rate is greater than the instantaneous secrecy rate. Assuming that the instantaneous rate of the link connecting node n_1 and node n_2 (i.e., $n_1 - n_2$ link) is $\mathbb{R}_{n_1,n_2}$, the instantaneous secrecy rate of k-th Alice transmission is given by

$$R_{\text{sec},k} = \left[\mathbb{R}_{k,\text{B}} - \mathbb{R}_{k,\text{E}}\right]^+ \leq \mathbb{R}_{k,\text{B}} \quad (10)$$

When $R_{\text{sec},k} \geq \mathcal{R}$, the information signal is perfectly secure. Otherwise, the confidentiality is compromised (i.e., Eve can partially or completely decode the information). If $\mathbb{R}_{k,\text{B}} < \mathcal{R}$, then $\mathcal{R} > R_{\text{sec},k}$ and a secrecy outage occurs. More specifically, the information cannot be decoded reliably at the legitimate receiver. In general, we can categorize the outage events in a communication system into two types:

1) **Connection Outage**: A link is said to be in connection outage when the rate of the Alice-Bob link is lower than the target secrecy rate $\mathcal{R}$.
2) **Secrecy Outage**: A link is said to be in secrecy outage (and unsecured) when the instantaneous secrecy rate of Alice's transmission is lower than the target secrecy rate $\mathcal{R}$.

B. WIRETAP CHANNEL CODING DESIGN

When the k-th Alice is selected for information transmission, she adaptively selects her transmission rate $\mathbb{R}_{k,\text{B}}$ to be close to the link rate such that no connection outage takes place. Denote the codebook used by Alice as $C(2^{n\mathbb{R}_{k,\text{B}}}, 2^{n\mathcal{R}}, n)$ where $\mathcal{R}$ is the target secrecy rate, n is the codeword length (i.e., number of symbol durations per a slot), $2^{n\mathbb{R}_{k,\text{B}}}$ is the size of the codebook (i.e., number of codewords), and $2^{n\mathcal{R}}$ is the number of potential confidential messages that Alice transmits. The $2^{n\mathbb{R}_{k,\text{B}}}$ codewords are randomly grouped into $2^{n\mathcal{R}}$ bins/messages. In a given time slot, to transmit a confidential message $m \in \{1, 2, \ldots, 2^{n\mathcal{R}}\}$, Alice randomly selects a codeword from bin m and transmits it over the wireless communication channel. Since Eve's instantaneous CSI is unknown at Alice, Alice cannot set the target secrecy rate to the instantaneous secrecy rate. However, Alice transmits with a fixed secrecy rate that is equal to the number of bits per packet divided by the number of channel uses.

C. SOP WITHOUT JAMMING

When Jim has less than $\hat{\mathcal{L}}_J$ energy packets, he cannot help the legitimate system. In a given time slot, when Bob's SINR is higher than Eve's SINR, the k-th Alice's transmission instantaneous secrecy rate is given by

$$\mathcal{R}_{\text{sec},k} = \log_2\left(1+\frac{P_k\beta_{k,\text{B}}}{\kappa W}\right) - \log_2\left(1+\frac{P_k\beta_{k,\text{E}}}{\kappa W}\right) \quad (11)$$

where $\beta_{k,\text{B}} > \beta_{k,\text{E}}$ is the condition to achieve a non-zero instantaneous secrecy rate with $\beta_{k,j} = |h_{k,j}|^2$ denoting the channel gain between node $k \in \{1, 2, 3, \ldots, \mathcal{M}\}$ and node $j \in \{\text{E}, B\}$.

When the k-th Alice is scheduled for information transmission and she has $s \geq \mathcal{L}_A$ energy packets, she transmits her information. Hence, the NSOP without jamming is given by

$$\overline{\mathcal{P}^{\text{nojam}}_{k,\hat{\mathcal{L}}_A}} = \Pr\left\{\mathcal{R} \leq \left[\log_2\left(\frac{1+\hat{\mathcal{L}}_A\gamma_k\beta_{k,\text{B}}}{1+\hat{\mathcal{L}}_A\gamma_k\beta_{k,\text{E}}}\right)\right]^+\right\} \quad (12)$$

Using the SOP expression in [28, eq. (7)], and substituting with our system's parameters, the NSOP without cooperative jamming is given by

$$\overline{\mathcal{P}^{\text{nojam}}_{k,\hat{\mathcal{L}}_A}} = \frac{1}{1+2^{\mathcal{R}}}\exp(-\mathcal{R}_\circ) \quad (13)$$

where $\mathcal{R}_\circ = \frac{2^{\mathcal{R}}-1}{\hat{\mathcal{L}}_A\gamma_k}$.

D. SOP WITH AN-ZF JAMMING

In the proposed jamming scheme, since Jim has up to $\mathcal{N}$ antennas that can be used to jam Eve and increase the k-th Alice secrecy rate under the condition that the injected AN (jamming signal) is canceled at Bob's receiver. We denote the j-th ($j \in \{1, 2, \ldots, \mathcal{N}\}$) antenna at Jim by J_j. To create a zero-forcing beamforming (ZF-BF) jamming signal, the number of transmit antennas at Jim must be at least 2, i.e., $\mathcal{N} \geq 2$.

Jim selects the AN-ZF beamformer weights such that the interference is canceled at Bob. For given channel realizations, when the SINR at Bob is higher than the SINR at Eve, the instantaneous secrecy rate of the k-th Alice transmission is given by

$$\mathcal{R}_{\text{sec},k} = \left[\log_2 \left(\frac{1 + \hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{B}}}{1 + \frac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}}} \right) \right]^{+} \tag{14}$$

where $\gamma_J = P_{\circ,J}/(\kappa W)$ is Jim's input SNR and the ν-th ($\nu \in \{1, 2, \ldots, \mathcal{N}-1\}$) column of the AN-precoding matrix $\mathbf{W}$ is $\mathbf{w}_\nu = [w_{J_1}, \ldots, w_{J_\mathcal{N}}]^{\top} \in \mathbb{C}^{\mathcal{N}\times 1}$ which represents the zero-forcing beamforming (ZF-BF) weight vector with w_{J_j} denoting the weight element used at Jim's j-th ($j \in \{1, 2, \ldots, \mathcal{N}\}$) antenna.

When the instantaneous SINR at Eve is higher than the instantaneous SINR at Bob, i.e., $\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{B}} \leq \frac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}}$, the instantaneous secrecy rate of the k-th Alice's transmission is zero, i.e., $R_{\text{sec},k} = 0$. This implies that secure communication is not possible and security is compromised since the eavesdropping channel is better than the legitimate channel. Considering the two cases of zero and non-zero instantaneous secrecy rates based on the receivers' SINRs, the instantaneous secrecy rate of the k-th Alice transmission, denoted by $R_{\text{sec},k}$, is given by

$$R_{\text{sec},k} = \begin{cases} \mathcal{R}_{\text{sec},k} & \text{if } \hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{B}} > \dfrac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}} \\ 0 & \text{if } \hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{B}} \leq \dfrac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}} \end{cases} \tag{15}$$

To maximize the secrecy rate of the wireless transmissions of the k-th Alice, $\mathcal{R}_{\text{sec},k}$ needs to be maximized over the AN-precoding matrix $\mathbf{W}$. This is equivalent to minimizing Eve's rate $\log_2 \left(1 + \frac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}}\right)$, which is the only term that depends on the AN-precoding matrix $\mathbf{W}$. Since the logarithmic function is a monotonically increasing function, and for a given $(\mathcal{L}_A, \mathcal{L}_J)$ pair, the instantaneous secrecy rate optimization problem becomes

$$\begin{aligned} \max_{\mathbf{W}} : \mathcal{R}_{\text{sec},k} &\Rightarrow \min_{\mathbf{W}} : \frac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}} \\ &\Rightarrow \max_{\mathbf{W}} : |\mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}|^2 \end{aligned} \tag{16}$$

Since Eve's instantaneous CSI is unknown at Jim, he cannot design the jamming precoding matrix to maximize the term in (16). He will rather spread the AN signal (isotropically) in all the directions that are orthogonal to the Jim-Bob channel vector direction.

Recall that J_j denotes the j-th antenna at Jim. Let $\mathbf{h}_{\text{J}-E} = [h_{J_1,\text{E}}, \ldots, h_{J_\mathcal{N},\text{E}}]^{\top} \in \mathbb{C}^{\mathcal{N}\times 1}$ denote the channel coefficient vector from Jim's antennas to Eve and $\mathbf{h}_{\text{J}-B} = [h_{J_1,\text{B}}, \ldots, h_{J_\mathcal{N},\text{B}}]^{\top} \in \mathbb{C}^{\mathcal{N}\times 1}$ denote the channel coefficient vector from Jim's antennas to Bob. The optimal AN precoding matrix $\mathbf{W}$ that maximizes $|\mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}|^2$ subject to the orthonormality of the precoding matrix $\mathbf{W}$, i.e., $\mathbf{W}^{*}\mathbf{W} = \mathbf{I}_{\mathcal{N}-1}$, and the removal of the interference at Bob's receiver, $|\mathbf{h}_{\text{J}-B}^{\top} \mathbf{W}| = \mathbf{0}$, is computed by solving the following problem

$$\begin{aligned} &\max_{\mathbf{W}} : \text{ Constant} \\ &\text{s.t. } |\mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}| = 0, \\ &\quad \mathbf{W}^{*}\mathbf{W} = \mathbf{I}_{\mathcal{N}-1} \end{aligned} \tag{17}$$

where (17) is a feasibility problem which finds all possible solutions that satisfy the constraints. The optimal matrix $\mathbf{W}$ should cancel the cooperative jamming signal at Bob. Hence, to solve the optimization problem in (17), the columns of the optimal $\mathbf{W}$ should be orthogonal to $\mathbf{h}_{\text{J}-B}^{\top}$. After obtaining the orthogonal directions to the channel vector $\mathbf{h}_{\text{J}-B}^{\top}$, Jim distributes his total transmit energy over those directions.

The NSOP of the AN-ZF jamming is given by

$$\overline{\mathcal{P}}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J} = \Pr\left\{ \mathcal{R} \leq \left[\log_2 \left(\frac{1 + \hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{B}}}{1 + \frac{\hat{\mathcal{L}}_A \gamma_k \beta_{k,\text{E}}}{1 + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} \mathbf{h}_{\text{J}-E}^{\top} \mathbf{W}\mathbf{W}^{*} (\mathbf{h}_{\text{J}-E}^{\top})^{*}}} \right) \right]^{+} \right\} \tag{18}$$

Lemma 1: Under cooperative jamming, the NSOP when Alice and Jim use $\hat{\mathcal{L}}_A$ and $\hat{\mathcal{L}}_J$ energy packets in information transmission and cooperative jamming, respectively, is given by

$$\overline{\mathcal{P}}^{jam}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J} = \overline{\mathcal{P}}^{no\ Eve}_{k,B} \frac{Z(\mathcal{N}-2, \mathcal{R}_1) + \frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} Z(\mathcal{N}-1, \mathcal{R}_1)}{\frac{\hat{\mathcal{L}}_J \gamma_J}{\mathcal{N}-1} (\mathcal{N}-2)!} \tag{19}$$

with

$$\begin{aligned} Z(K, u) &= \int_0^{\infty} \frac{x^K}{x+u} \exp(-x) dx \\ &= (-1)^{K-1} u^K \exp(u) Ei(-u) + \sum_{n=1}^{K} (n-1)! (-u)^{K-n} \end{aligned} \tag{20}$$

where $\mathcal{N} \geq 2$ for the AN-cancellation condition at Bob to be satisfied, $\mathcal{R}_\circ = \frac{2^{\mathcal{R}}-1}{\hat{\mathcal{L}}_A\gamma_k}$, $\mathcal{R}_1 = \frac{1+2^{\mathcal{R}}}{\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}}$, $\mathcal{P}_{k,B}^{no\ Eve} = 1-\exp(-\mathcal{R}_\circ)$ is the NSOP when there is no eavesdropping which represents the performance upper-bound of a security scheme, and $Ei(\cdot)$ is the exponential integral.[4]

Proof: See Appendix -B □

From (19), the NSOP given that the link between Alice and Bob is reliable (i.e., not in connection outage) is given by $\zeta = \frac{\overline{\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}}}{\overline{\mathcal{P}^{\text{no Eve}}_{k,\text{B}}}} = \frac{\text{Z}(\mathcal{N}-2,\mathcal{R}_1)+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}\text{Z}(\mathcal{N}-1,\mathcal{R}_1)}{\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}(\mathcal{N}-2)!}$. The SOP represents two outage events: outage due to eavesdropping and outage due to link disconnection. The probability ζ represents the impact of eavesdropping only and it quantifies the reduction in the NSOP due to the presence of eavesdropping attacks. As we can see from its expression, the probability ζ does not depend on the information average transmit power or the input SNR, given by $\hat{\mathcal{L}}_A\gamma_k$. However, it depends on several other factors such as the number of antennas at Jim, $\mathcal{N}$, the target secrecy rate, $\mathcal{R}$, and the average input jamming SNR, $\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}$. From (19), the NSOP, $\overline{\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}}$, is monotonically nondecreasing with $\hat{\mathcal{L}}_A\gamma_k$. As $\hat{\mathcal{L}}_A\gamma_k \to \infty$, $\overline{\mathcal{P}^{\text{no Eve}}_{k,\text{B}}} = \exp(-\mathcal{R}_\circ) = 1$. However, the probability ζ does not change with $\hat{\mathcal{L}}_A\gamma_k$. This implies that, even if the legitimate source nodes, Alices, transmit with infinite input SNRs, the SOP can never be zero and there will always be an SOP which is given by $1-\zeta$. In other words, the SOP saturates at ζ as $\hat{\mathcal{L}}_A\gamma_k \to \infty$.

Corollary 1: As $\gamma_J \to \infty$, the NSOP is given by

$$\overline{\mathcal{P}^{jam}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}} = \frac{\exp(-\mathcal{R}_\circ)}{(\mathcal{N}-2)!}Z(\mathcal{N}-1,0) = \exp(-\mathcal{R}_\circ) = \overline{\mathcal{P}^{no\ Eve}_{k,B}} \quad (21)$$

Proof: See Appendix -C. □

Corollary 1 suggests that, when $\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}$ is high, the SOPs in the presence of eavesdropping attacks will be equal to the connection outage probabilities. Hence, our proposed ZF-BF jamming scheme eliminates the impact of eavesdropping attacks. It is noteworthy that there is a connection outage probability which is independent of Eve's presence in the network.

Corollary 2: As Jim's number of transmit antennas tends to infinity, i.e., $\mathcal{N} \to \infty$, the NSOP is becomes independent of $\mathcal{N}$. That is, $|\mathbf{h}_{J-E}^\top \mathbf{W}|^2 \to \mathcal{N}$ and, hence, the instantaneous secrecy rate is given by

$$\mathcal{R}_{sec,k} = \left[\log_2\left(\frac{1+\hat{\mathcal{L}}_A\gamma_k\beta_{k,B}}{1+\frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,E}}{1+\hat{\mathcal{L}}_J\gamma_J}}\right)\right]^+ \quad (22)$$

and the NSOP is given by

$$\overline{\mathcal{P}^{jam}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}} = \frac{\hat{\mathcal{L}}_A\gamma_k}{\hat{\mathcal{L}}_A\gamma_k + 2^{\mathcal{R}}\frac{\hat{\mathcal{L}}_A\gamma_k}{1+\hat{\mathcal{L}}_J\gamma_J}}\exp(-\mathcal{R}_\circ) \quad (23)$$

[4]The expression in (20) is found in [29, eq. (3.353.5)].

Corollary (2) implies that, even though increasing the number of transmit antennas at Jim significantly will not directly increase the secrecy rate, it will make the impact of the jamming signal more powerful.

E. CSI ESTIMATION OVERHEAD

To estimate the required channels to perform the AN-ZF scheme, Bob broadcasts a set of known pilots signal so that Alice can compute her achievable information rate (and also the outage status of her links to Bob) and Jim can estimate his channels to Bob. Then, the Alice scheduled for information transmission sends a set of known pilot signals to Bob so that he can estimate his channels to that Alice. Note that Jim does not need to transmit any feedback signal to Bob since he designs the AN precoding matrix according to his channels to Bob. Since the AN signal is transparent to Bob, he does not need to know any information about it. Assume that Bob and Alice transmit a set of $f_\text{p} \geq 1$ pilot signals.[5] Since a bit duration is $1/W$ seconds, the time spent to realize the feedback and CSI estimation is too short and is equal to $\tau = 2f_\text{p}/W$ seconds. As the bandwidth W becomes very high, the feedback duration will be approximately zero. The portion of the time slot utilized for CSI estimation is then given by $\frac{\tau}{T} = 2f_\text{p}/(WT)$. Hence, the fraction of the time slot used for information transmission is $1 - \frac{2f_\text{p}}{WT} - \frac{\tau_f}{T}$, where $\frac{\tau_f}{T}$ is the fraction of the time slot used for reporting the decodability status of the information packet and is controlled by the upper layers. Thus, the target secrecy information rate is given by $\mathcal{R} = \frac{K_b}{(1-\frac{2f_\text{p}}{WT}-\frac{\tau_f}{T})WT}$ bits/sec/Hz.

IV. INFORMATION QUEUES STABILITY AND PROBLEM FORMULATION

In this section, we present our QoS-based optimization formulation which is critical for energy-limited wireless nodes equipped with information buffers.

A. QUEUE STABILITY

A fundamentally important performance measure of a communication network is the stability of its queues [24]. Our goal is to obtain the secrecy throughput region of the considered wireless system under queue stability and secure-throughput constraints which specifies the theoretical limit on information rates.

An information queue is stable when the probability of that queue being empty remains non-zero as time $t \to \infty$ [30]. The information queue $Q_{\text{d},k}$ is thus stable when

$$\lim_{y\to 0}\lim_{t\to\infty}\Pr\{Q^t_{\text{d},k} = y\} > 0. \quad (24)$$

Since the arrival and service processes at the information queues are strictly stationary, we can apply Loynes' theorem to check for queue stability conditions [24], [31]. Loynes' theorem states that if the arrival and service processes of an

[5]The value of f_p controls the quality of channel estimation.

information queue are strictly stationary, the queue is stable when the average service rate is higher than the average arrival rate of the queue.

B. OPTIMIZATION PROBLEM

The maximum Alices' secure-throughput region, if the system's information queues are stable and under certain tolerable secrecy throughput for each Alice, is obtained by solving the following optimization problem

$$\begin{aligned}\max_{\substack{\mathcal{L}_A,\mathcal{L}_J\in\{1,2,\ldots,\mathcal{E}_{\max}\}\\ 0\le\{\omega_k\}_{k=1}^{\mathcal{M}}\le 1}} .\ & \mu_{\mathrm{sec},k}\\ \text{s.t. } & \mu_{\mathrm{sec},\ell}\ge\mu_{\mathrm{req},\ell},\quad \forall \ell\neq k,\\ & \mu_{\mathrm{d},\ell}\ge\lambda_{\mathrm{d},\ell},\quad \forall \ell\neq k,\\ & \sum_{\ell=1}^{\mathcal{M}}\omega_\ell=1\end{aligned}\tag{25}$$

The constraint $\lambda_{\mathrm{d},k}\le\mu_{\mathrm{d},k}$ represents the k-th Alice's queue stability and the constraint $\mu_{\mathrm{sec},\ell}\ge\mu_{\mathrm{req},\ell}$, where $\mu_{\mathrm{req},\ell}$ is an application-specific secrecy throughput constraint, which represents QoS requirements for the Alices measured by a certain secure throughput constraint. For the problem to be feasible, the two QoS constraints need to be satisfied for all users.

The optimization problem in (25) can be reformulated as

$$\begin{aligned}\max_{\substack{\mathcal{L}_A,\mathcal{L}_J\in\{1,2,\ldots,\mathcal{E}_{\max}\}\\ 0\le\{\omega_k\}_{k=1}^{\mathcal{M}}\le 1}} : & \ \omega_k\frac{\lambda_{\mathrm{e},k}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}\right.\\ & \left.+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{k,\mathcal{L}_A,\mathcal{L}_J}}\right]\\ \text{s.t. } & \omega_\ell\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}\right.\\ & \left.+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{\mathrm{A}_\ell,\mathcal{L}_A,\mathcal{L}_J}}\right]\ge\mu_{\mathrm{req},\ell},\quad \forall \ell\neq k,\\ & \frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\exp\left(-\frac{2^{\mathcal{R}}-1}{\mathcal{L}_A\gamma_k}\right)\ge\lambda_{\mathrm{d},\ell},\quad \forall \ell\neq k,\\ & \sum_{\ell=1}^{\mathcal{M}}\omega_\ell=1\end{aligned}\tag{26}$$

For a given pair $(\mathcal{L}_J,\mathcal{L}_A)$, (26) is a linear programming optimization problem. The objective function will become ω_k, which is the only term that depends on the optimization variables. Substituting in the objective function with the equality constraint $\sum_{\ell=1}^{\mathcal{M}}\omega_\ell=1$, the objective function becomes $\omega_k=1-\sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\omega_\ell$. Removing the constant term, the objective function becomes $-\sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\omega_\ell$. Hence, the modified optimization problem is written as

$$\begin{aligned}\min_{0\le\{\omega_k\}_{k=1}^{\mathcal{M}}\le 1} : & \sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\omega_\ell\\ \text{s.t. } & \max\left\{\frac{\mu_{\mathrm{req},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{\mathrm{A}_\ell,\mathcal{L}_A,\mathcal{L}_J}}\right]},\tilde{\lambda}_\ell\right\}\\ & \le\omega_\ell,\quad \forall \ell\end{aligned}\tag{27}$$

where $\ell\neq k$ and $\tilde{\lambda}_\ell=\frac{\lambda_{\mathrm{d},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\exp\left(-\frac{2^{\mathcal{R}}-1}{\mathcal{L}_A\gamma_k}\right)}$. The objective function in (27) is minimized when the constraint becomes an equality, i.e., when $\{\omega_\ell\}_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}$ are adjusted to their lower limits, namely, $\omega_\ell=\max\{\frac{\mu_{\mathrm{req},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{\mathrm{A}_\ell,\mathcal{L}_A,\mathcal{L}_J}}\right]},\tilde{\lambda}_\ell\}$, $\forall \ell\neq k$. Then, from the equality constraint $\sum_{\ell=1}^{\mathcal{M}}\omega_\ell=1$, $\omega_k=1-\sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\omega_\ell$. Mathematically, the optimal time-slot allocation probabilities are given by

$$\begin{aligned}\omega_\ell^\star &= \max\left\{\frac{\mu_{\mathrm{req},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{\mathrm{A}_\ell,\mathcal{L}_A,\mathcal{L}_J}}\right]},\tilde{\lambda}_\ell\right\},\\ &\qquad \forall \ell\neq k,\\ \omega_k^\star &= 1-\sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\max\{\frac{\mu_{\mathrm{req},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{\mathrm{A}_\ell,\mathcal{L}_A,\mathcal{L}_J}}\right]},\\ &\qquad \tilde{\lambda}_\ell\}\end{aligned}\tag{28}$$

The secure-throughput region is thus given by

$$\mathcal{S}=\left\{\sum_{\ell=1}^{\mathcal{M}}\max\left\{\frac{\mu_{\mathrm{req},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\left[\left(1-\frac{\lambda_J}{\mathcal{L}_J}\right)\overline{\mathcal{P}^{\mathrm{nojam}}_{k,\mathcal{L}_A}}+\frac{\lambda_J}{\mathcal{L}_J}\overline{\mathcal{P}^{\mathrm{jam}}_{\mathrm{A}_\ell,\mathcal{L}_A,\mathcal{L}_J}}\right]},\tilde{\lambda}_\ell\right\}<1\right\}\tag{29}$$

with $\tilde{\lambda}_\ell=\frac{\lambda_{\mathrm{d},\ell}}{\frac{\lambda_{\mathrm{e},\ell}}{\mathcal{L}_A}\exp\left(-\frac{2^{\mathcal{R}}-1}{\mathcal{L}_A\gamma_k}\right)}$.

V. SIMULATION RESULTS

We consider the wireless network shown in Fig. 1 and evaluate the performance gains of our proposed design. We plot the maximum secure throughput of several benchmarks such as (1) the no-Eve case which represents an upper bound on secure throughput, and (2) the no-jammer case where Jim does not exist in the network. We compare the secure throughput of these two benchmarks with the secure throughput of our proposed scheme. All closed-form expressions derived in this paper are verified numerically. Unless otherwise stated

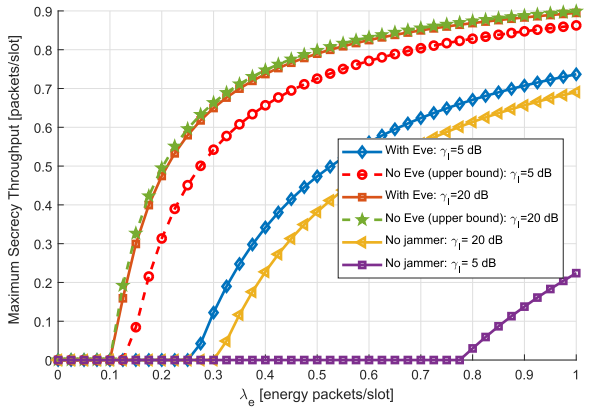


FIGURE 3. Maximum secure throughput versus λ_e.

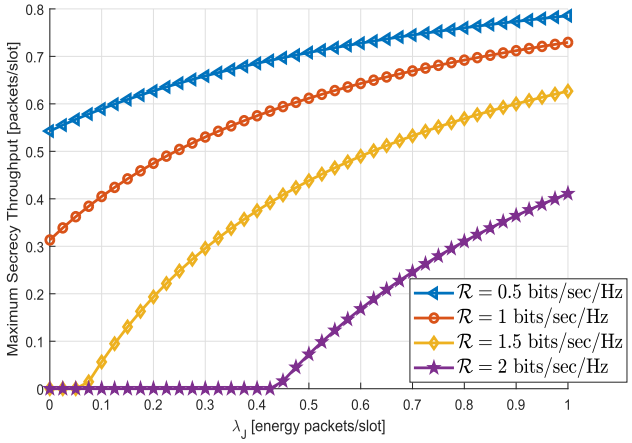


FIGURE 4. Maximum secure throughput versus λ_J for different values of $\mathcal{R}$.

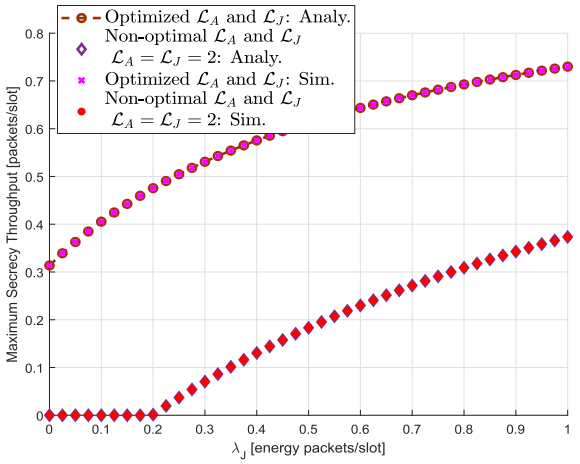


FIGURE 5. Maximum secure throughput versus λ_J for both un-optimized and optimized $\mathcal{L}_A$ and $\mathcal{L}_J$.

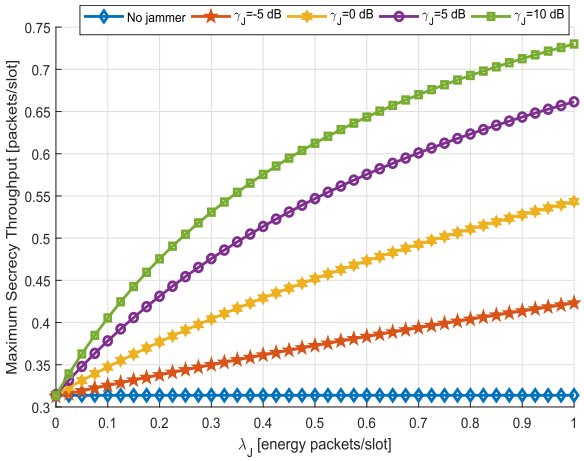


FIGURE 6. Maximum secure throughput versus λ_J for different γ_J.

explicitly, we use the following system's parameters: $\mu_{\text{req},\ell} = \mu^{\text{req}} = 0.1$ packets/time slot, $b = 1000$ bits, $WT = 1000$, $\mathcal{R}_\circ = K_b/(WT) = 1$ bits/sec/Hz, $\frac{\tau_f}{T} = 0.05$, $\gamma_k = \gamma_I = 5$ dB, $\gamma_J = 10$ dB, $\mathcal{N} = 5, f_{\text{p}} = 5, \mathcal{E}_{\max} = 6$, and $\mathcal{M} = 2$ source nodes. Since the secure throughput of the entire system is an $\mathcal{M}$-dimensional region, we simplify the presentation of the numerical results by assuming that $\lambda_{\text{d},2} = \lambda = 0.05$ packets/slot for the Alice 2.

Fig. 3 demonstrates the maximum throughput versus the average energy arrival rate at the Alices' batteries. As the energy arrival rate increases, the maximum throughput increases. As the Alice's transmit power increases, the secure throughput increases and it becomes closer to the upper bound (i.e., the case when there is no eavesdropping). Fig. 3 also shows the impact of having Jim in the network. Jim can significantly increase the secure throughput to the point where the eavesdropper has no impact on the system's security. Fig. 4 shows the impact of the target secrecy rate $\mathcal{R}$ and the average energy arrival rate at Jim on the maximum secure throughput. As $\mathcal{R}$ increases, the secure throughput decreases which is intuitive since the SOP increases as well. As the energy arrival rate at Jim increases, the ability of Jim to jam the eavesdropper increases and the security is enhanced. When $\lambda_J = 0$, this case is equivalent to the no-Jim case. When $\mathcal{R} = 1.5$ and $\mathcal{R} = 2$, the secure throughput is zero for the given parameters. Then, by increasing λ_J, the secure throughput increases significantly. This shows that, without Jim, the security can be highly compromised.

Fig. 5 demonstrates the impact of optimizing the transmission parameters $\mathcal{L}_A$ and $\mathcal{L}_J$ at both the Alices and Jim, respectively. As shown in the figure, optimizing $\mathcal{L}_A$ and $\mathcal{L}_J$ can significantly improve the security and the secure throughput gain is 400% at $\lambda_{\text{J}} = 0.5$ energy packets/slot. In Fig. 6, we plot the maximum secure throughput for different input SNR levels at Jim, denoted by γ_J. The figure also shows the case when there is no Jim and the security gains due to his presence. The curve of the no-Jim case is flat since Jim is absent. As the jamming transmit power at Jim increases, the secure throughput increases from almost 0.3 packets/slot to 0.75 packets/slot at $\lambda_J = 1$ energy packets/slot with a gain of almost 150%.

Finally, Fig. 7 shows the impact of the required QoS secure throughput on the secure throughput region. As the requirements of the second Alice, i.e., Alice 2, given by $\mu_{\text{req},\ell} = \mu^{\text{req}}$, increase, the secure throughput of Alice 1 decreases since the remaining resources decrease. In particular, as the QoS requirement increases, more time slots will be assigned to the users with higher QoS requirements and the remaining time slot resources will determine the envelope of the secure-throughput region which will decrease.

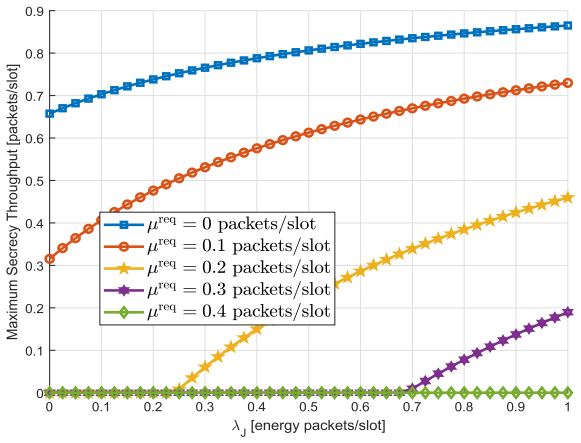


FIGURE 7. Maximum secure throughput versus λ_J for different QoS requirements.

VI. CONCLUSIONS

In this paper, we investigated the security of rechargeable-battery buffered source nodes communicating with their base station in the presence of eavesdropping nodes. The channel is shared through a TDMA scheme with probabilistic time-slot allocations. We designed new scheme for information and jamming signals transmissions given the battery constraints. We investigated the impact of the presence of a rechargeable jamming node on the secure throughput of the users. At the PHY layer, we proposed an AN-aided scheme employed by the cooperative jammer to reduce the SOPs and improve the users' QoS. We optimized the assignment probabilities to satisfy the QoS requirements of the legitimate users. We derived time-slot allocation probabilities and obtained their closed-form expressions and showed the impact of the energy states and the energy-harvesting parameters on the optimal assignments. We quantified the impact of the energy arrival rates at energy queues, the impact of the required QoS at Alices, the impact of target secrecy rate, and the impact of transmit power levels on the maximum secure throughput. The main conclusions are as follows

- The SOPs of our proposed AN-aided scheme depend on the energy arrival parameters at different nodes in addition to other parameters such as the number of transmit antennas at Jim.
- At high arrival rate at the jamming nodes and large energy packet size, the impact of the eavesdropping attack can be mitigated using cooperative jamming even in the presence of a limited-energy cooperative jammer.
- The optimal time-slot allocation probabilities are functions of the system's parameters, the secrecy outage probabilities, information packet sizes, the mean information arrival rates at the information queues, the mean arrival rates at Alices' energy batteries, and the mean arrival rate at the cooperative jammer's battery.
- The presence of Jim can increase the secure throughput by a gain of almost 150%. Moreover, optimizing the proposed scheme parameters and the used number of energy packets in a transmission can achieve again of 400%.
- Our proposed optimization approach can achieve close performance to the upper bound where Eve is not present. In addition, our approach showed a significant secure throughput gain relative to the case of non-optimized number of used energy packets for information and AN transmissions.

APPENDIX

A. MARKOV CHAIN GENERAL SOLUTION

In this appendix, we analyze the Markov chain of the energy queues (i.e., the Alices' energy queues and Jim's energy queue) shown in Fig. 8. We assume that the energy arrival at the energy queue is λ_e, where $\lambda_e = \lambda_{e,k}$ and $\lambda_e = \lambda_{J,k}$ for the energy queue of the k-th Alice and the energy queue of Jim, respectively. Since the arrival processes at the energy queues are Bernoulli, in a given time slot duration, the number of energy packet arrivals cannot exceed one. In addition, in a given time slot, the number of energy packet departures is $S_e \geq \mathcal{L}$ when the energy queue maintains S_e energy packets. Let us denote by π_ℓ the probability of the energy queue having ℓ energy packets. The general Markov chain is depicted in Fig. 8 where we solve the Markov chain of each Alice with the associated parameters a, b, $a_i = af_i$, $b_i = bf_i$, c_i, and f_i. For Jim's energy queue Markov chain parameters, Jim sends a jamming signal whenever his battery accumulates the appropriate amount of energy packets. Hence, his Markov chain should follow the Markov chain in Fig. 8. If Alice sends a binary signal to Jim indicating her activity status (sending information or not or at least the outage status of her channel to Bob), then Jim's battery Markov chain follows the Markov chain in Fig. 8. Otherwise, Jim's battery Markov chain should follow the Markov chain in Fig. 2.

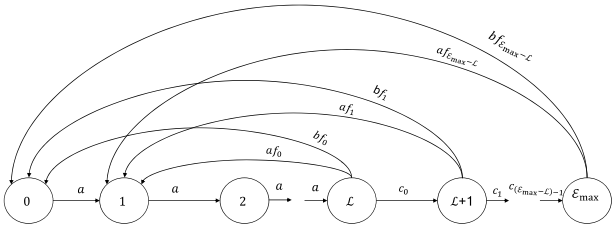


FIGURE 8. The Markov chain that models an energy queue. For visual clarity, the state-self transitions are eliminated from the graph.

To obtain the steady state distributions of the states, we rely on solving the balance equations at all states. The balance equation around state 0 is given by

$$\pi_0 a = (f_0\pi_{\mathcal{L}} + f_1\pi_{\mathcal{L}+1} + \cdots + f_{\mathcal{E}_{\max}-\mathcal{L}}\pi_{\mathcal{E}_{\max}})b \quad (30)$$

where $a = \lambda_e$ and $\mathcal{E}_{\max}$ is the maximum buffer size, $f_i = \omega_k\overline{\mathcal{P}_{k,\mathcal{L}+i}}$, with $\overline{\mathcal{P}_{k,\mathcal{L}+i}} = \exp\left(-\frac{2^{\mathcal{R}}-1}{\hat{\mathcal{L}}_A\gamma_k}\right)$, represents the no connection outage probability when $\mathcal{L}+i$ energy packets are used at the k-th Alice when she is selected for transmission, and $c_i = a(1-\omega_k\overline{\mathcal{P}_{k,\mathcal{L}+i}})$. When we solve Jim's energy queue Markov chain, $f_i = \sum_{k=1}^{\mathcal{M}}\omega_k\overline{\mathcal{P}_{k,\mathcal{L}+i}}$ and $c_i = a(1-\sum_{k=1}^{\mathcal{M}}\omega_k\overline{\mathcal{P}_{k,\mathcal{L}+i}})$. The state balance equation at state 1 is given by

$$\pi_1 a = \pi_0 a + (f_0\pi_{\mathcal{L}} + f_1\pi_{\mathcal{L}+1} + \ldots + f_{\mathcal{E}_{\max}-\mathcal{L}}\pi_{\mathcal{E}_{\max}})a \quad (31)$$

where $b = \overline{\lambda_e}$. The state balance equation at state 2 is given by

$$\pi_2 = \pi_1 \quad (32)$$

Similarly, for all states from state 3 to state $\mathcal{L}-1$, we have

$$\pi_2 = \pi_3 = \cdots = \pi_{\mathcal{L}-1} \quad (33)$$

The balance equation around state $\mathcal{L}$ is given by

$$\pi_{\mathcal{L}}(f_0\, a + f_0\, b + c_0) = \pi_{\mathcal{L}-1}a = \pi_1 a \quad (34)$$

The balance equation around state $\mathcal{L}+1$ is given by

$$\pi_{\mathcal{L}+1}(f_1\, a + f_1\, b + c_1) = \pi_{\mathcal{L}}c_0 = \pi_1 a \quad (35)$$

The balance equation around the final state, i.e., state $\mathcal{E}_{\max}$, is given by

$$\pi_{\mathcal{E}_{\max}}(f_{\mathcal{E}_{\max}-\mathcal{L}}a + f_{\mathcal{E}_{\max}-\mathcal{L}}b) = \pi_{\mathcal{E}_{\max}-1}c_{(\mathcal{E}_{\max}-\mathcal{L})-1} \quad (36)$$

Now, we are ready to solve the above equations together. From Eqns. (30) and (31), we see that

$$\pi_1 = \pi_0(1+\frac{a}{b}) = \pi_0\frac{1}{b} \quad (37)$$

Using (37), and from (33), we can obtain all states up to state $\pi_{\mathcal{L}-1}$. Furthermore, we have

$$\pi_{\mathcal{L}}(a_0+b_0+c_0) = \pi_1 a = \frac{a}{b}\pi_0 \quad (38)$$

Hence,

$$\pi_{\mathcal{L}} = \frac{1}{(a_0+b_0+c_0)}\frac{a}{b}\pi_0 \quad (39)$$

Then, we can relate the steady-state probability of state $\mathcal{L}+1$ and state 0 as follows

$$\pi_{\mathcal{L}+1} = \frac{a}{b}\pi_0\frac{c_1}{(a_1+b_1+c_1)(a_0+b_0+c_0)} \quad (40)$$

Hence, in general, for state $\mathcal{L}+r$ and excluding the final state since it will have a different formula, we have

$$\pi_{\mathcal{L}+r} = \frac{a}{b}\pi_0\prod_{j=0}^{r}\frac{c_j}{c_0(a_j+b_j+c_j)} \quad (41)$$

The final buffer state will be

$$\pi_{\mathcal{E}_{\max}} = \frac{\frac{a}{b}\pi_0}{(a\mathcal{E}_{\max}-\mathcal{L}+b\mathcal{E}_{\max}-\mathcal{L})}\prod_{j=0}^{(\mathcal{E}_{\max}-\mathcal{L})-1}\frac{c_j}{c_0(a_j+b_j+c_j)} \quad (42)$$

Then, we can get π_0 from the fact that the sum over all states must be 1 (i.e., we use the normalization condition). Hence,

$$\pi_0 + (\mathcal{L}-1)\frac{1}{b}\pi_0 + \pi_{\mathcal{L}} + \frac{a}{b}\pi_0\sum_{j=0}^{\mathcal{E}_{\max}-\mathcal{L}-1}\prod_{j=0}^{r}\frac{c_j}{c_0(a_j+b_j+c_j)} + \frac{\pi_0\frac{a}{b}}{(a\mathcal{E}_{\max}-\mathcal{L}+b\mathcal{E}_{\max}-\mathcal{L})}\prod_{j=0}^{(\mathcal{E}_{\max}-\mathcal{L})-1}\frac{c_j}{c_0(a_j+b_j+c_j)} = 1 \quad (43)$$

The probability that the energy queue (battery) is empty is given by (44) at the top of the next page. Moreover, the probability that the energy queue, Q_e, has more than $\mathcal{L}$ energy packets is given by (45) at the top of the next page.

Using the expression in (44), when $f_i = 1$ (i.e., the connection probability is negligible), $c_i = 0$ for all i. Hence, the steady-state probabilities become the ones in Eqns. (6) and (7) with $\pi_0 = \frac{b}{\mathcal{L}} = \frac{\overline{\lambda_e}}{\mathcal{L}}$.

B. PROOF OF LEMMA 1

Following the same procedures in [23], the NSOP for the k-th Alice's transmission can be written as follows

$$\begin{aligned}
&1-\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J} \\
&= \Pr\left\{\mathcal{R}\le R_{\text{sec},k},\, \beta_{k,\text{B}} \ge \frac{\beta_{k,\text{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\text{J}-E}^{\top}\mathbf{W}|^2}\right\} \\
&\quad + \Pr\left\{\mathcal{R}\le R_{\text{sec},k},\, \beta_{k,\text{B}} < \frac{\beta_{k,\text{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\text{J}-E}^{\top}\mathbf{W}|^2}\right\} \\
&= \Pr\left\{\mathcal{R}\le R_{\text{sec},k},\, \beta_{k,\text{B}} \ge \frac{\beta_{k,\text{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\text{J}-E}^{\top}\mathbf{W}|^2}\right\} \quad (46)
\end{aligned}$$

The last equality in (46) holds from the fact that, when $\beta_{k,\text{B}} < \frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,\text{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\text{J}-E}^{\top}\mathbf{W}|^2}$, the instantaneous secrecy rate is zero and, hence, $\Pr\{\mathcal{R}\le R_{\text{sec},k}\}$ is equal to zero when $\mathcal{R}>0$.

The probability in (46) can be rewritten as

$$\begin{aligned}
\overline{\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}} &= \Pr\left\{2^{\mathcal{R}} \le \frac{1+\hat{\mathcal{L}}_A\gamma_k\beta_{k,\text{B}}}{1+\frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,\text{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\text{J}-E}^{\top}\mathbf{W}|^2}}\right\} \\
&= \Pr\left\{\beta_{k,\text{B}} \ge \frac{2^{\mathcal{R}}\left(1+\frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,\text{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\text{J}-E}^{\top}\mathbf{W}|^2}\right)-1}{\hat{\mathcal{L}}_A\gamma_k}\right\} \quad (47)
\end{aligned}$$

$$\pi_0 = \frac{1}{1+(\mathcal{L}-1)\frac{1}{b}+\frac{a}{b}+\frac{a}{b}\sum_{j=0}^{\mathcal{E}_{\max}-\mathcal{L}-1}\prod_{j=0}^{r}\frac{c_j}{c_0(a_j+b_j+c_j)}+\frac{\frac{a}{b}}{(a\mathcal{E}_{\max}-\mathcal{L}+b\mathcal{E}_{\max}-\mathcal{L})}\prod_{j=0}^{(\mathcal{E}_{\max}-\mathcal{L})-1}\frac{c_j}{c_0(a_j+b_j+c_j)}} \tag{44}$$

$$\begin{aligned}\Pr\{Q_{\mathrm{e}}\geq\mathcal{L}\} &= 1-\pi_0-(\mathcal{L}-1)\pi_1 = 1-(1+(\mathcal{L}-1)\frac{1}{b})\pi_0\\ &= 1-\frac{1+(\mathcal{L}-1)\frac{1}{b}}{1+(\mathcal{L}-1)\frac{1}{b}+\frac{a}{b}+\frac{a}{b}\sum_{j=0}^{\mathcal{E}_{\max}-\mathcal{L}-1}\prod_{j=0}^{r}\frac{c_j}{c_0(a_j+b_j+c_j)}+\frac{\frac{a}{b}}{(a\mathcal{E}_{\max}-\mathcal{L}+b\mathcal{E}_{\max}-\mathcal{L})}\prod_{j=0}^{(\mathcal{E}_{\max}-\mathcal{L})-1}\frac{c_j}{c_0(a_j+b_j+c_j)}}\\ &= \frac{a}{b}\frac{1+\sum_{j=0}^{\mathcal{E}_{\max}-\mathcal{L}-1}\prod_{j=0}^{r}\frac{c_j}{c_0(a_j+b_j+c_j)}+\frac{1}{(a\mathcal{E}_{\max}-\mathcal{L}+b\mathcal{E}_{\max}-\mathcal{L})}\prod_{j=0}^{(\mathcal{E}_{\max}-\mathcal{L})-1}\frac{c_j}{c_0(a_j+b_j+c_j)}}{1+(\mathcal{L}-1)\frac{1}{b}+\frac{a}{b}+\frac{a}{b}\sum_{j=0}^{\mathcal{E}_{\max}-\mathcal{L}-1}\prod_{j=0}^{r}\frac{c_j}{c_0(a_j+b_j+c_j)}+\frac{\frac{a}{b}}{(a\mathcal{E}_{\max}-\mathcal{L}+b\mathcal{E}_{\max}-\mathcal{L})}\prod_{j=0}^{(\mathcal{E}_{\max}-\mathcal{L})-1}\frac{c_j}{c_0(a_j+b_j+c_j)}}\end{aligned} \tag{45}$$

Since Rayleigh fading is assumed, $\beta_{k,\mathrm{B}}$ is an exponentially-distributed random variable with unit mean. Hence, for given channel realizations $\beta_{k,\mathrm{E}}$ and $|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2$, we get

$$\begin{aligned}\Pr\left\{\beta_{k,\mathrm{B}}\geq\frac{2^{\mathcal{R}}\left(1+\frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,\mathrm{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2}\right)-1}{\hat{\mathcal{L}}_A\gamma_k}\middle|\beta_{k,\mathrm{E}},|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2\right\}\\ =\exp\left(-\frac{2^{\mathcal{R}}\left(1+\frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,\mathrm{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2}\right)-1}{\hat{\mathcal{L}}_A\gamma_k}\right)\end{aligned} \tag{48}$$

Averaging over $\beta_{k,\mathrm{E}}$, we get

$$\begin{aligned}&\int_0^{\infty}\exp\left(-\frac{2^{\mathcal{R}}\left(1+\frac{\hat{\mathcal{L}}_A\gamma_k\beta_{k,\mathrm{E}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2}\right)-1}{\hat{\mathcal{L}}_A\gamma_k}\right)\\ &\quad\times\exp(-\beta_{k,\mathrm{E}})d\beta_{k,\mathrm{E}}\\ &=\exp(-\mathcal{R}_{\circ})\int_0^{\infty}\exp\left(-\eta\beta_{k,\mathrm{E}}\right)\exp(-\beta_{k,\mathrm{E}})d\beta_{k,\mathrm{E}}\\ &=\frac{\exp(-\mathcal{R}_{\circ})}{1+\eta}\end{aligned} \tag{49}$$

where $\mathcal{R}_{\circ}=\frac{2^{\mathcal{R}}-1}{\hat{\mathcal{L}}_A\gamma_k}$ and $\eta=\frac{2^{\mathcal{R}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2}$.

Since the columns of $\mathbf{W}$ are orthonormal, the product of $\mathbf{W}$ and the channel i.i.d. vector $\mathbf{h}_{\mathrm{J}-E}^{\top}$ is still an i.i.d. Gaussian vector. Following the discussions in [32], the random variable $x=|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2$ is Chi-square with $2(\mathcal{N}-1)$ degrees of freedom. The probability density function (PDF) of x is given by

$$\mathcal{F}_x(\theta)=\frac{1}{(\mathcal{N}-2)!}\theta^{\mathcal{N}-2}\exp(-\theta),\quad\theta\geq 0 \tag{50}$$

where $\mathcal{N}\geq 2$. Taking the expectation of the expression in (49) over $x=|\mathbf{h}_{\mathrm{J}-E}^{\top}\mathbf{W}|^2$, the NSOP is

$$\begin{aligned}&1-\mathcal{P}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}^{\mathrm{jam}}\\ &\quad=\int_0^{\infty}\frac{\exp(-\mathcal{R}_{\circ})}{1+\frac{2^{\mathcal{R}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}x}}\frac{1}{(\mathcal{N}-2)!}x^{\mathcal{N}-2}\exp(-x)dx\\ &\quad=\frac{\exp(-\mathcal{R}_{\circ})}{(\mathcal{N}-2)!}\int_0^{\infty}\frac{x^{\mathcal{N}-2}}{1+\frac{2^{\mathcal{R}}}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}x}}\exp(-x)dx\end{aligned} \tag{51}$$

This probability is rewritten as

$$\begin{aligned}&\overline{\mathcal{P}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}^{\mathrm{jam}}}\\ &=\frac{\exp(-\mathcal{R}_{\circ})}{(\mathcal{N}-2)!}\int_0^{\infty}\frac{x^{\mathcal{N}-2}(1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}x)}{1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}x+2^{\mathcal{R}}}\exp(-x)dx\\ &=\frac{\exp(-\mathcal{R}_{\circ})}{(\mathcal{N}-2)!}\frac{1}{\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}}\int_0^{\infty}\frac{x^{\mathcal{N}-2}(1+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}x)}{x+\mathcal{R}_1}\exp(-x)dx\\ &=\frac{\exp(-\mathcal{R}_{\circ})}{(\mathcal{N}-2)!}\frac{1}{\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}}\left(\int_0^{\infty}\frac{x^{\mathcal{N}-2}}{x+\mathcal{R}_1}\exp(-x)dx\right.\\ &\quad\left.+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}\int_0^{\infty}\frac{x^{\mathcal{N}-1}}{x+\mathcal{R}_1}\exp(-x)dx\right)\\ &=\frac{\exp(-\mathcal{R}_{\circ})}{(\mathcal{N}-2)!}\frac{\left(\mathrm{Z}(\mathcal{N}-2,\mathcal{R}_1)+\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}\mathrm{Z}(\mathcal{N}-1,\mathcal{R}_1)\right)}{\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}}\end{aligned} \tag{52}$$

where $\mathcal{N}\geq 2$ and the expression of $\mathrm{Z}(\cdot,\cdot)$ [29, eq. (3.353.5)] is given by (20) with $\mathrm{Ei}(\cdot)$ denoting the exponential integral function.

The term $\exp(-\mathcal{R}_{\circ})$ in (20) represents the NSOP when there is no eavesdropping attacks on the network. Hence,

it can be rewritten as follows

$$\overline{\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}} = \overline{\mathcal{P}^{\text{no Eve}}_{k,\text{B}}} \frac{\text{Z}\left(\mathcal{N}-2,\mathcal{R}_1\right) + \frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}\text{Z}\left(\mathcal{N}-1,\mathcal{R}_1\right)}{\frac{\hat{\mathcal{L}}_J\gamma_J}{\mathcal{N}-1}(\mathcal{N}-2)!} \tag{53}$$

where $\mathcal{P}^{\text{no Eve}}_{k,\text{B}} = 1 - \exp\left(-\mathcal{R}_\circ\right)$.

C. PROOF OF COROLLARY 1

From (19) in Lemma 1, as $\gamma_J \to \infty$, we have

$$\lim_{\gamma_J\to\infty} \overline{\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}} = \overline{\mathcal{P}^{\text{no Eve}}_{k,\text{B}}} \frac{\text{Z}\left(\mathcal{N}-1,0\right)}{(\mathcal{N}-2)!} \tag{54}$$

From (20), $\text{Z}\left(\mathcal{N}-1,0\right) = \Gamma(\mathcal{N}-1) = (\mathcal{N}-2)!$, where $\Gamma(\cdot)$ is the Gamma function. Hence,

$$\lim_{\gamma_J\to\infty} \overline{\mathcal{P}^{\text{jam}}_{k,\hat{\mathcal{L}}_A,\hat{\mathcal{L}}_J}} = \overline{\mathcal{P}^{\text{no Eve}}_{k,\text{B}}} = \exp\left(-\mathcal{R}_\circ\right) \tag{55}$$

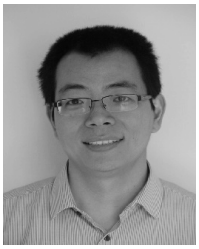
This completes the proof.

REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[2] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
[3] Y. Zhong, X. Ge, H. H. Yang, T. Han, and Q. Li, "Traffic matching in 5G ultra-dense networks," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 100–105, Aug. 2018.
[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[6] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
[7] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.
[8] T.-X. Zheng, H.-M. Wang, R. Huang, and P. Mu, "Secrecy-throughput-optimal artificial noise design against randomly located eavesdroppers," in *Proc. IEEE ICNC*, Feb. 2016, pp. 1–5.
[9] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
[10] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Security of an ordered-based distributive jamming scheme," *IEEE Commun. Lett.*, vol. 21, no. 1, pp. 72–75, Jan. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7582356/
[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP 15th Workshop Statist. Signal Process.*, Aug. 2009, pp. 417–420.
[12] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Security of rechargeable energy-harvesting transmitters in wireless networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 384–387, Aug. 2016.
[13] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.
[14] X. Zhou, M. Tao, and R. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Proc. IEEE ICC*, Jun. 2012, pp. 2339–2344.
[15] C. Wang, H. M. Wang, X. G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May 2015.
[16] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, Jr., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, Jan. 2015.
[17] Y. Zhong, X. Ge, T. Han, Q. Li, and J. Zhang, "Tradeoff between delay and physical layer security in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1635–1647, Jul. 2018.
[18] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
[20] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On-off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6075–6088, Aug. 2016.
[21] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.
[22] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.
[23] A. El Shafie, T. Q. Duong, and N. Al-Dhahir, "QoS-aware enhanced-security for TDMA transmissions from buffered source nodes," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1051–1065, Feb. 2017.
[24] A. K. Sadek, K. J. R. Liu, and A. Ephremides, "Cognitive multiple access via cooperation: Protocol design and performance analysis," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3677–3696, Oct. 2007.
[25] A. A. El-Sherif, A. K. Sadek, and K. Liu, "Opportunistic multiple access for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 704–715, Apr. 2011.
[26] A. Sultan, "Sensing and transmit energy optimization for an energy harvesting cognitive radio," *IEEE Wireless Commun. Lett.*, vol. 1, no. 5, pp. 500–503, Oct. 2012.
[27] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.
[28] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Jul. 2006, pp. 356–360.
[29] D. Zwillinger, *Table of Integrals, Series, and Products*. Amsterdam, The Netherlands: Elsevier, 2014.
[30] O. Simeone, Y. Bar-Ness, and U. Spagnolini, "Stable throughput of cognitive radios with and without relaying capability," *IEEE Trans. Commun.*, vol. 55, no. 12, pp. 2351–2360, Dec. 2007.
[31] R. M. Loynes, "The stability of a queue with non-independent inter-arrival and service times," *Math. Proc. Cambridge Philos. Soc.*, vol. 58, no. 3, pp. 497–520, Jul. 1962.
[32] J. Liu, W. Chen, Z. Cao, and Y. J. A. Zhang, "Cooperative beamforming for cognitive radio networks: A cross-layer design," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1420–1431, May 2012.

AHMED EL SHAFIE received the B.Sc. degree (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2009, the M.Sc. degree in communication and information technology from Nile University, Cairo, Egypt, in 2014, and the Ph.D. degree from The University of Texas at Dallas, Richardson, TX, USA, in 2018. Since 2018, he has been a Senior Systems Engineer with Qualcomm Technologies, Inc., San Diego, CA, USA. He is an IEEE Senior Member. He was a recipient of the David Daniel Best Doctoral Thesis Award, in 2018, and the Jonsson School Industrial Advisory Council Fellowship Award, in 2017. He received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award, in 2015, 2016, and 2017. He also received the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer Award, in 2016. He is nominated for the 2018 CGS/ProQuest Distinguished Dissertation Award. He currently serves as an Editor for the IEEE COMMUNICATIONS LETTERS, *Physical Communications*, and *Transactions on Emerging Technologies in Telecommunications*. In addition, he serves as a Guest Editor for the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS and NETWORKING.

NAOFAL AL-DHAHIR received the Ph.D. degree in electrical engineering from Stanford University. From 1994 to 2003, he was a Principal Member of the Technical Staff at GE Research and the AT&T Shannon Laboratory. He is currently the Erik Jonsson Distinguished Professor with The University of Texas at Dallas. He has co-invented 41 issued U.S. patents and has co-author over 400 papers. He was a co-recipient of four IEEE best paper awards. He is the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS.



ZHIGUO DING received the B.Eng. degree in electrical engineering from the Beijing University of Posts and Telecommunications, in 2000, and the Ph.D. degree in electrical engineering from Imperial College London, in 2005. From 2005 to 2018, he was with Queen's University Belfast, Imperial College London, Newcastle University, and Lancaster University. From 2012 to 2018, he was an Academic Visitor with Princeton University. Since 2018, he has been with the University of Manchester as a Professor in communications. His research interests are 5G networks, game theory, cooperative and energy harvesting networks, and statistical signal processing. He was an Editor of the IEEE WIRELESS COMMUNICATION LETTERS and the IEEE COMMUNICATION LETTERS, from 2013 to 2016. He is serving as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the *Journal of Wireless Communications and Mobile Computing*. He received the Best Paper Award in the IET ICWMC-2009 and the IEEE WCSP-2014, the EU Marie Curie Fellowship, in 2012–2014, the Top IEEE TVT Editor Award, in 2017, the IEEE Heinrich Hertz Award, in 2018, and the IEEE Jack Neubauer Memorial Award, in 2018.

TRUNG Q. DUONG received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden, in 2012. He was a Lecturer (Assistant Professor) with Queen's University Belfast, U.K., from 2013 to 2017, where he has been a Reader (Associate Professor), since 2018. He has authored or co-authored over 300 technical papers published in scientific journals (181 articles) and presented in international conferences (130 papers). His current research interests include the Internet of Things, wireless communications, molecular communications, and signal processing. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference, in 2013, the IEEE International Conference on Communications, in 2014, the IEEE Global Communications Conference, in 2016, and the IEEE Digital Signal Processing Conference, in 2017. He was a recipient of the prestigious Royal Academy of Engineering Research Fellowship (2016–2021) and the prestigious Newton Prize, in 2017. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON COMMUNICATIONS, and the *IET Communications* and as a Lead Senior Editor for the IEEE COMMUNICATIONS LETTERS.

RIDHA HAMILA received the M.Sc. degree, the Licentiate of Technology degree (Hons.), and the Doctor of Technology degree from the Department of Information Technology, Tampere University of Technology (TUT), Tampere, Finland, in 1996, 1999, and 2002, respectively, where he held various research and teaching positions with the Department of Information Technology, from 1994 to 2002. From 2002 to 2003, he was a System Specialist with the Nokia Research Center and Nokia Networks, Helsinki. From 2004 to 2009, he was with the Etisalat University College, Emirates Telecommunications Corporation, United Arab Emirates. He served as a Supervisor for a large number of bachelor's/master's students and Postdoctoral fellows. He is currently an Associate Professor with the Department of Electrical Engineering, Qatar University, Qatar. He is also an Adjunct Professor with the Department of Communications Engineering, TUT. He has been involved in several past and current industrial projects, Qtel, QNRF, Finnish Academy projects, TEKES, Nokia, EU research, and education programs. His current research interests include mobile and broadband wireless communication systems, cellular and satellites-based positioning technologies, and synchronization and DSP algorithms for flexible radio transceivers.