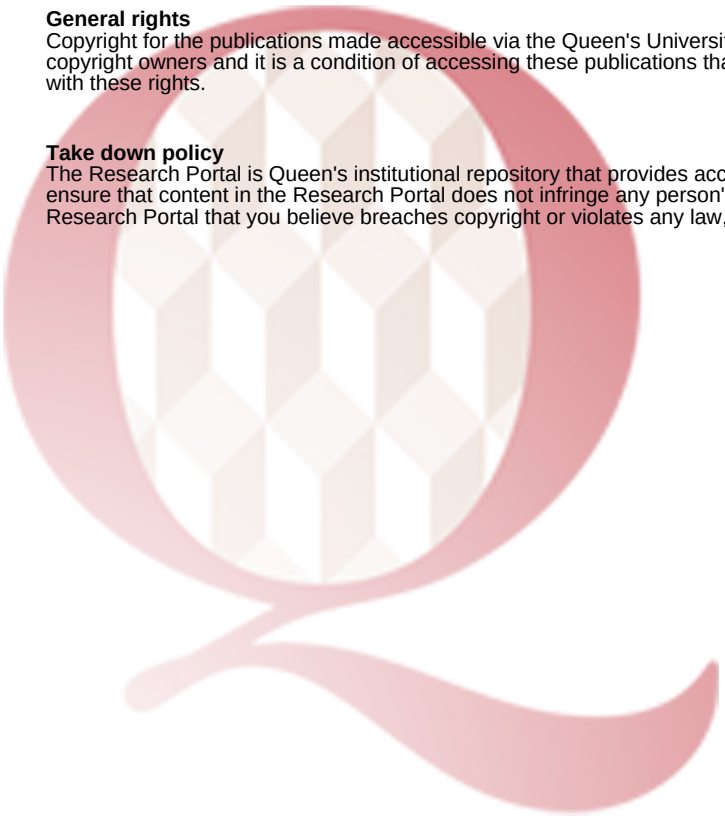
QoS-Aware Enhanced-Security for TDMA Transmissions from Buffered Source Nodes

El Shafie, A., Duong, T. Q., & Al-Dhahir, N. (2016). QoS-Aware Enhanced-Security for TDMA Transmissions from Buffered Source Nodes. IEEE Transactions on Wireless Communications. DOI: 10.1109/TWC.2016.2636201

Published in:
IEEE Transactions on Wireless Communications

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal



QoS-Aware Enhanced-Security for TDMA Transmissions from Buffered Source Nodes

Ahmed El Shafie, Trung Q. Duong, and Naofal Al-Dhahir

***Abstract*—This paper proposes a cross-layer design to secure a set of buffered legitimate source nodes wishing to communicate with a common destination node using a time-division multiple-access scheme. The users' assignment probabilities to the time slots are optimized to satisfy a certain quality-of-service (QoS) requirement for all the legitimate source nodes. To further improve the system security, we propose beamforming-based cooperative jamming schemes subject to the availability of the channel state information (CSI) at the legitimate nodes. We derive closed-form expressions for the instantaneous secrecy rate for each scheme as well as the secrecy outage probability. Moreover, we derive the secrecy stable-throughput and delay-requirement regions. In our proposed scheme, if a node is not selected for data transmission, it is a cooperative jamming node. We impose an average transmit power constraint on each source node. We investigate the cases where a global CSI is assumed at the legitimate nodes and where there is no eavesdropper's CSI. The case where there is no CSI at the jamming nodes is also investigated and a new scheme is proposed. Our proposed jamming schemes achieve significant increases in the secure throughput over existing schemes from the literature and over the no-jamming scheme.**

***Index Terms*—Cooperative jamming, queues, secrecy rate.**

I. Introduction

Secure communications in an information-theoretic sense was first investigated in the seminal work of Wyner [2] which is currently well-known as the physical (PHY) layer security. In PHY-layer security, the system security is measured by the secrecy capacity of the link connecting the legitimate parties, which is the maximum transmission rate that can be achieved without information leakage to an eavesdropping node.

The instantaneous secrecy rate can be efficiently increased in two ways: (1) by improving the signal-to-noise ratio (SNR) of the legitimate receiver and/or (2) by reducing the SNR of the eavesdropper (e.g. by adding controlled artificial noise (AN) or interference). Hence, interference emerges as a viable resource for enhancing wireless security. The legitimate communication partners can cooperate to increase the noise level (interference) of the eavesdropper link and ensure higher secure communication rates. This idea has already appeared in the PHY-layer security literature under the name of AN [3]–[6] or cooperative jamming [7]. In [4], [5], the problem of secure communication with multi-antenna transmission in fading channels was investigated. The source node simultaneously transmits an information bearing signal to the intended destination node and AN signals to confuse the eavesdropping node. A comprehensive survey of PHY-layer security in multi-user wireless networks including jamming techniques is found in [8].

Part of this paper has been accepted for publication in the global communications conference (Globecom) 2016 [1].

A. El Shafie and N. Al-Dhahir are with the University of Texas at Dallas, USA, e-mails: {ahmed.elshafie}{aldhahir}@utdallas.edu. The work of A. El Shafie and N. Al-Dhahir was made possible by NPRP grant number 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.

T. Q. Duong is with Queens University Belfast, Belfast BT7 1NN, U.K. e-mail: trung.q.duong@qub.ac.uk. The work of T. Q. Duong was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, by the Newton Institutional Link under Grant ID 172719890, and by the Royal Society Research Grant under Grant ID RG160302.

A. Related Work

The single-jammer selection problem was investigated in many works, e.g., [9]. The authors of [9] proposed various jamming schemes based on the available channel state information (CSI) at the legitimate nodes. In [10] and [11], the authors assumed that a transmitter communicates with its destination in the presence of a multi-antenna cooperative jammer and an eavesdropper. The cooperative jammer was assumed to transmit AN signals to maximize the instantaneous secrecy rate. The eavesdropper's CSI was assumed known at the legitimate nodes. The optimal beamforming (BF) vector and power allocation at the cooperative jammer were designed to increase the system instantaneous secrecy rate. Using the same jamming BF technique as in [10], the authors of [12] considered the presence of a set of amplify-and-forward relay nodes which helps in forwarding the source packets in addition to jamming the eavesdropper. The authors assumed that the eavesdropper's CSI is not available at the legitimate nodes. However, the above works did not derive closed-form expressions for important performance metrics, such as the secrecy outage probability.

In [13], a modified slotted-ALOHA protocol is proposed where each legitimate transmitter either transmits its data or acts as a cooperative jammer according to a message transmission probability. In [14], the authors study a single-input, multi-output, multi-eavesdropper wiretap channel with multiple friendly single-antenna cooperative jammers. Random networks are considered where the cooperative jammers and the eavesdroppers are distributed according to independent two-dimensional homogeneous Poisson point processes (PPP). To confound the eavesdroppers, an opportunistic jammer selection scheme is proposed, where the cooperative jammers whose channels are nearly orthogonal to the legitimate channel are selected to transmit independent and identically distributed (i.i.d.) Gaussian jamming signals. In [15], the authors investigated the secure AN-aided multi-antenna transmission in multiple-input single-output (MISO) slow fading channels. The eavesdroppers are distributed as PPP. The authors aimed at maximizing the secrecy throughput subject to a certain secrecy outage constraint.

The authors of [16] investigated PHY-layer security for 5G networks and discussed three most promising technologies: heterogenous networks, massive multiple-input multiple-output, and millimeter wave. In [17], the authors considered the problem of secure communication with multi-antenna transmission in fading channels with single-antenna legitimate receive node and multiple single-antenna eavesdropping nodes. The transmitting node simultaneously transmits a data signal to the legitimate receiver and an AN signal to confuse the eavesdroppers. An analytical closed-form expression of an achievable secrecy rate was obtained and the transmit power allocation between the data and the AN signals was optimized to maximize the instantaneous secrecy rate. The authors investigated both cases of noncolluding and colluding eavesdroppers. In [18], an on-off transmission scheme was proposed for wiretap channels with outdated CSI. The authors considered the outdated CSI from the legitimate receiver under two distinct scenarios, depending on whether or not the outdated CSI from the eavesdropper is known at the legitimate transmitter. New closed-form expressions for the transmission probability, the connection outage probability, the secrecy outage probability, and the reliable and secure transmission probability were derived to characterize the achievable system's performance. The authors of [19] investigated the secure transmission design in practical scenarios by considering channel estimation errors at the legitimate receiver and investigating both fixed- and variable-rate transmissions.

In [20], the authors proposed a new secure transmission scheme in a multiple-input multiple-output multiple-eavesdropper (MIMOME) wiretap channel. The legitimate transmitter adopts transmit antenna selection (TAS) to choose the antenna that maximizes the instantaneous SNR at the legitimate receiver. Both the legitimate receiver and the eavesdropper adopt maximal-ratio combining (MRC) to combine the received signals from the legitimate transmitter. The authors assumed that the CSI during the TAS process is outdated and proposed a new transmission scheme to mitigate the effect of the outdated CSI on the wiretap codes design at the legitimate transmitter. Moreover, they investigated the impact of the spatial correlation at the receiver. It was shown that the outdated TAS reduces the secrecy diversity order. Moreover, antenna correlation improves the secrecy performance in the low SNR regime but degrades the secrecy performance in the moderate and high SNR regimes. In [21], the authors investigated PHY-layer security in an underlay cognitive radio (CR) network in the presence of randomly distributed eavesdroppers. For different CSI knowledge at the transmitting node, the authors proposed four transmission protocols to improve the secure transmission in the CR network. The optimal design parameter for each transmission protocol was obtained by solving a constrained optimization problem that maximizes the secrecy throughput subject to both security and reliability constraints.

All the above-mentioned papers did not consider the impact of cross-layer (i.e. medium access control (MAC) and network layers along with the PHY layer) design on the security of the system and users' quality-of-service (QoS) requirements. In this paper, we consider a set of buffered source nodes using a time-division multiple-access (TDMA) scheme to communicate with their common destination in the presence of an eavesdropper. We assume a slotted-time system in which the time is partitioned into slots. In a given time slot, one of the source nodes is chosen for data transmission. If a node is not assigned for data transmission, then it is a potential cooperative jammer. To satisfy the legitimate user QoS requirements, we optimize the fraction of time slots assigned to each legitimate user. We emphasize the practical relevance of the work presented in this paper. Our model deals with the uplink scenario of a TDMA network. As argued in the wireless communication literature [22], [23], TDMA is widely used in many networks such as the GSM cellular networks, Bluetooth personal area networks, IEEE 802.16a WiMax broadband wireless access networks, and more. Therefore, by assuming the general framework of TDMA networks, our work can be applied to any TDMA-based network.

B. Contributions

The contributions of this paper are summarized as follows

- We propose a three-layer optimization approach to enhance the security of the multiple-access system under investigation. That is, we optimize the PHY-layer by increasing the probability of secure transmissions. This is realized through AN injection in the direction of the eavesdropper and optimal allocation of the average power assigned to data transmission and that assigned to AN transmission to satisfy a certain average power constraint. Then, we optimize the MAC and network layers by designing the fraction of time slots to satisfy the queue-stability and user-QoS constraints.
- We investigate two types of QoS-constrained optimization problems. More specifically, we derive the secrecy stable-throughput region of the network, which characterizes the maximum stable secrecy throughput of each user such that all users' queues are stable. We show analytically that the optimal time slot assignment is a function of the users' secrecy outage probabilities. In addition, we investigate the queueing delay of the users and derive a closed-form expression for the average queueing delay of the queues. We characterize the delay-requirement region which determines the minimum achievable secure queueing delay of a node given certain delay requirements for the other nodes in the network. In this case, the optimal time slot assignment is a function of the users' secrecy outage probabilities, average arrival rates to the queues, and the delay requirement of each user.
- Through improving the instantaneous secrecy rate and reducing the secrecy outage probability, we can better satisfy the QoS requirements of the users. Hence, we propose and compare BF-based cooperative jamming schemes that depend on the availability of CSI at the legitimate nodes and the number of jamming nodes participating in confounding the eavesdropper. Each of the jamming schemes results in a different set of secrecy outage probabilities for the legitimate users which vary the time-assignment probabilities. We derive the instantaneous secrecy rate and secrecy outage probability under each of our proposed schemes.

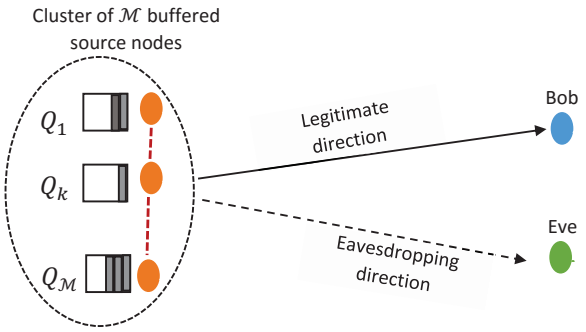


Fig. 1. Network Model. Each source node is equipped with a buffer to store its own data traffic. The number of source nodes is $\mathcal{M}$. All nodes are equipped with a single antenna.

Notation: $(\cdot)^*$ denotes complex-conjugate operation. $(\cdot)^\top$ denotes 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. The function $\min(\cdot,\cdot)$ ($\max(\cdot,\cdot)$) returns the minimum (maximum) among the values enclosed between brackets. $\mathbb{E}\{\cdot\}$ 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. A list of the key variables is given in Table I.

II. System Model and Assumptions

Assume a set of $\mathcal{M}$ source nodes sharing the same frequency band and wishing to communicate with a common destination (base-station) in the presence of an eavesdropper as shown in Fig. 1. The source nodes are labeled $1,2,\ldots,\mathcal{M}$. The eavesdropper (*Eve*) and the destination (*Bob*) are denoted by E and B, respectively. All nodes are assumed to be equipped with one antenna.

We assume Rayleigh flat-fading channels. The channel coefficient between Node $n_1 \in \{1,2,\ldots,\mathcal{M},\mathrm{B},\mathrm{E}\}$ and Node $n_2 \in \{1,2,\ldots,\mathcal{M},\mathrm{B},\mathrm{E}\}$, denoted by h_{n_1,n_2}, remains constant during a time slot, but changes identically and independently from one time slot to another. Each channel coefficient is modeled as a circularly-symmetric Gaussian random variable with zero mean and unit variance. The thermal noise at a receiving node is modeled as an additive white Gaussian noise (AWGN) with zero mean and variance κ. We assume that the time is slotted into durations of T seconds [22], [23]. In a given time slot, Transmitter $k \in \mathcal{T}$ (which we refer to as *Alice*), where $\mathcal{T} = \{1,2,\ldots,\mathcal{M}\}$, is chosen for data transmission with probability $0 \le \omega_k \le 1$. Thus, $\sum_{k=1}^{\mathcal{M}} \omega_k \le 1$ [22], [23]. The time slot assignment probabilities $(\omega_1,\omega_2,\ldots,\omega_{\mathcal{M}})$ are optimized to satisfy the QoS of the source nodes, such as queue stability or certain queueing delay requirements for each user. This will be discussed in detail in Section III.

A. Queue Model and Node Transmit Power

The set of all source nodes **excluding** the one assigned to the time slot for data transmission (i.e. Node k) is denoted by $\mathcal{J} = \{1,2,\ldots,k-1,k+1,\ldots,\mathcal{M}\}$, where $k \notin \mathcal{J}$. We assume that Node k maintains a buffer Q_k to store its incoming traffic. The arrivals at Node k are Bernoulli random variables with mean λ_k packets/slot [22]. This model is generic as it includes the case of source nodes that may participate in jamming Eve from one time slot to another, and the case of a jamming node which is **permanently** dedicated for jamming Eve whenever needed. If $\lambda_k = 0$, Node k is a potential jamming node that participates in confusing Eve in every time slot. We assume that the average transmit power employed by Node $k \in \mathcal{T}$ for information transmission in each time slot is P_I Watts/Hz. The AN signals used in jamming are modeled as zero-mean circularly-symmetric complex Gaussian random variables [13], [27]. The average jamming power in each time slot is constrained by P_J Watts/Hz. Moreover, we impose an average transmit power P (averaged across time slots) on each source node. Hence, the source nodes should distribute their average transmit powers *throughout the network operation* (averaged across the time slots) between data and AN transmissions to satisfy the QoS requirements.

B. Data and Secrecy Rates

We assume that the time needed for channel estimation of all links and transmission of control signals is $\tau < T$. Thus, the data transmission time of a legitimate node is $T-\tau$. Assuming that the packet size of a transmitter is b bits and the channel bandwidth is W Hz, the target secrecy rate is $\mathcal{R} = \frac{\mathcal{R}_\circ}{1-\frac{\tau}{T}} = \frac{b}{(T-\tau)W}$ with $\mathcal{R}_\circ = \frac{b}{WT}$. The secrecy outage happens when the target secrecy rate exceeds the instantaneous secrecy rate. Letting $\mathbb{R}_{n_1,n_2}$ denote the channel rate of the $n_1 - n_2$ link, the instantaneous secrecy rate of Transmitter k is given by [9], [10], [12], [28]

$$R_{\mathrm{s},k} = [\mathbb{R}_{k,\mathrm{B}} - \mathbb{R}_{k,\mathrm{E}}]^+ \le \mathbb{R}_{k,\mathrm{B}} \tag{1}$$

where $[\cdot]^+ = \max(\cdot,0)$ denotes the maximum between the enclosed values in brackets and *zero*. Since we assume fixed-rate transmissions, if the target secrecy rate, denoted by $\mathcal{R}$, is greater than the $k-\mathrm{B}$ link rate $\mathbb{R}_{k,\mathrm{B}}$, then it is greater than the instantaneous secrecy rate $R_{\mathrm{s},k}$ since $\mathbb{R}_{k,\mathrm{B}} \ge R_{\mathrm{s},k}$. Hence, the data cannot be decoded reliably and securely at Bob. For this reason, we assume that if $\mathcal{R}$ exceeds the direct link rate, the node assigned for data transmission remains idle to save its power. We define two types of outage events

1) **Connection outage**: The connection outage is defined as the event that the rate of the Alice-Bob link is below the target secrecy rate $\mathcal{R}$.
2) **Secrecy outage**: The secrecy outage is defined as the event that the instantaneous secrecy rate of the Alice-Bob link is below the target secrecy rate $\mathcal{R}$.

C. Wiretap Code Design

Consider the scenario that the kth Alice transmits a data packet to Bob. In a given time slot $t \in \{1,2,3,\ldots\}$, Alice

adaptively adjusts her transmission rate $\mathbb{R}_{k,\mathrm{B}}$ to be arbitrarily close to the link rate such that no outage events occur. We assume that Alice uses a codebook $C(2^{n\mathbb{R}_{k,\mathrm{B}}}, 2^{n\mathcal{R}}, n)$ where $\mathcal{R}$ is the target secrecy rate (i.e. packet size in bits/sec/Hz), n is the codeword length, $2^{n\mathbb{R}_{k,\mathrm{B}}}$ is the size of the codebook, and $2^{n\mathcal{R}}$ is the number of confidential messages to transmit. The $2^{n\mathbb{R}_{k,\mathrm{B}}}$ codewords are randomly grouped into $2^{n\mathcal{R}}$ bins. To transmit confidential message $w \in \{1, \ldots, 2^{n\mathcal{R}}\}$, Alice uses a stochastic encoder to randomly select a codeword from bin w and transmit it over the channel. Since the instantaneous CSI for the Alice-Eve link is not available at Alice, we assume the encoder will set a fixed value for the intended positive secrecy rate $\mathcal{R}$ (which represents the spectral efficiency of one packet transmission).

D. High-Level Framework

Our objective is to securely transmit the data packets of a set of buffered nodes in the presence of a potential eavesdropper. The high-level framework we adopt in this paper consists of three main parts

- **Secure Transmission:** We propose a set of jamming schemes based on the availability of the CSI at the legitimate nodes and derive the instantaneous secrecy rate and secrecy outage probability of each scheme. The jamming schemes differ in the CSI requirements at nodes.
- **Nodes Access and QoS:** We propose a TDMA access scheme where one of the source nodes is selected for data transmission in a given time slot with certain probability. The time slot assignment probabilities are optimized to satisfy certain QoS requirements for the legitimate users.
- **Queueing Analysis:** We investigate the queue evolutions of the source nodes and derive several important network-layer metrics such as queue stability, maximum secure stable throughput, and the queueing delay of the source node. Furthermore, we investigate the queueing delay requirement region, which defines the minimum achievable delay at a source node when the requirements of the other nodes are specified.

III. Queueing Analysis

In this section, we analyze the Markov chain of the legitimate nodes queues. In addition, we provide close-form expressions for the average queueing delays.

A. Queue Stability

A fundamental performance measure of a communication network is the stability of its queues [22]. We aim at characterizing the secrecy stable-throughput region of the considered system which describes the theoretical limit on rates that can be pushed through the system while maintaining the stability of the queues. We are interested in the queues sizes. More rigourously, stability can be defined as follows [29].

Definition: A queue is said to be stable if and only if its probability of being empty remains non-zero for time t that grows to infinity [29]. That is, queue Q_k is stable, if

$$\lim_{y\to 0}\lim_{t\to\infty}\Pr\{Q_k^t = y\} > 0. \tag{2}$$

If the arrival and service processes are strictly stationary, then we can apply Loynes' theorem to check for stability conditions [22], [30]. This theorem states that if the arrival process and the service process of a queue are strictly stationary, and the average service rate is greater than the average arrival rate of the queue, then the queue is stable.

B. Mean Service Rates

Let $\mathbb{P}_{k,\mathrm{B}} = \Pr\{R_{\mathrm{s},k} \leq \mathcal{R}\}$ denote the secrecy outage probability of the kth user transmission. A packet at the head of Q_k leaves the system securely and reliably if Node k is selected for data transmission and there is no secrecy outage. Hence, the mean secure service rate (i.e. the average number of securely and correctly received packets at Bob from Node k) of the kth queue is given by

$$\mu_k = \omega_k(1 - \mathbb{P}_{k,\mathrm{B}}) \tag{3}$$

which is also defined as the probability that the kth transmitter is allocated to the time slot and that its transmission is decoded securely at Bob. We emphasize that μ_k is a function of 1) ω_k, which represents the fraction of time slots that is allocated to User k for data transmission, and 2) the complement of the secrecy outage probability, $1 - \mathbb{P}_{k,\mathrm{B}}$. Hence, for a given ω_k, to increase the service rate of Queue Q_k (i.e. increase the secure throughput of User k), the secrecy outage probability $\mathbb{P}_{k,\mathrm{B}}$ should be reduced. The outage probability $\mathbb{P}_{k,\mathrm{B}}$ can be reduced by increasing the secrecy rate of the transmission. From (1), the secrecy rate increases with decreasing Eve's rate. Hence, in the following section, we propose a BF-based cooperative jamming scheme where the jammers design their BF weights to decrease Eve's rate while completely removing the interference at Bob.

C. Queue Q_k Markov Chain

In a given time slot, each node either transmits at most one data packet, receives at most one data packet (due to the Bernoulli arrival model), or operates as a jamming node. Hence, the Markov chain of a queue is modeled as a *birth-death* process. For Q_k, the probability of moving from State $n \in \{1, 2, \ldots, \infty\}$ to State $n-1$ is given by the probability of having no arrived packets at the queue, which is given by $1-\lambda_k$, multiplied by the probability of a packet being served securely, which is given by μ_k. Moreover, the probability of moving from State n to State $n+1$ is the probability of having an arrived packet in the given time slot, which is given by λ_k, multiplied by the probability that the packet at the queue head cannot be decoded securely at Bob, which is given by $1-\mu_k$. Mathematically, the probability of moving one packet up and the probability of moving one packet down are given, respectively, by

$$p_{k,\mathrm{up}} = \lambda_k\,(1-\mu_k),\ p_{k,\mathrm{down}} = (1-\lambda_k)\,\mu_k \tag{4}$$

Analyzing the Markov chain of Q_k, the probability of the queue being in State $n \geq 0$, denoted by $\epsilon_{k,n}$, is given by

$$\epsilon_{k,n} = \epsilon_{k,0}\beta_k^n,\ \epsilon_{k,0} = 1 - \frac{\lambda_k}{\mu_k} \tag{5}$$

where $\beta_k = p_{k,\mathrm{up}}/p_{k,\mathrm{down}}$ and $\lambda_k < \mu_k$ represents the necessary condition to maintain the queue Q_k stable.

Symbol	Description	Symbol	Description
$\mathcal{M}$	# source nodes	$\mathcal{T}$	Set of source nodes
$\mathcal{J}$	Set of jamming nodes	T and W	Slot duration and channel bandwidth
$\mathcal{R}$	Target secrecy rate	P	Average transmit power by a node
P_I	Average transmit information power	P_J	Average transmit jamming power
κ	Thermal noise variance	ω_k	Probability of assigning User k to a time slot
Q_k	Queue (buffer) at User k	μ_k	Mean service rate of Q_k
λ_k	Mean arrival rate at Q_k	$\mathcal{M}-1$	Cardinality of the potential jamming set
$\mathbb{R}_{n_1,n_2}$	Channel rate of the n_1-n_2 link	$R_{\mathrm{s},k}$	Instantaneous secrecy rate of Transmitter k
h_{n_1,n_2}	Channel coefficient between Node n_1 and Node n_2	$\theta_{n_1,n_2}=\lvert h_{n_1,n_2}\rvert^2$	Channel gain between Node n_1 and Node n_2
$\mathbb{P}_{k,\mathrm{B}}$	Probability of secrecy outage of the $k-\mathrm{B}$ link	$\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}}$	Probability of secrecy outage of the $k-\mathrm{B}$ link when there is no Eve

TABLE I
LIST OF KEY VARIABLES.

D. Queueing Delay

Using Little's theorem, the average queueing delay at Q_k is

$$D_k = \frac{1-\lambda_k}{\mu_k-\lambda_k} \tag{6}$$

with $\mu_k > \lambda_k$. The average queueing delay of Node k is proportionally decreasing with μ_k and proportionally increasing with the arrival rate λ_k.

If we aim at minimizing the nodes' queueing delays, we should either decrease the arrival rates $\{\lambda_k\}_{k=1}^{\mathcal{M}}$ or increase the service rates $\{\mu_k\}_{k=1}^{\mathcal{M}}$. The arrival rate at Node k is uncontrollable and is a given parameter from the upper layers. On the other hand, the service rate μ_k is controllable by an appropriate design of ω_k and $(1-\mathbb{P}_{k,\mathrm{B}})$. Thus, we need to optimize ω_k to satisfy the users' QoS, which will be designed in Section V, and to minimize/reduce $\mathbb{P}_{k,\mathrm{B}}$ (or equivalently, improve/increase $1-\mathbb{P}_{k,\mathrm{B}}$) to further enhance the system security and nodes' throughput. The outage probability $\mathbb{P}_{k,\mathrm{B}}$ can be decreased by increasing the secrecy rate of the transmission. Hence, we propose a BF-based cooperative jamming scheme in the following section. We also propose two variations of the proposed jamming scheme based on the availability of channel CSI at the legitimate nodes. We first investigate the case of perfect CSI at the legitimate nodes including Eve's CSI. Then, we investigate the cases of no Eve's CSI at the legitimate nodes and no jammers-Bob links' CSI.

IV. PROPOSED JAMMING SCHEMES

To improve the QoS of the legitimate users described in the previous section, we propose a BF-based jamming schemes to reduce the secrecy outage probabilities of the users' transmissions. This part represents the PHY-layer optimization of the proposed formulation to enhance the system security. That is, it considers the PHY structure of the network under investigation and allows the legitimate nodes to transmit the jamming signal to enhance the instantaneous secrecy rates.

In the following subsections, we investigate the proposed jamming techniques which differ in terms of their CSI requirements. Moreover, the instantaneous secrecy rate and secrecy outage probability change from one jamming scheme to another.

A. Optimal-BF Jamming

In this scheme, we assume that the set of nodes in $\mathcal{J}$ create a cooperative beamformer jamming signal to maximize the instantaneous secrecy rate of the data transmitting node k under the condition that the interference of the jamming signal is canceled at Bob. Global CSI is assumed at all nodes as in [10]. This assumption is valid when Eve is an active node in the network (or a non-hostile node that communicates with the destination (Bob) from one time to another).[1] A similar jamming scheme was proposed in, e.g., [10], [12], with a different network setting. In our scenario, the jamming set changes from one time slot to another. More importantly, we derive closed-form expressions for the optimal weight vector used at the cooperative jammers, the secrecy rate, and the secrecy outage probability.

We assume that the source nodes are close to each other so that they can share the same Gaussian noise symbols using a short range signaling that is completely hidden from the

[1]This is a common assumption in the PHY-layer security literature [8]–[10]. It is justified by the fact that Eve can be another *active* node in the network that communicates with Bob. Accordingly, Eve's CSI can be estimated at all nodes through her transmitted pilot signals which are also received by Bob. Moreover, different nodes can share a certain link CSI through channel feedback.

eavesdropper as in, e.g., [12] and the references therein.[2] The source nodes in $\mathcal{J}$ confound Eve using the same Gaussian noise symbols but with different weight coefficients. The weights are chosen to null the interference at Bob while maximizing the interference at the eavesdropper's receiver. For given channel realizations, when the signal-to-interference-plus-noise ratio (SINR) at the legitimate destination is greater than that at the eavesdropper, the instantaneous secrecy rate of Node k is given by

$$\begin{aligned}\mathcal{R}_{\mathrm{s},k} = &\log_2\left(1+\frac{P_I\theta_{k,\mathrm{B}}}{\kappa}\right)\\ &-\log_2\left(1+\frac{P_I\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right)\end{aligned} \tag{7}$$

where $\frac{\theta_{k,\mathrm{B}}}{\kappa} > \frac{\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}$ is the condition to achieve a non-zero secrecy rate. Moreover, $\theta_{k,j} = |h_{k,j}|^2$ denotes the channel gain (i.e. squared-magnitude of the channel coefficient $h_{k,j}$) between Node $k \in \{1,2,3,\ldots,\mathcal{M}\}$ and Node $j \in \{\mathrm{E},\mathrm{B}\}$, and $\mathbf{g} = [g_1,\ldots,g_{k-1},g_{k+1},\ldots,g_{\mathcal{M}}]^\top \in \mathbb{C}^{(\mathcal{M}-1)\times 1}$ is the BF weight vector with g_j as the weight used by node $j \in \mathcal{J}$. The jamming transmit power by Node $j \in \mathcal{J}$ is given by

$$P_j = |g_j|^2 P_J \tag{8}$$

Hence, the average transmit power used in jamming by Node j is given by

$$\mathbb{E}\{P_j\} = \mathbb{E}\{|g_j|^2\}P_J \tag{9}$$

For given channel realizations, if the SINR at the eavesdropper's receiver is greater than that at the legitimate destination, i.e., $\frac{P_I\theta_{k,\mathrm{B}}}{\kappa} \leq \frac{P_I\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}$, the instantaneous secrecy rate of User k is *zero*. That is, $R_{\mathrm{s},k} = 0$, which means that there is no secure communications since the ability of Eve to decode the data is higher than Bob's ability. Combining the two above-mentioned cases, the instantaneous secrecy rate of Node k, $R_{\mathrm{s},k}$, is given by

$$R_{\mathrm{s},k} = \begin{cases} \mathcal{R}_{\mathrm{s},k} & \text{if } \frac{P_I\theta_{k,\mathrm{B}}}{\kappa} > \frac{P_I\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2} \\ 0 & \text{if } \frac{P_I\theta_{k,\mathrm{B}}}{\kappa} \leq \frac{P_I\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2} \end{cases} \tag{10}$$

Maximizing $\mathcal{R}_{\mathrm{s},k}$ over the weight vector $\mathbf{g}$ is equivalent to minimizing $\log_2\left(1+\frac{P_I\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right)$. Since the logarithm function is a monotonically increasing function, the problem reduces to the maximization of the following objective function

$$\max_{\mathbf{g}}:\ \mathcal{R}_{\mathrm{s},k} \Rightarrow \min_{\mathbf{g}}:\ \frac{P_I\theta_{k,\mathrm{E}}}{\kappa+P_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2} \Rightarrow \max_{\mathbf{g}}:\ |\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2 \tag{11}$$

Let $\mathbf{h}_{\mathrm{E}} = [h_{1,\mathrm{E}},\ldots,h_{k-1,\mathrm{E}},h_{k+1,\mathrm{E}},\ldots,h_{\mathcal{M},\mathrm{E}}]^\top \in \mathbb{C}^{(\mathcal{M}-1)\times 1}$ denote the channel coefficient vector from the legitimate source nodes in $\mathcal{J}$ to Eve and $\mathbf{h}_{\mathrm{B}} = [h_{1,\mathrm{B}},\ldots,h_{k-1,\mathrm{B}},h_{k+1,\mathrm{B}},\ldots,h_{\mathcal{M},\mathrm{B}}]^\top \in \mathbb{C}^{(\mathcal{M}-1)\times 1}$ denote the channel coefficient vector from the source nodes in $\mathcal{J}$ to Bob. The optimal weight vector $\mathbf{g} = [g_1,\ldots,g_{k-1},g_{k+1},\ldots,g_{\mathcal{M}}]^\top$ that maximizes $|\mathbf{g}^*\mathbf{h}_{\mathrm{E}}|^2 = |\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2$ subject to (s.t.) the normalization constraint $\|g\|^2 = 1$ and the total cancellation of the interference at Bob, i.e., $|\mathbf{g}^*\mathbf{h}_{\mathrm{B}}| = \mathbf{0}$, can be computed by solving the following constrained optimization problem

$$\begin{aligned}\max_{\mathbf{g}}:\ & |\mathbf{g}^*\mathbf{h}_{\mathrm{E}}|^2 \\ \text{s.t.}\ & |\mathbf{g}^*\mathbf{h}_{\mathrm{B}}| = 0 \\ & \|\mathbf{g}\|^2 = 1\end{aligned} \tag{12}$$

The optimal weight vector $\mathbf{g}$ must null the interference at Bob. Thus, to solve the optimization problem in (12), the optimal weight vector is orthogonal to $\mathbf{h}_{\mathrm{B}}$ and should belong to a subspace that is orthogonal to the channel vector $\mathbf{h}_{\mathrm{B}}$. Let $\mathbb{H}$ denote the orthogonal complement subspace of the subspace spanned by $\mathbf{h}_{\mathrm{B}}$. After that, we choose the weight vector that belongs to $\mathbb{H}$ and maximizes the term $|\mathbf{g}^*\mathbf{h}_{\mathrm{E}}|^2$. Using the closest point theorem [31], the optimal weight vector should be the orthogonal projection of $\mathbf{h}_{\mathrm{E}}$ onto the subspace $\mathbb{H}$. From the last constraint in (12), the optimal weight vector has a unit norm. Hence, the projection vector is divided by its magnitude. Accordingly, the optimal weight vector is given by

$$\mathbf{g} = \frac{\Psi\mathbf{h}_{\mathrm{E}}}{\|\Psi\mathbf{h}_{\mathrm{E}}\|} \tag{13}$$

where Ψ is the projection matrix which is given by $\Psi = \mathbf{I}_{\mathcal{M}-1} - \frac{\mathbf{h}_{\mathrm{B}}\mathbf{h}_{\mathrm{B}}^*}{\|\mathbf{h}_{\mathrm{B}}\|^2}$, and $\mathbf{I}_{\mathcal{M}-1}$ denotes the identity matrix whose size is $\mathcal{M}-1 \times \mathcal{M}-1$.

The secrecy outage probability of the BF-based jamming scheme with perfect CSI is given by

$$\mathbb{P}_{k,\mathrm{B}} = \Pr\left\{\mathcal{R} \geq \log_2(1+\gamma_I\theta_{k,\mathrm{B}}) - \log_2\left(1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right)\right\} \tag{14}$$

where $\gamma_I = P_I/\kappa$ and $\gamma_J = P_J/\kappa$.

Lemma 1. *The no secrecy outage probability (i.e. complement probability of secrecy outage) of the optimal-BF jamming scheme with perfect CSI at the legitimate nodes is given by*

$$1-\mathbb{P}_{k,\mathrm{B}} = (1-\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}})\frac{\mathrm{F}\left(\mathcal{M}-3,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)+\gamma_J\mathrm{F}\left(\mathcal{M}-2,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)}{\gamma_J(\mathcal{M}-3)!} \tag{15}$$

where $\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}} = 1-\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)$ *is the probability of no secrecy outage when there is no eavesdropping and* $\mathrm{F}(\cdot,\cdot)$ *is given in* (16) *at the top of the next page with* $\mathrm{Ei}(\cdot)$ *as the exponential integral.*[3]

Proof. See Appendix A □

The factor $\mathcal{E}_{\mathrm{OBF}} = \frac{\mathrm{F}\left(\mathcal{M}-3,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)+\gamma_J\mathrm{F}\left(\mathcal{M}-2,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)}{\gamma_J(\mathcal{M}-3)!}$ in (15) represents the reduction in the no secrecy outage probability due to eavesdropping. *It also represents the probability of no secrecy outage given that there is no connection outage.* Interestingly, the factor $\mathcal{E}_{\mathrm{OBF}}$ is independent of the average transmit data SNR γ_I. It is only a function of the number of

[2]The AN can be a pseudo-random signal which is perfectly known at the source nodes but not at the eavesdropper. This can be efficiently realized by using a short secret key as seed information for the Gaussian pseudo-random sequence generator used for generating the noise sequences, where the legitimate nodes regularly change the key seeds to maintain the sequence secured from the eavesdropper [27].

[3]The closed-form expression in (16) can be found in [32, Eqn. 3.353.5].

$$\mathrm{F}(K,a)=\int_0^{\infty}\frac{\alpha^K}{\alpha+a}\exp(-\alpha)d\alpha=(-1)^{K-1}a^K\exp(a)\mathrm{Ei}(-a)+\sum_{n=1}^{K}(n-1)!(-a)^{K-n} \tag{16}$$

source nodes in the network $\mathcal{M}$, the target secrecy rate $\mathcal{R}$, and the average jamming SNR γ_J. The following observations are in order

1) From (15), the no secrecy outage probability, $1-\mathbb{P}_{k,\mathrm{B}}$, is monotonically non-increasing with γ_I. As $\gamma_I\to\infty$, $(1-\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}})=\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)=1$. However, the factor $\mathcal{E}_{\mathrm{OBF}}$ will not change. This means that, even if Alice transmits with infinite power, there will remain secrecy outage which is given by $1-\mathcal{E}_{\mathrm{OBF}}$. More specifically, the no secrecy outage probability saturates as $\gamma_I\to\infty$ at $1-\mathcal{E}_{\mathrm{OBF}}$.
2) From the definition of $\mathrm{F}(\cdot,\cdot)$ in (16), it is monotonically decreasing with $a=\frac{2^{\mathcal{R}}+1}{\gamma_J}$. Hence, the no secrecy outage probability is monotonically increasing with γ_J. This is very encouraging since the jamming power only affects Eve (since the jamming signal is transmitted in the null space of the orthogonal direction to the jammers-Bob channel vector). Moreover, the no secrecy outage probability is monotonically decreasing with $\mathcal{R}$ (i.e. target secrecy rate) since $\Pr\{R_{\mathrm{s},k}\geq\mathcal{R}\}$ decreases with increasing of $\mathcal{R}$.
3) When $\gamma_J>2^{\mathcal{R}}+1$, as $\mathcal{M}\to\infty$, $\mathcal{E}_{\mathrm{OBF}}\to 1$. This implies that increasing the number of source nodes to infinity can ensure the mitigation of the secrecy outage probabilities.

Lemma 2. *As $\gamma_J\to\infty$, the no secrecy outage probability is given by*

$$1-\mathbb{P}_{k,\mathrm{B}}\approx\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{(\mathcal{M}-3)!}\mathrm{F}\left(\mathcal{M}-2,0\right)=\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right) \tag{17}$$

Proof. See Appendix C. □

Lemma 2 implies that, at high γ_J levels, the secrecy outage probability with and without eavesdropping is almost the same. Hence, the proposed BF-based jamming scheme is able to completely secure the transmission in the sense that it eliminates the impact of Eve. However, there will still be a **connection** outage probability which is not affected by the presence or absence of Eve.

Remark 1. *If the CSI of the eavesdropper is unknown at the legitimate nodes, the solution of the optimization problem in (12) will be a weighted-sum of the vectors in the subspace orthogonal to the subspace spanned by the channel vector between the jamming nodes in $\mathcal{J}$ and the legitimate destination node. In this case, the beamformer is a precoding matrix $\mathbf{G}$ which represents the solution of $\mathbf{h}_{\mathrm{B}}^{\top}\mathbf{G}=\mathbf{0}$. The columns of the precoding matrix $\mathbf{G}$ represents the orthogonal directions to the jammers-Bob links. Since $\mathbf{h}_{\mathrm{B}}$ is $(\mathcal{M}-1)\times 1$, $\mathbf{G}$ is $(\mathcal{M}-1)\times(\mathcal{M}-2)$. The weights used to combine the columns of $\mathbf{G}$ are complex Gaussian random variables with zero-mean and variance $P_J/(\mathcal{M}-2)$ each. We discuss this scenario in the numerical simulations section.*

To perform the channel estimation, Bob broadcasts a known pilot signal so that each node estimates its channel. Then, over $\mathcal{M}$ bit durations, each source node transmits a known pilot signal to Bob. After that, Bob computes the optimal weights and feed them back to the jamming nodes. Assuming that f bits are used for the quantization of each weight, the total number of bits required to announce all weights is $(\mathcal{M}-1)f$. Since a bit duration is $1/W$ seconds, the time spent to realize this operation is $\tau=(\mathcal{M}+1+(\mathcal{M}-1)f)/W$ seconds. The fraction of the time slot used for this operation is then given by $\varrho=\frac{\tau}{T}=(\mathcal{M}+1+(\mathcal{M}-1)f)/(WT)$. The remaining time fraction for data transmission is $1-\varrho$. Hence, the target secrecy rate is $\mathcal{R}=\frac{b}{(1-\varrho)WT}$ bits/sec/Hz.

B. Random-BF Jamming

To avoid the estimation of the channels between Bob and the jamming nodes in a given time slot, we propose a new scheme that only requires the estimation of the power caused by sending a known signal to Bob. Each node in the jamming set randomly generates a sequence of m uniform phases, where m is an integer. Afterwards, over m bit durations, the potential jamming nodes transmit known pilot signals (i.e. signals with known values at all nodes in the network including Eve) to Bob multiplied by phase shifts using the generated phases. Since a bit duration is $1/W$ second, the time spent to realize this operation is m/W seconds. Bob then feeds back the **index** of the best weight used at the cooperative jamming nodes, i.e., the weight which yields the lowest interference power at Bob's receiver, using $\lceil\log_2(m)\rceil$ bits. Hence, the total consumed time to realize this scheme is $\tau=(m+\lceil\log_2(m)\rceil)/W$ seconds. The fraction of the time slot used for this operation is then given by $\zeta=\frac{\tau}{T}=(m+\lceil\log_2(m)\rceil)/(WT)$. The remaining time fraction for data transmission is $1-\zeta$. Hence, the target secrecy rate is $\mathcal{R}=\frac{b}{(1-\zeta)WT}$ bits/sec/Hz.

The received signal strength indicator (RSSI) at Bob during the qth trial by the cooperative jammers, denoted by s_q, is given by

$$s_q=|\sum_{j\in\mathcal{J}}\phi_{q,j}h_{j,\mathrm{B}}|^2 \tag{18}$$

where $q\in\{1,2,\ldots,m\}$ and $\phi_{q,j}=\exp(-\sqrt{-1}\rho)$, $-\pi\leq\rho\leq\pi$, is a uniformly-distributed random variable. The weight vector which yields the minimum received RSSI value is selected for jamming Eve. That is, Bob selects the index q that satisfies $\min\limits_{q}:\ s_q$. We can force a threshold on this minimum RSSI such that, if this threshold is not met, the cooperative jammers remain silent during the current time slot. As m increases, the time consumed for detecting the best weight vector increases; however, the probability of finding a better

weight vector increases as well. Note that $\phi_{q,j}$ and the AN are randomly generated at the jamming nodes; hence, they are unknown at both Bob and Eve. Furthermore, Bob does not need to know the CSI to the cooperative jammers.

To maintain the average jamming transmit power fixed at P_J Watts/Hz, we let each jamming node in the set of cooperative jammers, whose cardinality is $(\mathcal{M}-1)$, transmit with power $P_J/(\mathcal{M}-1)$. For given channel realizations, when the SINR at Bob is greater than that at Eve, the instantaneous secrecy rate of Node k is given by

$$R_{\mathrm{s},k} = \left[\log_2 \left(1+\frac{\gamma_I \theta_{k,\mathrm{B}}}{1+\frac{\gamma_J}{(\mathcal{M}-1)} \min\limits_{q} : |\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}|^2} \right) - \log_2 \left(1+\frac{\gamma_I \theta_{k,\mathrm{E}}}{1+\frac{\gamma_J}{(\mathcal{M}-1)} |\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{E}}|^2} \right) \right]^+ \tag{19}$$

where $\tilde{q} = \mathrm{argmin}_q |\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}|^2$. Because the BF weight, $\phi_{q,j}$, represents a rotation and $h_{j,\mathrm{B}}$ is an i.i.d. complex Gaussian random variable with zero mean and unit variance, $\phi^*_{q,j} h_{j,\mathrm{B}}$ is also distributed as an i.i.d. complex Gaussian random variable with zero mean and unit variance[4]. Hence, the distribution of $\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}$ is a circularly-symmetric Gaussian random variable with zero mean and variance $(\mathcal{M}-1)$. The squared-magnitude of $\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}$ is exponentially-distributed random variable and the same holds for the squared-magnitude of $\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{E}}$.

Following Appendix B, the secrecy outage probability for fixed $|\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{B}}|^2$ and $|\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{E}}|^2$ is given by

$$\begin{aligned} &\Pr\left\{ \begin{matrix}\text{secrecy}\\ \text{outage}\end{matrix} \middle| |\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{B}}|^2, |\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{E}}|^2 \right\} \\ &= 1 - \frac{\exp(-\frac{2^{\mathcal{R}}-1}{\frac{\gamma_I}{1+\frac{\gamma_J}{(\mathcal{M}-1)}|\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{B}}|^2}})}{1+2^{\mathcal{R}} \frac{1+\frac{\gamma_J}{(\mathcal{M}-1)}|\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{B}}|^2}{1+\frac{\gamma_J}{(\mathcal{M}-1)}|\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{E}}|^2}} \end{aligned} \tag{20}$$

The best performance of this scheme is achieved when the interference at Bob is completely eliminated, i.e., $\min\limits_{q} : |\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}|^2 \to 0$. This will be the case when m is sufficiently large since it is most likely that the randomly-generated phases at the cooperative jammers will result in a complete AN removal at Bob. The instantaneous secrecy rate in this case is given by

$$R_{\mathrm{s},k} = \left[\log_2 (1+\gamma_I \theta_{k,\mathrm{B}}) - \log_2 \left(1+\frac{\gamma_I \theta_{k,\mathrm{E}}}{1+\frac{\gamma_J}{(\mathcal{M}-1)}|\sum_{j\in\mathcal{J}} \phi^*_{\tilde{q},j} h_{j,\mathrm{E}}|^2} \right) \right]^+ \tag{21}$$

Since the legitimate nodes do not know Eve's CSI, and the design of the weight vector only depends on the legitimate links CSI, the secrecy outage probability becomes independent of m as m increases. As $\min\limits_{q} : |\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}|^2$ becomes very small, the secrecy outage probability becomes independent of m. This will be verified numerically in Section V. An exact expression for the complement secrecy outage probability of the random-BF jamming scheme when $\min\limits_{q} : |\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}|^2 \to 0$ is provided in the following lemma.

Lemma 3. *As* $\min\limits_{q} : |\sum_{j\in\mathcal{J}} \phi^*_{q,j} h_{j,\mathrm{B}}|^2 \to 0$*, the probability of no secrecy outage is given by*

$$1-\mathbb{P}_{k,\mathrm{B}} = \frac{\exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})}{\gamma_J} \left(\mathrm{F}(0, \frac{1+2^{\mathcal{R}}}{\gamma_J}) + \gamma_J \mathrm{F}(1, \frac{1+2^{\mathcal{R}}}{\gamma_J}) \right) \tag{22}$$

Proof. See Appendix D. □

The reduction in the no secrecy outage probability under the random-BF scheme is given by $\mathcal{E}_{\mathrm{RBF}} = \frac{\mathrm{F}(0, \frac{1+2^{\mathcal{R}}}{\gamma_J}) + \gamma_J \mathrm{F}(1, \frac{1+2^{\mathcal{R}}}{\gamma_J})}{\gamma_J}$. Similar to the observations made on the optimal BF-based jamming, the no secrecy outage outage reduction factor is independent of the average transmit data SNR γ_I. It is only a function of the target secrecy rate $\mathcal{R}$ and the average jamming SNR γ_J. As $\gamma_I \to \infty$, the factor $\mathcal{E}_{\mathrm{RBF}}$ will remain unchanged. This implies that, even if Alice transmits with infinite power, there will remain secrecy outage which is given by $1-\mathcal{E}_{\mathrm{RBF}}$. More specifically, the no secrecy outage probability saturates as $\gamma_I \to \infty$ at $1-\mathcal{E}_{\mathrm{RBF}}$.

Lemma 4. *As* $\gamma_J \to \infty$*, the no secrecy outage probability is given by*

$$1-\mathbb{P}_{k,\mathrm{B}} \approx \exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I}) \tag{23}$$

Proof. See Appendix E. □

Since the secrecy outage probability is equal to the Alice-Bob link outage probability (i.e. connection outage probability), the random-BF scheme can mitigate the secrecy outage probability when the direct link is connected, i.e., when there is no connection outage in the Alice-Bob link.

Remark 2. *From the description of the random-BF scheme, we note that the legitimate nodes do not need Eve's CSI or even her channel statistics. In addition, the cooperative jammers and Alice do not need to know their CSI to Bob. Bob needs Alice's CSI to decode her information and to announce the outage states to Alice if the Alice-Bob link is in outage.*

V. Problem Formulations

In this section, we investigate two important network-layer metrics for wireless nodes equipped with data buffers. We will focus our design on the perfect CSI scenario and present the other two scenarios in the numerical simulations section due to space limitation. However, the analysis presented here is not restricted to the BF jamming scheme with perfect CSI and the other two cases can be handled in the exact same manner.

We assume that there is an average constraint on each node transmit power. Assuming that a node has an average power constraint of P Watts/Hz, the average transmit power of Node k (averaged across time slots), denoted by $P_{\mathrm{av},k}$, is given by

$$\begin{aligned} P_{\mathrm{av},k} &= \omega_k \Pr\{Q_k>0\}(1-\mathbb{P}_{k,\mathrm{B}}) P_I \\ &\quad + \left(\sum_{\ell\in\mathcal{J}} \omega_\ell \Pr\{Q_\ell>0\}(1-\mathbb{P}_{\ell,\mathrm{B}}) \right) \mathbb{E}\left\{ |g^*_k|^2 \right\} P_J \le P, \ \forall k \end{aligned} \tag{24}$$

[4]Circularly-symmetric Gaussian random variables are invariant to rotations [33].

The expression in (24) is explained as follows. Node k transmits a data packet with average power P_I Watts/Hz when it is selected for data transmission, its channel to Bob can securely support a packet transmission, and its queue is nonempty. If Node k is not selected for data transmission, it operates as a jamming node with an average jamming power of $\mathbb{E}\left\{|g_k^*|^2\right\} P_J$ Watts/Hz when the node that is selected for data transmission, say Node ℓ, has data to send and its channel is secured. From the queueing analysis in Section III, $\Pr\{Q_k > 0\} = \frac{\lambda_k}{\mu_k} = \frac{\lambda_k}{\omega_k(1-\mathbb{P}_{k,\mathrm{B}})}$. Hence, the average power constraint becomes

$$P_{\mathrm{av},k} = \lambda_k P_I + \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J \leq P,\ \forall k \tag{25}$$

Interestingly, the power levels of a node are weighted by the average arrival rate at that node's queue and the sum average arrival rates at all the other nodes' queues.

A. Secure Stable-Throughput Region

The secrecy stable-throughput region is characterized by the closure of the rate-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_{\mathcal{M}})$ which is obtained by solving the following constrained optimization problem

$$\begin{aligned} \max_{\substack{0\leq\omega_k\leq 1\\ P_I\geq 0, P_J\geq 0}} :\quad & \mu_k \\ \text{s.t.}\quad & \mu_\ell > \lambda_\ell, \forall \ell \neq k, \\ & \sum_{\ell=1}^{\mathcal{M}} \omega_\ell = 1, \\ & \omega_k \Pr\{Q_k>0\} P_I + \sum_{\ell\in\mathcal{J}} \omega_\ell \Pr\{Q_\ell>0\} \mathbb{E}\left\{|g_k^*|^2\right\} P_J \leq P, \forall k \end{aligned} \tag{26}$$

where $\mu_\ell > \lambda_\ell$ is the condition of queue stability of Transmitter ℓ according to Loynes theorem [22], [30]. If the optimization problem in (26) is infeasible, the queues cannot be stable for the given set of arrival rates. Hence, the system is not stable. The optimization problem in (26) can be reformulated as

$$\begin{aligned} \max_{\substack{0\leq\omega_k\leq 1\\ P_I\geq 0, P_J\geq 0}} :\quad & \omega_k(1-\mathbb{P}_{k,\mathrm{B}}) \\ \text{s.t.}\quad & \omega_\ell(1-\mathbb{P}_{\ell,\mathrm{B}}) > \lambda_\ell, \forall \ell \neq k, \\ & \sum_{\ell=1}^{\mathcal{M}} \omega_\ell = 1, \\ & \lambda_k P_I + \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J \leq P,\ \forall k \end{aligned} \tag{27}$$

We notice that the third constraint is not a function of $\{\omega_\ell\}_{\ell=1}^{\mathcal{M}}$. For a fixed power allocation (P_I, P_J), the optimization problem in (27) is a linear program. Substituting with the equality constraint, $\sum_{\ell=1}^{\mathcal{M}} \omega_\ell = 1$, we get

$$\begin{aligned} \min_{0\leq\omega_k\leq 1} :\quad & \sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}} \omega_\ell, \\ \text{s.t.}\quad & \frac{\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}} \leq \omega_n, \forall n \neq k \end{aligned} \tag{28}$$

To minimize the objective function in (35), we set $\{\omega_\ell\}_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}$ to their lowest feasible values. That is, $\omega_\ell = \frac{\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}}$, $\forall \ell \neq k$. Then, ω_k is obtained from the equality constraint $\omega_k + \sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}} \omega_\ell = 1$. The optimal time-sharing assignments are

$$\omega_\ell^\star = \frac{\lambda_\ell}{(1-\mathbb{P}_{\ell,\mathrm{B}})}, \forall \ell \in \mathcal{J},\ \omega_k^\star = 1 - \sum_{\ell\in\mathcal{J}} \omega_\ell^\star \tag{29}$$

with $\lambda_k P_I + \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J \leq P,\ \forall k$. To satisfy all the constraints in (27), the optimal information signal power level is upper-bounded as $P_I \leq \min_{k\in\mathcal{T}} :\ \frac{P - \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J}{\lambda_k}$. Since the secrecy outage probability $\mathbb{P}_{k,\mathrm{B}}$ is monotonically decreasing with the transmit data and jamming signal power levels, the inequality becomes an equality (i.e. the transmit data power level is set to its highest feasible value). That is, $P_I = \min_{k\in\mathcal{T}} :\ \frac{P - \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J}{\lambda_k}$.

Solution to optimization problem (26): We solve the optimization problem in (26) as follows. We generate a power level P_J. Then, we obtain P_I from $P_I = \min_{k\in\mathcal{T}} :\ \frac{P - \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J}{\lambda_k}$. Afterwards, we obtain the optimal values of $\{\omega_k^\star\}_{k=1}^{\mathcal{M}}$ using the closed-form expressions in (29). Then, we substitute with the generated (P_I, P_J) and $\{\omega_k^\star\}_{k=1}^{\mathcal{M}}$ in the original optimization problem stated in (26) and compute the value of the objective function. Finally, we select the power-level pair (P_I, P_J) and the corresponding $\{\omega_k^\star\}_{k=1}^{\mathcal{M}}$ that yield the largest value for the objective function in (26).

For every power pair (P_I, P_J), the secrecy stable-throughput region is given by

$$\mathcal{S} = \{(\lambda_1, \lambda_2, \ldots, \lambda_{\mathcal{M}}) : \sum_{\ell=1}^{\mathcal{M}} \frac{\lambda_\ell}{(1-\mathbb{P}_{\ell,\mathrm{B}})} < 1\} \tag{30}$$

with $P_I = \min_{k\in\mathcal{T}} \frac{P - \left(\sum_{\ell\in\mathcal{J}} \lambda_\ell\right) \mathbb{E}\left\{|g_k^*|^2\right\} P_J}{\lambda_k}$. The maximum secrecy stable-throughput region is a convex set, i.e., a polyhedron. The secure stability region being a convex polyhedron corresponds to a regime in which when one of the users increases its rate, the other users' maximum supportable rates decrease linearly. In addition, the convexity of the secure stability region ensures that higher sum rates can be achieved. Moreover, since the secure stability region is convex, if two rate pairs are securely stable, then the line segment connecting those two rate pairs is also composed of stable rate pairs.

B. Secure Delay-Requirement Region

Our second formulation is concerned with the minimization of one of the average queueing delays subject to conditions on the queueing delays of the other queues. We refer to this region as the *delay-requirement region*. This region is obtained via solving the following constrained optimization problem

$$\begin{aligned} \min_{\substack{0\leq\omega_k\leq 1\\ P_I\geq 0, P_J\geq 0}} :\quad & D_k = \frac{1-\lambda_k}{\omega_k(1-\mathbb{P}_{k,\mathrm{B}}) - \lambda_k}, \\ \text{s.t.}\quad & \mu_\ell > \lambda_\ell, \forall \ell \neq k, \\ & D_n = \frac{1-\lambda_n}{\omega_n(1-\mathbb{P}_{n,\mathrm{B}}) - \lambda_n} \leq \mathcal{D}_n, \forall n \neq k, \\ & \sum_{\ell=1}^{\mathcal{M}} \omega_\ell \leq 1 \end{aligned} \tag{31}$$

This problem can be reformulated as follows

$$\begin{aligned}\max_{\substack{0\le\omega_k\le 1\\ P_I\ge 0, P_J\ge 0}}\ & \omega_k(1-\mathbb{P}_{k,\mathrm{B}}),\\ \text{s.t.}\ & \omega_\ell(1-\mathbb{P}_{\ell,\mathrm{B}})>\lambda_\ell, \forall \ell\neq k,\\ & \frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n\le \omega_n(1-\mathbb{P}_{n,\mathrm{B}}), \forall n\neq k,\\ & \sum_{\ell=1}^{\mathcal{M}}\omega_\ell\le 1,\\ & \lambda_k P_I+\left(\sum_{\ell\in\mathcal{J}}\lambda_\ell\right)\mathbb{E}\left\{|g_k^*|^2\right\}P_J\le P,\ \forall k\end{aligned} \tag{32}$$

The queueing-delay requirement of Q_n, denoted by $\mathcal{D}_n$, represents an additional constraint on μ_n. This constraint subsumes the stability constraint. Thus, the union of both constraints is $\mu_n\ge\lambda_n+\frac{1-\lambda_n}{\mathcal{D}_n}$, where $\lambda_n+\frac{1-\lambda_n}{\mathcal{D}_n}\ge\lambda_n$. The optimization problem is then given by

$$\begin{aligned}\max_{\substack{0\le\omega_k\le 1\\ P_I\ge 0, P_J\ge 0}}\ & \omega_k(1-\mathbb{P}_{k,\mathrm{B}}),\\ \text{s.t.}\ & \frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n\le \omega_n(1-\mathbb{P}_{n,\mathrm{B}}), \forall n\neq k,\\ & \sum_{\ell=1}^{\mathcal{M}}\omega_\ell\le 1,\\ & \lambda_k P_I+\left(\sum_{\ell\in\mathcal{J}}\lambda_\ell\right)\mathbb{E}\left\{|g_k^*|^2\right\}P_J\le P,\ \forall k\end{aligned} \tag{33}$$

This optimization problem can be solved using the approach explained below (29). For a fixed power pair (P_I,P_J), the optimization problem is a linear program and can be stated as follows

$$\begin{aligned}\max_{0\le\omega_k\le 1}\ & \omega_k,\\ \text{s.t.}\ & \frac{\frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}}\le\omega_n, \forall n\neq k,\\ & \sum_{\ell=1}^{\mathcal{M}}\omega_\ell\le 1\end{aligned} \tag{34}$$

with $P_I=\min\limits_{k\in\mathcal{T}}\frac{P-\left(\sum_{\ell\in\mathcal{J}}\lambda_\ell\right)\mathbb{E}\left\{|g_k^*|^2\right\}P_J}{\lambda_k}$. Substituting with the equality constraint, $\sum_{\ell=1}^{\mathcal{M}}\omega_\ell=1$, we get

$$\begin{aligned}\min_{0\le\omega_k\le 1}\ & \sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\omega_\ell,\\ \text{s.t.}\ & \frac{\frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}}\le\omega_n, \forall n\neq k\end{aligned} \tag{35}$$

To minimize the objective function in (35), we set $\{\omega_\ell\}_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}$ to their lowest feasible values. That is, $\omega_\ell=\frac{\frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}}$, $\forall\ell\neq k$. Then, ω_k is obtained from the equality constraint $\omega_k+\sum_{\substack{\ell=1\\ \ell\neq k}}^{\mathcal{M}}\omega_\ell=1$. Hence, the optimal allocation vector $(\omega_1^\star,\omega_2^\star,\ldots,\omega_{\mathcal{M}}^\star)$ is then given by

$$\omega_n^\star=\frac{\frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}}, \omega_k^\star=1-\sum_{\substack{n=1\\ n\neq k}}^{\mathcal{M}}\omega_n^\star \tag{36}$$

For a given (P_I,P_J), the set of queueing delay requirements, denoted by $(\mathcal{D}_1,\mathcal{D}_2,\ldots,\mathcal{D}_{\mathcal{M}})$, is governed by the following relation

$$\mathcal{D}=\{(\mathcal{D}_1,\mathcal{D}_2,\ldots,\mathcal{D}_{\mathcal{M}}):\sum_{n=1}^{\mathcal{M}}\frac{\frac{1-\lambda_n}{\mathcal{D}_n}+\lambda_n}{1-\mathbb{P}_{n,\mathrm{B}}}\le 1\} \tag{37}$$

This tuple is defined as the set of delay requirements that can be supported by the network at hand such that all user requirements are satisfied. It can be easily shown that the delay-requirement region has a positive semi-definite diagonal Hessian matrix. Hence, the region is a convex region. Since the secure delay-requirement region is convex, if two requirement pairs are achievable, then the line segment connecting those two delay-requirement pairs is also achievable.

When all channels are modeled as i.i.d. random variables, $\mathbb{P}_{n,\mathrm{B}}=\mathbb{P}_{\mathrm{B}}$ for all n. The delay-requirement region can be rewritten as

$$\sum_{n=1}^{\mathcal{M}}\frac{1-\lambda_n}{\mathcal{D}_n}\le(1-\mathbb{P}_{\mathrm{B}})-\sum_{n=1}^{\mathcal{M}}\lambda_n \tag{38}$$

In what follows, we investigate the case of symmetric-load users, where $\lambda_k=\lambda$ for all k. In this case, the optimal time-sharing parameter is $\omega_k=1/\mathcal{M}$ for all k. Hence, the queueing delay of queue k is given by

$$D_k=D=\frac{1-\lambda}{\frac{1-\mathbb{P}_{\mathrm{B}}}{\mathcal{M}}-\lambda}, \forall k \tag{39}$$

The average queueing delay of the network is $D_{\mathrm{av}}=D$. As the number of legitimate source nodes increases, i.e., $\mathcal{M}$ increases, the instantaneous secrecy rate and the complement probability of secrecy outage, $1-\mathbb{P}_{\mathrm{B}}$, increase. However, the time allocated to each user decreases as well, which is controlled by $1/\mathcal{M}$. Hence, $(1-\mathbb{P}_{\mathrm{B}})/\mathcal{M}$ represents a trade-off between *increasing the number of users to enhance the security of the transmission* and *the probability of servicing a user in a given time slot*. Accordingly, there is an optimal value for $\mathcal{M}$ such that $(1-\mathbb{P}_{\mathrm{B}})/\mathcal{M}$ is maximized.

VI. Numerical Simulations

In this section, we present some numerical simulations showing the performance gains of our proposed schemes. We investigate the secure stable-throughput region of several schemes from the literature such as the best single-jammer scheme, where the node that maximizes the instantaneous secrecy rate is chosen for jamming the eavesdropper, and the fixed-jamming scheme, where a single node is assigned for jamming. We also compare their performance to our proposed scheme performance. We emphasize here that the closed-form expressions presented in this paper have been verified numerically. However, we did not show the curves since adding them will make the figure too crowded and also the legend will block the curves. Unless otherwise stated, we use the following system's parameters: $b=1000$ bits, $WT=1000$, $\mathcal{R}_\circ=b/(WT)=1$ bits/sec/Hz, $P/\kappa=20$ dB, $\gamma_I=14$ dB, $\gamma_J=7$ dB, $f=4$, and $\mathcal{M}=5$ source nodes. To simplify the numerical evaluation of the secrecy stable-throughput region, which is an $\mathcal{M}$-dimensional region, we assume that $\lambda_k=\lambda$ for nodes $2,3,\ldots,\mathcal{M}$. Figure 2

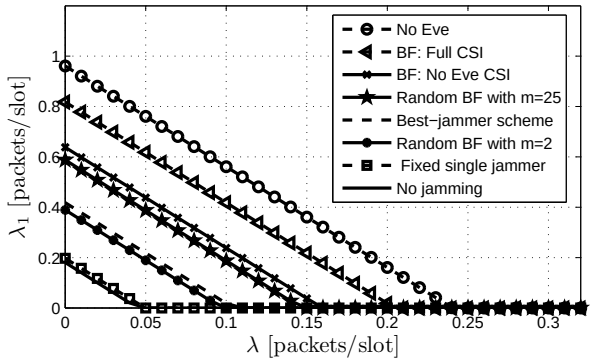


Fig. 2. The secrecy stable-throughput regions of the TDMA-jamming based schemes.

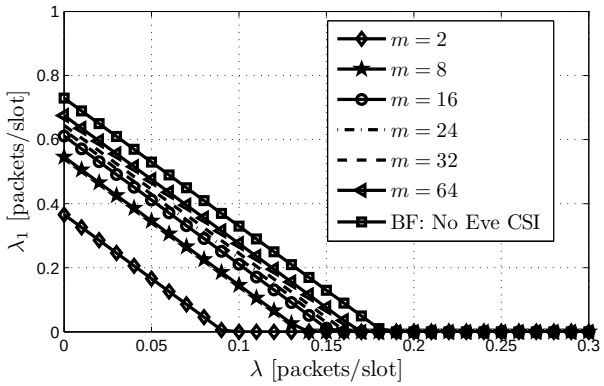


Fig. 3. Secure stable-throughput region for the random BF versus different values of m. We also plotted the optimal-BF jamming scheme when Eve's CSI is unknown at the legitimate nodes for comparison purpose.

shows the secrecy stable-throughput regions for our proposed jamming schemes in addition to the: (1) no-eavesdropper case which represents an upper bound on performance, (2) fixed-jamming scheme, where we have a known cooperative jammer that confounds the eavesdropper in each time slot, (3) best-jammer scheme [9], where the single cooperative jammer which maximizes the instantaneous secrecy rate is selected in each time slot, (4) the no-jamming case, where there is no jamming.

To implement the fixed (deterministic) jamming scheme, and given that we cannot fix the jamming nodes since a jamming node in a given time slot can be scheduled for data transmission in the following time slot, we assume that there are two fixed cooperative jammers such that when one of them is selected for data transmission, the other one acts as a cooperative jammer. The case of no eavesdropper's CSI at the transmitter can achieve much higher throughput than the case of complete CSI knowledge when choosing the single cooperative jammer that maximizes the instantaneous secrecy rate of the transmitting node in a given time slot. This case provides a stable-throughput region close to that achieved with complete CSI knowledge in the case of BF jamming but at the expense of not knowing the eavesdropper's channel gains. The random BF with $m = 25$ achieves relatively close performance to the BF scheme with no Eve's CSI at the legitimate nodes. The random-BF scheme with $m = 2$, which uses a small number of phase sequences at the cooperative jammers, is still better than the fixed-jamming and the no-jammer scenarios. It also achieves a performance very close to the best-jammer scheme, which requires Eve's CSI and a global CSI at a central control unit to decide the best jammer in every time slot, without the need for knowledge of Eve's CSI or a global CSI of the legitimate links at the legitimate nodes. For $\lambda > 0.1$ packets/slot, the random-BF jamming scheme, optimal-BF jamming scheme with no Eve's CSI, and optimal-BF jamming scheme with full CSI achieve a maximum secrecy stable throughput of 0.2, 0.21, and 0.4 packets/slot, respectively, for User 1 while all the other schemes achieve zero throughput for User 1. This demonstrates the gains of our proposed BF-based jamming schemes relative to the existing schemes.

Fig. 3 shows the network maximum secrecy stable-throughput region when applying the random-BF jamming scheme. It demonstrates the impact of increasing the number of possible phases at the cooperative jammers to eliminate the AN at Bob. The case of optimal BF, which requires full CSI knowledge of the legitimate channels at a control unit to compute the optimal BF weights, is also plotted to show that our proposed random BF scheme can achieve performance close to that of the optimal BF without the need for CSI knowledge of all legitimate links at the jamming nodes. This figure is generated using $\mathcal{M} = 4$. The optimal BF is always superior to the random BF since it is designed using the optimal weights to null the AN at Bob based on the CSI of the legitimate links.

In Fig. 4, we show the delay-requirement region of the optimal-BF jamming scheme with full CSI and the random-BF scheme. The assumed system's parameters are $\lambda_1 = 0.1$ packets/slot, $\lambda_2 = 0.2$ packets/slot, $\lambda_k = 0$ for all $k \geq 3$, and $\mathcal{M} = 5$. In the figure, the arrowheads point to the direction of the achievable delay requirements. As shown in the figure, the region is convex which implies that all points belonging to any line connecting two achievable delay pairs are also achievable. As the queueing-delay requirement of User 2 increases, the achievable average queueing delay of User 1 decreases. For example, in the case of the optimal-BF jamming scheme, if User 1 requires a queueing delay of 20 time slots, the minimum queueing delay of User 2 is 2.5 time slots. However, if User 1 requires an average queueing delay of 10 time slots, the minimum queueing delay of User 2 is 3.5 time slots. Hence, the minimum queueing delay of User 2 is increased since User 1 requests a lower queueing delay. As expected, the optimal-BF jamming scheme outperforms the random-BF scheme since the former is obtained using the appropriate BF weights designed based on full CSI of all links at the legitimate transmitting nodes (i.e. Eve's and the legitimate links' CSI).

Fig. 5 shows the secrecy outage probabilities of the proposed jamming schemes versus the average information-bearing signal SNR, γ_I, for different values of the number of source nodes, $\mathcal{M}$. The secrecy outage probabilities are monotonically nonincreasing with $\mathcal{M}$ and γ_I. The optimal-BF jamming scheme with full CSI achieves the lowest secrecy

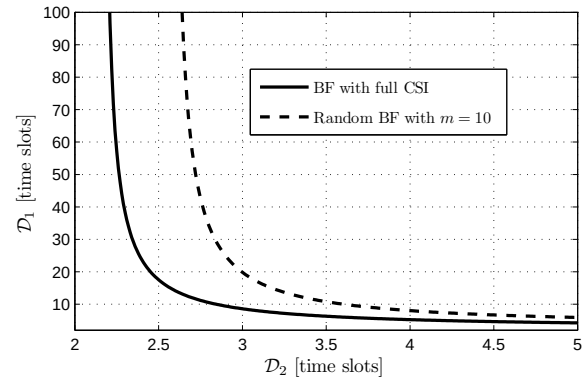


Fig. 4. Delay-requirement region for the BF jamming case when $\lambda_1 = 0.1$ packets/slot, $\lambda_2 = 0.2$ packets/slot, $\lambda_k = 0$ for all $k \geq 3$, $b = 1000$ bits, $WT = 1000$, and $\mathcal{M} = 5$.

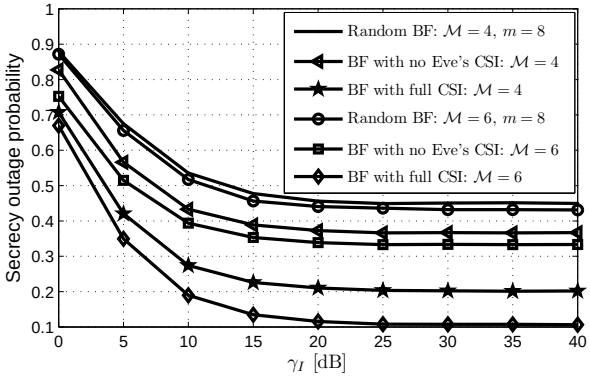


Fig. 5. Secrecy outage probabilities of the proposed BF-based jamming schemes versus γ_I for different values of $\mathcal{M}$.

outage probability. Moreover, the optimal-BF jamming scheme with no Eve's CSI achieves the second best performance. This is because both BF-based jamming schemes require more CSI than the random-BF scheme, which does not require Eve's CSI or the legitimate nodes CSI at the transmitting nodes. The secrecy outage probabilities saturate at high γ_I. The saturation levels of the secrecy outage probabilities for the optimal BF-based jamming and random-BF jamming schemes are $1-\mathcal{E}_{\mathrm{RBF}}$ and $1-\mathcal{E}_{\mathrm{OBF}}$, respectively, as explained earlier.

VII. Conclusions

In this paper, we proposed a joint PHY-MAC-network layers design for buffered-aided source nodes communicating with their common destination. The source nodes share the channel using a TDMA scheme with probabilistic time slot assignment. The assignment probabilities were designed to satisfy given QoS requirements for the legitimate source nodes (e.g. throughput, queue stability, average queueing delay) and their optimal values are functions of the system's parameters, the secrecy outage probabilities, and mean arrival rates at the queues. To reduce the secrecy outage probabilities and improve the users' QoS, we proposed a BF-based jamming scheme that enhances the instantaneous secrecy rate of the legitimate nodes. We showed that using cooperative BF-based jamming with global CSI at the legitimate nodes can achieve a performance, in terms of the maximum secure stable-throughput, that is close to the case when there is no eavesdropping. Moreover, we proposed a random-BF jamming scheme where the weights/phases that eliminate the AN at Bob are generated randomly at the cooperative jammers without the need for the jammers-Eve or the jammers-Bob links' CSI. This scheme outperformed the maximum-jamming-link scheme, where the cooperative jammer that maximizes the instantaneous secrecy rate of the transmitting node is selected in each time slot which requires global CSI at the legitimate nodes, and achieved a performance level close to that of the optimal BF without Eve's CSI. We derived the instantaneous secrecy rates and secrecy outage probabilities of the links as well as the maximum stable-throughput region and the delay-requirement region of the network for the proposed jamming schemes.

Appendix A
Proof of Lemma 1

Using the total probability theorem, the *complement* probability of secrecy outage for Transmitter k is given by

$$\begin{aligned}1-\mathbb{P}_{k,\mathrm{B}} =& \Pr\left\{\theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\} \\ &\times \Pr\left\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}} | \theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\} \\ &+\Pr\left\{\theta_{k,\mathrm{B}} < \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\} \\ &\times \Pr\left\{\mathcal{R} \leq R_{k,\mathrm{B}} | \theta_{k,\mathrm{B}} < \frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\}\end{aligned} \tag{40}$$

Note that the probability $\Pr\{\theta_{k,\mathrm{B}} \geq \frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\}$ is equal to the probability that the instantaneous secrecy rate is greater than or equal to zero. Thus, we compute this probability by setting $\mathcal{R}$ to zero in the expression of $\mathbb{P}_{k,\mathrm{B}}$. The probability $\Pr\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}} | \theta_{k,\mathrm{B}} \geq \frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\}$ can be rewritten as

$$\begin{aligned}&\Pr\left\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}} | \theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\} \\ &= \frac{\Pr\left\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}}, \theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\}}{\Pr\left\{\theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\}}\end{aligned} \tag{41}$$

The probability that $\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}}\}$ subsumes the probability that $\{\theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\}$. Thus, the joint probability is just the probability of the event $\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}}\}$. Accordingly, we have

$$\begin{aligned}&\Pr\left\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}} | \theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\} \\ &= \frac{\Pr\{\mathcal{R} \leq \mathcal{R}_{k,\mathrm{B}}\}}{\Pr\left\{\theta_{k,\mathrm{B}} \geq \frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}} g_j^* h_{j,\mathrm{E}}|^2}\right\}}\end{aligned} \tag{42}$$

Next, we move our attention to the second term of (40). Since it is given that the SINR at the eavesdropper's receiver

is greater than the SINR at Bob, the instantaneous secrecy rate is $\mathcal{R}_{k,\mathrm{B}}=0$. Thus,

$$\Pr\left\{\mathcal{R}\leq R_{\mathrm{s},k}=0\Big|\theta_{k,\mathrm{B}}<\frac{\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}\right\}=0 \quad (43)$$

Here, we used the fact that the rate, $\mathcal{R}$, is a nonnegative value, i.e., $\mathcal{R}\geq 0$.

The probability in (40) can be rewritten as

$$\begin{aligned}1-\mathbb{P}_{k,\mathrm{B}}&=\Pr\left\{2^{\mathcal{R}}\leq\frac{1+\gamma_I\theta_{k,\mathrm{B}}}{1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}}\right\}\\&=\Pr\left\{\theta_{k,\mathrm{B}}\geq\frac{2^{\mathcal{R}}\left(1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}\right)-1}{\gamma_I}\right\}\end{aligned} \quad (44)$$

Since $\theta_{k,\mathrm{B}}$ is an exponentially-distributed random variable with unit mean, for fixed $\theta_{k,\mathrm{E}}$ and $|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2$, we get

$$\begin{aligned}&\Pr\left\{\theta_{k,\mathrm{B}}\geq\frac{2^{\mathcal{R}}\left(1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}\right)-1}{\gamma_I}\Big|\theta_{k,\mathrm{E}},|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2\right\}\\&\quad=\exp\left(-\frac{2^{\mathcal{R}}\left(1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}\right)-1}{\gamma_I}\right)\end{aligned} \quad (45)$$

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

$$\begin{aligned}\mathcal{I}&=\int_0^\infty\exp\left(-\frac{2^{\mathcal{R}}\left(1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}\right)-1}{\gamma_I}\right)\exp(-\theta_{k,\mathrm{E}})d\theta_{k,\mathrm{E}}\\&=\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)\int_0^\infty\exp\left(-\eta\theta_{k,\mathrm{E}}\right)\exp(-\theta_{k,\mathrm{E}})d\theta_{k,\mathrm{E}}\\&=\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{1+\eta}\end{aligned} \quad (46)$$

where $\eta=\frac{2^{\mathcal{R}}}{1+\gamma_J|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2}$.

It can be shown, following [34], that the random variable $\alpha=|\mathbf{g}^*\mathbf{h}_{\mathrm{E}}|^2$ is Chi-square with $2(\mathcal{M}-2)$ degrees of freedom. Its probability density function (PDF) is characterized by

$$\mathcal{F}_\alpha(\Theta)=\frac{1}{(\mathcal{M}-3)!}\Theta^{\mathcal{M}-3}\exp(-\Theta),\Theta\geq 0 \quad (47)$$

Averaging over $\alpha=|\mathbf{g}^*\mathbf{h}_{\mathrm{E}}|^2=|\sum_{j\in\mathcal{J}}g_j^*h_{j,\mathrm{E}}|^2$, the probability of no secrecy outage is

$$\begin{aligned}1-\mathbb{P}_{k,\mathrm{B}}&=\int_0^\infty\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{1+\frac{2^{\mathcal{R}}}{1+\gamma_J\alpha}}\frac{1}{(\mathcal{M}-3)!}\alpha^{\mathcal{M}-3}\exp(-\alpha)d\alpha\\&=\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{(\mathcal{M}-3)!}\int_0^\infty\frac{\alpha^{\mathcal{M}-3}}{1+\frac{2^{\mathcal{R}}}{1+\gamma_J\alpha}}\exp(-\alpha)d\alpha\end{aligned} \quad (48)$$

This probability is rewritten as

$$\begin{aligned}1-\mathbb{P}_{k,\mathrm{B}}&=\int_0^\infty\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{1+\frac{2^{\mathcal{R}}}{1+\gamma_J\alpha}}\frac{1}{(\mathcal{M}-3)!}\alpha^{\mathcal{M}-3}\exp(-\alpha)d\alpha\\&=\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{(\mathcal{M}-3)!}\int_0^\infty\frac{\alpha^{\mathcal{M}-3}(1+\gamma_J\alpha)}{1+\gamma_J\alpha+2^{\mathcal{R}}}\exp(-\alpha)d\alpha\\&=\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{(\mathcal{M}-3)!}\frac{1}{\gamma_J}\int_0^\infty\frac{\alpha^{\mathcal{M}-3}(1+\gamma_J\alpha)}{\alpha+\frac{1+2^{\mathcal{R}}}{\gamma_J}}\exp(-\alpha)d\alpha\\&=\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{(\mathcal{M}-3)!}\frac{1}{\gamma_J}\\&\times\left(\int_0^\infty\frac{\alpha^{\mathcal{M}-3}}{\alpha+\frac{1+2^{\mathcal{R}}}{\gamma_J}}\exp(-\alpha)d\alpha+\gamma_J\int_0^\infty\frac{\alpha^{\mathcal{M}-2}}{\alpha+\frac{1+2^{\mathcal{R}}}{\gamma_J}}\exp(-\alpha)d\alpha\right)\\&=\frac{\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)}{(\mathcal{M}-3)!}\frac{\left(\mathrm{F}\left(\mathcal{M}-3,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)+\gamma_J\mathrm{F}\left(\mathcal{M}-2,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)\right)}{\gamma_J}\end{aligned} \quad (49)$$

where $\mathrm{F}(\cdot,\cdot)$ is given in (16) with $\mathrm{Ei}(\cdot)$ as the exponential integral function. $\mathrm{F}(\cdot,\cdot)$ is given in [32, Eqn. 3.353.5].

The term $\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)$ in (16) represents the no secrecy outage probability when there is no eavesdropping in the network. Hence, we can rewrite as follows

$$1-\mathbb{P}_{k,\mathrm{B}}=(1-\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}})\frac{\mathrm{F}\left(\mathcal{M}-3,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)+\gamma_J\mathrm{F}\left(\mathcal{M}-2,\frac{1+2^{\mathcal{R}}}{\gamma_J}\right)}{\gamma_J(\mathcal{M}-3)!} \quad (50)$$

where $\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}}=1-\exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right)$.

Appendix B

In this appendix, we compute the following probability

$$\Pr\left\{\frac{1+\frac{\gamma_I\theta_{k,\mathrm{B}}}{1+X_2}}{1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+X_1}}>2^{\mathcal{R}}\right\} \quad (51)$$

where $\theta_{k,\mathrm{B}}$, $\theta_{k,\mathrm{E}}$, X_1 and X_2 are random variables. Letting $x=\theta_{k,\mathrm{B}}$ and $y=\theta_{k,\mathrm{E}}$, (51) is rewritten as

$$\mathbb{P}=\Pr\left\{x>\frac{2^{\mathcal{R}}-1}{\frac{\gamma_I}{1+X_2}}+2^{\mathcal{R}}\frac{1+X_2}{1+X_1}y\right\} \quad (52)$$

For fixed y, $E_1=2^{\mathcal{R}}\frac{1+X_2}{1+X_1}$ and $E_2=\frac{2^{\mathcal{R}}-1}{\frac{\gamma_I}{1+X_2}}$, we have

$$\begin{aligned}\Pr\left\{\frac{1+\frac{\gamma_I\theta_{k,\mathrm{B}}}{1+X_2}}{1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+X_1}}>2^{\mathcal{R}}|y,E_1,E_2\right\}&=\Pr\left\{x>E_1y+E_2|y,E_1,E_2\right\}\\&=\exp(-(E_1y+E_2))\end{aligned} \quad (53)$$

Since y is exponentially-distributed random variable with unit mean, averaging over it results in

$$\begin{aligned}\mathcal{G}&=\Pr\left\{\frac{1+\frac{\gamma_I\theta_{k,\mathrm{B}}}{1+X_2}}{1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+X_1}}>2^{\mathcal{R}}\Big|E_1,E_2\right\}\\&=\exp(-E_2)\int_{y=0}^\infty\exp(-(E_1+1)y)dy\\&=\frac{\exp(-E_2)}{E_1+1}=\frac{\exp(-\frac{2^{\mathcal{R}}-1}{\frac{\gamma_I}{1+X_2}})}{1+2^{\mathcal{R}}\frac{1+X_2}{1+X_1}}\end{aligned} \quad (54)$$

Since E_1 and E_2 are functions of X_1 and X_2, the closed-form expression of $\Pr\left\{\frac{1+\frac{\gamma_I\theta_{k,\mathrm{B}}}{1+X_2}}{1+\frac{\gamma_I\theta_{k,\mathrm{E}}}{1+X_1}} > 2^{\mathcal{R}}\right\}$ can be obtained by averaging over X_1 and X_2.

APPENDIX C
PROOF LEMMA 2

From (15) in Lemma 1, as $\gamma_J \to \infty$, we have

$$\lim_{\gamma_J\to\infty}(1-\mathbb{P}_{k,\mathrm{B}}) = (1-\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}})\frac{\mathrm{F}(\mathcal{M}-2,0)}{(\mathcal{M}-3)!} \tag{55}$$

From (16), $\mathrm{F}(\mathcal{M}-2,0) = \Gamma(\mathcal{M}-2) = (\mathcal{M}-3)!$, where $\Gamma(\cdot)$ is the Gamma function. Hence,

$$\lim_{\gamma_J\to\infty}(1-\mathbb{P}_{k,\mathrm{B}}) \approx (1-\mathbb{P}_{k,\mathrm{B}}^{\mathrm{noEve}}) = \exp\left(-\frac{2^{\mathcal{R}}-1}{\gamma_I}\right) \tag{56}$$

This completes the proof.

APPENDIX D
PROOF OF LEMMA 3

Starting with the instantaneous secrecy rate expression in (21), the secrecy outage probability for a fixed $|\sum_{j\in\mathcal{J}}\phi_{\tilde{q},j}^* h_{j,\mathrm{E}}|^2$ is given by

$$\Pr\left\{\begin{matrix}\text{secrecy}\\ \text{outage}\end{matrix}\middle| |\sum_{j\in\mathcal{J}}\phi_{\tilde{q},j}^* h_{j,\mathrm{E}}|^2\right\} = 1 - \frac{\exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})}{1+2^{\mathcal{R}}\frac{1}{1+\frac{\gamma_J}{\mathcal{M}-1}|\sum_{j\in\mathcal{J}}\phi_{\tilde{q},j}^* h_{j,\mathrm{E}}|^2}} \tag{57}$$

Averaging over $\mathcal{X}_2 = \frac{|\sum_{j\in\mathcal{J}}\phi_{\tilde{q},j}^* h_{j,\mathrm{E}}|^2}{\mathcal{M}-1}$, we get the secrecy outage probability as follows

$$\mathbb{P}_{k,\mathrm{B}} = 1 - \exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})\int_{\mathcal{X}_2=0}^{\infty}\frac{\exp(-\mathcal{X}_2)}{1+2^{\mathcal{R}}\frac{1}{1+\gamma_J\mathcal{X}_2}}d\mathcal{X}_2 \tag{58}$$

The probability of no secrecy outage is given by

$$\begin{aligned}
1-\mathbb{P}_{k,\mathrm{B}} &= \exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})\int_{\mathcal{X}_2=0}^{\infty}\frac{(1+\gamma_J\mathcal{X}_2)\exp(-\mathcal{X}_2)}{1+\gamma_J\mathcal{X}_2+2^{\mathcal{R}}}d\mathcal{X}_2\\
&= \frac{\exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})}{\gamma_J}\int_0^{\infty}\frac{(1+\gamma_J\mathcal{X}_2)\exp(-\mathcal{X}_2)}{\mathcal{X}_2+\frac{1+2^{\mathcal{R}}}{\gamma_J}}d\mathcal{X}_2\\
&= \frac{\exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})}{\gamma_J}\\
&\times\left(\int_0^{\infty}\frac{\exp(-\mathcal{X}_2)}{\mathcal{X}_2+\frac{1+2^{\mathcal{R}}}{\gamma_J}}d\mathcal{X}_2+\int_0^{\infty}\frac{(\gamma_J\mathcal{X}_2)\exp(-\mathcal{X}_2)}{\mathcal{X}_2+\frac{1+2^{\mathcal{R}}}{\gamma_J}}d\mathcal{X}_2\right)\\
&= \frac{\exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})}{\gamma_J}\left(\mathrm{F}(0,\frac{1+2^{\mathcal{R}}}{\gamma_J})+\gamma_J\mathrm{F}(1,\frac{1+2^{\mathcal{R}}}{\gamma_J})\right)
\end{aligned} \tag{59}$$

where $\mathrm{F}(\cdot,\cdot)$ is given in (16). This completes the proof.

APPENDIX E
PROOF LEMMA 4

As $\gamma_J \to \infty$, from (22) in Lemma 3, the no secrecy outage probability is given by

$$\lim_{\gamma_J\to\infty}(1-\mathbb{P}_{k,\mathrm{B}}) \approx \exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I})\mathrm{F}(1,0) \tag{60}$$

From (16), $\mathrm{F}(1,0) = \int_0^{\infty}\exp(-\alpha)d\alpha = 1$. Hence,

$$\lim_{\gamma_J\to\infty}(1-\mathbb{P}_{k,\mathrm{B}}) \approx \exp(-\frac{2^{\mathcal{R}}-1}{\gamma_I}) \tag{61}$$

This completes the proof.

REFERENCES

[1] A. El Shafie, T. Q. Duong, and N. Al-Dhahir, "QoS-Based design for security enhancement in TDMA-Based wireless networks," Accepted in IEEE Globecom 2016.

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

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

[4] 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.

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

[6] 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.

[7] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[8] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[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] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Cooperative jamming for wireless physical layer security," in *IEEE/SP 15th Workshop on Statistical Sig. Process.*, Aug. 2009, pp. 417–420.

[11] A. E. Shafie, D. Niyato, and N. Al-Dhahir, "Security of rechargeable energy-harvesting transmitters in wireless networks," *Accepted for Publication in IEEE Wireless Commun. Lett.*, 2016.

[12] 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 Sig. Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[13] X. Zhou, M. Tao, and R. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Proc. IEEE ICC*, Jun. 2012, pp. 2339–2344.

[14] 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.

[15] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.

[16] 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.

[17] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Tech.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[18] 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. Tech.*, 2015. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7247767

[19] 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.

[20] 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.

[21] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

[22] A. Sadek, K. 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.

[23] A. El-Sherif, A. K. Sadek, K. Liu *et al.*, "Opportunistic multiple access for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 704–715, Apr. 2011.

[24] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6–28, 2004.
[25] I. Krikidis, J. Thompson, S. McLaughlin, and N. Goertz, "Amplify-and-forward with partial relay selection," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 235–237, 2008.
[26] D. B. da Costa and S. Aissa, "Performance analysis of relay selection techniques with clustered fixed-gain relays," *IEEE Sig. Process. Lett.*, vol. 17, no. 2, pp. 201–204, Feb. 2010.
[27] D. Ng, E. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
[28] 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.
[29] 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.
[30] R. Loynes, "The stability of a queue with non-independent inter-arrival and service times," in *Proc. Cambridge Philos. Soc*, vol. 58, no. 3. Cambridge Univ. Press, Jul. 1962, pp. 497–520.
[31] C. D. Meyer, *Matrix analysis and applied linear algebra*. Siam, 2000.
[32] D. Zwillinger, *Table of integrals, series, and products*. Elsevier, 2014.
[33] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.
[34] 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 his B.Sc. degree in Electrical Engineering from Alexandria University, Alexandria, Egypt, in 2009 with accumulative grade of distinction with honor. He received his M.Sc. degree in Communication and Information Technology from Nile University in 2014. He is currently pursuing the Ph.D. degree at the University of Texas at Dallas, USA. He received the IEEE Transactions on Communications Exemplary Reviewer 2015.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include small-cell networks, physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of 230 technical papers published in scientific journals (120 articles) and presented at international conferences (110 papers).

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, and IET COMMUNICATIONS. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014, and IEEE Global Communications Conference (GLOBECOM) 2016. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2016-2021).

Naofal Al-Dhahir (F'07) is Erik Jonsson Distinguished Professor at UT-Dallas. He earned his PhD degree in Electrical Engineering from Stanford University, CA, USA, in 1994. From 1994 to 2003, he was a principal member of the technical staff at GE Research and AT&T Shannon Laboratory. He is co-inventor of 41 issued US patents, co-author of over 325 papers with over 7800 citations, and co-recipient of 4 IEEE best paper awards including the 2006 IEEE Donald G. Fink award. He is the Editor-in-Chief of IEEE Transactions on Communications and an IEEE Fellow.