Enhanced Secrecy Performance of Multihop IoT Networks with Cooperative Hybrid-Duplex Jamming

Zaid Abdullah, *Member, IEEE,* Gaojie Chen, *Senior Member, IEEE,* Mohammed A. M. Abdullah, *Member, IEEE,* and Jonathon A. Chambers, *Fellow, IEEE*

***Abstract*—As the number of connected devices is exponentially increasing, security in Internet of Things (IoT) networks presents a major challenge. Accordingly, in this work we investigate the secrecy performance of multihop IoT networks assuming that each node is equipped with only two antennas, and can operate in both Half-Duplex (HD) and Full-Duplex (FD) modes. Moreover, we propose an FD Cooperative Jamming (CJ) scheme to provide higher security against randomly located eavesdroppers, where each information symbol is protected with two jamming signals by its two neighbouring nodes, one of which is the FD receiver. We demonstrate that under a total power constraint, the proposed FD-CJ scheme significantly outperforms the conventional FD Single Jamming (FD-SJ) approach, where only the receiving node acts as a jammer, especially when the number of hops is larger than two. Moreover, when the Channel State Information (CSI) is available at the transmitter, and transmit beamforming is applied, our results demonstrate that at low Signal-to-Noise Ratio (SNR), higher secrecy performance is obtained if the receiving node operates in HD and allocates both antennas for data reception, leaving only a single jammer active; while at high SNR, a significant secrecy enhancement can be achieved with FD jamming. Our proposed FD-CJ scheme is found to demonstrate a great resilience over multihop networks, as only a marginal performance loss is experienced as the number of hops increases. For each case, an integral closed-form expression is derived for the secrecy outage probability, and verified by Monte Carlo simulations.**

***Index Terms*—IoT, Multihop, Cooperative jamming, Full-duplex, Secrecy outage probability, Stochastic geometry**

I. Introduction

THERE is no doubt that the Internet of Things (IoT) is one of the biggest trends in today's wireless technology, where billions of connected devices are expected to be utilized to enable smart cities [1]. The reason behind this massive interest in IoT networks is due to the fact that these connected devices can be used in a wide range of different applications, such as home automation, eHealth, environmental and industrial applications, and Internet of Vehicles [2]. Depending on the specific application, some of the data exchanged via IoT devices can be highly sensitive and confidential, such as personal data, financial information, etc, and given the fact that these devices exchange their data through wireless channels, it becomes quite clear that the security aspect in IoT networks is a challenge of great importance [3], [4].

To that end, Physical Layer Security (PLS) is considered as a promising way to enhance security in IoT networks [5]. One of the main advantages of using PLS over conventional encryption techniques, is that even if the eavesdropper has powerful tools, a secure link can still be guaranteed [6]. Thanks to its simplicity and security enhancement, PLS has been widely investigated in recent years, and in different forms. For example, with multiple antenna systems, PLS can be achieved by injecting the data with Artificial Noise (AN). This is usually applied in downlink transmissions of cellular networks where the Base Station (BS) is equipped with multiple antennas and has an accurate knowledge of the Channel State Information (CSI) of legitimate users. Another way of applying PLS is by assigning a single or multiple trusted nodes to transmit jamming signals while a pair of source-destination nodes exchange their data. Finally, the Full-Duplex (FD) scheme was adopted for PLS enhancement where the receiving node broadcasts a jamming signal while receiving the data at the same time.

A. Related work

In [7], the authors adopted a stochastic geometry approach to analyze the performance of FD Device-to-Device (D2D) communications in multi-tier wireless networks with optimal spectrum partition between D2D and cellular modes. The authors in [8] analysed the achievable secrecy rate utilizing FD relays under a total power constraint, and they showed that FD relays can achieve a significant performance enhancement over Half-Duplex (HD) relays. However, their work considered only a single eavesdropper scenario, and was based on the following assumptions: (a) there is no link between the source and the eavesdropper, (b) the Self-Interference (SI) is perfectly cancelled at the receiving node, and (c) global CSI is available. The authors in [9] studied the secrecy performance of a single-hop Multiple-Input Multiple-Output (MIMO) system utilizing beamforming and AN techniques. In their work, they assumed a Poisson Point Process (PPP) distribution for the multi-antenna eavesdroppers, and all nodes operated in HD mode. In addition, the authors in [10] proposed an AN-aided transmission for a two-hop system with randomly located eavesdroppers. In their work, it was assumed that the source, relay, destination, and eavesdroppers are all equipped with multiple antennas and work in HD mode. The authors in [11] considered a two-hop system where the HD source and

This work was supported by EPSRC grant number EP/R006377/1 ("M3NETs").

Z. Abdullah, G. Chen and J. A. Chambers are with the School of Engineering, University of Leicester, LE1 7HB, UK. Emails: {zaid.abdullah; gaojie.chen; jonathon.chambers}@leicester.ac.uk.

M. Abdullah is with the Department of Computer and Information Engineering, College of Electronics Engineering, Ninevah University, Mosul, 41002, Iraq. Email: mohammed.abdulmuttaleb@uoninevah.edu.iq

destination communicate via an FD relay in the presence of randomly located eavesdroppers. The authors in [12] proposed a joint user and FD relay selection to enhance the end-to-end (e2e) secrecy performance in the presence of a single eavesdropper. It was assumed in their work that no direct link between the source and the eavesdropper exists. Moreover, the authors in [13] analyzed the performance of a two-hop system in the presence of a single eavesdropper, where the multi-antenna source adopts an AN-aided precoding scheme to enhance the secrecy rate. The authors in [14] studied the secrecy performance of downlink transmission in cellular networks, where the HD BSs, mobile users, and eavesdroppers are all randomly distributed according to independent PPPs. Furthermore, the authors in [15] investigated finding a secure path over Randomize-and-Forward (RaF) relaying in a multihop ad hoc network in the presence of inhomogeneous eavesdropper clusters; while the authors in [16] carried out a secrecy rate optimization for FD multihop systems in the presence of a single jammer and a single eavesdropper. The authors in [17] analyzed the secrecy performance of modify-and-forward relaying, and they proposed three relay-selection criteria subject to the availability of CSI. In addition, the authors in [18] proposed optimal and suboptimal relay-selection schemes for an FD multi-hops network, to enable secure communication between multiple source-destination pairs under multiple eavesdropper attacks. The authors in [19] investigated the secrecy performance of FD relaying in a two-hop system with a single eavesdropper. Their work demonstrated that FD jamming can provide a significant performance improvement compared to an HD scheme. The authors in [20] analyzed the performance of downlink transmission with randomly located eavesdroppers, where the BS employs antenna-selection to enhance the secrecy performance. Furthermore, the authors in [21] studied the trade-off between throughput and security in decentralized wireless networks, and they found that to achieve high network security, a significant sacrifice in the throughput must be made. The authors in [22] adopted a stochastic geometry approach to study the secrecy performance in large cellular networks, where the positions of both BSs and mobile users are modelled according to two different PPPs. The authors in [23] studied the enhancement of a system's security by means of Cooperative Jamming (CJ) and power optimization. However, in their work they assumed that all nodes work in HD mode, and global CSI is available, including that of the eavesdroppers. The authors in [24] studied joint relay and jammer selection in two-way relay systems, where all nodes work in HD mode and a single eavesdropper case was assumed. The authors in [25] proposed a CJ scheme for a two-hop, multi-antenna relay network in the presence of a single eavesdropper, where the source, relay, destination, and eavesdropper all operate in HD mode. Moreover, in [26], the authors investigated the secrecy performance of a three-hop relay system with CJ for IoT applications, where the signal travels from the source to the destination through two untrusted relays, and it was assumed that each node had a single antenna and operated in HD mode. Their work was further extended in [27] to include hardware impairments and channel estimation errors. Finally, the authors in [28] proposed a proactive eavesdropping scheme that utilized multi-antenna FD spoofing relays and a single multi-antenna cooperative jammer to covertly wiretap the communication between a pair of suspicious users.

B. Motivation and contribution

Despite the interesting work found in the literature, there are many challenges and/or assumptions that need to be addressed. For example, most of the work assumes a two-hop system [10]–[13], [19], [25], while in many real-life scenarios the signal needs to go through multiple hops to reach the destination. In addition, although utilizing multiple antennas to perform AN-aided beamforming can dramatically improve the performance, it adds much complexity and might not be suitable to adopt in IoT networks for many reasons. For example, to enable massive IoT networks, connected devices must have low cost and low complexity [29], in addition, AN-aided beamforming depends on the accuracy of CSI at the transmitter, and given the fact that only limited feedback will be available in IoT networks [5], this can result in poor secrecy performance due to the low channel estimation accuracy, which in return results in noise leakage to the legitimate receiving node [30]–[32].

Motivated by the above, in this work we aim to investigate and enhance secrecy performance in IoT networks. In particular, we propose a CJ scheme for multihops systems with hybrid-duplex relays, where the source, $(N-1)$ relays and destination are each equipped with two antennas, and can be switched between HD and FD modes. Moreover, we assume that the receiving node always has knowledge of the CSI, and investigate the secrecy performance subject to the availability of CSI at the transmitter side. Accordingly, we consider three different scenarios: (a) no CSI is available at the transmitting node, (b) CSI is available at the transmitter, and the receiver works in FD mode, and (c) CSI is available at the transmitter, and the receiver exploits both antennas for data reception. Our main contributions can be summarized as follows

1) We propose a CJ scheme such that when the ith node S_i, is transmitting an information symbol, both the receiving node S_{i+1}, and node S_{i-1} act as jammers. In general, nodes S_i and S_{i-1} are used for data transmission and jamming, respectively, and always operate in HD mode. Moreover, when the CSI is not available at S_i, it employs only a single antenna to transmit the data, while the receiving node S_{i+1}, operates in FD mode and utilizes both antennas to simultaneously receive the data and broadcasts a jamming signal.
2) When the CSI is available at S_i, a transmit beamforming is performed utilizing both antennas, while at the receiving end, there are two possible cases: (a) the receiving node S_{i+1} operates in FD mode similar to the first scenario, and (b) S_{i+1} operates in HD mode and employs both antennas for data reception, leaving S_{i-1} as the only jammer. Our results demonstrate that under a total power constraint, case (b) provides better performance at low Signal-to-Noise Ratio (SNR), while the FD-CJ scheme with transmit beamforming in (a) is shown to be the best choice at high SNR.

3) For each case, we derive closed-form expressions for the Probability Density Function (PDF) of the legitimate link, and the Cumulative Distribution Function (CDF) of the eavesdropper link. The final integral is solved numerically yielding results which closely match the Monte Carlo simulations. Our results demonstrate that the proposed FD-CJ scheme, with or without transmit beamforming, has a great advantage over the conventional FD single jamming scheme in multihop networks, as only a negligible performance degradation is experienced as the number of hops increases.

To the best of the authors' knowledge, the secrecy performance of a multihop network with hybrid-duplex dual CJ relays has not been investigated in any previously published work, regardless of the availability of CSI of legitimate nodes and/or eavesdroppers.

The rest of this paper is organized as follows. In Section II, we introduce the system model and formulate the received signals for each case. In Section III, we perform the secrecy analysis for the proposed system. In Section IV, different numerical results are presented along with their discussions. Finally, conclusions are drawn in Section V.

Notations: matrices and vectors are denoted by boldface upper and lower case letters, respectively. $|a|$ represents the absolute value of a, $\|\mathbf{a}\|$ is the Frobenius norm of vector $\mathbf{a}$, while $\mathbf{a}^*$, $\mathbf{a}^T$, and $\mathbf{a}^H$ are the conjugate, transpose, and Hermitian transpose of the same vector, respectively. $\mathbb{P}(.)$ and $\mathbb{E}(.)$ denote the probability and expectation operators, respectively, and $\boldsymbol{I}_N$ is the $N \times N$ identity matrix.

II. System Model

In our work, we consider a system with one source S_0, one destination S_N, and $N-1$ RaF[1] relays ($S_i, i \in \{1, 2, ..., N-1\}$) as shown in Fig. 1. We assume that the source is located at the origin of a $2-$D plane, and the $N-1$ relays and the destination are located at fixed distances from the origin. All nodes are equipped with two antennas, and can switch between HD and FD modes according to the system's needs as well as the availability of CSI. In addition, the locations of the independent (non-colluding) eavesdroppers are modelled as a homogeneous PPP, Φ_E, within a circle of radius R and a density of λ_E. Throughout this work, we assume that all eavesdroppers are passive and equipped with a single antenna. Moreover, all channels between any two nodes i and j are assumed to undergo both small and large scale fading, and can be expressed as $g_{i,j} = h_{i,j} d_{i,j}^{-\alpha/2}$, where $h_{i,j}$ is the small-scale, independent and identically distributed (i.i.d.), Rayleigh fading coefficient with zero mean and unit variance. In contrast, $d_{i,j}^{-\alpha/2}$ is the large-scale fading, where d is the distance and α is the path-loss exponent. Therefore, the channel gains expressed as $|g_{i,j}|^2$ are independent and exponentially distributed random variables with an average power of $d_{i,j}^{-\alpha}$.

In this work, our main goal is to investigate and enhance the secrecy performance of the e2e system for three different cases: (a) when no CSI is available at the transmitter, (b) the CSI is available at the transmitter and the receiver works in FD mode, and (c) the CSI is available at the transmitter and the receiver works in HD mode. For each of these cases, we analyse the performance of the system in terms of the e2e secrecy outage probability. In the following subsections, we start with formulating the Signal-to-Interference plus Noise Ratio (SINR) for each of the three aforementioned cases.

[1]In the RaF relaying scheme, the well-known Wyner wiretap code is used at different transmission time slots, such that each hop will employ different codebooks with independent randomness.

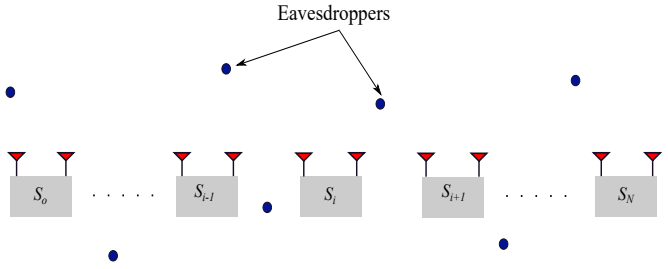

Fig. 1. System model with randomly located eavesdroppers.

A. No CSI at the transmitter

In this case, we assume that the transmitter has no knowledge about the CSI due to limited feedback. Therefore, the transmitting node S_i, which operates in HD mode, uses only one antenna to transmit the signal, while the second antenna remains idle. On the other hand, we assume that the receiving node S_{i+1}, works in FD mode and employs two antennas to simultaneously receive the data and send a jamming signal. Since only one antenna is employed at the transmitter and the receiver to exchange the data, this scenario is referred to as Single-Input Single-Output (SISO). The received signal at S_{i+1} can be given as follows

$$y_{S_{i+1}}^{\text{SISO}} = \frac{\sqrt{P_t} h_{i+1,i}}{d_{i+1,i}^{\alpha/2}} x_i + \sqrt{P_{j_1}} h_{i+1,i+1} x_{j_1} + z_{i+1}, \qquad (1)$$

where x_i and x_{j_1} are the transmitted information and jamming signals, respectively, with $\mathbb{E}\{|x_k|^2\} = 1$ ($k \in \{i, j_1\}$), P_t and P_{j_1} are the total transmit and jamming powers, respectively, and z_{i+1} is the Additive White Gaussian Noise (AWGN) at the receiver with zero mean and variance of σ^2. Accordingly, and in the interference-limited scenario, the Signal-to-Interference Ratio (SIR) at the receiving node $\gamma_{S_{i+1}}^{\text{SISO}}$, can be given as follows

$$\gamma_{S_{i+1}}^{\text{SISO}} = \frac{\frac{P_t |h_{i+1,i}|^2}{d_{i+1,i}^{\alpha}}}{P_{j_1} |h_{i+1,i+1}|^2 + \sigma^2} \approx \frac{\frac{P_t |h_{i+1,i}|^2}{d_{i+1,i}^{\alpha}}}{\gamma_{SI}}, \qquad (2)$$

where γ_{SI} is the residual self-interference power after applying self-interference cancellation techniques.

To provide a better protection for the transmitted data, we propose a CJ between the nodes. However, during the first hop ($n = 1$), only a single jammer (S_1) will be active, while for all subsequent hops, two nodes will be transmitting jamming signals to enhance the secrecy performance[2]. Specifically,

[2]We assume in this work that due to the path loss and shadowing, the receiving node can only be affected by signals transmitted from adjacent nodes [33]. Therefore, the received signal at the legitimate node in (1) will not be affected by the second jammer, since nodes S_{i+1} and S_{i-1} are not neighbouring nodes.

assume that for the nth hop ($n \in \{2,3,...,N\}$), S_i ($i = n-1$) will transmit the information symbol, while both adjacent nodes S_{i+1} and S_{i-1}, will be used for jamming purposes. However, and unlike the receiving node, S_{i-1} operates in HD mode[3]. The received signal at the eavesdropper can be expressed as

$$y_{e,i}^{\text{SISO}} = \varpi \frac{\sqrt{P_{j2}} h_{e,i-1}}{d_{e,i-1}^{\alpha/2}} x_{j_2} + \frac{\sqrt{P_t} h_{e,i}}{d_{e,i}^{\alpha/2}} x_i + \frac{\sqrt{P_{j1}} h_{e,i+1}}{d_{e,i+1}^{\alpha/2}} x_{j_1} + z_e, \tag{3}$$

where x_{j_2} is the second jamming signal with $\mathbb{E}\{|x_{j_2}|^2\} = 1$, P_{j2} is the transmit jamming power at S_{i-1}, z_e is the AWGN at the eavesdropper with zero mean and variance of σ^2, and

$$\varpi = \begin{cases} 0, & \text{if } n = 1 \text{ (i.e. the first hop)} \\ 1, & \text{otherwise.} \end{cases} \tag{4}$$

Therefore, and considering the interference limited case, the maximum SIR at any eavesdropper, i.e. the worst-case scenario for the legitimate receiver, can be given as follows

$$\gamma_{e,i}^{\text{SISO}} = \max_{e \in \Phi_E} \left(\frac{\frac{P_t |h_{e,i}|^2}{d_{e,i}^{\alpha}}}{\varpi \frac{P_{j_2} |h_{e,i-1}|^2}{d_{e,i-1}^{\alpha}} + \frac{P_{j_1} |h_{e,i+1}|^2}{d_{e,i+1}^{\alpha}}} \right). \tag{5}$$

B. CSI available at the transmitter with FD receiver

When the CSI is available at the transmitter, it can utilize both antennas for data transmission through transmit beamforming. This case is known as Multiple-Input Single-Output (MISO), since at the receiving node, and similar to the SISO case, the two antennas will be utilized to simultaneously receive the data and broadcast a jamming signal. Therefore, the received signal at the legitimate node can be given as follows

$$y_{S_{i+1}}^{\text{MISO}} = \frac{\sqrt{P_t} \mathbf{h}_{i+1,i}^T \mathbf{w}_0}{d_{i+1,i}^{\alpha/2}} x_i + \sqrt{P_{j_1}} h_{i+1,i+1} x_{j_1} + z_{i+1}, \tag{6}$$

where $\mathbf{h}_{i+1,i} = [h_{i+1,i}^{[1]}, \ h_{i+1,i}^{[2]}]^T$ is the channel vector between the two transmitting antennas at S_i, and the receiving antenna at S_{i+1}, $\mathbf{w}_0 \in \mathbb{C}^{2\times 1}$ is the Maximum Ratio Transmission (MRT) precoding vector, and can be defined as

$$\mathbf{w}_0 = \frac{\mathbf{h}_{i+1,i}^*}{\|\mathbf{h}_{i+1,i}\|}, \tag{7}$$

and the SIR at the legitimate node can be given as follows

$$\gamma_{S_{i+1}}^{\text{MISO}} = \frac{\frac{P_t}{d_{i+1,i}^{\alpha}} |\mathbf{h}_{i+1,i}^T \mathbf{w}_0|^2}{\gamma_{SI}}. \tag{8}$$

In contrast, the received signal at the eavesdropper for the MISO case can be expressed as follows

$$y_{e,i}^{\text{MISO}} = \varpi \frac{\sqrt{P_{j_2}} h_{e,i-1}}{d_{e,i-1}^{\alpha/2}} x_{j_2} + \frac{\sqrt{P_t} \mathbf{h}_{e,i}^T \mathbf{w}_0}{d_{e,i}^{\alpha/2}} xi + \frac{\sqrt{P_{j_1}} h_{e,i+1}}{d_{e,i+1}^{\alpha/2}} x_{j_1} + z_e, \tag{9}$$

where $\mathbf{h}_{e,i} = [h_{e,i}^{[1]}, \ h_{e,i}^{[2]}]^T$ is the channel vector between the two transmitting antennas at S_i and the eavesdropper. It should be noted that S_{i-1} uses only one antenna to send the jamming signal, while the second antenna remains idle. Moreover, and considering the worst-case scenario, the SIR at the eavesdropper for the MISO case can be given as

$$\gamma_{e,i}^{\text{MISO}} = \max_{e \in \Phi_E} \left(\frac{\frac{P_t |\mathbf{h}_{e,i}^T \mathbf{w}_0|^2}{d_{e,i}^{\alpha}}}{\varpi \frac{P_{j_2} |h_{e,i-1}|^2}{d_{e,i-1}^{\alpha}} + \frac{P_{j_1} |h_{e,i+1}|^2}{d_{e,i+1}^{\alpha}}} \right). \tag{10}$$

C. CSI is available at the transmitter with HD receiver

When the receiver works in HD mode, MIMO diversity can be obtained by means of transmit/receive beamforming over the maximum eigenvalue. In particular, the Singular Value Decomposition (SVD) of the channel matrix between the transmit and receiving nodes, $\mathbf{H}_{i+1,i} \in \mathbb{C}^{2\times 2}$, can be expressed as follows

$$\mathbf{H}_{i+1,i} = \mathbf{U}_{i+1,i} \mathbf{D}_{i+1,i} \mathbf{V}_{i+1,i}, \tag{11}$$

where $\mathbf{D}_{i+1,i} \in \mathbb{R}^{2\times 2}$ is a diagonal matrix with real and non-negative singular values, $\mathbf{U}_{i+1,i} \in \mathbb{C}^{2\times 2}$ and $\mathbf{V}_{i+1,i} \in \mathbb{C}^{2\times 2}$ are the unitary matrices of the corresponding receive and transmit singular vectors, respectively. Moreover, since we are dealing with a 2×2 system, there are two singular values in the diagonal of $\mathbf{D}_{i+1,i}$, λ_1 and λ_2, with $\lambda_1 > \lambda_2$. Therefore, the corresponding transmit and receive weight vectors are the first columns of $\mathbf{V}_{i+1,i}$ and $\mathbf{U}_{i+1,i}$, respectively. The combined signal at S_{i+1} can be given as follows

$$y_{S_{i+1}}^{\text{MIMO}} = \frac{\sqrt{P_t} \mathbf{u}_{max}^T \mathbf{H}_{i+1,i} \mathbf{v}_{max}}{d_{i+1,i}^{\alpha/2}} x_i + \mathbf{u}_{max}^T \mathbf{z}_{i+1}, \tag{12}$$

where $\mathbf{v}_{max}$ and $\mathbf{u}_{max}$ are the unit-norm transmit beamforming and receive combining vectors, respectively, and $\mathbf{z}_{i+1}$ is a 2×1 AWGN vector with $\mathbb{E}\{\mathbf{z}_{i+1}\mathbf{z}_{i+1}^H\} = \sigma^2 \boldsymbol{I}_2$. The maximum output SNR at the receiving node can be given as follows [34]

$$\gamma_{S_{i+1}}^{\text{MIMO}} = \frac{\frac{P_t}{d_{i+1,i}^{\alpha}}}{\sigma^2} \Lambda_{max}, \tag{13}$$

where Λ_{max} is the maximum eigenvalue of the cross-correlation channel matrix $\mathbf{H}_{i+1,i}\mathbf{H}_{i+1,i}^H$, and it is equal to the square of the maximum singular value of $\mathbf{H}_{i+1,i}$, i.e. $\Lambda_{max} = \lambda_1^2$.

At the eavesdropper, the received signal can be given as follows

$$y_{e,i}^{\text{MIMO}} = \varpi \frac{\sqrt{P_{j_2}} h_{e,i-1}}{d_{e,i-1}^{\alpha/2}} x_{j_2} + \frac{\sqrt{P_t} \mathbf{h}_{e,i}^T \mathbf{v}_{max}}{d_{e,i}^{\alpha/2}} x_i + z_e, \tag{14}$$

and the correspondent maximum SINR can be expressed as

$$\gamma_{e,i}^{\text{MIMO}} = \max_{e \in \Phi_E} \left(\frac{\frac{P_t |\mathbf{h}_{e,i}^T \mathbf{v}_{max}|^2}{d_{e,i}^{\alpha}}}{\varpi \frac{P_{j_2} |h_{e,i-1}|^2}{d_{e,i-1}^{\alpha}} + \sigma^2} \right). \tag{15}$$

III. Secrecy Outage Probability Analysis

In this section, we investigate the secrecy performance between nodes S_i and S_{i+1} ($i \in \{0,1,...,N-1\}$), for the three different cases introduced in Section II in terms of the secrecy outage probability, which can be defined as follows

$$P_{so_{(n)}}^{\varepsilon} = \mathbb{P}(R_n^{\varepsilon} < R_s), \tag{16}$$

[3]Note that for higher data rates, a different transmission protocol can be adopted where S_{i-1} operates in FD mode to receive the subsequent information symbol from S_{i-2}, $\forall i \in \{2,...,N-1\}$. However, here we focus on the e2e secrecy outage probability of a single information symbol which is irrelevant to the two different transmission protocols.

where $\varepsilon \in \{\text{SISO}, \text{MISO}, \text{MIMO}\}$, R_s is a pre-defined target secrecy rate, and R_n is the secrecy rate of the nth hop, and can be expressed as

$$R_n^{\varepsilon} = \left[\log_2(1+\gamma_{S_{i+1}}^{\varepsilon}) - \log_2(1+\gamma_{e,i}^{\varepsilon})\right]^+. \tag{17}$$

where $[x]^+ = \max(0, x)$. To simplify the analysis, and over a high SNR regime, the secrecy outage probability for the nth hop can be approximated to

$$P_{so_{(n)}}^{\varepsilon} \approxeq \mathbb{P}\Big(\frac{\gamma_{S_{i+1}}^{\varepsilon}}{\gamma_{e,i}^{\varepsilon}} < \beta\Big), \tag{18}$$

where $\beta = 2^{R_s}$. Moreover, for a system with N hops, the e2e secrecy outage probability can be defined as follows

$$P_{so_{(e2e)}}^{\varepsilon} = 1 - P_{sc_{(e2e)}}^{\varepsilon} = 1 - \prod_{n=1}^{N}\Big(1 - P_{so_{(n)}}^{\varepsilon}\Big), \tag{19}$$

where $P_{sc_{(e2e)}}^{\varepsilon}$ is the e2e secrecy connectivity probability. In the following subsections, and for each of the three different cases, we derive closed-form expressions for the PDF of the legitimate link $f_X^{\varepsilon}(x)$, as well as the CDF of the eavesdropper's link $F_W^{\varepsilon}(w)$. Accordingly, the secrecy outage probability in (18) can be expressed as follows

$$P_{so_{(n)}}^{\varepsilon} = 1 - \int_0^{\infty} f_X^{\varepsilon}(x) F_W^{\varepsilon}(\frac{x}{\beta})\mathrm{d}x, \tag{20}$$

where the integral in (20) can be solved numerically using software programs such as MATLAB.

A. Performance analysis of the SISO case

1) The legitimate link: Let G be the numerator of $\gamma_{S_{i+1}}^{\text{SISO}}$ in (2), i.e. $G = \frac{P_t|h_{i+1,i}|^2}{d_{i+1,i}^{\alpha}}$, and since the channel gain follows an exponential distribution, its PDF can be given as $f_G(g) = \frac{d_{i+1,i}^{\alpha}}{P_t} e^{\frac{-d_{i+1,i}^{\alpha} g}{P_t}}$. Similarly, and by letting $V = P_{j_1}|h_{i+1,i+1}|^2$, the PDF of the SI channel is $f_V(v) = \frac{1}{\gamma_{SI}} e^{\frac{-v}{\gamma_{SI}}}$. Therefore, and by letting $X = G/V$, the CDF of the SIR for the SISO case can be given as

$$F_X^{\text{SISO}}(x) = \int_0^{\infty}\int_0^{xv} f_G(g) f_V(v)\ \mathrm{d}g\mathrm{d}v = \frac{d_{i+1,i}^{\alpha}\gamma_{SI} x}{d_{i+1,i}^{\alpha}\gamma_{SI} x + P_t}. \tag{21}$$

Next, the PDF can be found by taking the derivative with respect to x as follows

$$f_X^{\text{SISO}}(x) = \frac{\mathrm{d}}{\mathrm{d}x} F_X^{\text{SISO}}(x) = \frac{\gamma_{SI} d_{i+1,i}^{\alpha} P_t}{\left(d_{i+1,i}^{\alpha}\gamma_{SI} x + P_t\right)^2}. \tag{22}$$

2) The eavesdropper link: The CDF of the eavesdropper link $\gamma_{e,i}^{SISO}$ is given in (23) at the top of the next page, where $\mathrm{arcsinh}(.)$ and $\mathrm{arctanh}(.)$ are the inverse hyperbolic sine and inverse hyperbolic tangent functions, respectively.

Proof: see Appendix A.

B. Performance analysis of the MISO case

1) The legitimate link: The channel gain for the legitimate link $|\mathbf{h}_{i+1,i}^T \mathbf{w}_0|^2$ follows a Gamma distribution with a shape parameter of 2 (since we have 2 transmit antennas), and a scale parameter of $\frac{P_t}{d_{i+1,i}^{\alpha}}$ [35]. Therefore, the PDF of the numerator of $\gamma_{S_{i+1}}^{\text{MISO}}$ can be given as

$$f_S(s) = \left(\frac{P_t}{d_{i+1,i}^{\alpha}}\right)^{-2} s\ e^{\frac{-d_{i+1,i}^{\alpha} s}{P_t}}. \tag{24}$$

In addition, given that the self-interference channel has a PDF of $f_V(v) = \frac{1}{\gamma_{SI}} e^{\frac{-v}{\gamma_{SI}}}$, the CDF of $\gamma_{S_{i+1}}^{\text{MISO}}$ can be expressed as

$$\begin{aligned} F_X^{\text{MISO}}(x) &= \int_0^{\infty}\int_0^{xv} f_S(s) f_V(v)\ \mathrm{d}s\mathrm{d}v \\ &= \frac{\gamma_{SI}^2 d_{i+1,i}^{2\alpha} x^2}{\gamma_{SI}^2 d_{i+1,i}^{2\alpha} x^2 + 2\gamma_{SI} d_{i+1,i}^{\alpha} P_t x + P_t^2}, \end{aligned} \tag{25}$$

and the correspondant PDF can be found by taking the derivative with respect to x as follows

$$f_X^{\text{MISO}}(x) = \frac{\mathrm{d}}{\mathrm{d}x} F_X^{\text{MISO}}(x) = \frac{2 d_{i+1,i}^{2\alpha}\gamma_{SI}^2 P_t\ x}{(d_{i+1,i}^{\alpha}\gamma_{SI} x + P_t)^3}. \tag{26}$$

2) The eavesdropper link: The channel gain between S_i and the eavesdropper for the MISO case $|\mathbf{h}_{e,i}^T \mathbf{w}_0|^2$ follows an exponential distribution with a scale parameter of $\frac{P_t}{d_{i+1,i}^{\alpha}}$ [35]. Therefore, the CDF of the eavesdropper's link for the MISO case is exactly the same as that for the SISO case given in (23), i.e. $F_W^{\text{MISO}}(w) = F_W^{\text{SISO}}(w)$.

C. Performance analysis of the MIMO case

1) The legitimate link: : The PDF of the maximum eigenvalue Λ_{max} for a 2×2 system can be expressed as [36]

$$f_{\Lambda_{max}}(m) = e^{-m}\Big(m^2\Gamma(1,m) - 2m\Gamma(2,m) + \Gamma(3,m)\Big), \tag{27}$$

where $\Gamma(k,m)$ is the incomplete gamma function defined as

$$\Gamma(k,m) = \int_0^m y^{k-1}\exp(-y)\ \mathrm{d}y, \tag{28}$$

accordingly, the PDF of the maximum output instantaneous SNR at S_{i+1} can be given as

$$f_X^{\text{MIMO}}(x) = \frac{1}{\gamma_b} f_{\Lambda_{max}}\Big(\frac{x}{\gamma_b}\Big), \tag{29}$$

where γ_b is the received SNR per branch at node S_{i+1} and is equal to $\frac{P_t/d_{i+1,i}^{\alpha}}{\sigma^2}$.

2) CDF of the eavesdropper link: The CDF for the eavesdropper's link for the first hop and subsequent hops is derived in this section. However, it should be noted that the channel gain between S_i and the eavesdropper $|\mathbf{h}_{e,i}^T \mathbf{v}_{max}|^2$ follows an exponential distribution, as the channel distribution is invariant under independent unitary transformation [37].

a) The first hop ($\varpi = 0$): In this case, there is no interference at the eavesdropper's end, and the correspondent CDF of $\gamma_{e,i}^{\text{MIMO}}$ can be derived as (30) at the top of next page, where the equality in (a) holds by applying the probability generating functional (PGFL) for an homogeneous PPP distribution of eavesdroppers [38], and (b) holds for $\alpha = 2$.

$$F_W^{\text{SISO}}(w|\Phi_E) =$$

$$\begin{cases} \exp\Bigg[\frac{-\lambda_E\pi}{(P_{j_1}w+P_t)^3}\Bigg(d_{i+1,i}^2P_tP_{j_1}w(P_{j_1}w-P_t)\ \text{arcsinh}\Big(\frac{(P_{j_1}w+P_t)^2R^2+d_{i+1,i}^2P_t(P_{j_1}w-P_t)}{2P_t^{3/2}\sqrt{P_{j_1}}\sqrt{w}d_{i+1,i}^2}\Big) - (P_{j_1}^2w^2+P_{j_1}P_tw) \\ \times\sqrt{\Big((R+d_{i+1,i})^2P_t+R^2wP_{j_1}\Big)\Big((R-d_{i+1,i})^2P_t+R^2wP_{j_1}\Big)} - d_{i+1,i}^2P_tP_{j_1}w(P_{j_1}w-P_t)\text{arcsinh}\Big(\frac{P_{j_1}w-P_t}{2\sqrt{P_{j_1}\sqrt{P_t}\sqrt{w}}}\Big) \\ +\Big(P_{j_1}^2R^2w^2+2P_{j_1}w\Big[R^2+\frac{d_{i+1,i}^2}{2}\Big]P_t+P_t^2R^2\Big)\Big(P_{j_1}w+P_t\Big)\Bigg)\Bigg], & \varpi=0 \\ \exp\Bigg[\frac{-\lambda_E\pi}{\sqrt{P_t}(P_Jw+P_t)^4}\Bigg(\frac{P_J^2P_td_{i+1,i}^2w^2(P_Jw+P_t)^{\frac{3}{2}}}{2}\text{arctanh}\Bigg(\frac{\Big((P_Jw+P_t)R^2-P_td_{i+1,i}^2\sqrt{P_t}\Big)}{\sqrt{\Big((R+d_{i+1,i})^2P_t+P_JR^2w\Big)\Big((R-d_{i+1,i})^2P_t+P_JR^2w\Big)}\sqrt{P_Jw+P_t}}\Bigg) \\ -2\ \text{arcsinh}\Bigg(\frac{(P_Jw+P_t)^2R^2+d_{i+1,i}^2P_t(P_Jw-Pt)}{2P_t^{\frac{3}{2}}\sqrt{P_J}\sqrt{w}d_{i+1,i}^2}\Bigg)P_t^{\frac{7}{2}}P_Jd_{i+1,i}^2w - wP_J\Big(\sqrt{P_t}w^2P_J^2+3wP_JP_t^{\frac{3}{2}} \\ +2P_t^{\frac{5}{2}}\Big)\sqrt{\Big((R+d)^2P_t+P_JR^2w\Big)\Big((R-d)^2P_t+P_JR^2w\Big)} + 2P_t^{\frac{7}{2}}d_{i+1,i}^2P_Jw\ \text{arcsinh}\Big(\frac{P_Jw-P_t}{2\sqrt{P_J}\sqrt{P_t}\sqrt{w}}\Big) \\ +\frac{P_J^2P_td_{i+1,i}^2w^2(P_Jw+P_t)^{\frac{3}{2}}}{2}\text{arctanh}\Big(\frac{\sqrt{P_t}}{\sqrt{P_Jw+P_t}}\Big) + 4P_Jw\Big(R^2+\frac{d_{i+1,i}^2}{2}\Big)P_t^{\frac{7}{2}} + 4\Big(R^2+\frac{d_{i+1,i}^2}{2}\Big)P_J^3w^3P_t^{\frac{3}{2}} \\ +6P_J^2w^2\Big(R^2+\frac{d_{i+1,i}^2}{2}\Big)P_t^{\frac{5}{2}} + R^2(\sqrt{P_t}P_J^4w^4+P_t^{\frac{9}{2}})\Bigg)\Bigg] & \varpi=1 \end{cases} \tag{23}$$

$$\begin{aligned} F_W^{\text{MIMO}}(w|\Phi_E)_{|\varpi=0} &= \mathbb{P}\left(\max_{e\in\Phi_E}\left(\frac{P_t|\mathbf{h}_{e,i}^T\mathbf{v}_{max}|^2/d_{e,i}^{\alpha}}{\sigma^2}<w\right)\right) = \mathbb{E}_{\Phi_E}\left[\mathbb{P}\left(\max_{e\in\Phi_E}\left(\frac{P_t|\mathbf{h}_{e,i}^T\mathbf{v}_{max}|^2}{d_{e,i}^{\alpha}\sigma^2}<w|\Phi_E\right)\right)\right] \\ &= \mathbb{E}_{\Phi_E}\left[\prod_{e\in\Phi_E}\left(1-e^{-\frac{d_{e,i}^{\alpha}\sigma^2w}{P_t}}\right)\right] \overset{a}{=} \exp\left(-\lambda_E\int_0^R\int_0^{2\pi}r.e^{-\frac{r^{\alpha}\sigma^2w}{P_t}}\text{d}\theta\text{d}r\right) \overset{b}{=} \exp\left(\frac{\pi\lambda_EP_t\Big(e^{-\frac{R^2\sigma^2w}{P_t}}-1\Big)}{\sigma^2w}\right), \end{aligned} \tag{30}$$

$$\begin{aligned} F_W^{\text{MIMO}}(w|\Phi_E)|_{\varpi=1} =& \exp\Bigg[\frac{-\lambda_E\pi}{(P_{j_2}w+P_t)^3}\Bigg(d_{i-1,i}^2P_tP_{j_2}w(P_{j_2}w-P_t)\ \text{arcsinh}\Big(\frac{(P_{j_2}w+P_t)^2R^2+d_{i-1,i}^2P_t(P_{j_2}w-P_t)}{2P_t^{3/2}\sqrt{P_{j_2}}\sqrt{w}d_{i-1,i}^2}\Big) \\ &- (P_{j_2}^2w^2+P_{j_2}P_tw)\sqrt{\Big((R+d_{i-1,i})^2P_t+R^2wP_{j_2}\Big)\Big((R-d_{i-1,i})^2P_t+R^2wP_{j_2}\Big)} - d_{i-1,i}^2P_tP_{j_2}w(P_{j_2}w-P_t) \\ &\times\text{arcsinh}\Big(\frac{P_{j_2}w-P_t}{2\sqrt{P_{j_2}\sqrt{P_t}\sqrt{w}}}\Big)+\Big(P_{j_2}^2R^2w^2+2P_{j_2}w\Big[R^2+\frac{d_{i-1,i}^2}{2}\Big]P_t+P_t^2R^2\Big)\Big(P_{j_2}w+P_t\Big)\Bigg)\Bigg]. \end{aligned} \tag{31}$$

b) Subsequent hops ($\varpi = 1$): Following the same approach as that shown in (32) in Appendix A, the CDF of $\gamma_{e,i}^{\text{MIMO}}$ when $\alpha = 2$, is shown in (31) at the top of this page.

IV. Results and Discussions

In this section, both analytical and Monte Carlo simulations are presented to evaluate the secrecy performance of our proposed CJ scheme. Before we discuss our results, we introduce the different parameters used in this work. Unless stated otherwise, all nodes were located in a 2D plane at locations $(x_0, 0), ..., (x_N, 0)$, with $x_0 = 0$, and the distances between any two neighbouring nodes S_i and S_{i+1} is 2 m (i.e. $x_{i+1} - x_i = d_{i+1,i} = 2,\ \forall i \in \{0, 1, ..., N-1\}$). In addition, the target secrecy rate R_s was set to 0.1 bps/Hz, the residual SI γ_{SI} was set to 10 dB, the path-loss exponent $\alpha = 2$, and the noise variance $\sigma^2 = 1$.

Fig. 2 demonstrates the secrecy performance when the CSI is not available at the transmitter, and only a single antenna is utilized for data transmission with a fixed transmit power gain of 45 dB (i.e. $P_t/\sigma^2 = 45$ dB). The proposed scheme with FD-CJ significantly outperforms the conventional FD-SJ approach where only the receiving node broadcasts a jamming signal. For example, to achieve a secrecy outage of 10^{-1}, the proposed method has a 3.4 dB gain compared to the SJ scheme when $N = 2$, while a 6 dB gain is obtained to achieve the same secrecy outage when the number of hops is 4. Moreover, at high jamming power gain, i.e. in the interference-limited regime, the analytical results closely match the Monte Carlo simulations which validates our analysis in Section III.

In addition, Fig. 3 demonstrates the performance of the same system under different densities of eavesdroppers. It is clear from both Figs. 2 and 3, that the proposed FD-CJ scheme has

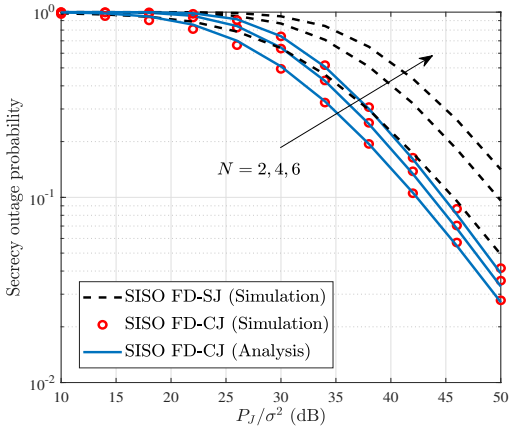

Fig. 2. Secrecy outage probability vs per-node jamming SNR (P_J/σ^2) for SISO case when $R = 7$ m, $\lambda_E = 5 \times 10^{-2}$ m^{-2}, $P_{j_1} = P_{j_2} = P_J$, and $P_t/\sigma^2 = 45$ dB.

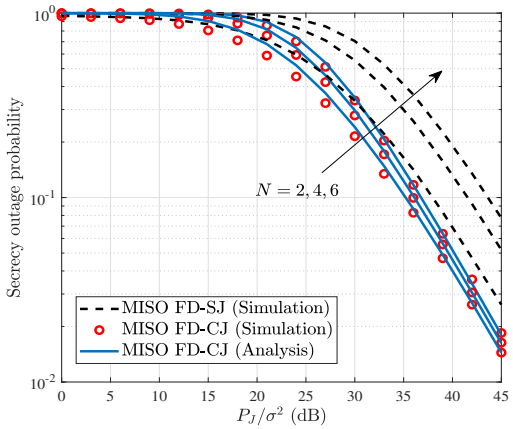

Fig. 4. Secrecy outage probability vs per-node jamming SNR (P_J/σ^2) for MISO case when $R = 6$ m, $\lambda_E = 5 \times 10^{-2}$ m^{-2}, $P_{j_1} = P_{j_2} = P_J$, and $P_t/\sigma^2 = 25$ dB.

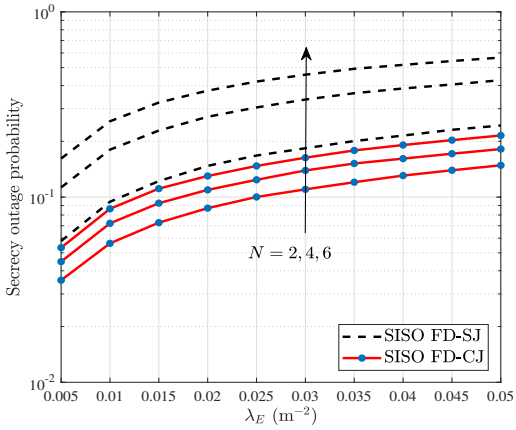

Fig. 3. Secrecy outage probability vs density of eavesdroppers for SISO case when $R = 20$ m, and $P_t/\sigma^2 = P_{j_1}/\sigma^2 = P_{j_2}/\sigma^2 = 45$ dB.

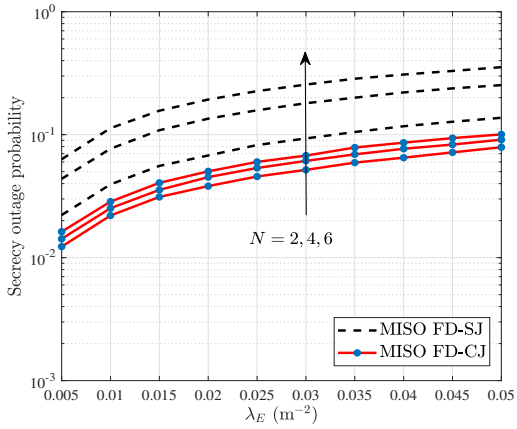

Fig. 5. Secrecy outage probability vs density of eavesdroppers for MISO case when $R = 20$ m, $P_{j_1}/\sigma^2 = P_{j_2}/\sigma^2 = 40$ dB, and $P_t/\sigma^2 = 25$ dB.

a great advantage over the conventional FD-SJ as the number of hops increases, as only a marginal performance degradation is experienced for the proposed CJ approach.

When the CSI is available at the transmitter side, both antennas can be utilized for data transmission by applying MRT precoding. Similar to the SISO case, the proposed scheme significantly outperforms the SJ approach, especially when the number of hops is greater than two. In particular, and from a total jamming power point of view, the proposed CJ scheme employs one extra jamming node compared to the SJ approach. Given the general case where both jamming nodes, S_{i+1} and S_{i-1}, transmit with the same amount of power (i.e. $P_{j_1} = P_{j_2}$), the CJ scheme would consume an extra 3 dB of jamming power. However, from Fig. 4, when $N = 4$ and the transmit power gain $P_t/\sigma^2 = 25$ dB, the proposed CJ requires 36 dB of per-node jamming power (P_J/σ^2) to achieve a secrecy outage of 10^{-1}, compared to 41.5 dB for the SJ scheme, which results in 2.5 dB of overall jamming power saving for the proposed scheme. Similarly, for $N = 6$, the CJ method outperforms the SJ by 6.8 dB, which results in a significant 3.8 dB of jamming power saving for the CJ scheme.

Moreover, Fig. 5 shows the performance of the MISO case for a wide range of λ_E. Again, the proposed CJ scheme shows a great advantage over the conventional SJ scheme, as unlike the latter, the CJ approach experiences only a negligible performance degradation as the number of hops increases.

MIMO diversity can further enhance the secrecy performance only at low jamming power gain as demonstrated in Fig. 6. However, at high jamming power gain, the secrecy outage experiences a noise floor and cannot be further enhanced. This is due to the fact that during the first hop, there is no jamming signal as both transmit and receiving nodes employ their two antennas for data transmission/reception, unlike the SISO and MISO schemes with FD receivers, where in the first hop, the receiving node will be broadcasting a jamming signal. Furthermore, since the analyses were carried out in the interference-limited scenario, and given the fact that there is only a single jammer in this case, the analytical results match the simulations at high jamming power gain where the

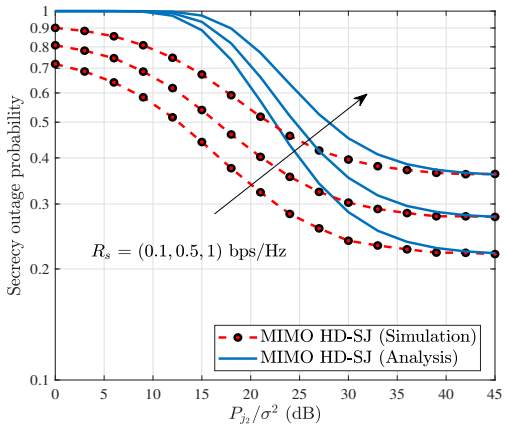

Fig. 6. Secrecy outage probability vs jamming SNR (P_{j2}/σ^2) for MIMO case when $R = 6$ m, $\lambda_E = 5 \times 10^{-2}$ m^{-2}, $N = 6$, and $P_t/\sigma^2 = 25$ dB.

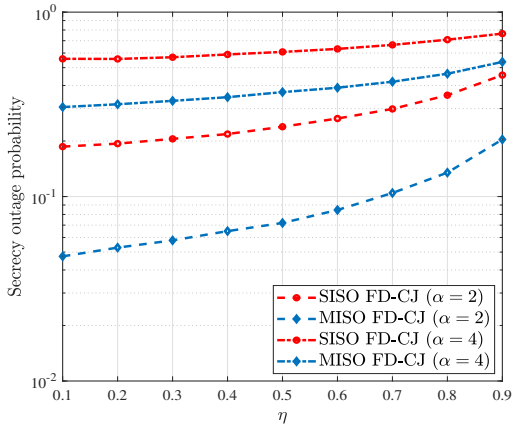

Fig. 8. Secrecy outage vs $\eta = \frac{P_t}{P_t + P_{j_1}}$ when $N = 4$, $R = 6$ m, $\lambda_E = 5 \times 10^{-2}$ m^{-2}, $P_{j_2}/\sigma^2 = 40$ dB, and $P_{j_1} + P_t = P_{j_2}$.

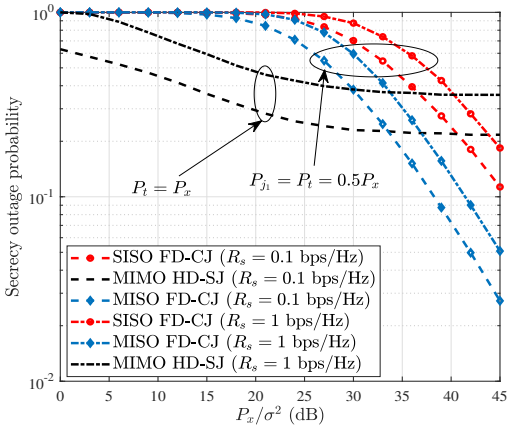

Fig. 7. Secrecy outage probability vs total SNR for different schemes when $N = 4$, $R = 6$ m, $\lambda_E = 5 \times 10^{-2}$ m^{-2}, and $P_{j_2} = P_x$.

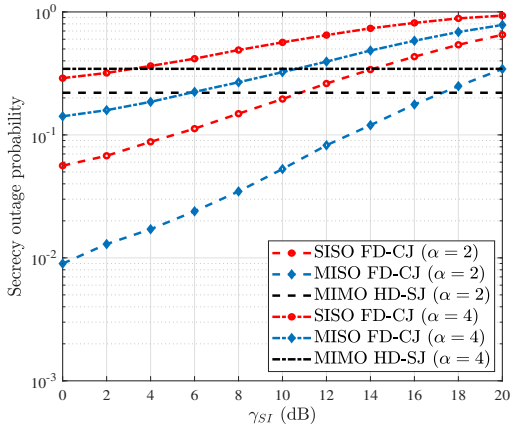

Fig. 9. Secrecy outage probability vs γ_{SI} when $N = 4$, $R = 6$ m, $\lambda_E = 5 \times 10^{-2}$ m^{-2}, $P_{j_2}/\sigma^2 = 40$ dB, $P_t + P_{j_1} = P_{j_2}$, and $\eta = 25\%$.

jamming signal becomes a dominant factor.

It should be noted that for the MIMO case, the total radiated power is $P_t + P_{j_2}$, while for both SISO and MISO, the receiving node broadcasts a jamming signal with a jamming power of P_{j_1}. Therefore, to have a fair comparison between the three different cases (SISO, MISO, and MIMO), Fig. 7 shows the performance of the different schemes under a total power constraint. More specifically, we assume that for the SISO and MISO cases $P_t + P_{j_1}$ is equal to P_x, which in return is equal to the transmit power of the MIMO case, while P_{j_2} is the same for all three cases. The results show that utilizing the MIMO diversity is better when the CSI is available at both ends only at low to medium SNRs, while at high SNRs, utilizing the FD with CJ can significantly improve the performance. Moreover, for the MIMO case, the noise floor becomes worse when increasing the target secrecy rate, while no such problem occurs when FD jamming is utilized.

Furthermore, Fig. 8 shows that for both SISO and MISO cases, when operating under a total power constraint, allocating less power for the transmitting node and more power for the FD jamming node can lead to improved secrecy performance, regardless of the value of α.

Meanwhile, Fig. 9 demonstrates the performance of the proposed FD jamming schemes under different levels of residual SI. It is clear that the quality of SI cancellation has a marked effect on the secrecy performance, as high residual SI can lead to a large performance degradation. Moreover, and compared to the HD MIMO case, even when the CSI is available at both ends, it is better to utilize the FD with MISO scheme as long as the residual SI is sufficiently suppressed, in this case if γ_{SI} is less than 17 dB when $\alpha = 2$, or less than 10.7 dB when $\alpha = 4$; while the MIMO with HD-SJ scheme is preferable for higher thresholds of γ_{SI}.

Fig. 10 demonstrates that for fixed locations of S_0 and S_N, increasing the number of hops leads to a significant enhancement in the secrecy performance under fixed power constraints. In particular, we restrict the total transmit SNR of information to 50 dB (i.e. $NP_t/\sigma^2 = 50$ dB), and similarly the total available SNR for jamming is fixed to the same value such that $P_{j1} = P_{j2} = P_J$, and $(2N - 1)P_J/\sigma^2 = 50$ dB,

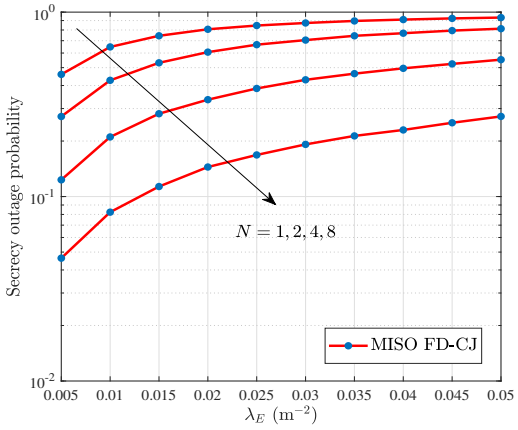

Fig. 10. Secrecy outage probability vs λ_E for different number of hops when $R = 20$ m, $d_{N,0} = 20$ m, $(x_0, y_0) = (0, 0)$, $(x_i, y_i) = (x_{i-1} + (d_{N,0}/N), 0), \forall i \in \{1, ..., N\}$.

since the proposed CJ approach requires $2N - 1$ jamming signal transmissions to protect the data.

Finally, it is worth highlighting that for practical implementations, the jamming power of S_{i-1} should be carefully chosen based on the distance between nodes S_{i-1} and S_{i+1}, such that the received signal at the latter should not be hindered by the jamming from the former. In fact, the performance of such CJ scheme can be highly improved with optimal power allocation, relay placement, route optimization, and so forth, which we leave to investigate in future work. Moreover, employing multiple (more than two) nodes to broadcast jamming signals can lead to further enhancement in the secrecy performance. However, this will make obtaining analytical closed-form expressions at the eavesdroppers highly complicated, and the focus should rather be on optimizing the resource allocation which is out of the scope of this work.

V. Conclusions

In this paper, an FD-CJ scheme was proposed for enhancing PLS in multihop IoT networks in the presence of randomly located eavesdroppers, and subject to different availability conditions of CSI. In particular, under limited feedback, the proposed SISO FD-CJ scheme showed an impressive performance gain compared to the conventional SISO FD-SJ scheme, especially when the number of hops is larger than two. On the other hand, when the CSI is available at both ends, our results demonstrated that at low SNRs, better secrecy performance can be obtained by utilizing the MIMO diversity with an HD receiver. In contrast, at high SNR, the MISO FD-CJ with MRT beamforming leads to a significant performance gain. Moreover, the proposed scheme showed a great resilience against multihop transmission, as only a marginal performance loss was experienced as the number of hops increased. Integral closed-form expressions were derived in the interference limited scenario for the secrecy outage probability for each case, and closely matched the Monte Carlo simulations.

Appendix A

Here we derive the CDF expression of $\gamma_{e,i}^{\text{SISO}}$ in the interference-limited scenario for two different cases as follows

a) First hop ($\varpi = 0$): let $X_1 = \frac{P_t|h_{e,i}|^2}{d_{e,i}^{\alpha}}$ and $Y_1 = \frac{P_{j_1}|h_{e,i+1}|^2}{d_{e,i+1}^{\alpha}}$, then the PDFs of $X1$ and $Y1$ can be given as $f_{X_1}(x_1|d_{e,i}) = \frac{d_{e,i}^{\alpha}}{P_t} e^{-\frac{d_{e,i}^{\alpha} x_1}{P_t}}$ and $f_{Y_1}(y_1|d_{e,i+1}) = \frac{d_{e,i+1}^{\alpha}}{P_{j_1}} e^{-\frac{d_{e,i+1}^{\alpha} y_1}{P_{j_1}}}$, respectively. By letting $W = X_1/Y_1$, the CDF of $\gamma_{e,i}^{\text{SISO}}$ can be derived as shown in (32), where $\psi_+ = \sqrt{r^2 + d_{i+1,i}^2 - 2rd_{i+1,i}\cos(\theta)}$, and equality (a) holds by applying the probability generating functional (PGFL) [38]. For the case where $\alpha = 2$, a closed-form result for the double integral in (32) is shown as the first part of (23).

b) Subsequent hops ($\varpi = 1$): In this case, there are two interference terms in the denominator of $\gamma_{e,i}^{\text{SISO}}$. Let $U_1 = \frac{P_{j_2}|h_{e,i-1}|^2}{d_{e,i-1}^{\alpha}}$, and its PDF can be expressed as $f_{U_1}(u_1|d_{e,i-1}) = \frac{d_{e,i-1}^{\alpha}}{P_{j_2}} e^{-\frac{d_{e,i-1}^{\alpha} u_1}{P_{j_2}}}$. The CDF and PDF of $Z = Y_1 + U_1$ can then be given as expressed in (33) and (34), respectively, at the top of the next page. Next, and by letting $W = X_1/Z$, the CDF of $\gamma_{e,i}^{\text{SISO}}$ can be derived as shown in (35) in the next page, where we have $\psi_- = \sqrt{r^2 + d_{i-1,i}^2 - 2rd_{i-1,i}\cos(\pi - \theta)}$, and (a) holds by applying the PGFL function [38]. For the case where $\alpha = 2$, and assuming $P_{j_1} = P_{j_2} = P_J$, the result of the double integral in (35) is shown as the second part of (23).

References

[1] Y. Mehmood, N. Haider, M. Imran, A. Timm-Giel, and M. Guizani, "M2M communications in 5G: state-of-the-art architecture, recent advances, and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 194–201, Sep. 2017.

[2] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband Internet of Things: Implementations and applications," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2309–2314, Dec. 2017.

[3] M. Elsaadany, A. Ali, and W. Hamouda, "Cellular LTE-A technologies for the future Internet-of-Things: Physical layer features and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2544–2572, 4th Quarter, 2017.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[5] J. Hu, N. Yang, and Y. Cai, "Secure downlink transmission in the Internet of Things: How many antennas are needed?" *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1622–1634, Jul. 2018.

[6] 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.

[7] Y. Z. Yueping Wang, Xuan Zhang, "Joint spectrum partition and performance analysis of full-duplex D2D communications in multi-tier wireless networks," *Computers, Materials & Continua*, vol. 61, no. 1, pp. 171–184, 2019.

[8] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE commun. lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[9] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC) Workshops*, Kyoto, Japan, Jun., 2011, pp. 1–5.

[10] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

$$
\begin{aligned}
F_W^{\text{SISO}}(w|\Phi_E)_{|\varpi=0} &= \mathbb{P}\left(\max_{e\in\Phi_E}\left(\frac{X_1}{Y_1}<w\right)\right) = \mathbb{E}_{\Phi_E}\left[\mathbb{P}\left(\max_{e\in\Phi_E}\left(\frac{X_1}{Y_1}<w|\Phi_E\right)\right)\right] \\
&= \mathbb{E}_{\Phi_E}\left[\prod_{e\in\Phi_E}\int_0^{\infty}\int_0^{wy_1} f_{X_1}(x_1|\Phi_E)f_{Y_1}(y_1|\Phi_E)\mathrm{d}x_1\mathrm{d}y_1\right] = \mathbb{E}_{\Phi_E}\left[\prod_{e\in\Phi_E}\frac{d_{e,i}^{\alpha}P_{j_1}w}{d_{e,i}^{\alpha}P_{j_1}w+P_t d_{e,i+1}^{\alpha}}\right] \\
&\overset{a}{=} \exp\left(-\lambda_E\int_0^{R}\int_0^{2\pi} r\left[1-\frac{r^{\alpha}P_{j_1}w}{r^{\alpha}P_{j_1}w+P_t\psi_+^{\alpha}}\right]\mathrm{d}\theta\mathrm{d}r\right),
\end{aligned} \tag{32}
$$

$$
F_Z(z|d_{e,i-1},d_{e,i+1}) = \int_0^{z}\int_0^{z-u_1} f_{Y_1}(y_1|d_{e,i+1})f_{U_1}(u_1|d_{e,i-1})\mathrm{d}y_1\mathrm{d}u_1 = 1+\frac{d_{e,i+1}^{\alpha}e^{-\frac{d_{e,i-1}^{\alpha}z}{P_{j_2}}}P_{j_2}-d_{e,i-1}^{\alpha}e^{-\frac{d_{e,i+1}^{\alpha}z}{P_{j_1}}}P_{j_1}}{d_{e,i-1}^{\alpha}P_{j_1}-d_{e,i+1}^{\alpha}P_{j_2}}, \tag{33}
$$

$$
f_Z(z|d_{e,i-1},d_{e,i+1}) = \frac{\mathrm{d}}{\mathrm{d}z}F_Z(z) = -\frac{d_{e,i-1}^{\alpha}d_{e,i+1}^{\alpha}\left(e^{-\frac{d_{e,i-1}^{\alpha}z}{P_{j_2}}}-e^{\frac{d_{e,i+1}^{\alpha}z}{P_{j_1}}}\right)}{d_{e,i-1}^{\alpha}P_{j_1}-d_{e,i+1}^{\alpha}P_{j_2}}. \tag{34}
$$

$$
\begin{aligned}
F_W^{\text{SISO}}(w|\Phi_E)_{|\varpi=1} &= \mathbb{P}\left(\max_{e\in\Phi_E}\left(\frac{X_1}{Z}<w\right)\right) = \mathbb{E}_{\Phi_E}\left[\mathbb{P}\left(\max_{e\in\Phi_E}\left(\frac{X_1}{Z}<w|\Phi_E\right)\right)\right] = \mathbb{E}_{\Phi_E}\left[\prod_{e\in\Phi_E}\int_0^{\infty}\int_0^{wz} f_{X_1}(x_1|\Phi_E)f_Z(z|\Phi_E)\mathrm{d}x_1\mathrm{d}z\right] \\
&= \mathbb{E}_{\Phi_E}\left[\prod_{e\in\Phi_E}\frac{d_{e,i}^{2\alpha}P_{j_1}P_{j_2}w^2+P_t d_{e,i}^{\alpha}(d_{e,i+1}^{\alpha}P_{j_2}+d_{e,i-1}^{\alpha}P_{j_1})w}{d_{e,i}^{2\alpha}P_{j_2}P_{j_1}w^2+P_t d_{e,i}^{\alpha}(d_{e,i+1}^{\alpha}P_{j_2}+d_{e,i-1}^{\alpha}P_{j_1})w+d_{e,i-1}^{\alpha}d_{e,i+1}^{\alpha}P_t^2}\right] \\
&\overset{a}{=} \exp\left(-\lambda_E\int_0^{R}\int_0^{2\pi} r\left[1-\frac{r^{2\alpha}P_{j_1}P_{j_2}w^2+P_t r^{\alpha}(\psi_+^{\alpha}P_{j_2}+\psi_-^{\alpha}P_{j_1})w}{r^{2\alpha}P_{j_2}P_{j_1}w^2+P_t r^{\alpha}(\psi_+^{\alpha}P_{j_2}+\psi_-^{\alpha}P_{j_1})w+\psi_-^{\alpha}\psi_+^{\alpha}P_t^2}\right]\mathrm{d}\theta\mathrm{d}r\right).
\end{aligned} \tag{35}
$$

[11] D. Jung and J. H. Lee, "Secrecy performance of full-duplex relay system with randomly located eavesdroppers," in *86th IEEE Veh. Tech. Conf. (VTC-Fall)*, Toronto, Canada, Sep., 2017, pp. 1–5.

[12] Y. Feng, Z. Yang, S. Yan, N. Yang, and B. Lv, "Physical layer security enhancement in multi-user multi-full-duplex-relay networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May, 2017, pp. 1–7.

[13] Y. Li, R. Zhao, X. Tan, and Z. Nie, "Secrecy performance analysis of artificial noise aided precoding in full-duplex relay systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, Dec., 2017, pp. 1–6.

[14] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[15] G. Chen, J. P. Coon, and S. E. Tajbakhsh, "Secure routing for multihop ad hoc networks with inhomogeneous eavesdropper clusters," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10 660–10 670, Nov. 2018.

[16] F. Tian, X. Chen, S. Liu, X. Yuan, D. Li, X. Zhang, and Z. Yang, "Secrecy rate optimization in wireless multi-hop full duplex networks," *IEEE Access*, vol. 6, pp. 5695–5704, Mar. 2018.

[17] S.-I. Chu, "Secrecy analysis of modify-and-forward relaying with relay selection," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1796–1809, Feb. 2018.

[18] S. Atapattu, N. Ross, Y. Jing, Y. He, and J. S. Evans, "Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1216–1232, Feb. 2019.

[19] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[20] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.

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

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

[23] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2009.

[24] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2011.

[25] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[26] A. Kuhestani, M. T. Mamaghani, and H. Behroozi, "A new secure multi-hop untrusted relaying scheme," *[Online]. Available: http://arxiv.org/abs/1905.09384*, 2019.

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

[28] J. Moon, H. Lee, C. Song, S. Kang, and I. Lee, "Relay-assisted proactive eavesdropping with cooperative jamming and spoofing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6958–6971, Oct. 2018.

[29] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular IoT: Potentials and limitations," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 55–61, Sep. 2017.

[30] 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.

[31] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[32] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-noise-aided secure transmission scheme with limited training and feedback

overhead," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 193–205, Jan. 2016.
[33] G. Chen, J. P. Coon, A. Mondal, B. Allen, and J. A. Chambers, "Performance analysis for multihop full-duplex IoT networks subject to poisson distributed interferers," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3467–3479, Apr. 2019.
[34] P. A. Dighe, R. K. Mallik, and S. S. Jamuar, "Analysis of transmit-receive diversity in Rayleigh fading," *IEEE Trans. Commun.*, vol. 51, no. 4, pp. 694–703, Apr. 2003.
[35] X. Zhou, J. Guo, S. Durrani, and I. Krikidis, "Performance of maximum ratio transmission in ad hoc networks with SWIPT," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 529–532, Oct. 2015.
[36] J. Li, X.-D. Zhang, Q. Gao, Y. Luo, and D. Gu, "BEP analysis of MRT/MRC diversity in Rayleigh fading channels," in *Procc. IEEE Veh. Tech. Conf. (VTC-Spring)*, Singapore, May, 2008, pp. 385–389.
[37] S. Jin, X. Gao, and M. R. McKay, "Ordered eigenvalues of complex noncentral wishart matrices and performance analysis of SVD MIMO systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, USA, Jul., 2006, pp. 1564–1568.
[38] M. Haenggi, *Stochastic geometry for wireless networks*. Cambridge University Press, 2012.

Zaid Abdullah (M'18) was born in Mosul, Iraq, where he received the B.Sc. degree in electronics and communications engineering, in 2012. In 2014, he received the M.Sc. degree in communications and signal processing from Newcastle University, Newcastle upon Tyne, UK. He then received a funded scholarship from Newcastle University to pursue his Ph.D. in communications and signal processing, and was awarded the Ph.D. degree in 2019. He is currently a Postdoctoral Research Assistant with the Digital Communications and Intelligent Sensing Group, School of Engineering, University of Leicester, UK. His main research interests include Massive MIMO systems, M2M, IoT, physical layer security, intelligent reflecting surfaces, full-duplex, and low complexity algorithms design.

Gaojie Chen (S'09-M'12-SM'18) received the B.Eng. and B.Ec. degrees in electrical information engineering and international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, Loughborough, U.K., in 2008 and 2012, respectively. From 2008 to 2009, he was a Software Engineering with DTmobile, Beijing, China, and from 2012 to 2013, he was a Research Associate with the School of Electronic, Electrical and Systems Engineering, Loughborough University. He was a Research Fellow with 5GIC, Faculty of Engineering and Physical Sciences, University of Surrey, U.K., from 2014 to 2015. Then he was a Research Associate with the Department of Engineering Science, University of Oxford, U.K., from 2015 to 2018. He is currently a Lecturer with the School of Engineering, University of Leicester, U.K. He current research interests include information theory, wireless communications, cooperative communications, cognitive radio, Internet of Things, secrecy communication, and random geometric networks. He received the Exemplary Reviewer Certificates of the IEEE Wireless Communications Letters in 2018 and IEEE Transaction on Communications in 2019. He currently serves as an Associate Editor for IEEE Communications Letters and IET Electronics Letters.

Mohammed A. M. Abdullah (M'10) received the B.Sc. and M.Sc. degrees in computer engineering from the University of Mosul, Iraq, in 2008 and 2010, respectively, and the Ph.D. degree from the School of Electrical and Electronic Engineering, Newcastle University, U.K., in 2017. In 2018, he worked as a Post-Doctoral Researcher with the Department of Engineering, University of Leicester, U.K. He is currently a Lecturer with the Department of Computer Engineering, Ninevah University. His research interests are in the fields of biometrics, machine learning, signal processing, and wireless communication. He is a member of the International Biometric Society (IBS) and the British Machine Vision Association (BMVA). He is also an Associate Fellow of the U.K. Higher Education Academy (AFHEA).

Jonathon Chambers (S'83–M'90–SM'98–F'11) received the Ph.D. and D.Sc. degrees in signal processing from the Imperial College of Science, Technology and Medicine (Imperial College London), London, U.K., in 1990 and 2014, respectively. From 1991 to 1994, he was a Research Scientist with the Schlumberger Cambridge Research Center, Cambridge, U.K. In 1994, he returned to Imperial College London as a Lecturer in signal processing and was promoted to Reader (Associate Professor), in 1998. From 2001 to 2004, he was the Director of the Center for Digital Signal Processing and a Professor of signal processing with the Division of Engineering, King's College London. From 2004 to 2007, he was a Cardiff Professorial Research Fellow with the School of Engineering, Cardiff University, Cardiff, U.K. From 2007 to 2014, he led the Advanced Signal Processing Group, School of Electronic, Electrical and Systems Engineering, Loughborough University, where he is currently a Visiting Professor. In 2015, he joined the School of Electrical and Electronic Engineering, Newcastle University, where he was a Professor of signal and information processing and led the ComS2IP Group and is also a Visiting Professor. In 2017, he became the Head of the School of Engineering, University of Leicester. He is also an International Honorary Dean and a Guest Professor with Harbin Engineering University, China, with support from the 1000 Talents Scheme. He is a coauthor of the books: Recurrent Neural Networks for Prediction: Learning Algorithms, Architectures and Stability (New York, NY, USA: Wiley, 2001) and EEG Signal Processing (New York, NY, USA: Wiley, 2007). He has advised more than 90 researchers through to Ph.D. graduation and published more than 500 conference papers and journal articles, many of them are in the IEEE journals. His research interests include adaptive signal processing, and machine learning and their applications. He is also a Fellow of the Royal Academy of Engineering, U.K., and the Institution of Electrical Engineers. In 2007, he received the first QinetiQ Visiting Fellowship for his outstanding contributions to adaptive signal processing and his contributions to QinetiQ, as a result of his successful industrial collaboration with the international defense systems company QinetiQ. He was the Technical Program Chair of the 15th International Conference on Digital Signal Processing and the 2009 IEEE Workshop on Statistical Signal Processing, both held at Cardiff, U.K., and a Technical Program Co-Chair of the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing, Prague, Czech Republic. He has served on the IEEE Signal Processing Theory and Methods Technical Committee for six years and the IEEE Signal Processing Society Awards Board for three years, together with the Jack Kilby Award Committee. He has served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING for two terms over the periods 1997–1999 and 2004–2007 and as a Senior Area Editor, from 2011 to 2014.