A Lightweight Secure and Resilient Transmission Scheme for the Internet-of-Things in the Presence of a Hostile Jammer

Mehdi Letafati, *Student Member, IEEE*, Ali Kuhestani, *Member, IEEE*, Kai-Kit Wong, *Fellow, IEEE*, and Md. Jalil Piran, *Member, IEEE*

***Abstract*—In this paper, we propose a lightweight security scheme for ensuring both *information confidentiality and transmission resiliency* in the Internet-of-Things (IoT) communication. A single-antenna transmitter communicates with a half-duplex single-antenna receiver in the presence of a sophisticated multiple-antenna-aided *passive eavesdropper* and a multiple-antenna-assisted hostile jammer (HJ). A low-complexity artificial noise (AN) injection scheme is proposed for drowning out the eavesdropper. Furthermore, for enhancing the resilience against HJ attacks, the legitimate nodes exploit their own local observations of the wireless channel as the source of randomness to agree on shared secret keys. The secret key is utilized for the frequency hopping (FH) sequence of the proposed communication system. We then proceed to derive a new closed-form expression for the achievable secret key rate (SKR) and the ergodic secrecy rate (ESR) for characterizing the secrecy-benefits of our proposed scheme, in terms of both information secrecy and transmission resiliency. Moreover, the optimal power sharing between the AN and the message signal is investigated with the objective of enhancing the secrecy rate. Finally, through extensive simulations, we demonstrate that our proposed system model outperforms the state-of-the-art transmission schemes in terms of secrecy and resiliency. Several numerical examples and discussions are also provided to offer further engineering insights.**

***Index Terms*—Internet-of-Things, physical layer security, information security, transmission resiliency.**

I. Introduction

THE demand for high data rate and high reliability in wireless communications is relentlessly increasing as user density is predicted to increase exponentially due to the emergence of cyber-physical systems and the Internet-of-Things (IoT) [1]. The applications of IoT span a wide range including medical monitoring, device-to-device (D2D) communication in cellular network, industrial applications, air-to-ground transmission, and advanced communication networks. These worldwide networking services need a migration from traditional centralized networks to distributed ones with many peer-to-peer connected devices [2], [3]. In this case, however, if the confidential information is not strictly secured, the transmissions are vulnerable to security or safety risks including passive attacks like eavesdropping and traffic analysis, or active attacks such as hostile jamming, spoofing, untrustworthy data reporting [3], [4], and denial-of-service (DoS) attack [1], [5].

A. Motivation

In recent years, as a complementary approach to the common cryptography techniques, *physical layer security* (PLS) has been extensively adopted to protect wireless communications against security threats [5]–[8]. In contrast to the conventional security solutions, which rely on the cryptographic methods at higher layers of the network protocol stack, PLS exploits the intrinsic features of communication channel to realize a reliable and secure transmission. Therefore, the PLS, which imposes less overhead compared to the conventional methods [7], is excessively applicable for distributed communication networks such as wireless sensor networks (WSNs), massive IoT, industrial IoT, IoT healthcare, unmanned aerial vehicle (UAV) networks [9], and etc., where low-cost devices with low-power consumption are used. Additionally, by exploring the radio frequency fingerprint (RFF), PLS can offer efficient low-complexity techniques to facilitate the handshake procedure and reduce network latency for a number of wireless techniques, such as ZigBee, Bluetooth, and Long Range (LoRa) communications [10].

Generally, PLS solutions are categorized into two groups: key-less and key-based secrecy techniques, respectively [7]. The research of key-less PLS was first initiated by Wyner's pioneering work [11], where the secrecy capacity was formulated for degraded wiretap channel. According to the secrecy capacity, secure communication is achievable if and only if the legitimate receiver has better channel quality than the eavesdropper (Eve) does. So far, various key-less PLS techniques were proposed in the literature including the cooperative jamming, also named as artificial noise (AN) injection scheme [12], secure beamforming [13], [14], the relay-based techniques [15], power allocation schemes [16], etc.

To reinforce the systems' security, key-based PLS methods can also be utilized which provides an extra level of secrecy in IoT devices. For example, in Industry 4.0 and massive IoT applications, numerous number of IoT devices are connected

The work is supported in part by EPSRC under grant EP/M016005/1.

M. Letafati is with the Department of Electrical Engineering, Sharif University of Technology, Tehran 1365-11155, Iran (e-mail: mletafati@ee.sharif.edu).

A. Kuhestani is with the Communications and Electronics Department, Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom 3716146611, Iran (e-mail: kuhestani@sharif.edu).

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

Md. Jalil Piran is with the Department of Computer Science and Engineering, Sejong University, Seoul, 05006, South Korea (email: piran@sejong.ac.kr).

to each other [1], [5]. In such heterogeneous IoT networks, implementing effective key distribution and management is challenging. Toward this end, key generation at physical layer can mitigate this issue by utilizing the intrinsic randomness of wireless channels [10], [17]. The main idea of physical layer secret key generation (SKG) is that if the Eves are located far enough from the legitimate nodes, i.e., more than half wavelength, the legitimate nodes experience independent channels to Eves, which facilitates generating a secret key at legitimate nodes. In the context of physical layer SKG, based on the pioneering work of Shannon's one-time-pad principle, perfect security is achieved when the secret key length is not less than the confidential message length [18]. Therefore, the secret key rate (SKR) is a key performance indicator in SKG-based methods [10], [17], [18].

Beside Eves, active attackers termed as hostile jammer (HJ) may exist in wireless networks and propagate noise-like signals with the aim of degrading the communication link quality [19]. This attack may detriment the state-of-the-art IoT networks, such as mission-critical and civilian applications [20], WSNs [21], and multi-frequency IoT communications [22]. To mitigate this drawback, spread-spectrum techniques, e.g., direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) are implemented in commercial networks [23]–[26]. Compared with DSSS, FHSS technique is easier to setup, more robust against narrow-band interference and capable of preventing unauthorized users' access. Furthermore, FHSS is scalable to dense networks, and hence, is more suitable for decentralized IoT and ad-hoc networks [24]. Traditionally, the jamming mitigation capability of FHSS technique relied on *static pre-distributed* secret keys (or frequency hopping (FH) sequences) named as hopping pattern as proposed in [25], [26]. However, in future large-scale decentralized wireless networks, e.g., the fifth generation (5G)-enabled IoT, where many peer-to-peer communications can occur simultaneously, if this pre-distributed key is compromised, the entire system will be broken. Accordingly, it is essential to find a key generation method with requirements of low overhead and low complexity implementation, while enjoying from an updating mechanism. Therefore, different from many studies, e.g., [19]–[26], the resiliency over HJ attacks can be attained via utilizing the physical layer characteristics of wireless channel as a trustworthy source of randomness [17], [27], [28]. It is also worth mentioning that to effectively overcome HJ in resource-limited IoT networks, flexible resource allocation and power control [29] is also a key parameter in network design. For instance, an anti-jamming IoT network by configuring the sub-carrier and power allocation of each node was proposed in [30].

B. Related Works

In the area of PLS, most previous contributions of keyless secrecy techniques proposed to exploit different degrees of freedom at the legitimate side, such as exploiting external relays [13], [15], multiple-input multiple-output (MIMO technology) [8], [14], [16], or advanced full-duplex receiver with high-level self-interference cancellation techniques [8]. To be more specific, the authors in the recent work of [15] proposed a cooperative-based secure communication over a three-hop untrusted relaying network, where a single-antenna transmitter wishes to forward its secret message to a half-duplex receiver. However, the effect of existing *totally passive* external Eve was not considered in their proposed system model. Besides, deploying two successive relays as intermediate nodes in the network results in implementation costs and system overhead from the view-point of network design. Hu *et. al.* in [31] proposed a secure transmission from a multi-antenna controller to an actuator in an IoT network by deploying AN injection technique and utilizing an external multi-antenna cooperative jammer. Recently, the researchers in [32] have proposed a practical testbed to ensure secure transmission for a point-to-point communication. They utilized an external node as the cooperative jammer to overcome the passive eavesdropping.

Nevertheless, none of the aforementioned works have considered the effect of HJ attack on the performance of their proposed systems. Accordingly, to overcome HJ in the IoT-healthcare application, a lightweight secret key-based PLS scheme was proposed in the recent work of [17]. An external untrusted intermediate node was deployed in their proposed system model to convey the vital data from a source to the destination node. However, the effect of external passive Eve on the proposed SKG-based scheme was not mentioned in their work. In [33], a transmission scheme for a D2D pair in an IoT communication network was designed with the goal of mitigating jamming attack by utilizing game-based analysis. Then, an optimal power allocation (OPA) was proposed to control the transmission power of the nodes. In [34], from the perspective of HJ, the researchers examined the secrecy performance of direct communication between a legitimate pair in the presence of a full-duplex multiple-antenna HJ. The source node in their proposed system model was equipped with multiple antennas to realize some degrees of freedom at the physical layer. To the best of the authors' knowledge, there are very few works on the study of *perfectly secure* communication over a simple but practical IoT-based D2D communication which is facing with both passive and active attacks. In particular, it is challenging to guarantee secure and resilient communication between a single-antenna legitimate transmitter and a half-duplex receiver in the presence of a *multiple-antenna* passive Eve and a *multiple-antenna-aided* active HJ, without utilizing any additional equipment (such as multiple antennas at the transmitter or receiver, or massive MIMO technology) or helper nodes.

C. Our Contributions

Motivated by the aforementioned discussions, a question is raised that: "Is it possible to have a secure and resilient communication between a pair of single-antenna devices in a D2D network, in the presence of multiple-antenna-aided Eve and multiple-antenna assisted full-duplex HJ?" To address the mentioned question, we present a novel study to ensure both *information security* and *transmission resiliency* in a simple but practical wireless communication system in this paper. Accordingly, in our considered system model, a D2D transmitter communicates with a D2D receiver in the existence of a multiple-antenna-aided *totally passive* Eve (which was not

considered in many works such as the recent papers [15], [17]) and an advanced multiple-antenna-assisted full-duplex HJ. The network nodes in our considered system model take advantage of FH technique in their communication protocol. Different from many works (e.g. [12]–[16]) and similar to our recent work [17], we consider both the training (channel estimation/handshaking) and message transmission phases instead of assuming the availability of the full channel state information (CSI). In the considered system model, a worst-case scenario is assumed, where the HJ attacks both the training (which leads to pilot contamination) and transmission phases (which has not been considered in most existing works, e.g., [33]–[35]) to realize more harmful attack. In our proposed system model, in order to assure the secrecy and resiliency requirements, we establish both the key-based SKG scheme and the easy-to-implement AN injection key-less secrecy technique: During the training phase, by performing channel estimation, the D2D nodes take advantage of the local observations of wireless channel to generate a secret key. This key is utilized by legitimate nodes to dynamically determine their pattern of hopping over time[1]. Then, they agree on a common FH sequence for starting message transmission on that shared sub-channel. Meanwhile, the full-duplex HJ wiretaps the pilot exchange of D2D nodes. During the message transmission phase, the perfectly secure AN injection scheme is applied to realize the required channel quality of the legitimate link compared to the eavesdropping link and protect the communication phase against the Eve's attack. We remark that in contrast to [12], our system model is a point-point communication network that suffers from an external passive Eve and also a multiple-antenna-assisted HJ. Additionally, different from [12], we also propose a jamming-resilient transmission scheme for the considered system. It is worth noting that in AN-aided communication networks, the system performance is highly subject to the AN power level. If the AN power level is very low, the quality of received signal at the Eve is not degraded adequately. On the other hand, if the AN power level is very high, the reliability of communication is harmed due to the low quality of information signal at the destination. Motivated by this fact, we also take into account the optimal power allocation (OPA) between the message signal and the AN in our paper.

The main contributions of this paper are summarized as follows:

- To highlight the FH rate of the proposed scheme, we derive a novel closed-form expression for the achievable SKR. Our results reveal that the SKR performance does not depend on the Eve's channel features. Then we discuss on the constraints needed to ensure the jamming resiliency of the proposed scheme based on the obtained hopping rate. We also derive a new closed-from formula for the probability of successful handshaking in the existence of jamming attack.
- For the message transmission phase, we present a tight lower bound on the ergodic legitimate rate and the exact expression for the ergodic eavesdropping rate. Accordingly, the ergodic secrecy rate (ESR) metric is obtained to determine the performance of the proposed perfectly-secured transmission.
- With the aim of maximizing the ESR, an optimization problem is designed to find the OPA between the AN and message signal. The proposed OPA can be effectively solved via the lightweight bisection method. Our results show that the optimal allocation obtained from the bisection algorithm matches well with the results of the exhaustive search method.
- Extensive comparisons with the state-of-the-arts are provided in the paper to highlight the priority of our proposed scheme. In particular, we compare the performance of our scheme with the the traditional direct transmission (DT) [16], the fully-jammed scenario [20] as a special case, the non-frequency hopping approach [35], and the multi-frequency data transmission [48].

The remainder of this paper is organized as follows. In Section II, our proposed system model is introduced. We also indicate some of the main applications of our proposed scheme in this section. In Section III, we present our proposed secure scheme in detail. The training phase, including channel probing and CSI estimation, and the message transmission phase are described in this section. Moreover, a closed-form expression for the achievable SKR obtained from the channel probing is derived as well. In Section IV, we study the jamming-resiliency performance of our FH-based scheme by analyzing the probability of successful handshaking. In addition, the secrecy performance analysis of the proposed scheme is investigated by calculating the ESR metric. Moreover, to boost the performance of the system, optimal allocation of power between AN and the message signal is examined at the end of this section. Section V presents and analyzes the numerical simulation results. Finally, Section VI concludes the paper and presents useful insights for future research directions.

Notations: We denote the transpose, the conjugate transpose, and ℓ^2 norm of a vector by $(\cdot)^T$, $(\cdot)^\dagger$, and $||\cdot||$, respectively. The zero and the identity matrices are shown by $\mathbf{0}$ and $\mathbf{I}$, respectively. $\mathcal{CN}(\mu,\sigma^2)$ represents a complex variable with mean μ and variance σ^2. A random variable (RV) corresponding to a signal symbol is denoted by the uppercase character of that symbol. The expected value, the probability density function (pdf), and the cumulative distribution function (CDF) of RV X are denoted by $\mathbb{E}(X)$, $f_X(x)$, and $F_X(x)$, respectively. The mutual information of two RVs X and Y is shown by $I(X;Y)$. We also denote $[x]^+ = \max(x,0)$ and $C(x) = \log_2(1+x)$. $\mathrm{Ei}(\cdot)$, $\psi(\cdot)$, and $\Phi = 0.577$ are the exponential integral [51, Eq. (8.211)], the Psi function [51, Eq. (8.36)], and the Euler's constant, respectively.

[1]We stress that the secret key obtained from the physical layer characteristics can be utilized in various communication systems with the requirements of security. More specifically, the generated keys can be used for the symmetric encryption schemes in different layers of the protocol stack, e.g., the Wi-Fi Protected Access (WPA) for the MAC layer encryption or for Transport Layer Security (TLS). The generated secret key can also be used in a hybrid cryptosystem, serving as the shared session key for legitimate entities. This key is further utilized for symmetric encryption to improve the secrecy of information transmission [10]. In this article, we exploit the secret key to generate the FH pattern of our communication system [27], [28].

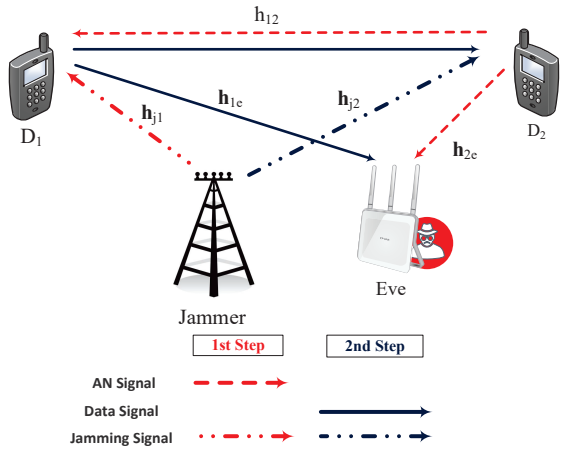

Fig. 1. Proposed transmission scheme for D2D communication.

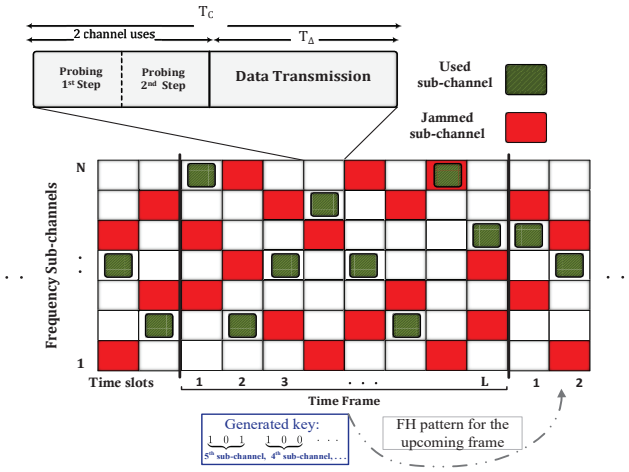

Fig. 2. Time-frequency grid for the proposed scheme.

II. System Model

We consider a point-to-point[2] wiretap system over quasi-static Rayleigh fading channel, where the secret message is sent from the D2D transmitter (D_1) to the D2D receiver (D_2) in the presence of an Eve equipped with M antennas, as depicted in Fig. 1. The Eve implements selection combining (SC), i.e., she selects signal with the highest instantaneous signal-to-noise ratio (SNR) due to complexity constraints[3]. Beside the wiretapping attack of Eve, a powerful HJ, which is equipped with the advanced full-duplex technology [34] exists in our secure D2D communication model. To be more specific, the multiple-antenna-assisted HJ, which is equipped with A_J antennas, can transmit a noise-like signal and concurrently, can wiretap the packet exchange between the D2D nodes. In our system model, the D2D nodes are equipped with single-antenna[4] and they operate under half-duplex mode, which restricts them to transmit and receive simultaneously.

Possible Applications in IoT Networks:

The considered system model and communication protocol are applicable in many state-of-the-art IoT applications, including (but not limited to):

- The D2D communications between sensor nodes in IoT-based WSNs, where jammer node with sensorial capability smartly launches jamming attack to disturb the confidential information transmission [21], [33];
- The IoT applications of 5G cellular networks, where a pair of D2D user equipments (UEs) directly talk to each other to mitigate network overhead and save the cellular resource blocks [29]; In such a scenario, the jamming signal treated in this work can be considered as an unwanted interference from adjacent cellular devices.
- Cyber-physical systems, e.g., industrial IoT (IIoT) or smart grid, where the actuator directly receives control signals from a central controller to perform corresponding operations; In this scenario, it is critically important to ensure information secrecy, while maintaining transmission resiliency against potential attackers [31], [36].
- LoRa networking as an emerging low power wide area networking (LPWAN) technology in IoT paradigm [37]; Currently, LoRa technology utilizes symmetric key cryptographic approach with advanced encryption standard (AES), without any update. Hence, it is vulnerable to eavesdropping attack. In addition, it is shown that this technology is also prone to jamming attacks [38]. Our proposed secure and resilient approach can be utilized to guarantee reliable communication for LoRa networking.
- Bluetooth as a low-energy wireless technique for short range communications, which is widely implemented in smartphones, healthcare devices, and laptops; Bluetooth technique employs FH to avoid channel collisions. Therefore, our proposed FH-based method can be utilized for Bluetooth communications to provide them both secure and reliable transmission requirements [10].

We consider an FH-based system with N_c available orthogonal frequency sub-channels. The D2D nodes can hop to any one of the N_c sub-channels in each time slot to communicate. The sequence of channels chosen in a time frame for communication is termed as FH sequence (hopping pattern) of that frame. Furthermore, we assume that the HJ is capable of randomly jamming $N_j(\leq N_c)$ sub-channels simultaneously in each time slot. Additionally, a constant jamming power P_j is divided evenly among N_j jammed sub-channels. As discussed in [39], the uniform distribution of jamming power is optimal for the HJ from the perspective of minimizing the legitimate channel capacity. Besides, we assume that HJ is synced to each time-slot and has no interference to the Eve.

[2]Considering D2D communications in IoT networks facilitates spectrum reuse, which improves spectral efficiency and enhances energy efficiency. Therefore, this model is applicable for IoT applications, where the majority of devices follow D2D communication.

[3]This assumption applies to applications such as WSN, where the devices are subject to resource limitations. For example, a single-chip is implemented into the device for the sake of power-saving and cost reduction. Performance analysis of an Eve capable of maximal-ratio combining (MRC) would be investigated in our future works.

[4]The assumption of the D2D nodes which are equipped with single-antenna transceivers, is a common cost-efficient, power-efficient, and thus, a practical consideration for the low-cost IoT devices [5].

As depicted in Fig. 2, the whole time is split into several frames, each has L time slots with duration of T_c. The channels remain static within each time slot, but vary independently from one time slot to another one. Each time slot is also split into two phases: a probing (or training) phase and a message transmission phase (See Fig. 2). In the training phase, the D2D nodes take turns transmitting pilot signals to allow channel estimation at the opposite side. Then after agreeing on a particular sub-channel which is based on the estimated channels, the D2D nodes begin to transmit the message signal. The message transmission phase is executed under a time-division multiple-access (TDMA) protocol: As illustrated in Fig. 1, each round of message transmission is twofold: In the first step, the destination D_2 sends AN over the air; In the second step, the source node D_1 combines its message signal with the received AN and sends the resulting signal to D_2. The transmitted signal is then received by D_2 and Eve, while the HJ tries to attack the communication by emitting malicious noise-like jamming signals. Within a time frame, the FH sequence (the secret pattern of hopping) is selected with equal probability among all possible choices. Remarkably, based on Fig. 2, the FH sequence for each time frame is designated by the secret key which was generated by exploiting the wireless channels in the previous frame[5] (this is investigated in Section III). The jamming protocol of HJ in each time slot is as follows: During the training phase, it carefully wiretaps the pilot exchange between the legitimate devices by $A_J - 1$ of its antennas to obtain a high-quality interpretation of the CSIs. Simultaneously, it emits jamming signal by one of its antennas (the remained one) to disrupt the training phase[6]. To highlight the efficiency of our proposed scheme, we assume that HJ has the ability to obtain the perfect CSIs of jamming links. This assumption can be considered as the worst-case scenario from the security perspective [34]. In the message transmission phase, in order to make the jamming more destructive, the HJ sends the jamming signal by $A_J - 1$ of its antennas (which were wiretapping the pilot exchange in the training phase) toward the D2D legitimate devices. The HJ utilizes the MRT beamforming which is a widely-adopted precoder, and is a cost-efficient technique with satisfying performance [34]. The one remaining antenna of $\mathcal{J}$ is idle in this phase [13].

The communication channels are assumed to be reciprocal, and the instantaneous channel gains of D_1-to-D_2, D_1-to-Eve, and D_2-to-Eve links are presented by $h_{12}^{(\mathcal{K})}$, $\mathbf{h}_{1e}^{(\mathcal{K})}$, and $\mathbf{h}_{2e}^{(\mathcal{K})}$, respectively. These links follow the Rayleigh fading model, i.e., $h_{12}^{(\mathcal{K})} \sim \mathcal{CN}(0, \delta_{12}^2)$, $\mathbf{h}_{1e}^{(\mathcal{K})} \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \delta_{1e}^2 \mathbf{I}_{M\times 1})$, and $\mathbf{h}_{2e}^{(\mathcal{K})} \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \delta_{2e}^2 \mathbf{I}_{M\times 1})$, respectively, where δ_{12}^2, δ_{1e}^2, and δ_{2e} are the channel gains based on the distant-dependent path loss of each link. Moreover, $\mathcal{K} \in \{1, 2, \cdots, N_{sc}\}$ denotes the index of the used sub-channel. Finally, the instantaneous fading channel from HJ to each of the receiving D2D nodes is denoted by $\mathbf{h}_{\text{jn}}^{(\mathcal{K})} \sim \mathcal{CN}(\mathbf{0}_{A\times 1}, \delta_{jn}^2 \mathbf{I}_{A\times 1})$, $n \in \{1, 2\}$, where δ_{jn}^2 is the channel gain from each antenna branch of $\mathcal{J}$ to the receiving node n and A denotes the number of active antennas at HJ. We mention that since the communication between D_1 and D_2 during each time slot is accomplished on a specific sub-channel, hence, for the ease of representation, we omit the superscript $(\mathcal{K})$ in the remainder of the paper. Moreover, without loss of generality, we assume that the noise at each node is additive white Gaussian noise (AWGN) and follows $\mathcal{CN}(0, N_0)$.

[5]Similar to many communication protocols [40], [41], in order to obtain a secret FH pattern for the first frame, an initialization phase is performed which only comprises the pilot exchange.

[6]We presume that the self-interference effect of the active antenna is negligible on the other antennas of HJ. Evaluating the self-interference isolation techniques is out of the scope of this paper. Moreover, the authors in [34] showed that increasing the number of antennas at HJ can mitigate the effect of the self-interference imposed by the full-duplex mechanism.

III. Design of the Secure Scheme

A. Training Phase for Key Establishment

In this subsection, we investigate the channel estimation procedure performed by the D2D nodes. These nodes utilize the local observations of the D2D channel to achieve a secretly-shared key. This is done with the goal of obtaining a secret hopping pattern for the transmission; hence, ensuring the resiliency against active adversary. We derive a closed-form expression for the achievable SKR and the probability of successful transmission when facing jamming.

1) Channel Probing-Estimation Phase: As the first step for training each time slot, the nodes try to estimate the wireless channels. Channel probing makes the legitimate D2D devices able to obtain raw random sequence, i.e., the estimated channels, for future process leading to key generation of the upcoming frame. In order to estimate the direct channel of h_{12} in each time slot, both D_1 and D_2 take turns into transmitting pilot signal $x_p = 1$ with power P_1^τ and P_2^τ, respectively [27]. Then they estimate the direct channel from their received signals. Simultaneously, HJ wiretaps the pilot exchange between D_1 and D_2 with $A_J - 1$ of its antennas and, via the remained antenna, emits jamming signal x_j with $\mathbb{E}\{|x_j|^2\} = 1$ to the devices which are in receiving mode[7]. Consequently, the received pilots at D_1 and D_2 can be written, respectively as

$$y_{D_1} = \sqrt{P_2^\tau} h_{12} x_p + s\sqrt{\frac{P_j}{N_j}} h_{j1} x_j + n_1,$$
$$y_{D_2} = \sqrt{P_1^\tau} h_{12} x_p + s\sqrt{\frac{P_j}{N_j}} h_{j2} x_j + n_2, \quad (1)$$

where $s \in \{0, 1\}$ is a binary variable which follows Bernoulli distribution and has the value 1, i.e., when jamming exists in the used sub-channel, with probability $\frac{N_j}{N_c}$, and has the value 0, otherwise. Moreover, h_{jn}, $n \in \{1, 2\}$ denotes the jamming link from the active antenna of HJ to node n. Also, the received signal at Eve in training phase is given by

$$y_E^{(i)} = \sqrt{P_i^\tau} h_{ie} x_p + s\sqrt{\frac{P_j}{N_j}} h_{je} x_j + n_e, \quad (2)$$

[7]In the training phase, where the nodes are initiating some packet exchanges to estimate their channels, the HJ is not aware of the jamming links. As such, it blindly emits the jamming signal x_j over the air, which is received by the nodes which are in the receiving mode.

where $i \in \{1,2\}$ indicates whether the received signal is sent by D_1, or D_2. Also, h_{je} denotes the jamming link from the active antenna of HJ to Eve. By invoking the received signals y_{D_1} and y_{D_2} formulated in (1), the estimation of the D2D channel at D_1 and D_2 can be obtained, respectively as

$$\hat{h}_{12}^{D_1} = \frac{y_{D_1}}{\sqrt{P_2^\tau} x_p} = h_{12} + \hat{z}_1, \quad \hat{h}_{12}^{D_2} = \frac{y_{D_2}}{\sqrt{P_1^\tau} x_p} = h_{12} + \hat{z}_2, \tag{3}$$

where the superscripts D_1 and D_2 indicate that the estimation is conducted at these two, respectively. Moreover, $\hat{z}_i \sim \mathcal{CN}(0, \hat{\sigma}_{z_i}^2)$, $i \in \{1,2\}$ is the channel estimation error which is independent of h_{12} [42] with the variance of

$$\hat{\sigma}_{\mathcal{E}_1}^2 = (N_0 + s\frac{P_j}{N_j}\delta_{j1}^2)/P_2^\tau, \quad \hat{\sigma}_{\mathcal{E}_2}^2 = (N_0 + s\frac{P_j}{N_j}\delta_{j2}^2)/P_1^\tau. \tag{4}$$

We note that the transmit power of the D2D nodes, the pilot signal, and the channel variances are publicly available at legitimate nodes. As such, the D2D nodes can conduct the channel estimations expressed in (3). Moreover, as mentioned in Section II, we assume that HJ obtains the perfect CSIs of jamming links from its piloting observations, and thus, the estimation procedure of the HJ is not formulated here.

2) Key Generation from Channel Estimation: The estimated CSIs at D_1 and D_2 during all training slots of a time frame can be concatenated to form the corresponding vectors $\hat{\mathbf{h}}_{12}^{\mathcal{N}} = [\hat{h}_{12}^{\mathcal{N}}(1), \cdots, \hat{h}_{12}^{\mathcal{N}}(L)]^T$, $\mathcal{N} \in \{D_1, D_2\}$. These correlated observations are used to generate the shared secret key (the aforementioned FH pattern) for the next frame. Similarly, all the received signals at Eve can be gathered in two vectors, namely $\mathbf{y}_E^{(1)}$ and $\mathbf{y}_E^{(2)}$, where $\mathbf{y}_E^{(i)} = [y_E^{(i)}(1), \cdots, y_E^{(i)}(L)]^T$. Moreover, all the nodes which are facing the malicious signals of HJ, will detect the existence of jamming at the end of each time slot [27], therefore, by collecting the binary states $s(t)$, $t \in \{1, 2, \cdots, L\}$ into a vector $\mathbf{s} = [s(1), \cdots, s(L)]^T$, both the D2D devices and Eve will obtain the vector $\mathbf{s}$ for further calculations.

In general, assume that two legitimate nodes A and B, and the Eve E obtain n realizations $X = (X_1, X_2, ..., X_n)$, $Y = (Y_1, Y_2, ..., Y_n)$, and $Z = (Z_1, Z_2, ..., Z_n)$, respectively. A and B can extract a common key from their observations X and Y, respectively. The work of [43] developed the information-theoretical fundamentals for key generation, leading to the following bound on the achievable secret key rate

$$R_{key} \geq I(X;Y) - \min[I(X;Z), I(Y;Z)]. \tag{5}$$

Remarkably, until $R_{key} > 0$ is satisfied, the key generation can be carried out securely. Motivated by the above discussion, we proceed to obtain a closed-form expression for the achievable SKR to investigate the key secrecy of the training phase in our proposed scheme. Therefore, invoking (5) for our proposed system, the achievable SKR can be written as follows:

$$R_{key} = \mathbb{E}\Big\{\Big[\max\{\underbrace{I(\hat{\mathbf{h}}_{12}^{D_1}; \hat{\mathbf{h}}_{12}^{D_2})}_{R_1} - \underbrace{I(\hat{\mathbf{h}}_{12}^{D_1}; \mathbf{y}_E^{(1)}, \mathbf{y}_E^{(2)})}_{T_1}, I(\hat{\mathbf{h}}_{12}^{D_2}; \hat{\mathbf{h}}_{12}^{D_2}) - \underbrace{I(\hat{\mathbf{h}}_{12}^{D_2}; \mathbf{y}_E^{(1)}, \mathbf{y}_E^{(2)})}_{T_2}\}\Big]^+ \Big| \mathbf{s}\Big\}, \tag{6}$$

where $I(X,Z;Y)$ is the mutual information of the jointly distributed random variables X and Y, and Z. In (6), R_1 denotes the key rate that can be achieved by utilizing the existing legitimate channel vector $\mathbf{h}_{12}$. Furthermore, recall that the secret key rate in the proposed scheme is generated from the local observations of the D2D link. Hence, the leaked rates to Eve denoted by T_1 and T_2 are zero. This is because the observations of Eve, derived in (2) for each time instance, are independent of the legitimate D2D channel $\mathbf{h}_{12}$[8]. Besides, we remark that the proposed scheme is a typical mobile communication system, in which multi-path fading contributes as the predominant factor of random deviation than large scale fading. As such, despite the positions or displacements of the legitimate D2D nodes being disclosed, the Eve cannot still derive any useful information about $\mathbf{h}_{12}$. Accordingly, we further simplify the expressions in (6) to obtain the closed-form expression for the achievable SKR of our proposed scheme as

$$\begin{aligned} R_{key} &\overset{(a)}{\geq} \Big[\mathbb{E}\big\{I(\hat{\mathbf{h}}_{12}^{D_1}; \hat{\mathbf{h}}_{12}^{D_2}) \mid \mathbf{s}\big\}\Big]^+ \\ &\overset{(b)}{=} (1 - \frac{N_j}{N_c}) C\Big(\frac{\delta_{12}^2}{\hat{\sigma}_{\mathcal{E}_{1|s=0}}^2 + \hat{\sigma}_{\mathcal{E}_{2|s=0}}^2 + \hat{\sigma}_{\mathcal{E}_{1|s=0}}^2 \hat{\sigma}_{\mathcal{E}_{2|s=0}}^2 / \delta_{12}^2}\Big) \\ &\quad + \frac{N_j}{N_c} C\Big(\frac{\delta_{12}^2}{\hat{\sigma}_{\mathcal{E}_{1|s=1}}^2 + \hat{\sigma}_{\mathcal{E}_{2|s=1}}^2 + \hat{\sigma}_{\mathcal{E}_{1|s=1}}^2 \hat{\sigma}_{\mathcal{E}_{2|s=1}}^2 / \delta_{12}^2}\Big), \end{aligned} \tag{7}$$

where (a) follows from the fact that $\mathbb{E}\{\max[X,Y]\} \geq \max[\mathbb{E}\{X\}, \mathbb{E}\{Y\}]$ [15] and (b) follows from some straightforward manipulations on the mutual information of two correlated Gaussian-distributed RVs [17]. Note that $\hat{\sigma}_{\mathcal{E}_{i|s=0}}^2$ and $\hat{\sigma}_{\mathcal{E}_{i|s=1}}^2$, $i \in \{1,2\}$ can be obtained by substituting $s=0$ and $s=1$ in (4), respectively. Notably, the derived expression for SKR in (7) satisfies $R_{key} > 0$ which implies that the secrecy of key is maintained in the training phase of our system. In our system model, if the pattern of the used sub-bands (FH sequence) is exposed to the HJ, then it can focus on the compromised sub-channels and dedicate its power budget to realize a deadly attack, which will degrade the performance of our proposed scheme. That is, to have a reliable transmission, it is important for D2D devices to have a *secret* and *non-static* FH sequence such that the HJ cannot obtain this pattern effortlessly. Obtaining the hopping sequence via utilizing the secret key generated from the physical layer of legitimate channels, *which has information-theoretic proofs* in terms of security, can help the overall system ensure a secure and reliable communication. Therefore, this common secret key is utilized as the FH pattern of the D2D nodes.

Remark 1: Invoking Eqs. (4) and (7), one can conclude on the negative effect of HJ on the achievable SKR. That is, increasing the jamming power P_j leads to higher estimation error variances (pilot contamination), which results in SKR reduction.

Remark 2 *(SKG in practice):* Design of an SKG system in physical layer is performed by implementing some blocks after the probing phase. More precisely, after organizing the probing

[8]This is a basic assumption in the context of physical layer SKG, known as spatial decorrelation. It states that any Eve positioned in more than one half-wavelength away from any user faces uncorrelated multi-path fading [10].

Protocol	Code Size (kb)	Cycles	Computation Energy (mJ)	Communication Energy (mJ)	Total (mJ)
Key Generation	1.137	$\approx$ 1345 k	5.206	0.187	5.393
ECDH	8.749	1,734,400 k	528.45	0.064	528.514

TABLE I
RESOURCE AND ENERGY CONSUMPTION COMPARISON BETWEEN SKG AND ECDH [44].

phase (handshaking for channel estimation), the correlated random observations of $\mathbf{y}_{D_1} = [y_{D_1}(1), \cdots y_{D_1}(L)]^T$ and $\mathbf{y}_{D_2} = [y_{D_2}(1), \cdots y_{D_2}(L)]^T$ are obtained by D2D nodes. Afterwards, each entity of these random vectors is mapped onto some bits by prevalent quantization algorithms. Next step is to reconcile the streams of bits between the two legitimate nodes, using some error correcting codes. Ultimately, a privacy amplification block, e.g., universal hash functions is applied to enhance the quality of secret bits and minimize the information leakage. More details about SKG blocks can be found in [10].

Remark 3 *(Energy consumption efficiency):* The SKG technique utilized in this paper is lightweight and uses limited resources. This is due to the fact that the SKG is carried out along with the channel measurements [10], [38]. In other words, no dedicated signaling transmission is acquired for key generation. This significantly saves power consumption, thus, meets the low energy constraints of IoT devices. To show the cost-efficiency of the utilized SKG method, as a practical example, the researchers in [44] implemented both the physical layer key generation scheme and a lightweight elliptic curves Diffie–Hellman key generation (ECDH), as a comparison. Using an 8-bit Intel MCS-51 micro-controller, the ECDH required about 8 times more code size, 98 times more energy, and imposed 1289 times higher complexity than that of the key generation protocol, respectively. The details of their experimental results are summarized in Table I.

B. Message Transmission Phase

In the message transmission phase, the information signal has to be transmitted from D_1 to D_2. For the message transmission phase, as illustrated in Fig. 1, the ANI technique is implemented to degrade the received signal quality at the Eve, such that it cannot estimate the confidential information. It is worth mentioning that the ANI scheme is shown to be low-cost, thus suitable for low-complex IoT nodes [7]. In each step of the message transmission phase, the HJ jams the legitimate D2D device. The jamming is conducted with $A_J - 1$ antennas of HJ by transmitting the noise-like signal x_j with power of P_j. The HJ utilizes the MRT transmit weight vectors $\mathbf{w}_{\mathrm{J}}^{(1)} = \frac{\mathbf{h}_{\mathrm{j1}}^{\dagger}}{||\mathbf{h}_{\mathrm{j1}}||} \in \mathbb{C}^{1\times(A_J-1)}$ and $\mathbf{w}_{\mathrm{J}}^{(2)} = \frac{\mathbf{h}_{\mathrm{j2}}^{\dagger}}{||\mathbf{h}_{\mathrm{j2}}||} \in \mathbb{C}^{1\times(A_J-1)}$ in the first and second step of transmission, respectively. These MRT vectors are obtained via eavesdropping the packet exchange procedure in the training phase of each time slot. The steps for establishing a secure message transmission between the D2D devices are as follows.

- First step. As it is shown with red dashed lines in Fig. 1, D_2 emits the pseudo random AN x_2 with power P_2^{μ} over the air, where $x_2 \sim \mathcal{CN}(0,1)$. The signal is then received by D_1 and Eve. At the same time, the HJ sends jamming signal x_j with $\mathbb{E}\{|x_j|^2\} = 1$ to D_1. Thus, the received signal at D_1 is

$$y_{D_1}^{(1)} = \sqrt{P_2^{\mu}} h_{12} x_2 + s\sqrt{\frac{P_j}{N_j}} \mathbf{w}_{\mathrm{J}}^{(1)} x_j \mathbf{h}_{\mathrm{j1}} + n_1. \quad (8)$$

- Second step. D_1 transmits x_1 with $\mathbb{E}\{|x_1|^2\} = 1$, which consists of the normalized information signal m, added with the received signal $y_{D_1}^{(1)}$ from the first step as follows

$$x_1 = \sqrt{\xi} m + \sqrt{1-\xi}\frac{y_{D_1}^{(1)}}{\sqrt{P_r}}, \quad (9)$$

where $\mathbb{E}\{|m|^2\} = 1$ and $0 < \xi \leq 1$ denotes the power splitting ratio between the information signal and the AN. Moreover, P_r is the power of the received signal $y_{D_1}^{(1)}$ which can be calculated as [9]

$$P_r = \mathbb{E}\{|y_{D_1}^{(1)}|^2\} = P_2^{\mu}|h_{12}|^2 + s\frac{P_j}{N_j}||\mathbf{h}_{\mathrm{j1}}||^2 + N_0. \quad (10)$$

The signal x_1 is transmitted with power P_1^{μ}, and is received by D_2 and Eve as shown in Fig. 1 with solid lines. Meanwhile, the HJ emits the malicious jamming signal (depicted by dash-dotted line in Fig. 1) to the legitimate receiver D_2 via the MRT vector $\mathbf{w}_{\mathrm{J}}^{(2)}$. The received signal at D_2 is given by

$$y_{D_2}^{(2)} = \sqrt{P_1^{\mu}} h_{12} x_1 + s\sqrt{\frac{P_j}{N_j}} \mathbf{w}_{\mathrm{J}}^{(2)} x_j \mathbf{h}_{\mathrm{j2}} + n_2. \quad (11)$$

Similarly, the receiving signal at each antenna of Eve, denoted by y_{E_i}, $i \in \{1, 2, \cdots, M\}$ is simply given by $y_{E_i}^{(2)} = \sqrt{P_1^{\mu}} h_{1e_i} x_1 + n_2$, where h_{1e_i} is the channel from D_1 to the i'th antenna of Eve, $i \in \{1, 2, \cdots, M\}$. We note that to realize a harmful attack from the security perspective, it is assumed that the HJ informs Eve of the beamfoming vector $\mathbf{w}_{\mathrm{J}}^{(2)}$ and the jamming signal x_j. Hence, Eve is able to cancel out the jamming in the second step with the aim of obtaining a higher level of signal-to-interference-plus-noise ratio (SINR).

Based on (11), the self-interference cancellation at D_2 is performed, using the estimated channel $\hat{h}_{12}^{D_2}$ obtained in (3) and (4) from the training phase[10]. Hence, we have

$$\tilde{y}_{D_2}^{(2)} = y_{D_2}^{(2)} - \sqrt{P_1^{\mu}}\sqrt{(1-\xi)P_2^{\mu}}(\hat{h}_{12}^{D_2})^2 \frac{x_2}{\sqrt{P_r}}, \quad (12)$$

[9] P_r can be obtained via common methods for calculating the power of signal [17]. We note that knowing the instantaneous values of channel gains are not required for power calculation, and the expression in (10) is just provided for further analysis.

[10] We remark that Eve may also carry out the same procedure as D_2 does. However, based on (8) and (9), to effectively decode the secret message, the estimation of legitimate channel h_{12} is required, which is not available at Eve.

$$\gamma_{D_2} = \frac{\xi P_1^{\mu} |h_{12}|^2 P_r}{(1-\xi)P_1^{\mu}|h_{12}|^2(s\frac{P_j}{N_j}||\mathbf{h}_{\mathrm{j1}}||^2+N_0) + P_r(s\frac{P_j}{N_j}||\mathbf{h}_{\mathrm{j2}}||^2+N_0) + (1-\xi)P_1^{\mu}P_2^{\mu} \mid h_{12}^2 - (\hat{h}_{12}^{D_2})^2 \mid^2}. \tag{13}$$

where $\tilde{y}_2^{(2)}$ denotes the interference-canceled signal at D_2.

Consequently, the received SINR at D_2 is expressed in (13) which is on top of the next page. Analogously, the received SINR at the i'th antenna of Eve, denoted by γ_{E_i}, $i \in \{1, 2, \cdots, M\}$ is

$$\gamma_{E_i} = \frac{\xi P_1^{\mu} |h_{1e_i}|^2}{(1-\xi)P_1^{\mu}|h_{1e_i}|^2 + N_0}. \tag{14}$$

For $m \in \{1,2\}$, $n \in \{1,2,e_i\}$ $(m \neq n)$, and $i \in \{1,2,\cdots M\}$, we define $\gamma_{mn} \triangleq \rho_m |h_{mn}|^2$, where $\rho_m \triangleq \frac{P_m^{\mu}}{N_0}$ denotes the transmit SNR of the D2D devices. Moreover, we define $\gamma_{jn} \triangleq \rho_j ||\mathbf{h}_{\mathrm{jn}}||^2$, where $\rho_j \triangleq \frac{P_j/N_j}{N_0}$. Afterward, considering the high SNR regime, we can approximate the SINR at Eve and D_2 which leads to the following equations.

$$\gamma_{E_i} \approx \frac{\xi\gamma_{1e_i}}{(1-\xi)\gamma_{1e_i}+1}, \tag{15}$$

$$\gamma_{D_2|s=0} \approx \frac{\xi\gamma_{12}\gamma_{21}}{(1-\xi)\gamma_{12}+\gamma_{21}+(1-\xi)\gamma_{\mathcal{E}1}\gamma_{\mathcal{E}2}}, \tag{16}$$

$$\gamma_{D_2|s=1} \approx \frac{\xi\gamma_{12}(\gamma_{21}+\gamma_{j1})}{(1-\xi)\gamma_{12}\gamma_{j1}+\gamma_{j2}(\gamma_{21}+\gamma_{j1})+(1-\xi)\gamma_{\mathcal{E}1}\gamma_{\mathcal{E}2}}, \tag{17}$$

where $\gamma_{\mathcal{E}n} \triangleq \frac{P_n^{\mu}}{N_0}|h_{12}^2 - (\hat{h}_{12}^{D_2})^2|$, $n \in \{1,2\}$.

Remark 4: In our proposed scheme, the training phase not only determines the required FH sequence, but also assists the destination node to decode the data signal in the message transmission phase via channel estimations. Hence, increasing the allocated power P^{τ} for training boosts both the FH rate and the channel estimation quality. This can be easily seen from (4), (7), and (12).

IV. Resiliency and Secrecy performance Analysis

A. Jamming Resilience Performance Analysis

1) Probability of successful handshaking under attack: In this subsection, we investigate the performance of the handshaking (channel probing and SKG) phase of the proposed system against the wide-band jamming attack. Similar to [21] and [28], we assume that the HJ is capable of obtaining the rate of the secret key, R_{key}, shared between legitimate nodes. Therefore, the HJ can generate all possible FH sequences. As a numerical example, consider the HJ is informed that the IoT nodes agree on a secret key of 6 bits and adopt this key for the FH pattern, it can then generate all 63 possible FH patterns. Due to the fact that the HJ does not know the exact pattern agreed between IoT nodes, the best treatment for the HJ would be to uniformly allocate its power among possible FH patterns and transmit the summation of these patterns. Therefore, the received signal at the receiver can be represented by

$$y_{D_2} = \sqrt{P_1^{\tau}} h_{12} x\mathcal{K} + \sqrt{\frac{P_j}{N_{\mathcal{K}}}} h_{j2} x_j \sum_{i=1}^{N_{\mathcal{K}}} \mathcal{K}_i + n_2, \tag{18}$$

where $\mathcal{K}$ is the shared secret hopping pattern with length $L_{\mathcal{K}} = \log_2(N_c)$ bits, $N_{\mathcal{K}} = 2^{R_{key}} - 1$ denotes the number of all possible patterns, and $\mathcal{K}_i$ denotes a possible pattern that the HJ generates. Based on (18), we can obtain the SINR of the receiver under jamming attack as follows.

$$\gamma_{D_2}^{(UA)} = \frac{\rho|h_{12}|^2}{\frac{\rho_j}{N_k}|h_{j2}|^2\mathcal{I} + \frac{1}{L_{\mathcal{K}}}}, \tag{19}$$

where $\rho = \frac{P_1^{\tau}}{N_0}$, $\rho_j = \frac{P_j}{N_0}$, $\mathcal{I} = \sum_{i=1}^{N_{\mathcal{K}}} \varphi_i$, and φ_i denotes the correlation between $\mathcal{K}_i$ and $\mathcal{K}$. We note that $\varphi_i = 1$ if $\mathcal{K}_i = \mathcal{K}$. In order to evaluate the resiliency performance of the D2D communication under jamming attack, we adopt the successful handshaking probability as the performance metric, which is defined as the probability that the received SINR at the receiver is larger than a certain threshold [21]. This can be expressed as

$$\mathcal{P}_s^{(UA)}(R_{key}, \gamma_{th}) = Pr\{\gamma_{D_2}^{(UA)} > \gamma_{th}\} \tag{20}$$

Accordingly, we proceed to examine the successful handshaking probability of scheme in the following lemma.

Lemma 1. *The successful handshaking probability of our system under jamming attack is given by*

$$\mathcal{P}_s^{(UA)}(R_{key}, \gamma_{th}) \approx \frac{\rho\delta_{12}^2 N_{\mathcal{K}} \exp(-\gamma_{th}/\rho\delta_{12}^2 L_{\mathcal{K}})}{\rho\delta_{12}^2 N_{\mathcal{K}} + \rho_j\delta_{j2}^2\gamma_{th}(1+\frac{2^{R_{key}-2}}{3L_{\mathcal{K}}})}. \tag{21}$$

Proof. Please see the proof provided in Appendix A. ■

Lemma 1 indicates that the probability of successful handshaking in the training phase of our scheme does not depend on the location of passive Eve, which is desirable from the security perspective.

2) Jamming-resilient condition: As previously mentioned, our proposed FH-based scheme requires a sufficient key rate. The SKR determines the FH rate of our scheme which interprets the ratio of robustness against jamming. Therefore, as a measure to verify whether our scheme is ahead of HJ or not, one must ensure that the key rate be large enough to meet the inequality $2^{R_{key}} \geq N_c$ [27]. In other words, in the proposed scheme with N_c available sub-channels, at least $L\log_2(N_c)$ bits are required to maintain the full hopping pattern for the next time frame (each time frame consists of L time slots). Thus, we must have

$$LR_{key} \geq L\log_2(N_c). \tag{22}$$

It is worth mentioning that having higher SKRs, in addition to getting rid of the jamming attack, has another advantage for the FH system. The higher SKR means having a secret hopping pattern which can be utilized for more upcoming time slots, and therefore, the network will spend less time for computational processes. This is because there would be no

need for frequently conducting SKG process. This benefit is desirable for resource-limited communication networks such as 5G-enabled IoT and WSNs.

Remark 5: Considering a total transmit power budget $P^{\tau} = P_1^{\tau} + P_2^{\tau}$ for training phase, the SKR is a monotonically increasing function of P^{τ}. This can be inferred from Eqs. (7) and (4). Hence, to find the minimum required transmit power for robustness, we must have $P^{\tau} \geq P^{\tau^*}$, where P^{τ^*} can be easily obtained by solving $R_{key}(P^{\tau^*}) = \log_2(N_c)$. This problem can be solved using prevalent numerical approaches such as bisection search method.

B. Secrecy Performance Analysis

An extensively-adopted secrecy metric to evaluate the secrecy performance of the wireless communication networks is the ESR performance. This metric measures the average rate below which any confidential transmission is achievable. Toward this end, based on the calculated SINRs, i.e., equations (15)–(17) in the previous section, the instantaneous secrecy rate for the transmitted massage can be expressed as [45]

$$R_s = \frac{1}{2\ln 2}\Big[\ln\Big(1+\gamma_{D_2}\Big) - \ln\Big(1+\gamma_E\Big)\Big]^+, \tag{23}$$

where $\gamma_E \triangleq \max\limits_{1\leq i\leq M} \gamma_{E_i}$, due to the fact that Eve adopts the SC technique. Consequently, the ESR performance can be validated as follows

$$\begin{aligned}\bar{R}_s &= \frac{1}{2\ln 2}\mathbb{E}\Big\{\big[\ln(1+\gamma_{D_2}) - \ln(1+\gamma_E)\big]^+ |\mathbf{s}\Big\} \\ &\geq \frac{1}{2\ln 2}\Big[\underbrace{\mathbb{E}\big\{\ln(1+\gamma_{D_2}) \mid \mathbf{s}\big\}}_{\triangleq\ \mathcal{F}_1} - \underbrace{\mathbb{E}\big\{\ln(1+\gamma_E) \mid \mathbf{s}\big\}}_{\triangleq\ \mathcal{F}_2}\Big]^+ \\ &\triangleq \bar{R}_s^{LB}.\end{aligned} \tag{24}$$

Based on (24), the ESR can be viewed as the difference between the ergodic legitimate rate, defined by $R_{\mathsf{L}} \triangleq \frac{1}{2\ln 2}\mathcal{F}_1$, and the ergodic eavesdropping rate, defined by $R_{\mathsf{E}} \triangleq \frac{1}{2\ln 2}\mathcal{F}_2$. In the following, we proceed to obtain the closed-form expression of $\bar{R}_s^{LB}$ in (24) by obtaining the expressions of R_{L} and R_{E}, respectively.

1) Ergodic Legitimate Rate: The ergodic legitimate rate R_{L} can be calculated as

$$R_{\mathsf{L}} = \frac{1}{2\ln 2}\left[(1-\frac{N_j}{N_c})\mathcal{F}_{1|s=0} + \frac{N_j}{N_c}\mathcal{F}_{1|s=1}\right], \tag{25}$$

where

$$\mathcal{F}_{1|s=0} = \ln\big(1+\frac{\mathcal{M}_0}{\mathcal{N}_0}\big), \tag{26}$$

with $\mathcal{M}_0 = \xi\rho_1\rho_2\delta_{12}^4 e^{-2\Phi}$ and $\mathcal{N}_0 = \big(\rho_2 + (1-\xi)\rho_1\big)\delta_{12}^2 + 2(1-\xi)\rho_1\rho_2\hat{\sigma}^2_{\mathcal{E}_2|s=0}(2\delta_{12}^2 + \hat{\sigma}^2_{\mathcal{E}_2|s=0})$, respectively. And,

$$\mathcal{F}_{1|s=1} = \ln\big(1+\frac{\mathcal{M}_1}{\mathcal{N}_1}\big), \tag{27}$$

with $\mathcal{M}_1 = \xi\rho_1\delta_{12}^2 e^{\mathcal{T}-\Phi}$ and $\mathcal{N}_1 = (1-\xi)\rho_1\delta_{12}^2(A_J-1)\rho_j\delta_{j1}^2 + (A_J-1)\rho_j\delta_{j2}^2(\rho_2\delta_{12}^2 + (A_J-1)\rho_j\delta_{j1}^2) + 2(1-\xi)\rho_1\rho_2\hat{\sigma}^2_{\mathcal{E}_2|s=1}(2\delta_{12}^2 + \hat{\sigma}^2_{\mathcal{E}_2|s=1})$, respectively. Moreover, $\mathcal{T}$ is given by

$$\mathcal{T} = \frac{\lambda_x}{(1-\frac{\lambda_x}{\lambda_y})^{A_J-1}}\Big(\mathcal{A}+\mathcal{B}\Big), \tag{28}$$

with $\lambda_x = 1/\rho_2\delta_{12}^2$, $\lambda_y = 1/\rho_j\delta_{j1}^2$, $\mathcal{A} = \frac{-(\Phi+\ln\lambda_x)}{\lambda_x}$, and $\mathcal{B} = \sum\limits_{m=0}^{A_J-2}(1-\frac{\lambda_x}{\lambda_y})^m\frac{(\ln\lambda_y - \psi(m+1))}{\lambda_y}$.

Proof. Please see Appendices B and C. ■

Eq. (27) indicates that the HJ can decrease the ergodic legitimate rate of D2D nodes by increasing its jamming power or utilizing more transmit antennas.

2) Ergodic Eavesdropping Rate:

Proposition 1. *The exact closed-form expression for the ergodic eavesdropping rate, R_{E}, is given by*

$$R_{\mathsf{E}} = \frac{\xi}{2m_e\ln 2}\sum_{k=0}^{M} p_k\frac{e^{c_k/\xi}}{c_k(1-\xi)}\left(e^{-c_k}\mathrm{Ei}(\frac{-c_k}{\xi}) - \mathrm{Ei}(\frac{-k}{m_e})\right), \tag{29}$$

where $m_e = \rho_1\delta_{1e}^2$, $p_k = (-1)^{k+1}k\binom{M}{k}$, $c_k = \frac{k\xi}{m_e(1-\xi)}$, and $\binom{n}{k}$ is the binomial coefficient.

Proof. Please see Appendix D. ■

Eq. (29) shows that the legitimate nodes can improve the secrecy rate by increasing their transmit power, leading to ergodic eavesdropping rate reduction.

Based on the above discussions, the achievable ESR can be obtained as the secrecy metric of our proposed scheme:

3) Ergodic Secrecy Rate: The closed-form expression for $\bar{R}_s^{LB}$, defined in (24), is given by

$$\bar{R}_s^{LB} = [R_{\mathsf{L}} - R_{\mathsf{E}}]^+, \tag{30}$$

where R_{L} and R_{E} are given by (25) and (29), respectively. So far, we have derived the expression for the achievable ESR. In the next subsection, we aim to improve the ESR by taking into account the optimal allocation of power.

C. Optimal Power Allocation

In this subsection, we take into account the OPA for message transmission by maximizing the ESR of our proposed scheme in the presence of an HJ and a multiple-antenna-aided passive Eve. Without loss of generality, we presume that both D2D nodes have fixed-value transmit powers denoted by P_1^{μ} and P_2^{μ} defined in Subsection III-B. This assumption is also compatible with the low-complex IoT nodes present in the network [46], [47]. Accordingly, optimizing the network from the security view-point is handled by adjusting the power splitting ratio ξ, which automatically adjusts the power allocated for injecting AN and the power of message transmission as well. We stress that instantaneous OPA between the AN signal from D_2 and the message signal from D_1 depends on the state of HJ, i.e., whether the jamming signal exists in the used sub-channel or not. Besides, the power allocation should be performed at the beginning of each time slot. However, in this paper, the low-complex IoT nodes are not capable of

detecting the presence of jamming attack at the start of each time slot. Thus, finding the OPA in an instantaneous manner is not applicable in our proposed scenario.

Taking these considerations into account, we utilize the closed-form expression $\bar{R}_s^{LB}$, obtained in the previous subsection (Subsection IV-B) for the ESR, to formulate the optimization problem as follows

$$\begin{aligned} \xi^* = \arg\max_{\xi} \quad & \bar{R}_s(\xi) \\ \text{s.t.} \quad & 0 < \xi \leq 1. \end{aligned} \tag{31}$$

In order to check the convexity of the problem in (31), we proceed to calculate the derivatives of $\bar{R}_s$. The first derivative of $\bar{R}_s^{LB}$ can be written as

$$\frac{\partial \bar{R}_s^{LB}}{\partial \xi} = \frac{1}{2\ln 2}\left[(1-\frac{N_j}{N_c})\mathcal{L}_0 + \frac{N_j}{N_c}\mathcal{L}_1 - \mathcal{M}\right], \tag{32}$$

where

$$\mathcal{L}_0 = \frac{\mathcal{M}_0}{\mathcal{M}_0+\mathcal{N}_0}(\frac{1}{\xi} - \frac{P_0}{\mathcal{N}_0}), \tag{33}$$

with $P_0 = -\rho_1\delta_{12}^2 - 2\rho_1\rho_2\hat{\sigma}^2_{\mathcal{E}|s=0}(2\delta_{12}^2 + \hat{\sigma}^2_{\mathcal{E}|s=0})$. Moreover,

$$\mathcal{L}_1 = \frac{\mathcal{M}_1}{\mathcal{M}_1+\mathcal{N}_1}(\frac{1}{\xi} - \frac{P_1}{\mathcal{N}_1}), \tag{34}$$

with $P_1 = -\rho_1\delta_{12}^2\rho_j\delta_{j1}^2(A_J-1) - 2\rho_1\rho_2\hat{\sigma}^2_{\mathcal{E}|s=1}(2\delta_{12}^2+\hat{\sigma}^2_{\mathcal{E}|s=1})$, and

$$\begin{aligned} \mathcal{M} = \sum_{k=0}^{M} p_k e^{c_k/\xi}\Bigg(&\frac{1}{m_e(1-\xi)^2}\left(\mathrm{Ei}(\frac{-c_k}{\xi}) - e^{-c_k}\mathrm{Ei}(\frac{-k}{m_e})\right) \\ &+ \frac{e^{-c_k/\xi}}{k(1-\xi)} + \frac{c_k}{\xi}\mathrm{Ei}(\frac{-k}{m_e})e^{-c_k}\Bigg). \end{aligned} \tag{35}$$

One can similarly take the second derivative of $\bar{R}_s^{LB}$ to see the ESR is a concave function of ξ in the feasible set $0 \leq \xi \leq 1$, where we omit the expressions due to space limitations. Moreover, by evaluating of the limits $\ell_0 = \lim_{\xi\to 0} \partial\bar{R}_s^{LB}/\partial\xi$ and $\ell_1 = \lim_{\xi\to 1} \partial\bar{R}_s^{LB}/\partial\xi$ via utilizing L'Hôpital's rule, one can easily infer that $\ell_0 > 0$ and $\ell_1 < 0$, hence a unique globally optimal point of ξ exists. This fact is also validated in our simulation results in Section V. Therefore, with the aim of maximizing the ESR in (31), it suffices to invoke (32) and solve $\frac{\partial\bar{R}_s^{LB}}{\partial\xi} = 0$. Toward this end, the well-known and easy-to-implement bisection approach is used in this paper [27]. The required algorithm for solving our proposed OPA problem is summarized in Algorithm 1, where ϵ is the tolerable error for solving the OPA.

Remark 6: In this subsection, we solved the OPA problem in an ergodic point of view by maximizing the ESR. This viewpoint has an advantage that the optimized value ξ^* for power splitting ratio only depends on the publicly-shared or fixed values of the network, such as transmit powers and channel variances [12]. Therefore, it is not required for the IoT nodes to frequently conduct the OPA, and whenever these public parameters are changed, e.g., altering the nodes' positions, the OPA is replayed for the network.

Remark 7: Based on the proposed scheme which has been introduced and analyzed from the security perspective, one can easily deduce that the proposed method utilizes lightweight security protocols. More specifically: i) In the training phase, the intrinsic fluctuations of wireless channel was the only source of common randomness utilized for SKG process, where the details for the complexity of physical layer SKG were provided in Table I. We also note that the resource and energy consumption of the key generation process can be decreased by optimally designing its stages. Therefore, key generation is highly recommended for IoT devices which are under the constraint of computational capability and battery power [10], and ii) In the message transmission phase, we utilized the easy-to-implement with low complexity AN injection method for the single-antenna legitimate entities, i.e., we didn't exploit any multiple-antenna beamforming methods, nor any intermediate helper node. This fact significantly reduces the implementation costs and the signaling overhead.

Algorithm 1 Optimizing the value of power splitting ratio ξ

procedure BISECTION($\bar{R}_s^{LB}$,ϵ)
  Set initial values of $0 < \xi^-, \xi^+ \leq 1$ such that $\left(\partial\bar{R}_s^{LB}(\xi^-)/\partial\xi\right)\left(\partial\bar{R}_s^{LB}(\xi^+)/\partial\xi\right) < 0$.
  Set $\xi^* \leftarrow (\xi^- + \xi^+)/2$.
  Compute $\partial\bar{R}_s^{LB}(\xi^*)/\partial\xi$ by substituting (33), (34), and (35) into (32).
  if $\partial\bar{R}_s^{LB}(\xi^*)/\partial\xi < 0$ **then**
    Set $\xi^- \leftarrow \xi^*$.
  else
    Set $\xi^+ \leftarrow \xi^*$.
  while $|\xi^+ - \xi^-| > \epsilon$ **do**
    Repeat 3 to 7.

V. Numerical Results and Discussions

In this section, we present several numerical examples to investigate our obtained closed-form expressions for the SKR and ESR metrics. Moreover, some related benchmarks are compared with our proposed scheme to show the efficiency of our scheme. The impact of HJ node on the performance of the proposed scheme and some insights on design parameters are also provided. The results for the proposed OPA problem are also validated in this section. For simulations, we consider a normalized two-dimensional region by placing the nodes D_1, D_2, Eve, and the HJ on positions $(-1,0)$, $(+1,0)$, $(1,+0.5)$, and $(0.0.5)$ respectively [45], [15]. In general, the variance δ_{12}^2 of wireless channel between nodes $\mathcal{N}_1$ and $\mathcal{N}_2$, is considered to be proportional to d_{12}^{-n}, where d_{12} is the distance between the nodes and n is the path loss exponent [45]. The numerical results of this section are obtained using Monte Carlo simulation over 10^5 realizations in MATLAB as the simulation tool. The distance-dependent path loss exponent is set to $n = 2.5$ and the noise power spectral density is considered to be $N_0 = 10^{-4}$. The total transmit power budgets $P^\tau = P_1^\tau + P_2^\tau$ and $P^\mu = P_2^\mu + P_1^\mu$ are evenly allocated to D_1 and D_2 in the training phase and message transmission phase, respectively. We further examine the OPA between AN and message signal by investigating the expressions obtained in Subsection IV-C. In this section, the number of Eve's antennas and the number of jammed sub-channels are set to $M = 4$ and $N_j = 40$, respectively. For Figs. 3–5 and 7, we set the

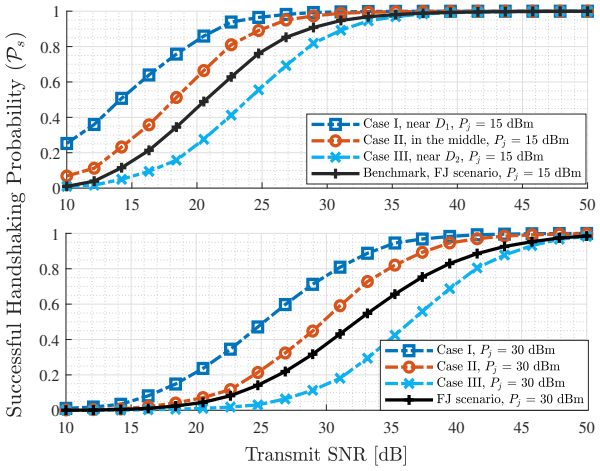

Fig. 3. Probability of successful handshaking vs. transmit SNR.

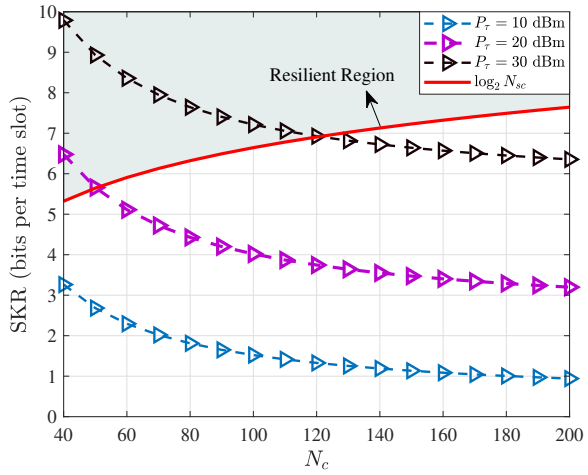

Fig. 4. Secret key rate vs. total number of used sub-channels.

number of HJ's antennas to be $A_J = 4$. For Figs. 3 and 5–7, we consider the total number of sub-channels $N_c = 128$. The power of the HJ is set to have the value of $P_j = 20$ dBm for Figs. 4, 5, and 7. Moreover, we consider $\xi = 0.5$ for the power splitting ratio in Figs. 3–6. The optimal value for ξ is examined in Fig. 7.

Fig. 3 depicts the probability of successful handshaking $\mathcal{P}_s$ with respect to the transmit SNR $\frac{P_1^\tau}{N_0}$ of the training phase for two levels of HJ's transmit power, i.e., $\frac{P_j}{N_0} = 15$ dB and $\frac{P_j}{N_0} = 30$ dB. It is clear from the figure that increasing the transmit SNR increases the probability of having a successful training phase. This can be easily concluded from (21). Moreover, based on the concepts presented in Remark 5, we can conclude that increasing the achievable SKR via enlarging the training power budget results in having a resilient handshaking procedure against active adversary. Furthermore, we can deduce from the figure that when the proposed system faces with an increase in the HJ's power, the D2D devices must increase their transmit power to have a successful transmission against the HJ. In this experiment, the effect of HJ's position on the resiliency of the proposed scheme is also examined by considering three cases: Case I, where the HJ is located in (normalized) position $(-1, 0.5)$ near D_1 (which is trying to have a resilient communication toward D_2), Case II, where the HJ is located in position $(0, 0.5)$, and Case III, where the HJ is located in position $(+1, 0.5)$ near the receiving node D_2. It is seen that the HJ is more destructive when it is near the receiving node. As another benchmark, we investigate the resiliency of our proposed scheme when the HJ is powerful enough to fully jam (FJ) all available sub-channels [20]. This special case can be easily analyzed by substituting $N_j = N_c$, taking the first term of (7), and finally, substituting the resultant R_{key} into (21). For this benchmark, the HJ is located in position $(0.0.5)$ and the benchmark shows that changing the location of HJ toward the receiving legitimate node is more effective than the FJ scenario. This is because in the FJ case, the power of HJ is reduced over each individual sub-channel.

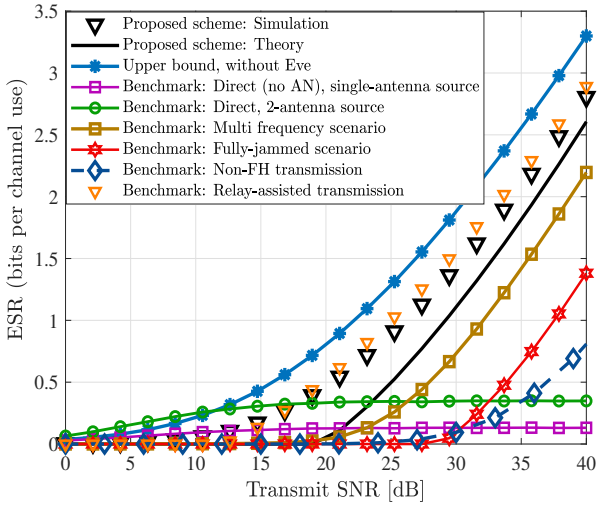

Fig. 5. Ergodic secrecy rate vs. transmit SNR.

Figure 4 shows the SKR (obtained in (7)) vs the total number of used sub-channels N_c for three different levels of training power. It is clear from the figure that increasing N_c reduces the achievable SKR. This observation is based on the jamming-resiliency condition discussed in Subsection IV-A, where an increase in the number of sub-channels makes the resiliency of the system challenging as the right side of (22) increases. However, the saturation in the figure implies that it is not mandatory to design a system with a large number of available sub-channels. Moreover, the red solid line depicts the boundary line above which the resiliency condition of (22) is satisfied. From the implementation view-point, as a conclusion from Fig. 4, a system designer can save the allocated frequency bandwidth, and also decrease some design costs, such as switches needed for altering the used sub-channel, by choosing an appropriate N_c. In other words, a suitable value for N_c can be found for different values of training power of D2D nodes, such that the resiliency is maintained in the system. For instance, when $P^\tau = 20$ dBm (or 100 mW), the appropriate

value for N_c is $N_j \leq N_c \leq 45$.

Fig. 5 illustrates the ESR vs the transmit SNR of message transmission phase $\frac{P_1^\mu}{N_0}$ which measures the confidential message transmission rate. In this figure, our analytic closed-form expression for the ESR derived in Subsection IV-B is depicted and it coincides with simulation results. In Fig. 5, we also compare our proposed resilient scheme with some state-of-the-arts:

1) An upper bound for the ESR is provided, in which there is no malicious Eve in the system [27]. In this case, D_2 is not obliged to inject jamming signal, thus, all the transmission power budget is utilized for transmitting the confidential message. Nevertheless, the proposed FH-based scheme is still utilized to combat jamming attack.
2) The traditional direct transmission (DT) scheme [16], where although the Eve exists in the network, the AN injection scheme is not employed. As depicted in Fig. 5, the performance of DT scheme is seriously poor. This is because the Eve can obtain a high-quality version of the message-bearing signal as there is no AN signal to confuse it. We also compare our proposed model with a DT scheme, where D_1 aims to exploit spatial diversity by two transmitting antennas. In this case, D_1 applies MRT beamforming to improve the quality of the legitimate link. However, we can see that the ESR of our proposed model is superior to that of the DT scheme, because of employing AN injection to degrade the Eve's receiving information signal. Moreover, a ceiling in the ESR of the DT scheme can be observed. This is because by increasing the transmit power, the quality of the received signal at both the legitimate receiver D_2 and Eve increases.
3) The multi-frequency (MF) transmission scheme [48], where the same message signal is conveyed over several (here we choose 60) sub-channels. The goal of this approach is to safely transport at least one message-bearing signal over a sub-channel, such that the message is not corrupted by the jamming. Our simulation result shows that the proposed FH-base scheme outperforms the MF transmission scheme. Besides, in order to establish such a multi hopping scheme, more bits must be dedicated to address the sequence of FH pattern. This fact may limit the performance of the system.
4) The fully-jammed (FJ) scenario [20], where $N_j = N_c$; It is obvious from the figure that a non-zero secrecy rate can still be achieved by our proposed FH-based scheme, even in the presence of a powerful HJ. Nonetheless, the ESR would become less than the partially-jammed case. The closed-form analytical expression for the ESR of this special case can be straightly obtained by substituting $N_j = N_c$ in (25) and taking the second term of it, and then put the resulting expression into (24).
5) A non-hopping transmission scheme was presented in [35], where the authors considered the whole transmission to be established on a fixed carrier frequency. Simulation result shows that the mentioned scheme starts to have a non-zero secrecy rate from the SNRs about 25 dB. In contrary, our proposed scheme which utilizes multi sub-channels, has a non-zero secrecy rate even with a very low transmit power. This implies the efficiency of our scheme, which has satisfying secrecy capacity without inquiring huge amount of transmit power.
6) The relay-assisted secure transmission, where an untrusted intermediate node amplifies and forwards the message-bearing signal to D_2. In this scenario, a relay is located in (0,0) to help conveying message from D_1 to D_2, while the AN is injected from D_2 to confuse both the untrusted relay and Eve. The resultant ESR in Fig. 5 shows that the relay-assisted scenario obtains slightly better secrecy performance compared with our proposed scheme. However, our proposed D2D scenario has a low-complexity deployment without any need for a helper node. Besides, the relay-assisted scenario has some drawbacks, including synchronization between the relay and D2D devices. In addition, the channel estimation and the procedure of sharing the estimated CSIs among legitimate nodes have some challenges in relay-based transmissions [15].

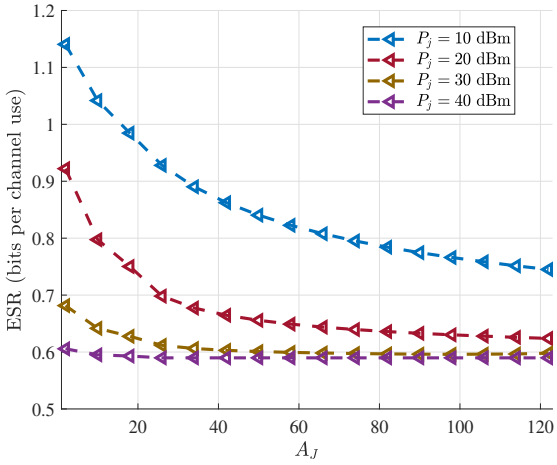

Fig. 6. Ergodic secrecy rate vs. number of jammer's antennas.

Fig. 6 depicts the ESR with respect to the total number of HJ's antennas for different levels of jamming power P_j. In this figure, the transmit power of message phase is considered $P_1^\mu = P_2^\mu = 20$ dBm. It is clear from the figure that increasing A_J results in decreasing the ESR performance of the system. The saturation which is seen in the figure can be inferred by invoking Eqs. (27) and (28), where by tending A_J to infinity results in (27) to become zero. Moreover, analogous to the results in Fig. 3, we see that the HJ can decrease the performance of the network in terms of the ESR by enlarging its jamming power.

The result of the OPA problem is plotted in Fig. 7 for different distances d_{12} between the D2D nodes and $P_1^\mu = P_2^\mu = 30$ dBm. In this figure, all the nodes are fixed, except D_1 which moves from position $(-1, 0)$ toward D_2 located in $(+1, 0)$. The figure shows that higher ESR can be achieved when the D2D nodes are closer to each other. This is because the D_1-to-D_2 link will have higher quality when the nodes are near each

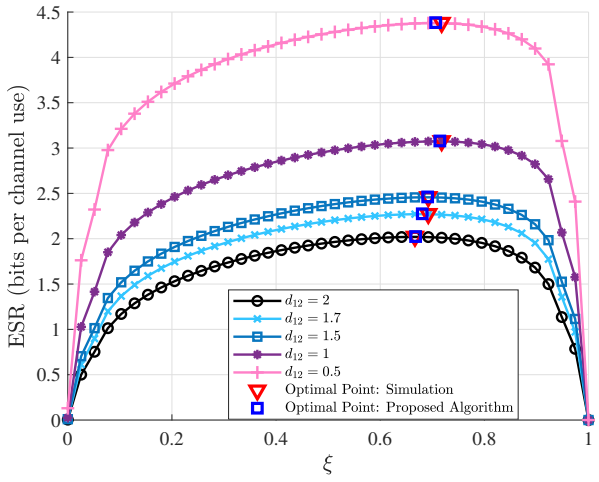

Fig. 7. Ergodic secrecy rate vs. power splitting ratio.

other. Additionally, the figure implies that by having the D2D nodes closer to each other, the optimal value for the power splitting ratio ξ tends to larger values. Because, the D2D link is high-quality enough; thus, the need for injecting AN signal to confuse the Eve decreases. Finally, Fig. 7 validates the optimality of the proposed bisection algorithm in Subsection IV-C. It can be seen from this figure that the optimal values of ξ^* (depicted by blue square) are well matched with the optimal points obtained from the exhaustive search result (the red triangles).

VI. Conclusion and Future Directions

In this paper, we proposed a lightweight jamming-resistance and anti-eavesdropping scheme for IoT communication. In our system model, a single-antenna transmitter communicates with a half-duplex single-antenna receiver in the presence of a multiple-antenna-aided passive Eve and a multiple-antenna HJ. The simple AN injection scheme was adopted to ensure secure transmission, while the physical layer SKG procedure was proposed for ensuring resiliency against jamming attack. For such a network structure, we obtained a new closed-form expression for the SKR to indicate the FH rate, and the ESR to highlight the secrecy efficiency of our proposed scheme. Moreover, an OPA with the aim of maximizing the secrecy rate was designed and solved. Eventually, numerical examples were provided to gain engineering insights behind the proposed communication scenario. Some of the future research directions which can be investigated are as follows:

- *Mobile Adversary in the Network:* Such adversary can explore spatial diversity techniques to boost its SINR. Besides, it could get closer to the target node to improve its data decoding chance. Accordingly, further investigations are required to establish the robustness of current security schemes against this type of adversaries.
- *Real Deployment Scenarios:* Providing experimental testbeds and open-source code could help the community to verify research findings. Moreover, the interpretation from simulation to experimental validation could help fine-tune the theoretical models and highlights technical challenges, such as network synchronization and interference cancellation.
- *Data Security Trust Mechanisms:* To maintain data security, trustworthiness of network nodes could be taken into account. The idea of the trust-based network mechanism is to assign trust evaluation values to different nodes. For example, if a node has an unusual data forwarding behavior, its trust degree should be reduced [2]–[4].

Appendix A

Based on (19), we derive the successful handshaking probability as

$$\begin{aligned}\mathcal{P}_s^{(UA)}(R_{key},\gamma_{th}) &= Pr\Big\{\frac{\rho|h_{12}|^2}{\frac{\rho_j}{N_\mathcal{K}}|h_{j2}|^2\mathcal{I}+\frac{1}{L_\mathcal{K}}}>\gamma_{th}\Big\}\\ &= Pr\left\{|h_{12}|^2>\frac{\gamma_{th}}{\rho}\Big(\frac{\rho_j}{N_\mathcal{K}}|h_{j2}|^2\mathcal{I}+\frac{1}{L_\mathcal{K}}\Big)\right\}\\ &\overset{(a)}{=}\int_0^\infty \exp\left(-\frac{\gamma_{th}}{\rho\delta_{12}^2}\Big(\frac{\rho_j}{N_\mathcal{K}}|h_{j2}|^2\mathcal{I}+\frac{1}{L_\mathcal{K}}\Big)\right)\\ &\times\frac{1}{\delta_{j2}^2}\exp\Big(-\frac{x}{\delta_{j2}^2}\Big)dx\\ &=\frac{\exp(-\gamma_{th}/\rho\delta_{12}^2L_\mathcal{K})}{1+\rho_j\delta_{j2}^2\gamma_{th}\mathcal{I}/\rho\delta_{12}^2N_\mathcal{K}},\end{aligned}\tag{36}$$

where (a) follows from the fact that $|h_{12}|^2\sim\exp(\delta_{12}^2)$ and $|h_{j2}|^2\sim\exp(\delta_{j2}^2)$. Consequently, based on the concepts of the multiple access interference (MAI) investigated in [49], the value of $\mathcal{I}$ can be approximated by $1+\frac{2^{R_{key}}-2}{3L_\mathcal{K}}$. Substituting this approximation into (36), a tight and efficient approximation for $\mathcal{P}_s^{(UA)}(R_{key},\gamma_{th})$ is obtained, and the proof is completed.

Appendix B

The ergodic legitimate rate R_L can be calculated as follows.

$$R_\mathsf{L}=\frac{\mathcal{F}_1}{2\ln 2}=\frac{1}{2\ln 2}\mathbb{E}\big\{\ln(1+\gamma_{D_2})\,\big|\,\mathbf{s}\big\}.\tag{37}$$

Conditioned on the jamming state vector $\mathbf{s}$, one can calculate the ergodic legitimate rate in (37) as[11]

$$R_\mathsf{L}=\frac{1}{2\ln 2}\left[(1-\frac{N_j}{N_c})\mathcal{F}_{1|s=0}+\frac{N_j}{N_c}\mathcal{F}_{1|s=1}\right],\tag{38}$$

where

$$\begin{aligned}\mathcal{F}_{1|s=0}&\triangleq\mathbb{E}_{\gamma_{D_2|s=0}}\big\{\ln(1+\gamma_{D_2})\,\big|\,\mathbf{s}=0\big\}\\ &\overset{(a)}{\geq}\ln\Big(1+\exp(\mathcal{F}_{1n0}-\mathcal{F}_{1d0})\Big),\end{aligned}\tag{39}$$

[11]To analyze the secrecy performance, one can derive the ESR following a unified approach by considering a Bernoulli-distributed RV, which indicates whether there is interference in the system or not. Inspired by this, we utilize the following approach for analyzing the ESR, which provides useful insights about the scenarios of jamming-experienced and jamming-free communication links. This approach also facilitates the analysis for the case where a powerful HJ jams all $N_j=N_c$ sub-channels.

where

$$\begin{aligned}\mathcal{F}_{1n0} &= \mathbb{E}\big\{\ln(\xi\gamma_{12}\gamma_{21})\big\}\\ &\overset{(b)}{=} \ln(\xi)+\ln(\rho_1\delta_{12}^2)+\ln(\rho_2\delta_{12}^2)-2\Phi, \qquad (40)\\ \mathcal{F}_{1d0} &= \mathbb{E}\Big\{\ln\Big(\big(\rho_2+(1-\xi)\rho_1\big)|h_{12}|^2+(1-\xi)\rho_1\rho_2\\ &\quad\times\big|\, h_{12}^2-(\hat{h}_{12}^{D_2})^2\,\big|^2\Big)\Big\}\\ &\overset{(c)}{\le} \ln\Big\{\big(\rho_2+(1-\xi)\rho_1\big)\delta_{12}^2+2(1-\xi)\rho_1\rho_2\\ &\quad\times\hat{\sigma}_{\mathcal{E}_2|s=0}^2(2\delta_{12}^2+\hat{\sigma}_{\mathcal{E}_2|s=0}^2)\Big\}, \qquad (41)\end{aligned}$$

where (a) and (c) follow from using Jensen's inequality[12] on the convex function $\ln(1+\exp(x))$ and the concave function $\ln(x)$, respectively, and (b) follows from using [51, Eq. (4.331.1)] and the fact that $|h_{12}|^2$ has exponential distribution with mean δ_{12}^2. We also remark that $\hat{h}_{12}^{D_2}$ and $\hat{\sigma}_{\mathcal{E}_2}^2$ can be obtained from (3) and (4), based on the channel estimation in the training phase. Analogously, we have

$$\begin{aligned}\mathcal{F}_{1|s=1} &\triangleq \mathbb{E}_{\gamma_{D_2}|s=1}\big\{\ln(1+\gamma_{D_2})\;\big|\;\mathbf{s}=1\big\}\\ &\ge \ln\Big(1+\exp(\mathcal{F}_{1n1}-\mathcal{F}_{1d1})\Big), \qquad (42)\end{aligned}$$

where

$$\begin{aligned}\mathcal{F}_{1n1} &= \mathbb{E}\Big\{\ln\big(\xi\gamma_{12}\big)\Big\}+\underbrace{\mathbb{E}\Big\{\ln\big(\gamma_{21}+\gamma_{j1}\big)\Big\}}_{\mathcal{T}}\\ &= \ln(\xi)+\ln(\rho_1\delta_{12}^2)-\Phi+\mathcal{T}, \qquad (43)\end{aligned}$$

where $\mathcal{T}$ is given in Appendix C. Using the same procedure as used in (41), we can rewrite

$$\begin{aligned}\mathcal{F}_{1d1} \le \ln\Big\{&(1-\xi)\rho_1\delta_{12}^2(A_J-1)\rho_j\delta_{j1}^2+(A_J-1)\rho_j\delta_{j2}^2\\ &\times(\rho_2\delta_{12}^2+(A_J-1)\rho_j\delta_{j1}^2)+2(1-\xi)\rho_1\rho_2\hat{\sigma}_{\mathcal{E}_2|s=1}^2\\ &\times(2\delta_{12}^2+\hat{\sigma}_{\mathcal{E}_2|s=1}^2)\Big\}. \qquad (44)\end{aligned}$$

Substituting (40) and (41) into (39) results in (26), and substituting (43) and (44) into (42) gives (27).

APPENDIX C

To obtain the expression for $\mathcal{T}=\mathbb{E}\{\ln(X+Y)\}$, with $X\triangleq\gamma_{21}$ and $Y\triangleq\gamma_{j1}$, first note that X is an exponentially distributed RV with mean $m_x=\rho_2\delta_{12}^2$ and Y is a summation of A_J-1 independent and identically distributed (i.i.d) exponential RVs each with mean $m_y=\rho_j\delta_{j1}^2$; thus, the pdf of Y is given by [50]

$$f_Y(y)=\frac{\lambda_y^{A_J-1}}{\Gamma(A_J-1)}e^{-\lambda_y y}y^{A_J-2}, \qquad (45)$$

where $\lambda_y=1/m_y$ and $\Gamma(\cdot)$ is the gamma function [51, Eq. (8.339)]. Accordingly, by defining $Z\triangleq X+Y$, the pdf of Z can be obtained, using the concept of convolution as follows

$$\begin{aligned}f_Z(z) &= \int_0^z f_X(x)f_Y(z-x)dx\\ &\overset{(a)}{=} \frac{\lambda_x}{(1-\frac{\lambda_x}{\lambda_y})^{A_J-1}}e^{-z\lambda_x}\frac{\gamma(A_J-1,-z(\lambda_x-\lambda_y))}{\Gamma(A_J-1)}\\ &\overset{(b)}{=} \frac{\lambda_x}{(1-\frac{\lambda_x}{\lambda_y})^{A_J-1}}\Big[e^{-\lambda_x z}-e^{-\lambda_y z}\sum_{m=0}^{A_J-2}(\lambda_y-\lambda_x)^m\frac{z^m}{m!}\Big], \qquad (46)\end{aligned}$$

where $\lambda_x=1/m_x$, (a) is obtained from [51, Eq. (3.382.1)], $\gamma(\alpha,\beta)$ is the lower incomplete gamma function [51, Eq. (8.35)] and (b) follows by utilizing the series representation for the incomplete gamma function.

Ultimately, the expression for $\mathcal{T}$ is calculated by the following steps

$$\mathcal{T}=\mathbb{E}\{\ln Z\}\overset{(a)}{=}\frac{\lambda_x}{(1-\frac{\lambda_x}{\lambda_y})^{A_J-1}}\Big(\mathcal{A}+\mathcal{B}\Big), \qquad (47)$$

where $\mathcal{A}=\frac{-(\Phi+\ln\lambda_x)}{\lambda_x}$, $\mathcal{B}=\sum_{m=0}^{A_J-2}(1-\frac{\lambda_x}{\lambda_y})^m\frac{(\ln\lambda_y-\psi(m+1))}{\lambda_y}$, and (a) follows by using [51, Eqs. (4.331.1) and (4.352.1)].

APPENDIX D

The ergodic eavesdropping rate R_{E} of our proposed scheme can be formulated as

$$R_{\mathsf{E}}=\frac{\mathcal{F}_2}{2\ln 2}, \qquad (48)$$

where $\mathcal{F}_2$ is given by

$$\mathcal{F}_2=\mathbb{E}\big\{\ln(1+\gamma_E)\big\}. \qquad (49)$$

By defining $W\triangleq\gamma_E=\max_{1\le i\le M}\gamma_{E_i}$, we can rewrite $\mathcal{F}_2$ as

$$\mathcal{F}_2=\int_0^\infty\ln(1+w)f_W(w)dw. \qquad (50)$$

In order to obtain the closed-form expression for $\mathcal{F}_2$, we first calculate the pdf of W. We remark that γ_{E_i}, for $i\in\{1,\cdots,M\}$ has the following CDF, which can be easily obtained using (15) and examining the definition of CDF for an RV.

$$F_{\gamma_{Ei}}(w)=1-\exp\big(\frac{-1}{m_e}(\frac{w}{\xi-w(1-\xi)})\big). \qquad (51)$$

Then, by invoking (15), we note that the instantaneous SINRs obtained by the antennas of Eve are independent from each other. Therefore, we have

$$F_W(w)=\prod_{i=1}^M F_{\gamma_{Ei}}(w)=\sum_{k=0}^M(-1)^k\binom{M}{k}\exp\big(\frac{-kw/m_e}{\xi-w(1-\xi)}\big). \qquad (52)$$

By taking the derivative of (52) with respect to w, the pdf of $f_W(w)$ is obtained, and the integral in (50) reduces to

$$\mathcal{F}_2=\frac{\xi}{m_e}\sum_{k=0}^M p_k\mathcal{I}_k, \qquad (53)$$

[12]As discussed in [45], the Jensen's inequality is sufficiently tight and hence, leads to a tight lower bound expression for the ESR performance. As will be observed in the simulations, the obtained closed-form expression for the ESR matches well with the exact one.

where p_k is defined in (29) and

$$\mathcal{I}_k = \int_0^{\frac{\xi}{1-\xi}} \frac{\ln(1+w)}{(\xi-(1-\xi)w)^2} \exp\big(\frac{-kw/m_e}{\xi-w(1-\xi)}\big)dw. \quad (54)$$

By changing the variable $v = (\xi-(1-\xi)w)^{-1}$ and simultaneously using integration by parts, through some straightforward manipulations, the integral of $\mathcal{I}_k$ also reduces to the following

$$\mathcal{I}_k = \frac{e^{c_k/\xi}}{c_k(1-\xi)}\left(e^{-c_k}\mathrm{Ei}(\frac{-c_k}{\xi}) - \mathrm{Ei}(\frac{-k}{m_e})\right). \quad (55)$$

Substituting (55) into (53) completes the proof.

ACKNOWLEDGEMENTS

The authors would like to thank Prof. Lajos Hanzo for constructive comments and discussions to improve the paper. The authors would also like to thank Dr. Hamid Behroozi and Dr. Derrick Wing Kwan Ng for their indispensable comments and collaboration which led to our joint prior works.

REFERENCES

[1] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet of Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[2] Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, "A trust-based minimum cost and quality aware data collection scheme in P2P network," *Peer-to-Peer Netw. Appl.*, pp. 1–24, Mar. 2020.

[3] T. Li, W. Liu, T. Wang, Z. Ming, X. Li, and M. Ma, "Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things," *Trans. Emerging. Tel. Tech.*, pp. 1–24, Jan. 2020.

[4] B. Jiang, G. Huang, T. Wang, J. Gui, and X. Zhu, "Trust based energy efficient data collection with unmanned aerial vehicle in edge network," *Trans Emerging Tel Tech*, pp. 1–32, Feb. 2020.

[5] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[6] J. Zhang, T. Q. Duong, R. F. Woods, and A. J. Marshall, "Securing wireless communications of the Internet of Things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, p. 1–16, Aug. 2017.

[7] L. Sun, Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 1–21, Sep. 2018.

[8] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.

[9] H. Shakhatreh, *et al.*, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, Apr. 2019.

[10] J. Zhang, G. Li, A. Marshall, A. Hu and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406–138446, Jul. 2020.

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

[12] B. He, Y. She and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, Oct. 2017.

[13] W. Wang, K. C. Teh and K. H. Li, "Relay selection for secure successive AF relaying networks with untrusted nodes," *IEEE Trans, Inf. Forensics Security*, vol. 11, no. 11, pp. 2466–2476, Nov. 2016.

[14] A. Kuhestani, A. Mohammadi and P. L. Yeoh, "Security-reliability trade-off in cyber-physical cooperative systems with non-ideal untrusted relaying," *IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 552–557.

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

[16] A. Kuhestani, A. Mohammadi, and M. Mohammadi "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol 13, no. 2, pp. 341–355, Feb. 2018.

[17] M. Letafati, A. Kuhestani, D. W. K. Ng, and H. Behroozi, "A new frequency hopping-aided secure communication in the presence of an adversary jammer and an untrusted relay," *IEEE ICC'20 Workshop*, Dublin, Ireland, Jun. 2020.

[18] C. E. Shannon, Communication Theory of Secrecy Systems, *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[19] T. Li, T. Song, Y. Liang, *Wireless Communications under Hostile Jamming: Security and Efficiency*, 1st ed. Singapore: Springer, 2018.

[20] S. Sciancalepore, and R. Di Pietro, "Bittransfer: Mitigating reactive jamming in electronic warfare scenarios," *IEEE Access*, vol. 7, pp. 156175–156190, 2019.

[21] D.-K. Jeong, J.-H. Wui, and D. Kim, "Random access performance of distributed sensors attacked by unknown jammers," *Sensors*, vol. 17, no. 11, p. 1–17, Nov. 2017.

[22] N. Namvar, W. Saad, N. Bahadori and B. Kelley, "Jamming in the Internet of Things: A game-theoretic perspective," *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–6.

[23] B. Sherlock, J. A. Neasham and C. C. Tsimenidis, "Spread-spectrum techniques for bio-friendly underwater acoustic communications," *IEEE Access*, vol. 6, pp. 4506–4520, Jan. 2018.

[24] D. Torrieri, S. Talarico and M. C. Valenti, "Analysis of a frequency-hopping millimeter-wave cellular uplink," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 7089–7098, Oct. 2016.

[25] G. Chang, J. Huang and Z. Wu, "A frequency hopping algorithm against jamming attacks under asynchronous environments," *2014 IEEE Global Commun. Conf.*, Austin, TX, 2014, pp. 324–329.

[26] Q. Wang, H. Zhang, Q. Lyu, X. Wang, and J. Bao, "A Novel physical channel characteristics-based channel hopping scheme for jamming-resistant in wireless communication," *International Journal of Network Security (IJNS)*, vol. 20, no. 3, pp. 439–446, May. 2018.

[27] C.-Y. Liu, Y.-P. Hong, P.-H. Lin, and E.-A. Jorswieck, "Jamming-resistant frequency hopping system with secret key generation from channel observations," *2016 IEEE Inf. Theory Workshop (ITW)*, Cambridge, 2016, pp. 46–50.

[28] P. Jay, C. Liu, J. Lee, and T. Q. S. Quek, "Self-controlled jamming resilient design using physical layer secret key," submitted to *IEEE Trans. Inf. Foren. Sec.*, arXiv:1803.07358v1, 2019.

[29] W. Lai, Y. Wang, H. Lin and J. Li, "Efficient resource allocation and power control for LTE-A D2D communication with pure D2D model," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3202–3216, Mar. 2020

[30] Z. Dou, G. Si, Y. Lin and M. Wang, "An adaptive resource allocation model with anti-jamming in IoT network," *IEEE Access*, vol. 7, pp. 93250–93258, 2019.

[31] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[32] W. Guo, H. Zhao and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 240–243, Feb. 2020.

[33] X. Tang, P. Ren and Z. Han, "Jamming mitigation via hierarchical security game for IoT communications," *IEEE Access*, vol. 6, pp. 5766–5779, Jan. 2018.

[34] N. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan and D. B. da Costa, "Full-Duplex cyber-weapon with massive arrays," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5544–5558, Dec. 2017.

[35] H. Saedi, A. Mohammadi, and A. Kuhestani, "Characterization of untrusted relaying networks in the presence of an adversary jammer", *Wireless Networks*, Jun. 2019.

[36] S. Li, Q. Ni, Y. Sun, G. Min and S. Al-Rubaye, "Energy-efficient resource allocation for industrial cyber-Physical IoT systems in 5G era," *IEEE Trans. Industr. Inform.*, vol. 14, no. 6, pp. 2618–2628, Jun. 2018.

[37] J. P. S. Sundaram, W. Du and Z. Zhao, "A survey on LoRa networking: Research problems, current solutions, and open issues," *IEEE Commun, Surv. Tutor.*, vol. 22, no. 1, pp. 371–388, Oct. 2020.

[38] W. Xu, S. Jha and W. Hu, "LoRa-key: Secure key generation system for LoRa-based network," *IEEE Internet of Things J.*, vol. 6, no. 4, pp. 6404–6416, Aug. 2019.

[39] T. Song, Y. Liang and T. Li, "Physical layer security of multiband communications under hostile jamming," *International Conference on Computing, Networking and Communications (ICNC)*, Santa Clara, CA, 2017, pp. 346–350.

[40] T. Jiang, Y. Shi, J. Zhang, and K. B. Letaief, "Joint activity detection and channel estimation for IoT networks: Phase transition and computation-estimation trade-off," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6212–6225, Aug. 2019.

[41] T. Kim and S. H. Chae, "A channel estimator via non-orthogonal pilot signals for uplink cellular IoT," *IEEE Access*, vol. 7, pp. 53419–53428, Apr. 2019.

[42] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

[43] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[44] C. T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, and C. Paar, "Authenticated key establishment for low-resource devices exploiting correlated random channels." *Comput. Netw.*, vol. 109, pp. 105–123, Nov. 2016.

[45] L. Sun, T. Zhang, Y. Li and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[46] W. Wang, S. L. Capitaneanu, D. Marinca and E. Lohan, "Comparative analysis of channel models for industrial IoT wireless communication," *IEEE Access*, vol. 7, pp. 91627–91640, Aug. 2019.

[47] P. Silva, V. Kaseva, and E. S. Lohan, "Wireless positioning in IoT: A look at current and future trends," *Sensors*, vol. 18, pp. 2470, Jul. 2018.

[48] J. Wan, D. Zhang, W. Xu, and Q. Guo, "Parameter estimation of multi frequency hopping signals based on space-time-frequency distribution", *Symmetry 2019*, vol. 11, no. 648, May. 2019.

[49] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.

[50] M. K. Simon and M.-S. Alouini, *Digital Communications over Fading Channels: A Unified Approach to Performance Analysis*. John Wiley, Inc., 2004.

[51] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York: Academic, 2007.