IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 16, 2017, accepted October 24, 2017, date of publication November 1, 2017, date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2768508

Securing Untrusted RF-EH Relay Networks Using Cooperative Jamming Signals

AHMED EL SHAFIE[1], (Member, IEEE), ASMA MABROUK[2], KAMEL TOURKI[3], (Senior Member, IEEE), NAOFAL AL-DHAHIR[1], (Fellow, IEEE), AND RIDHA HAMILA[4], (Senior Member, IEEE)

[1]Electrical Engineering Department, The University of Texas at Dallas, Richardson, TX 75080, USA
[2]HANA Research Laboratory, National School of Computer Sciences, Université de la Manouba, Manouba 2010, Tunisia
[3]Mathematical and Algorithmic Sciences Laboratory, France Research Center, Huawei Technologies France SASU, 92100 Huawei, France
[4]Department of Electrical Engineering, Qatar University, Doha, Qatar

Corresponding author: Ahmed El Shafie (ahmed.salahelshafie@gmail.com)

This work was supported by NPRP from the Qatar National Research Fund (a member of Qatar Foundation) under Grant 8-627-2-260. The statements made herein are solely the responsibility of the authors.

ABSTRACT We propose a new scheme to secure a wireless-powered untrusted cooperative-communication network, where a legitimate source node (Alice) transmits her information messages to a legitimate destination node (Bob) through the multiple amplify-and-forward untrusted relays. The relay nodes are assumed to be honest but curious nodes; hence, they are trusted at the service level but are untrusted at the information level. To reduce the energy consumption of the network, only one relay node is selected in each time slot to forward Alice's information signal. We assume a power-splitting-based energy-harvesting scheme, where each relay node splits its received signal into information and energy streams. Since the relay nodes are assumed to be untrusted at the information level, they attempt to decode the information intended to Bob while harvesting energy at the same time. When the relaying mode is selected, the scheme is realized over two non-overlapping time phases. To prevent any information leakage to the untrusted relay nodes, Bob and a cooperative jammer (John) inject jamming (artificial noise) signals during the first phase. During the second phase, the untrusted relay nodes that will not be forwarding the information signal must harvest energy to accumulate more energy to help Alice in future time slots. Moreover, the cooperative jammer will jam the untrusted relays to further power their batteries and prevent them from decoding the information-forwarding relay signal in case they decided to cheat and decode it. We model the battery state transitions at each relay as a finite-state Markov chain and analyze it. Our numerical results show the security gains of our proposed scheme relative to two benchmark schemes.

INDEX TERMS Battery, energy harvesting, secrecy, untrusted relaying, relay selection.

I. INTRODUCTION

Radio frequency (RF) energy-harvesting (EH) schemes have gained increased interest recently as a promising solution to energize the battery-based wireless communication nodes in a wireless communication network [1]. Under the RF-EH paradigm, the wireless nodes convert the ambient RF transmissions into a direct current (DC) electricity. This prolongs their battery lifetimes with self-sufficient energy supply. Since RF transmissions can simultaneously carry both information and energy, an EH node is capable of decoding the information in a signal and converting a portion of that signal into energy. This motivates simultaneous wireless information and power transfer (SWIPT) [2].

The efficiency of RF-EH schemes is a function of many parameters including the network topology as mentioned in, e.g., [3] and the references therein. In particular, due to channel randomness, where the channel gain can be low for some times and high for other times, and its monotonically-decreasing behavior with distance, only wireless nodes that are relatively close to the transmitting nodes (e.g., base-stations or uplink users) can benefit from the energy carried over the RF transmissions. These wireless nodes do not only collect more wireless energy during the downlink (DL) phase but also use less transmit power during the uplink (UL) phase as well. In contrast, the nodes that are distant from the base-station will harvest less energy and will have to use more transmit powers during the uplink phases. Hence, it is necessary to have cooperative relay nodes in the middle between the base-station and the legitimate users to mitigate

the channel fading effects and increase both information transmission and energy transfer rates. SWIPT schemes provide new opportunities for wireless-powered cooperative communications (WPCC), where the relays (which can be other legitimate entities/users in the network) are able to cooperate with the source node more frequently since they do not use their own energies [4]. In this energy-efficient system design, the wireless relays are solely depending on the energy collected from the RF transmissions to aid the source nodes.

Using SWIPT schemes, the relay nodes divide their received signals into two distinct streams. A stream that will be passed to the EH circuitry and the other stream will be used for data processing and information forwarding. The two most efficient relaying schemes proposed in the SWIPT literature are: 1) the time-switching relaying (TSR) where the time is orthogonally-divided between EH and information-decoding tasks [5]; and 2) the power-splitting relaying (PSR) where the signal splitting is performed in the power domain using a power splitter [5]. Chen *et al.* [6] investigated the PSR scheme in the multiple-user multiple-relay systems. Nasir *et al.* [7] investigated the relay interference channels [7]. Since the amount of harvested energy in a single-transmission period is small, the performance of the relayed transmissions is low. Hence, extensive research efforts have been directed to developing the harvest-store-use (HSU) scheme. In particular, instead of using the entire energy harvested in one transmission cycle, the harvested energy is first accumulated and stored in a battery for a while and then adaptively used for information transmissions [8]–[10]. In the TSR scheme, the relay nodes switch between EH and information forwarding from one transmission cycle to another. Under HSU-WPC schemes, the EH nodes use several EH blocks to accumulate enough energy for information transmissions. Hence, the reliability and secrecy of WPCC are enhanced with the minimum energy consumption [11].

A. RELATED WORKS

Since the EH relays are solely powered by the energy of the RF transmissions, in WPCC networks, the relays may not always be ready to help since the energy harvested is often much smaller than that required for data transmissions. Hence, the HSU approach is a promising solution to stabilize the energy supply for information transmissions over time. Nasir *et al.* [8] considered energy accumulation for a two-hop system with one relay node, where the relay first stores energy in an infinite energy-storage battery and starts the information forwarding mode as soon as it harvests enough energy to transmit with a constant predetermined transmit power. Krikidis *et al.* [9] assumed a finite energy storage at the relay node and proposed a greedy-switching scheme where the relay node transmits when its residual energy ensures reliable decoding at the destination node. Hence, the reception reliability and energy consumption are simultaneously improved. In practice, a set of relays should be deployed between the source and its destination to enhance both reliability and security by introducing diversity to mitigate channel fading.

Relay-selection schemes enhance the energy-efficiency and system's performance by selecting the best relay (or set of relays) for information forwarding [12], [13]. When the relay nodes are equipped with energy-storage batteries, the design of relay-selection schemes in WPCC systems differs from conventional cooperative networks where all nodes have reliable power supplies. In fact, the relay-selection criteria must take into consideration both available energy at the relays and the required information rate. Therefore, battery-aware relay-selection (BARS) schemes were proposed in [14]–[16] to improve the reliability of the multi-relay WPCC networks by exploiting both channel state information (CSI) and battery state information (BSI) to make the relay-selection decisions. In the BARS schemes, the relay nodes with battery energy levels exceeding a predetermined threshold required for information transmission will first form a subset, since not all relays will have the same energy level, then feedback their CSI to the source node. Afterwards, the source node selects the best relay among the subset of candidate relays to forward its information signal to the destination node. While the selected relay node decodes the source information signal, the remaining relay nodes scavenge energy from the source signal. Krikidis [17] investigated various relay-selection schemes for WPCC systems with multiple randomly-distributed relay nodes. The EH relay nodes help the source's transmission only when their batteries are full. Liu [14] assumed that each relay node accumulates a minimum energy level to be a candidate for selection. Then, each of the candidate relay nodes sends its CSI. These works assume finite-size batteries at the EH relay nodes which switch between energy harvesting and information forwarding from one coherence time (i.e., transmission block) to another.

Although the broadcast nature of wireless channels helps in energy transfer to many nodes at the same time, wireless channels are vulnerable to eavesdropping attacks and, hence, the confidentiality of data transmissions can be compromised. This is because any node with an RF transceiver can overhear the ongoing communications in a wireless network and, possibly, determine the identity of the communicating nodes. Secure communications in multiple-input multiple-output (MIMO) SWIPT systems were investigated in [18] where the source node splits its transmit power to send confidential messages to the information receiver and an artificial noise (AN) signal to prevent the energy receivers from eavesdropping the information. In this context, most existing research work has focused on the use of cooperative jamming (CJ) schemes to secure the WPCC systems [19]–[23]. In [19]–[22], the jammers harvest energy from the source node and then use the harvested energy to perform CJ. In [24], the secrecy of an EH relay network is improved by using the

commonly-used destination-based jamming (DBJ) scheme where the destination node sends AN signals to confuse the eavesdropper. The generated AN signal by the destination also serves as a new source of RF energy to be harvested by the EH nodes [23].

Sun *et al.* [25] showed that CJ enables secure two-hop communications through an untrusted relay which could be otherwise not possible. Kalamkar and Banerjee investigated the security of the wireless-powered untrusted cooperative communication (WPUCC) where the relay nodes eavesdrop on the legitimate transmissions although they are cooperating in forwarding the source's information. The authors showed that the secrecy performance is improved when the relay node is located closer to the destination. A sufficient and necessary condition for obtaining a positive secrecy rate for an RF-EH untrusted cooperative PSR scheme was derived in [27]. Mabrouk *et al.* [28] proposed a scheme to secure relay-aided transmissions when the relay is untrusted and in the presence of alien eavesdropping attacks. Wang *et al.* [29] proposed a secure communication scheme for untrusted two-way relaying systems. Zhao *et al.* [30] proposed a joint power-splitting and secure beamforming design. It was shown in [31] that, if there is a direct link between the source and its destination, the deployment of untrusted relays in the network will be useless when the target secrecy rate is large.

Although the BARS schemes have been investigated widely in the non-eavesdropping scenarios, energy accumulation under a secrecy constraint has not been well-investigated yet. In most existing work, the HSU model is investigated where information relaying is performed when enough energy is accumulated through the time-switching scheme. Zhou *et al.* [10], Yuan *et al.* [32], and Liu *et al.* [33] investigated energy accumulation in PSR-based systems where information transmission and energy transfer are employed simultaneously. This approach is called the harvest-use-store (HUS) scheme. Unlike the HSU scheme, in the HUS scheme, the expenditure of the collected energy is prioritized by information transmission and the remaining harvested energy will be stored in the nodes' batteries for future use. Zhou *et al.* [10] proposed the HUS relaying strategy with distributed beamforming in wirelessly-powered multiple-relay scenarios. Liu *et al.* [33] investigated the HUS scheme in a full-duplex relay network where the relay switches between two rechargeable batteries for charging and discharging during two consecutive communication cycles. Mabrouk *et al.* [34] proposed a relay-selection scheme for untrusted-relay networks when the source node transmits a jamming signal that is previously shared with the destination node. The assumption of previously shared jamming/AN signals might not always be possible. Unlike [34], we propose a new secure scheme when the destination transmits a jamming signal and in the presence of a cooperative jammer that helps in both powering and jamming the untrusted EH-RF relay nodes.

B. CONTRIBUTIONS

Motivated by the above work, we propose a joint DBJ and CJ scheme to reduce the secrecy outage probability (SOP) of the WPUCC systems under untrusted relaying. Moreover, since the untrusted relays have batteries to accumulate the RF harvested energy, they will be able to better serve the source node in forwarding its data to the destination. The relay that maximizes the instantaneous secrecy rate is selected in each time slot. Bao and Cuu [35] investigate a distributed switch-and-stay combining technique to secure a dual-hop relay network where the destination switches to and stays with either the direct link or the relaying link. In [36], based on the CSI estimate, the source performs DL information transmission either directly or cooperatively with the relay. Apart from recovering some of the spectral loss inherent to half-duplex cooperative relaying, the proposed scheme reduces energy constraints on the relay nodes so as to increase their batteries' lifetimes.

We propose a new jamming-based scheme to secure the transmissions in wireless-powered untrusted relay networks. The proposed scheme exploits both the CSI of the wireless links and the energy-state information (ESI) of the relays' batteries. Our contributions are summarized as follows

- Considering the energy constraint at the untrusted relay nodes, we design a new scheme to secure the transmissions from Alice to Bob where only a subset of the relays will be active during a time slot and only one relay is selected for information forwarding to reduce the energy expenditure in the network.
- Under the practical assumption of finite-capacity energy storage at the untrusted RF-EH relays, we analyze the dynamic behaviors of the relays' batteries by modelling each battery as a finite-state Markov chain. We derive closed-form expressions for the steady-state distributions. In addition, we analyze the instantaneous secrecy rate and the SOP of the system under the proposed scheme.

Notation: Unless otherwise stated, lower- and upper-case bold letters denote vectors and matrices, respectively. $\mathrm{F}_x(y) = \Pr\{x \leq y\}$ denotes the cumulative distribution function (CDF). $\mathbb{C}^{M\times N}$ denotes the set of all complex matrices of size $M \times N$. $(\cdot)^\top$ and $(\cdot)^*$ denote transpose and Hermitian (i.e., complex-conjugate transpose) operations, respectively. $|\cdot|$ cardinality of a set. $\mathbb{E}\{\cdot\}$ denotes statistical expectation. $\mathbf{0}_{M\times N}$ denotes the all-zero matrix with size $M \times N$. $\overline{\theta} = 1 - \theta$. $\mathrm{diag} = \{\cdot\}$ denotes a diagonal matrix with the enclosed elements as its diagonal elements. $[\cdot]^+ = \max\{0, \cdot\}$ returns the maximum between the argument and zero. A list of the key variables is given in Table 1.

II. SYSTEM MODEL AND SECURE PROTOCOL DESCRIPTION

We investigate a WPCC network composed of a half-duplex source node, Alice, that communicates with a half-duplex legitimate destination node, Bob, through a cluster of

TABLE 1. List of key variables.

Symbol	Description	Symbol	Description
K	# untrusted relay nodes	T and W	Slot (coherence time) duration and channel bandwidth
$\mathcal{R}_s$	Target secrecy rate	P_a	Average transmit information power by Alice
$P_\circ$	Average transmit information power by a relay node	P_b	Average transmit jamming power by Bob
P_J	Average transmit jamming power by John	ρ	Power factor used for energy harvesting
$(1-\rho)$	Power factor used for information processing	R_s^{DSHT}	Instantaneous secrecy rate of the DSHT mode
$R_{s,\ell}^{\mathrm{RDHT}}$	Instantaneous secrecy rate of the RDHT mode when relay node ℓ is selected for information forwarding	D_{ij}	Euclidean distance between node i and node j
L	# discrete energy levels	h_{n_1,n_2}	Channel coefficient between node n_1 and node n_2
$\mathbf{h}_{n_1,n_2}$	Channel vector between node n_1 and node n_2	$\mathbf{U}_i, i \in \{1,2\}$	John's AN precoding matrix for different time slots and modes

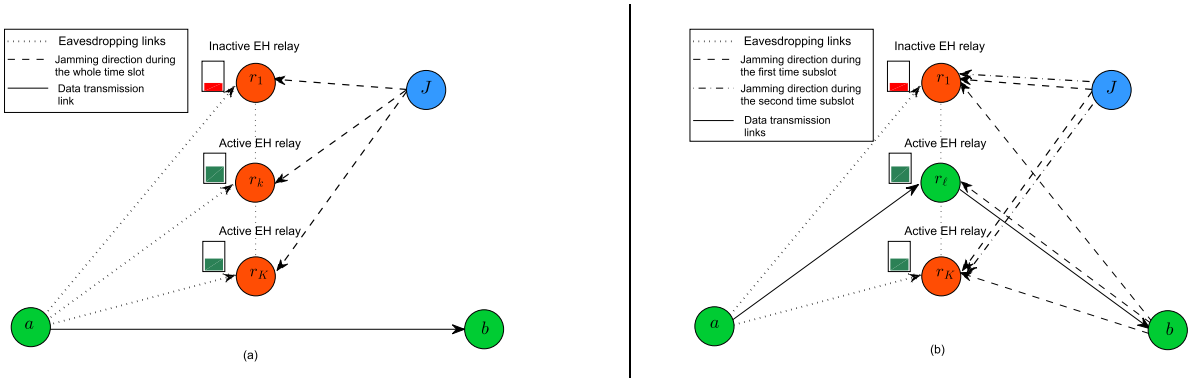

FIGURE 1. System and transmission models.

K untrusted amplify-and-forward (AF) half-duplex relay nodes[1] ($\{r_k\}_{k=1}^K$) in the presence of a cooperative half-duplex jamming node, John, as shown in Fig. 1. We consider that each relay is an EH node and equipped with an RF-EH circuitry with a finite-storage rechargeable battery whose capacity is $E_{\max}$ energy units. We assume that the relay nodes employ a PSR scheme and they can accumulate the harvested energy from the ambient RF transmissions before relaying the information to Bob. Alice, Bob, and the relays are equipped with a single antenna. However, John is equipped with N_J antennas.

The channel coefficient between node i and node j, where $i \in \{a, J, r_1, r_2, \ldots, r_K\}$ and $j \in \{r_1, r_2, \ldots, r_K, b\}$, is denoted by $h_{i,j}$. We assume a flat-fading channel model where a channel coefficient remains fixed for the duration of one transmission block of length T and changes independently from one transmission time to another. If the wireless channels exhibit Rayleigh fading, the channel gain $g_{i,j} \triangleq |h_{i,j}|^2$ is distributed as an exponential random variable with mean $D_{ij}^{-\beta}$, where D_{ij} is the Euclidean distance between node i and node j and β is the path-loss exponent. The thermal noise at a receiving node is modeled as an additive white Gaussian noise (AWGN) with zero mean and unit variance. For clarity, we define $\Delta_{i,j} = g_{i,j}P_i$ where P_i is the transmit power at node i.

A. WIRETAP CODE DESIGN

The random binning scheme is used to secure the transmissions [40]. Consider the scenario where Alice transmits her information packets to Bob without the aid of the relay nodes. In a given time slot, Alice adaptively selects her transmission rate to be close to the instantaneous rate of the Alice-Bob link such that no outage events occur. Alice uses a codebook $C(2^{nR_{\mathrm{A-B}}}, 2^{n\mathcal{R}_s}, n)$ where $R_{\mathrm{A-B}}$ is the instantaneous rate of the Alice-Bob link and $\mathcal{R}_s$ is the target secrecy rate (i.e., number of information bits per channel use), n is the codeword length, $2^{nR_{\mathrm{A-B}}}$ is the number of codewords in the codebook, and $2^{n\mathcal{R}_s}$ is the number of confidential information messages to transmit. The $2^{nR_{\mathrm{A-B}}}$ codewords are randomly grouped into $2^{n\mathcal{R}_s}$ bins. To transmit a confidential

[1]The relay nodes are assumed to be co-located in a clustered fashion close to each other. This can be realized with a long-term routing process. As discussed in [37]–[39], an efficient clustering scheme can be used to organize the relay nodes in a cluster based on average signal-to-noise ratio (SNR).

message $w \in \{1, 2, \ldots, 2^{n\mathcal{R}_s}\}$, Alice adopts a stochastic encoder to randomly select a codeword from bin w and transmit it over the wireless channel. In our scenario where the information is transmitted as a packet, the encoder will set a constant value for the target secrecy rate $\mathcal{R}_s$. When Alice's transmission is aided with one of the relay nodes, the same coding will be used but with the relevant transmission rate (i.e., the codebook rate will be the rate of the end-to-end transmission as will be shown shortly).

Since the information messages are transmitted at a fixed rate, there are two types of outage events

1) **Connection outage**: This outage event occurs when the instantaneous rate of the channel is below the target secrecy rate $\mathcal{R}_s$.
2) **Secrecy rate outage**: This outage event occurs when the instantaneous secrecy rate of channel is below the target secrecy rate $\mathcal{R}_s$.

B. TRANSMISSION MODEL

Since the two communication hops are intercepted by the untrusted relays, the DBJ in addition to the CJ scheme is adopted to protect the source's confidential information. Since the destination (Bob) generates the AN signal, he can cancel it prior to information decoding but the untrusted relays cannot. Similarly, we assume that the jammer designs its AN precoding matrix in such a way that it only affects the relay node that will not forward Alice's information. Hence, the jamming signal by John will not affect the relay selected for information forwarding or Bob. The precoding matrix at John for the various transmission modes and time phases are carefully designed in the next subsection.

The untrusted relay nodes are assumed to be non-colluding which means that they intercept the information independently. Alice, Bob, and John are assumed to be equipped with reliable power supplies and transmit at a constant transmit power levels P_a, P_b, and P_J, respectively. On the other hand, the untrusted relays are assumed to be low-cost nodes with RF-EH capability and they are solely powered by the ambient RF transmissions from the legitimate nodes. Hence, the additional data rate that will be achieved in the system due to the presence of the relays is attained with no extra power. A relay node that has stored (accumulated) enough wireless energy to transmit at the required power level $P_\circ$ is referred to as an *active relay*. The set of relays that have accumulated the required energy are referred to as the active relays. The relay nodes will try to eavesdrop on the ongoing transmissions from Alice. Hence, using the PSR protocol, the relay nodes perform information decoding and energy harvesting simultaneously. We assume that all relay nodes adopt the same power-splitting factor with energy-conversion efficiency $0 \leq \eta \leq 1$. The power-splitting ratios for information processing (decoding or forwarding) and energy harvesting are denoted as $\overline{\rho} = 1 - \rho$ and ρ, respectively.

In our proposed protocol, instead of relaying all the packets, a selected relay is used only to forward the information packets for which the transmission through the direct link (Alice-Bob link) is not secure (i.e., cannot securely support the target secrecy rate $\mathcal{R}_s$). To realize this scheme, based on the success/failure of the direct transmission, Alice selects to either directly communicate with Bob or communicate through only one of the untrusted relays. If the instantaneous secrecy rate from Alice to Bob lies above a target secrecy rate $\mathcal{R}_s$,[2] the direct single-hop transmission (DSHT) mode is selected otherwise the cooperative relay dual-hop transmission (RDHT) mode is selected. If the transmission is unsecured under both modes, the system is in secrecy outage and all nodes will remain idle.

In our proposed scheme, full CSI of the communication links should be available at the central unit which can be either Alice or Bob. Prior to information signal transmission, a two-phase training is used to acquire the instantaneous CSI of all links at Alice which will be used for transmission mode selection. In the first phase, Alice estimates the CSI corresponding to the Alice-Bob link, which can be achieved by using pilot signaling from Bob. The relay nodes and John also use the pilot signal to estimate their channel coefficients to Bob. Then, each relay node sends a one-symbol pilot signal (a deterministic known pilot signal transmitted over one symbol duration) so that Alice, Bob and John estimate their CSI to the relays. To make the channel estimation more accurate, a set of pilot symbols can be transmitted by each node instead of a single pilot symbol. The channels are then fed back to Alice to decide on the selected mode. If the RDHT mode is selected, Alice broadcasts the index of the relay selected for information forwarding to notify all the relay nodes, Bob, and John about the relay-selection process completion.

The transmission time (i.e., time slot) is divided into two time subslots of equal duration $\frac{T}{2}$. If the direct link is secure, the DSHT mode is selected and the two time subslots will be utilized by Alice to send the confidential information to Bob directly. If this mode is not secured, the RDHT mode is selected and one of the relays will be selected to forward the Alice's transmission. Our proposed scheme as shown in Fig. 2 is summarized as follows

- If the DSHT mode is selected, Alice broadcasts her information to Bob and the relays. All relays listen to the transmitted information over the entire time slot duration, and as mentioned earlier, they adopt the power-splitting scheme to simultaneously process the information and harvest energy. Simultaneously, John injects a jamming signal to degrade the channels of all relays but not Bob's channel to prevent causing any interference at Bob's receiver. Hence, the jamming signals are injected to only degrade the untrusted relays' channels.

[2]We assume a fixed-rate packet transmissions where the target secrecy rate is $\mathcal{R}_s$ bits/sec/Hz. That is, within a time slot of duration T, the information signal is transmitted in fixed-size packets of $\mathcal{H}_s$ bits. Assuming that the channel bandwidth is W Hz, the target secrecy rate is $\mathcal{R}_s = \frac{\mathcal{H}_s}{TW}$ bits/sec/Hz.

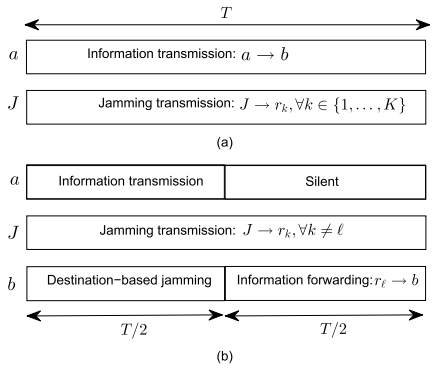

FIGURE 2. The transmission block structures for different transmission strategies. (a) Direct transmission. (b) Cooperative relay transmission.

- If the RDHT mode is selected, the transmission occurs over two time subslots as follows.
  - Assume that relay r_ℓ is selected for information forwarding. During the first time subslot, similar to the DSHT mode, Alice broadcasts her information to Bob and the relays. However, at the same time, Bob injects a jamming signal to hurt all the relays while John injects a jamming signal to hurt all relays except the information forwarding relay (relay ℓ) to prevent causing any interference at Bob when that relay forwards Alice's signal.[3]
  - During the second time subslot, if at least one of the relay nodes is active (i.e., has energy more than $P_\circ T/2$), this active relay will transmit an amplified-version of Alice's transmission. Simultaneously, John injects a jamming signal orthogonal to the direction of the channel vector of his link to Bob to avoid interfering with Bob while interfering with all relays (including relay r_ℓ). This jamming signal is important to i) further power the relay nodes; and ii) due to their malicious behavior, the relays may eavesdrop the information-forwarding relay's signal. By using this jamming signal, the received signal will have very low signal-to-interference-plus-noise ratio (SINR) and it will be useless for the relays. Hence, they cannot combine the received signals from Alice or the information-forwarding relay. Accordingly, the non-selected relay nodes will use the entire received signal from the information-forwarding relay for energy harvesting (i.e., they set $\rho = 1$).

During the RDHT mode, we have two time subslots. Hence, in the κ-th time subslot of transmission, $\kappa \in \{1, 2\}$, we denote the AWGN due to signal processing at receiver j by $n_j^{(\kappa)}$. As assumed in most of the SWIPT literature, the contribution of the antenna noise at relay r_k, $\forall k \in \{1, 2, \ldots, K\}$, is very small (and negligible). When the DSHT mode is used, the superscript κ in $n_j^{(\kappa)}$ is omitted. In the following, we provide the details of the proposed transmission modes.

[3]If the selected relay forwards John's jamming signal, the jamming signal will degrade Bob's receiver.

1) DSHT MODE

If direct transmission is secured (i.e., the instantaneous secrecy rate is higher than the target secrecy rate), it is useless and energy-inefficient to get any help from the untrusted relay nodes. Hence, Alice uses the entire time slot, T, for direct transmissions to Bob. At the same time, the relay nodes should harvest Alice's signal energy to accumulate more energy in their batteries, but since they are untrusted, they might eavesdrop on the confidential information. To prevent information leakage in such eavesdropping attacks, while Alice transmits her information signal, x, to Bob with transmit power level P_a, John transmits a jamming signal vector $\mathbf{z}_J$ with transmit power level P_J, where x and the elements of $\mathbf{z}_J$ are zero-mean circularly-symmetric random variables with unit variances. Hence, the received signal at Bob is given by

$$y_{a,b} = \sqrt{P_a} h_{a,b} x + \sqrt{\frac{P_J}{N_J - 1}} \mathbf{h}_{J,b} \mathbf{U}_1 \mathbf{z}_J + n_b. \quad (1)$$

where $\mathbf{h}_{J,b} \in \mathbb{C}^{1\times N_J}$ is the channel vector of the John-Bob link and $\sqrt{\frac{P_J}{N_J-1}} \mathbf{h}_{J,b} \mathbf{U}_1 \mathbf{z}_J$ is the AN signal vector transmitted by John. John selects his AN-precoding matrix, denoted by $\mathbf{U}_1$, to be canceled at Bob during the DSHT transmission. Hence, $\mathbf{U}_1$ is designed such that

$$\mathbf{h}_{J,b} \mathbf{U}_1 = \mathbf{0}_{1\times(N_J-1)}, \quad \mathbf{U}_1^* \mathbf{U}_1 = \mathbf{I}_{N_J-1}. \quad (2)$$

where $\mathbf{U}_1$ is the AN precoding matrix which should be orthonormal column to maintain the average transmit power fixed.[4] Since $\mathbf{h}_{J,b}$ is $1 \times N_J$, there are $(N_J - 1)$ directions that are orthogonal to $\mathbf{h}_{J,b}$. Thus, $\mathbf{U}_1$ has $(N_J - 1)$ columns. Hence, the direct transmission SNR at Bob is given by $\Gamma_{a,b} = \Delta_{a,b}$. On the other hand, the relays have no knowledge about the jamming signal. Thus, the received RF signal at the input of relay r_k is expressed as

$$y_{a,r_k} = \sqrt{P_a} h_{a,r_k} x + \sqrt{\frac{P_J}{N_J - 1}} \mathbf{h}_{J,r_k} \mathbf{U}_1 \mathbf{z}_J + n_{r_k}. \quad (3)$$

where $\mathbf{h}_{J,r_k} \in \mathbb{C}^{1\times N_J}$ is the channel vector of the link between John and relay r_k, and $\mathbf{U}_1 \in \mathbb{C}^{N_J\times(N_J-1)}$ is the AN-precoding matrix used at John. The relay nodes are assumed to be eavesdroppers that attempt to decode

[4]To obtain an orthonormal-column matrix $\mathbf{U}_1$, the singular value decomposition method can be used to obtain the solution of $\mathbf{h}_{J,b}\mathbf{U}_1 = \mathbf{0}_{1\times(N_J-1)}$ where the columns of $\mathbf{U}_1$ are the right singular vectors of $\mathbf{h}_{J,b}^\top$ corresponding to zero singular values. An alternative method to design $\mathbf{h}_{J,b}\mathbf{U}_1 = \mathbf{0}_{1\times(N_J-1)}$ is to set the columns of $\mathbf{U}_1$ to be $\frac{\mathbf{W}}{\sqrt{\mathrm{Tr}\{\mathbf{W}\mathbf{W}^*\}}}$ where $\mathbf{W} = \mathbf{I}_{N_J} - \mathbf{h}_{J,b}^\top \mathbf{h}_{J,b}$ is a projection matrix that projects a vector to a subspace orthogonal to $\mathbf{h}_{J,b}^\top$. In this case, the column size of $\mathbf{U}_1$ is N_J instead of $N_J - 1$. Hence, we need to change the size of $\mathbf{z}_J$ to N_J. However, the matrix $\frac{\mathbf{W}}{\sqrt{\mathrm{Tr}\{\mathbf{W}\mathbf{W}^*\}}}$ is not orthonormal-column matrix but it does not change the transmit power due to the normalization factor $\sqrt{\mathrm{Tr}\{\mathbf{W}\mathbf{W}^*\}}$.

the messages transmitted from Alice. Hence, based on the adopted power-splitting EH scheme, each relay node r_k splits the received signal into two streams: $\sqrt{\rho}y_{a,r_k}$ for harvesting energy and $\sqrt{\overline{\rho}}y_{a,r_k}$ for decoding the information signal. Similar to the literature, we ignore the harvested energy from the antenna noise [26]. Hence, the received signal to be used for information processing at relay r_k can be expressed as

$$y_{a,r_k}^{\text{process}} = \sqrt{\overline{\rho}P_a}h_{a,r_k}x + \sqrt{\overline{\rho}\frac{P_J}{N_J-1}}\mathbf{h}_{J,r_k}\mathbf{U}_1\mathbf{z}_J + n_{r_k}. \quad (4)$$

Based on (4), the instantaneous SINR at relay r_k is given by

$$\Gamma_{a,r_k} = \frac{\overline{\rho}\Delta_{a,r_k}}{\overline{\rho}\frac{P_J}{N_J-1}\|\mathbf{h}_{J,r_k}\mathbf{U}_1\|^2+1}. \quad (5)$$

Hence, when the DSHT mode is used, the achievable secrecy rate is given by

$$R_s^{\text{DSHT}} = \left[\log_2\left(\frac{1+\Gamma_{a,b}}{1+\max\limits_{k\in\{1,\ldots,K\}}\{\Gamma_{a,r_k}\}}\right)\right]^+. \quad (6)$$

Since Alice sends her information signal over the time slot duration, the harvested energy at the relay nodes during the DSHT mode is $E_{h,\text{DSHT}}^k$, $\forall k \in \{1,2,\ldots,K\}$, where

$$E_{h,\text{DSHT}}^k = \eta\rho\left(P_a g_{a,r_k} + \frac{P_J}{N_J-1}\|\mathbf{h}_{J,r_k}\mathbf{U}_1\|^2\right)T. \quad (7)$$

2) RDHT MODE

when the DSHT mode cannot satisfy the target secrecy rate requirement, the RDHT mode is selected where Alice transmits the information signal $\sqrt{P_a}x$, during the first time subslot, while all the relay nodes listen. Bob and John start to send jamming signals to confuse the relays where Bob sends the jamming signal to confuse all the relays while John sends a jamming signal to confuse all the relays except the one that will forward the data signal since jamming that information-forwarding relay will also jam Bob when he receives the jammed signal. In the first time subslot, the received signal at relay r_k is given by

$$y_{a,r_k} = \sqrt{P_a}h_{a,r_k}x + \sqrt{P_b}h_{b,r_k}z_b + \sqrt{P_J}\mathbf{h}_{J,r_k}\mathbf{U}_2\mathbf{z}_J + n_{r_k}, \quad (8)$$

where z_b is Bob's jamming signal which is modeled as a zero-mean circularly-symmetric random variable with unit variance, and $\mathbf{U}_2\mathbf{z}_J$ is John's jamming signal vector during the first subslot.

The received signal to be used for information processing at relay r_k can be expressed as

$$y_{a,r_k}^{\text{process}} = \sqrt{\overline{\rho}P_a}h_{a,r_k}x + \sqrt{\overline{\rho}P_b}h_{b,r_k}z_b + \sqrt{\overline{\rho}P_J}\mathbf{h}_{J,r_k}\mathbf{U}_2\mathbf{z}_J + n_{r_k}. \quad (9)$$

To avoid forwarding the AN signal by the selected relay at Bob, the jammer should cancel the AN at the relay selected for information forwarding. Hence, the AN precoding matrix during the first phase of the time slot is given by

$$\mathbf{h}_{J,r_\ell}\mathbf{U}_2 = \mathbf{0}_{1\times(N_J-1)}, \quad \mathbf{U}_2^*\mathbf{U}_2 = \mathbf{I}_{N_J-1}. \quad (10)$$

From (9), the instantaneous SINR at relay r_k is given by

$$\Gamma_{a,r_k} = \frac{\overline{\rho}\Delta_{a,r_k}}{\overline{\rho}\frac{P_J}{N_J-1}\|\mathbf{h}_{J,r_k}\mathbf{U}_2\|^2+\overline{\rho}g_{b,r_k}P_b+1}. \quad (11)$$

When $k=\ell$, since $\|\mathbf{h}_{J,r_\ell}\mathbf{U}_2\|^2 = 0$ from (10), we have

$$\Gamma_{a,r_\ell} = \frac{\overline{\rho}\Delta_{a,r_\ell}}{\overline{\rho}g_{b,r_\ell}P_b+1}. \quad (12)$$

The amount of harvested energy at all relays except the relay selected during the first time subslot of the RDHT mode is given by

$$E_{h,1}^k = \eta\rho(P_a g_{a,r_k} + P_b g_{b,r_k} + \frac{P_J}{N_J-1}\|\mathbf{h}_{J,r_k}\mathbf{U}_2\|^2)\frac{T}{2}. \quad (13)$$

The energy harvested at the selected relay for information forwarding is given by

$$E_{h,1}^\ell = \eta\rho(P_a g_{a,r_\ell} + P_b g_{b,r_\ell})\frac{T}{2}. \quad (14)$$

In the second time subslot, only one active relay r_ℓ (if any) amplifies the received signal from Alice, $\sqrt{\overline{\rho}}y_{a,r_\ell}$, by multiplying it with a weighting gain $\mathcal{G} = \sqrt{\frac{P_\ell}{\overline{\rho}P_a g_{a,r_\ell}+\overline{\rho}P_b g_{b,r_\ell}+1}}$ and forwards the resultant signal to Bob. The forwarded signal from the selected relay is given by

$$x_{r_\ell} = \mathcal{G}\left(\sqrt{\overline{\rho}P_a}h_{a,r_\ell}x + \sqrt{\overline{\rho}P_b}h_{b,r_\ell}z_b + n_{r_\ell}^{(1)}\right). \quad (15)$$

Since Bob knows the AN that he generated, he cancels it from the received signal prior to information decoding. Hence, the received signal at Bob, after removing his jamming signal z_b, is given by

$$y_{a,r_\ell,b} = \sqrt{\overline{\rho}P_a}\mathcal{G}h_{a,r_\ell}h_{r_\ell,b}x + \mathcal{G}h_{r_\ell,d}n_{r_\ell}^{(1)} + n_b^{(2)}. \quad (16)$$

The unselected relays (r_k ($k \neq \ell$)) can intercept the transmission during the second time subslot. The received signal at r_k is given by

$$y_{a,r_\ell,r_k} = \sqrt{\overline{\rho}P_a}\mathcal{G}h_{a,r_\ell}h_{r_\ell,r_k}x + \sqrt{\overline{\rho}P_b}\mathcal{G}h_{b,r_\ell}h_{r_\ell,r_k}z_b + \sqrt{\overline{\rho}\frac{P_J}{N_J-1}}\mathbf{h}_{J,r_k}\mathbf{U}_1\mathbf{z}_J + \mathcal{G}h_{r_\ell,r_k}n_{r_\ell}^{(1)} + n_{r_k}^{(2)}. \quad (17)$$

The purpose of the jamming signal from John during the second time subslot, given by $\sqrt{\overline{\rho}\frac{P_J}{N_J-1}}\mathbf{h}_{J,r_k}\mathbf{U}_1\mathbf{z}_J$, is to energize the relays for future transmissions and prevent them from performing maximal ratio combining. It is noteworthy that the precoder during the second time subslot of the RDHT mode is designed as in the DSHT mode since John can jam everywhere except the John-Bob vector direction.

In the RDHT mode, the non-selected relay nodes may attempt to eavesdrop on the transmission during the

second hop. Hence, they may combine the signals over the two time subslots (signal from Alice and from the information-forwarding relay) to decode Alice's information signal more reliably. However, since the selected relay uses an AF relaying scheme, combining the two received signals at the non-selected relays will not help in decoding the confidential information since the AN signals from both Bob and John and the additional relayed AWGN samples from the information-forwarding relay will significantly degrade the signal received over the second time subslot at the non-selected relays. In addition, John will also jam the second time subslot to further prevent the untrusted relays from eavesdropping and to further energize them. In other words, securing the Alice-relay transmissions is enough to ensure the security of the entire two-hop transmission since the relayed signal by the information-forwarding relay is actually the received signal from Alice (which is degraded by the jamming signal from Bob) in addition to the AWGN signal (due to signal processing at the selected relay) and the jamming signal from John. Hence, the received signal during the second subslot at the non-selected relays will be very weak for data decoding but is a good signal for accumulating more energy at the relays. In addition to the aforementioned reasons, the relays should collect as much energy as they can during the second time subslot to be able to help Alice in future time slots. Furthermore, as in the untrusted relaying literature [26], [27], [29]–[31], the relays nodes are assumed to be honest and trusted at the service level and untrusted at the information level. Hence, they should obey the legitimate system and follow the orders. Consequently, during the second time subslot of the RDHT mode, the non-selected relay nodes will harvest energy.

When the RDHT mode is used, the instantaneous secrecy rate is given by

$$R_{s,\ell}^{\mathrm{RDHT}} = \frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_{a,r_\ell,b}}{1+\max\limits_{k\in\{1,\ldots,K\}}\{\Gamma_{a,r_k}\}}\right)\right]^+, \quad (18)$$

where

$$\Gamma_{a,r_\ell,b} = \frac{\overline{\rho}\Delta_{a,r_\ell}\Delta_{r_\ell,b}}{\overline{\rho}\Delta_{a,r_\ell}+\overline{\rho}\Delta_{a,r_\ell}+\Delta_{r_\ell,b}+1} \quad (19)$$

denotes the received SNR at Bob from the signal received from the selected relay. The secrecy rate is reduced by a factor of two since Alice uses just half the time slot to transmit the same information. When the DSHT mode is insecure, the K relay nodes harvest energy from Alice's information transmission and John's jamming signal in the first time subslot. In the second time subslot, the selected relay node amplifies-and-forwards the received signal to Bob while the other relay nodes use the entire subslot duration to harvest energy with $\rho = 1$ from both the selected relay's transmission and the jamming signal transmission from John. Hence, the harvested energy at r_k ($k \neq \ell$) during the second time subslot is given by

$$E_{h,2}^k = \eta\Bigg(P_a g_{a,r_\ell}\mathcal{G}^2 g_{r_\ell,r_k} + P_b g_{b,r_\ell}\mathcal{G}^2 g_{r_\ell,r_k} + \frac{P_J}{N_J-1}\|\mathbf{h}_{J,r_k}\mathbf{U}_1\|^2 + \mathcal{G}^2 g_{r_\ell,r_k}\Bigg)\frac{T}{2}, \quad \forall k \neq \ell. \quad (20)$$

If the direct link is in secrecy outage and cannot support the target secrecy rate, the amount of harvested energy at the relay nodes r_ℓ and r_k ($k \neq \ell$) are given by $E_{h,1}^\ell$ and $E_{h,\mathrm{RDHT}}^k = E_{h,1}^k + E_{h,2}^k$, respectively. If none of the relay nodes had accumulated sufficient energy to transmit, Alice and the relay nodes remain silent and the overall system is in outage.

C. RELAY SELECTION SCHEME

We propose a two-step relay selection scheme which is based on both the CSI of the wireless links and the ESI of the batteries at the relay nodes. In the first step, based on the ESI at batteries, only a subset Θ with cardinality $|\Theta| \leq K$ of the relay nodes will be active. This active subset is representing the subset of the relays that can aid Alice. The subset Θ is constructed as

$$\Theta = \{r_k | E_{0,k} \geq P_\circ \frac{T}{2},\ \forall k \in \{1,\ldots,K\}\}, \quad (21)$$

where $E_{0,k}$ denotes the ESI of relay r_k at the beginning of the time slot. In the second step, the relay node in Θ with the highest secrecy rate is selected. That is, r_ℓ is selected as

$$\ell = \underset{r_k\in\Theta}{\mathrm{argmax}}\ R_{s,k}^{\mathrm{RDHT}}. \quad (22)$$

To ensure a secure transmission (i.e., perfect information secrecy), $R_{s,k}^{\mathrm{RDHT}} \geq \mathcal{R}_s$. Otherwise, the secrecy is compromised. If the best relay secrecy rate cannot guarantee the $\mathcal{R}_s$ bits/sec/Hz, then all other active relays cannot guarantee it. Hence, the system is in secrecy outage. If none of the active relays in set Θ satisfy $R_{s,k}^{\mathrm{RDHT}} \geq \mathcal{R}_s$, we define $\mathbb{I} = 0$ which implies that there is no relaying and all nodes will be idle.

III. PERFORMANCE ANALYSIS

A. ENERGY STORAGE MODEL

To analyze the performance of our proposed scheme, we characterize the dynamic behaviors of the relays' batteries. Since we assume a cluster of relay nodes, the DSHT mode corresponds to an increase of the battery energy levels for all relays with the same average amount of energy. When the RDHT mode is used, the first time subslot corresponds to an increase of the battery energy levels for all relays with different amounts of average energy. In the second time subslot, the battery energy level of the selected relay for information forwarding may decrease. Hence, the energy-accumulation process at the relay nodes depends on both the channel condition of the Alice-Bob link and their own energy storage levels. The probability of

secure transmission from Alice to Bob without relaying is given by

$$\mu^{\text{DSHT}} = \Pr\left[R_s^{\text{DSHT}} \geq \mathcal{R}_s\right]. \tag{23}$$

If both the DSHT mode and the RDHT mode are not secure, Alice and the selected relay should not send any information signals. Moreover, John and Bob remain idle and do not send jamming signals. Hence, relay nodes are only used when the RDHT mode satisfies the target secrecy rate.

In wireless networks, due to the time-varying channel conditions, the RF-EH rates at the EH nodes are randomly fluctuating over time. Moreover, the selected relay for information forwarding varies from one coherence time (time slot) to another. Based on these two facts, the batteries' state transitions are modeled as a discrete-time finite-state Markov chain (MC) that evolves on a finite state space $S = \{\psi_0, \ldots, \psi_L\}$, where L denotes the number of discrete energy levels. We define ψ_i as the state when the relay's residual energy in its battery is $\delta_i = \frac{iE_{\max}}{L} = i\delta_1$ where $\delta_1 = \frac{E_{\max}}{L}$. Thus, during the n-th time subslot, when the RDHT mode is used, the discretized amount of the harvested energy for relay r_k is given by

$$\xi_{h,n}^k = \left\lfloor \frac{E_{h,n}^k}{\delta_1} \right\rfloor \delta_1, \tag{24}$$

where $\lfloor\cdot\rfloor$ is the floor function. The total energy accumulated over the two subslots during the RDHT mode is given by $\xi_{h,\text{RDHT}}^k = \xi_{h,1}^k + \xi_{h,2}^k$. The amount of energy harvested during the DSHT mode is

$$\xi_{h,\text{DSHT}}^k = \left\lfloor \frac{E_{h,\text{DSHT}}^k}{\delta_1} \right\rfloor \delta_1, \tag{25}$$

When the RDHT mode is used, the discretized value of the transmission energy at the selected relay in the second time subslot is given by

$$\delta_t = \left\lceil \frac{P_\circ T}{2\delta_1} \right\rceil \delta_1, \tag{26}$$

where $\lceil\cdot\rceil$ is the ceiling function.

Let $E_{0,k}^m$ denote the battery energy level of the k-th relay at the beginning of the m-th transmission time slot and assume that relay ℓ is selected. Then, according to the proposed scheme, the battery energy level at the end of the m-th time slot (or at the beginning of the $(m+1)$-th time slot), denoted by $E_{0,k}^{m+1}$, is given by (27) at the top of the next page where $\mathbb{1}[\cdot]$ denotes an indicator function that equals one if its argument is true and zero otherwise.

A relay node is a candidate for selection if, in the beginning of a time slot, its battery energy level exceeds δ_t. Let ζ_i^k denote an indicator which is equal to one if the i-th battery energy level of the k-th relay is higher than the energy level required for information forwarding, $\delta_i \geq \delta_t$, and zero otherwise. On the other hand, the state transition may occur between the two consecutive time slots. Hence, the transition probabilities of the MC are time dependent and the MC is considered as a time non-homogeneous. In this case, a standard MC cannot capture the heterogeneity in battery energy level evolution over the two transmission phases. If the current battery state of the k-th relay node is ψ_i, it transits to state ψ_l at the first time subslot with probability $p_{k,(i,l)}^{(1)}$, then to state ψ_j in the second time subslot with probability $p_{k,(l,j)}^{(2)}$. Based on the Markov property, the transitions $\psi_i \to \psi_l$ and $\psi_l \to \psi_j$ are independent events. Hence, we split the state transition process into two stages and construct two independent transition probability matrices ($\mathbf{X}_k^{(1)}$ and $\mathbf{X}_k^{(2)}$), one for each stage, where the transition probability matrix is defined as $\left[\mathbf{X}_k^{(n)}\right]_{(i,j)} = p_{k,(i,j)}^{(n)}$, for $i, j = 0, \ldots, L$. To decouple the interaction among the relays' batteries, we assume while solving the MCs that a relay loses δ_t energy units when the relay is selected for relaying, which occurs with probability $1/K$ since the relays are located in a cluster, the relay is active (i.e., its battery level is higher than δ_t), and the relaying link is secured (i.e., its secrecy rate is at least equal to the target secrecy rate $\mathcal{R}_s$ bits/sec/Hz). Moreover, a transmission occurs under the RDHT mode when the selected relaying link can securely support the target secrecy rate. Hence, these approximations underestimate the performance of our proposed scheme. Let $\pi_i^{(n)}$, $i = 0, \ldots, L$, be the steady-state probability of being in the i-th state after the n-th time subslot of the transmission block at the k-th relay. The channels in the network are assumed to be independent and identically distributed (i.i.d.). Hence, all relay nodes have the same transition matrices, and then identical stationary distribution for all relay nodes. Hereinafter, unless necessary, we will omit the index k.

1) FIRST TIME SUBSLOT ANALYSIS

Regardless of the used transmission mode, the first phase implies an increase in the relays' batteries energy levels only. In the DSHT mode, all the relays' batteries energy levels increase with the same average amount of energy. However, in the RDHT mode, the non-selected relays will harvest more energy than the selected one because they will receive the jamming signal from John. Assuming that relays are in a cluster, each active relay has an equal chance to be selected with a probability given by $\frac{1}{|\Theta|}$, where $|\Theta|$ is the cardinality of Θ. As a function of the cardinality of the active set, this probability is time-dependent. On the other hand, the stationary distribution of each relay battery status is time-independent. Alternatively, we use the lower-bound $\frac{1}{K}$. We summarize all the transition probabilities into the following four general cases.

1) *The battery remains unchanged ($\psi_i \to \psi_i$ with $0 \leq i < L$)*: The battery remains unchanged if, during the first time subslot, the discretized amount of harvested energy from either the DSHT mode or the RDHT mode is less than one energy level, δ_1. The transition

$$E_{0,k}^{m+1}=\begin{cases}\min\left(E_{0,k}^{m}+\xi_{h,\mathrm{DSHT}}^{k},E_{\max}\right), & \text{if } R_{\mathrm{s}}^{\mathrm{DSHT}}\geq R_{\mathrm{s}}\\ \min\left(E_{0,k}^{m}+\xi_{h,1}^{k}+\xi_{h,2}^{k}(1-\mathbb{1}[k=\ell])-\delta_t\,\mathbb{1}[k=\ell],E_{\max}\right), & \text{if } \{R_{\mathrm{s}}^{\mathrm{DSHT}}<R_{\mathrm{s}}\}\cap\{\mathbb{I}=1\}\\ E_{0,k}^{m}, & \text{if } \{R_{\mathrm{s}}^{\mathrm{DSHT}}<R_{\mathrm{s}}\}\cap\{\mathbb{I}=0\}.\end{cases}\tag{27}$$

probability is thus given by

$$\begin{aligned}p_{(i,i)}^{(1)}&=\mu^{\mathrm{DSHT}}\Pr\left[\frac{\xi_{h,\mathrm{DSHT}}^{k}}{2}=0\right]+\overline{\mu^{\mathrm{DSHT}}}\gamma\\&\quad\times\left[\frac{\zeta_i^k}{K}\Pr\left[\xi_{h,1}^{\ell}=0\right]\right.\\&\qquad\left.+\left(\frac{\zeta_i^k(K-\gamma)}{K}+\overline{\zeta_i^k}\right)\Pr\left[\xi_{h,1}^{k}=0\right]\right]\\&=\mu^{\mathrm{DSHT}}\mathrm{F}_{E_{h,\mathrm{DSHT}}^{k}}(2\delta_1)+\overline{\mu^{\mathrm{DSHT}}}\gamma\\&\quad\times\left[\frac{\zeta_i^k}{K}\mathrm{F}_{E_{h,1}^{\ell}}(\delta_1)+\left(\frac{\zeta_i^k(K-\gamma)}{K}+\overline{\zeta_i^k}\right)\mathrm{F}_{E_{h,1}^{k}}(\delta_1)\right].\end{aligned}\tag{28}$$

where $\gamma=\Pr\left[R_{s,k}^{\mathrm{RDHT}}\geq\mathcal{R}_s\right]$ which is independent of the index k since the relays are located in a cluster.

2) *The battery remains fully charged ($\psi_L\rightarrow\psi_L$)*: Under the practical assumption of finite-capacity energy storage at the untrusted RF-EH relays, any received energy that overflows their capacity $E_{\max}$ cannot be stored and the extra energy will be lost. Hence, ψ_L is an absorbing state and the transition probability from state ψ_L to itself is given by

$$p_{(L,L)}^{(1)}=1.\tag{29}$$

3) *The battery is partially charged ($\psi_i\rightarrow\psi_j$ with $0\leq i\leq j<L$)*: When the battery is not full, (i.e., $\delta_i<\delta_L$), a non-zero discretized harvested energy less than $\delta_L-\delta_i$ will lead to an increase of the battery to an intermediate level j. The transition probability $\psi_i\rightarrow\psi_j$ is given by

$$\begin{aligned}p_{(i,j)}^{(1)}&=\mu^{\mathrm{DSHT}}\Pr\left[\delta_j-\delta_i<\frac{\xi_{h,\mathrm{DSHT}}^{k}}{2}<\delta_{j+1}-\delta_i\right]\\&\quad+\overline{\mu^{\mathrm{DSHT}}}\gamma\left[\frac{\zeta_i^k}{K}\Pr\left[\delta_j-\delta_i<\xi_{h,1}^{\ell}<\delta_{j+1}-\delta_i\right]\right.\\&\quad\left.+\left(\frac{\zeta_i^k(K-\gamma)}{K}+\overline{\zeta_i^k}\right)\Pr\right.\\&\qquad\left.\times\left[\delta_j-\delta_i<\xi_{h,1}^{k}<\delta_{j+1}-\delta_i\right]\right]\\&=\mu^{\mathrm{DSHT}}\left(\mathrm{F}_{E_{h,\mathrm{DSHT}}^{k}}\left(2\left(\delta_{j+1}-\delta_i\right)\right)\right.\\&\qquad\left.-\mathrm{F}_{E_{h,\mathrm{DSHT}}^{k}}\left(2\left(\delta_j-\delta_i\right)\right)\right)\\&\quad+\overline{\mu^{\mathrm{DSHT}}}\gamma\left[\frac{\zeta_i^k}{K}\left(\mathrm{F}_{E_{h,1}^{\ell}}\left(\delta_{j+1}-\delta_i\right)-\mathrm{F}_{E_{h,1}^{\ell}}\left(\delta_j-\delta_i\right)\right)\right.\\&\qquad+\left(\frac{\zeta_i^k(K-\gamma)}{K}+\overline{\zeta_i^k}\right)\\&\qquad\times\left(\mathrm{F}_{E_{h,1}^{k}}\left(\delta_{j+1}-\delta_i\right)\right.\\&\qquad\left.\left.-\mathrm{F}_{E_{h,1}^{k}}\left(\delta_j-\delta_i\right)\right)\right].\end{aligned}\tag{30}$$

4) *The non-full battery is fully charged ($\psi_i\rightarrow\psi_L$ with $0\leq i<L$)*: In this case, a non-zero discretized harvested energy higher than $\delta_L-\delta_i$ fully charges the battery. The state transition probability from level i to level L is given by

$$\begin{aligned}p_{(i,L)}^{(1)}&=\mu^{\mathrm{DSHT}}\Pr\left[\xi_{h,\mathrm{DSHT}}^{k}>\delta_L-\delta_i\right]\\&\quad+\overline{\mu^{\mathrm{DSHT}}}\gamma\left[\frac{\zeta_i^k}{K}\Pr\left[\xi_{h,1}^{\ell}>\delta_L-\delta_i\right]\right.\\&\quad\left.+\left(\frac{\zeta_i^k(K-\gamma)}{K}+\overline{\zeta_i^k}\right)\Pr\left[\xi_{h,1}^{k}>\delta_L-\delta_i\right]\right]\\&=\mu^{\mathrm{DSHT}}\left(1-\mathrm{F}_{E_{h,\mathrm{DSHT}}^{k}}\left(2\left(\delta_L-\delta_i\right)\right)\right)\\&\quad+\overline{\mu^{\mathrm{DSHT}}}\gamma\left[\frac{\zeta_i^k}{K}\left(1-\mathrm{F}_{E_{h,1}^{\ell}}\left(\delta_L-\delta_i\right)\right)\right.\\&\quad\left.+\left(\frac{\zeta_i^k(K-\gamma)}{K}+\overline{\zeta_i^k}\right)\left(1-\mathrm{F}_{E_{h,1}^{k}}\left(\delta_L-\delta_i\right)\right)\right].\end{aligned}\tag{31}$$

Since there is no energy expenditure in the first time subslot, only the transitions involving an increase in the battery energy level can occur. Therefore, the transition matrix $\mathbf{X}^{(1)}$ is upper triangular.

2) SECOND TIME SUBSLOT ANALYSIS

During the second time subslot, a relay's battery level can decrease by δ_t energy units only when the RDHT mode is activated and the relay was selected to retransmit Alice's transmission to Bob. Otherwise, the relay's battery can either increase or remain unchanged. In fact, if the DSHT mode is activated, the source continues its transmission while all the relays harvest. On the other hand, if the RDHT is activated, the non-selected relay nodes accumulate further energy in their batteries for future use. In the following, to compute the state distribution of the considered Markov model, we first find the state transition probabilities for the second time subslot.

1) *The battery remains unchanged ($\psi_i \rightarrow \psi_i$ with $0 \leq i < L$)*: The battery remains unchanged if the relay is harvesting energy during the second subslot. However, the harvested energy is low and incapable of powering the relay's battery. In this case, the transition probability from state ψ_i to state ψ_i is given by

$$\begin{aligned} p^{(2)}_{(i,i)} &= \mu^{\text{DSHT}} \Pr\left[\frac{\xi^k_{h,\text{DSHT}}}{2} = 0\right] \\ &\quad + \overline{\mu^{\text{DSHT}}}\gamma \left[\frac{\zeta^k_i(K-\gamma)}{K} + \overline{\zeta^k_i}\right] \Pr\left[\xi^k_{h,2} = 0\right] \\ &= \mu^{\text{DSHT}} \text{F}_{E^k_{h,\text{DSHT}}}(2\delta_1) \\ &\quad + \overline{\mu^{\text{DSHT}}}\gamma \left[\frac{\zeta^k_i(K-\gamma)}{K} + \overline{\zeta^k_i}\right] \text{F}_{E^k_{h,2}}(\delta_1). \end{aligned} \tag{32}$$

2) *The battery remains fully charged ($\psi_L \rightarrow \psi_L$)*: When the relay's battery is full, an overflow event occurs if either the DSHT mode is activated or the relay is not selected for information forwarding when the RDHT mode is activated. Hence, the transition probability is given by

$$p^{(2)}_{(L,L)} = \mu^{\text{DSHT}} + \overline{\mu^{\text{DSHT}}}\frac{(K-\gamma)}{K}. \tag{33}$$

3) *The battery is partially charged ($\psi_i \rightarrow \psi_j$ with $0 \leq i \leq j < L$)*: If the relay harvests a non-zero discretized amount of energy that is less than $\delta_L - \delta_i$, the battery energy level increase from energy level i to an intermediate energy level j with a transition probability given by

$$\begin{aligned} p^{(2)}_{(i,j)} &= \mu^{\text{DSHT}} \Pr\left[\delta_j - \delta_i < \frac{\xi^k_{h,\text{DSHT}}}{2} < \delta_{j+1} - \delta_i\right] \\ &\quad + \overline{\mu^{\text{DSHT}}}\gamma \left(\frac{\zeta^k_i(K-\gamma)}{K} + \overline{\zeta^k_i}\right) \Pr \\ &\quad \times \left[\delta_j - \delta_i < \xi^k_{h,2} < \delta_{j+1} - \delta_i\right] \\ &= \mu^{\text{DSHT}} \Big(\text{F}_{E^k_{h,\text{DSHT}}}\left(2\left(\delta_{j+1} - \delta_i\right)\right) \\ &\quad - \text{F}_{E^k_{h,\text{DSHT}}}\left(2\left(\delta_j - \delta_i\right)\right)\Big) \\ &\quad + \overline{\mu^{\text{DSHT}}}\gamma \left(\frac{\zeta^k_i(K-\gamma)}{K} + \overline{\zeta^k_i}\right) \\ &\quad \times \Big(\text{F}_{E^k_{h,2}}\left(\delta_{j+1} - \delta_i\right) - \text{F}_{E^k_{h,2}}\left(\delta_j - \delta_i\right)\Big) \end{aligned} \tag{34}$$

4) *The non-full battery is fully charged ($\psi_i \rightarrow \psi_L$ with $0 \leq i < L$)*: The relay's battery is fully charged with a probability given by

$$\begin{aligned} p^{(2)}_{(i,L)} &= \mu^{\text{DSHT}} \Pr\left[\frac{\xi^k_{h,\text{DSHT}}}{2} > \delta_L - \delta_i\right] \\ &\quad + \overline{\mu^{\text{DSHT}}}\gamma \left(\frac{\zeta^k_i(K-\gamma)}{K} + \overline{\zeta^k_i}\right) \Pr \\ &\quad \times \left[\xi^k_{h,2} > \delta_L - \delta_i\right] \\ &= \mu^{\text{DSHT}} \Big(1 - \text{F}_{E^k_{h,\text{DSHT}}}\left(2\left(\delta_L - \delta_i\right)\right)\Big) \\ &\quad + \overline{\mu^{\text{DSHT}}}\gamma \left(\frac{\zeta^k_i(K-\gamma)}{K} + \overline{\zeta^k_i}\right) \\ &\quad \times \Big(1 - \text{F}_{E^k_{h,2}}\left(\delta_L - \delta_i\right)\Big). \end{aligned} \tag{35}$$

5) *The non-empty battery is discharged ($\psi_i \rightarrow \psi_j$ with $0 \leq j \leq i \leq L$)*: If the relay is selected for information forwarding, which occurs with probability $1/K$ when the relays are clustered, the relay's battery is reduced by δ_t energy units. Hence, the transition probability is given by

$$p^{(2)}_{(i,j)} = \overline{\mu^{\text{DSHT}}}\gamma \frac{\zeta^k_i}{K} \times \mathbb{1}\left(\delta_i - \delta_t = \delta_j\right), \tag{36}$$

Based on the Chapman-Kolmogorov identity [41], [42],[5] the two-stage transition probabilities are given by

$$p_{(i,j)} = \sum_{l=i}^{L} p^{(1)}_{(i,l)} p^{(2)}_{(l,j)}. \tag{37}$$

It turns out that in general, computing $\mathbf{X}$ is accomplished via matrix multiplication

$$\mathbf{X} = \mathbf{X}^{(1)} \times \mathbf{X}^{(2)}. \tag{38}$$

Since the MC is finite-state, irreducible, and aperiodic, all states are positive recurrent and ergodic.[6] The steady-state distribution vector for the proposed protocol at an arbitrary relay is computed by calculating higher powers of the matrix as follows [42]

$$\boldsymbol{\pi} = \boldsymbol{\pi}^{(0)} \times \mathbf{X}^{\infty}, \tag{39}$$

where $\boldsymbol{\pi}$ is the steady-state distribution with its i-th element as the probability that the battery is in state i, denoted by π_i, and $\boldsymbol{\pi}^0$ is any initial steady-state distribution [42].

B. SECRECY OUTAGE PROBABILITY (SOP)

In our proposed scheme, whenever the target secrecy rate $\mathcal{R}_s$ is not satisfied under the DSHT mode, the relay nodes are involved to achieve the target secrecy rate through cooperative diversity. Hence, the communications system is in outage if the instantaneous secrecy rates of both DSHT mode and RDHT mode fall below the target secrecy rate, $\mathcal{R}_s$ bits/sec/Hz. Consequently, an outage event may occur if (1) the instantaneous secrecy rate of the Alice-Bob link without relaying fails to achieve the target secrecy rate, and (2) when the active-relay set, Θ, is empty or the transmission from the

[5]The transition matrix at time $t+s$, denoted by $\mathbf{P}(t+s)$, is equal to $\mathbf{P}(t)\mathbf{P}(s)$.

[6]An MC is said to be irreducible if and only if all states communicate [43]. Moreover, an MC is said to be aperiodic if all states are aperiodic; a state is aperiodic if and only if there exists a time t such that $\pi^{(t)}_{i,i} > 0$ and $\pi^{(t+1)}_{i,i} > 0$ [43].

selected relay fails to achieve the target secrecy $\mathcal{R}_s$. Hence, the SOP of the system is given by

$$P_{\text{out}} = \overline{\mu^{\text{DSHT}}} \left(\left(\sum_{i=0}^{\delta_t - 1} \pi_i \right)^K + \sum_{k=1}^{K} \binom{K}{k} \left(\sum_{i=\delta_t}^{L} \pi_i \right)^k \left(\sum_{i=0}^{\delta_t - 1} \pi_i \right)^{K-k} P_{\text{sec}}^k \right). \tag{40}$$

where $\binom{K}{k}$ is K choose k, and $P_{\text{sec}}^k = \Pr\left[\max_{k \in \Theta} R_{s,k}^{\text{RDHT}} < \mathcal{R}_s \right]$ is the probability that the instantaneous secrecy rate is lower than the target secrecy rate given that there are $k = |\Theta|$ active relays. It is noteworthy that since the relays are in a cluster, the probability P_{sec}^k is only a function of the number of active relays.

IV. NUMERICAL RESULTS

In this section, the analytical findings are verified through simulations. In addition, we provide the performance comparison between DSHT-only mode, RDHT-only mode, and the proposed scheme and investigate the impact of the system parameters on their SOPs. Without loss of generality, we consider a normalized relay network in a square of unit area, where all distances are normalized. The coordinates of the source (Alice) s the destination (Bob) d and the jammer (John) J are are (0, 0.5), (1, 0.5) and (0.5,0.6), respectively. The untrusted relay nodes in the network are grouped into a cluster and thus they have the same coordinate (0.5,0.5). Unless otherwise stated, we set the simulation parameters as follows: energy harvesting efficiency $\eta = 0.6$, path loss exponent $\beta = 3$, the number of antennas at the jammer is $N_J = 4$ and $P_b = P_J = P_r = 15$ dBm. The power splitting factor is $\rho = 0.5$. Each channel coefficient between any antenna pair is assumed to be a complex zero-mean circularly-symmetric Gaussian random variable with unit variance. For simplicity, all the noise powers are set to be 0 dBm.

In Figs. 3 and 4, the SOP is depicted versus Alice's transmission power for different jamming signals power levels at Bob and John. In these two figures, we compare the SOPs of the DSHT-only mode, the RDHT-only mode, and our proposed adaptive transmission scheme. Our proposed adaptive scheme always outperforms the conventional systems (DSHT and RDHT) when **both** the jammer and the destination help in reducing the leakage rate to the untrusted relays. In fact, as the number of jamming nodes increases, more confusion is caused for the untrusted relays and more energy is harvested at the relays. As a result, the SOP decreases due to increased secrecy rates and the availability of more active relays. Moreover, due to the time-varying nature of wireless fading channels, the relay link may not be always better than the direct link and vice versa. The DSHT mode

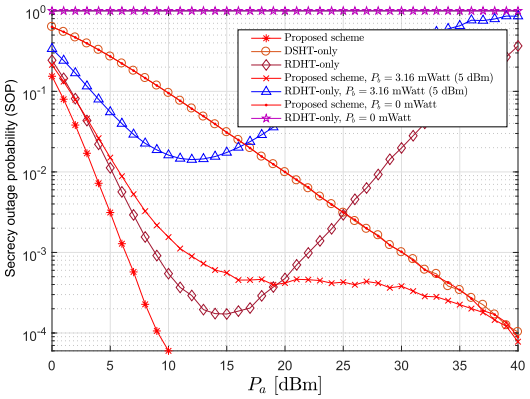

FIGURE 3. The SOP versus Alice's transmit power when $\mathcal{R}_s = 1$ bits/sec/Hz, $K = 5$, $N_J = 4$ and $E_{\max} = 50$.

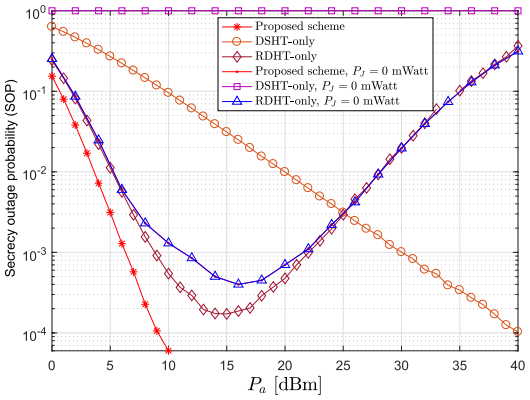

FIGURE 4. The SOP versus Alice's transmit power when $P_J = 5$ dBm, $P_b = 15$ dBm and $\mathcal{R}_s = 1$ bits/sec/Hz.

shows a good performance at high levels of P_a while the RDHT mode is very promising for low-to-medium levels of P_a. Clearly, the DSHT mode is better than the RDHT mode when the direct link is significantly stronger than the relaying link, while the RDHT mode will perform better when the direct link is relatively weak. Hence, a proper transmission mode selection scheme significantly enhances the system security, provided that perfect CSI is available at the control unit (e.g., Alice or Bob). Furthermore, as P_a increases, the SOPs of our proposed scheme and the DSHT mode decrease, although the SOP of the RDHT mode first decreases and then increases. This is because, the data rate of the Alice-relay link decreases as P_a decreases and, hence, Bob's jamming signal has more harmful impact on the relays. Accordingly, it becomes more difficult for the selected relay to successfully decode Alice's information signal. However, despite using the DBJ scheme, when P_a is larger than P_b, the data rate of the Alice-relay link may be higher than the direct link data rate which, in turn, increases the SOP. This reveals that the secrecy performance of the RDHT mode reduces when Alice uses a transmission power higher than Bob's jamming power P_b.

The effect of the jamming power at the destination is investigated in Fig. 3. The secrecy performance of the DSHT

mode is independent of P_b. However, when P_b decreases, the SOP of the RDHT mode increases. Since the RDHT mode is frequently selected for low values of P_a, the SOP of our proposed scheme increases as P_b increases. Hence, when $P_a = 40$ dBm, the direct link is strong enough to ensure the target secrecy rate $\mathcal{R}_s$ without the help of the relay nodes. If $P_b = 0$ (i.e., no jamming from Bob), since the selected relay for information forwarding r_ℓ will have better channel to Bob than Alice, the achievable secrecy rate of the RDHT mode is zero. Hence, the RDHT mode will not be used at all and the system's SOP will be the same as that of DSHT mode. On the other hand, the effect of P_J is shown in Fig. 4 where we observe that the SOP becomes high for the no-jamming cases for all schemes. Without jamming, the relay channel is better than the direct-link channel which leads to zero instantaneous secrecy rate through the use of the DSHT mode. Thus, Alice will always select the two-hop transmission mode where, for secrecy purpose, Bob ignores the direct link to transmit a jamming signal during the first phase.

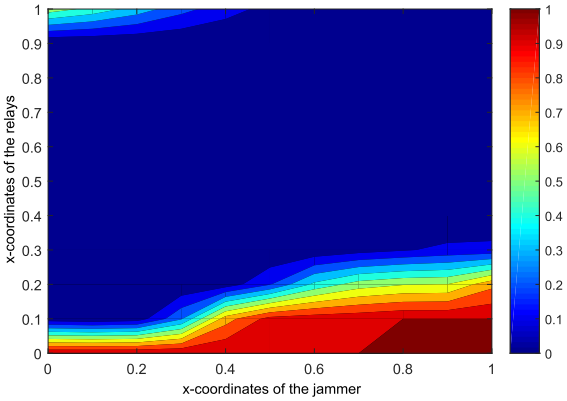

FIGURE 5. The SOP versus the x-coordinate of the relays and x-coordinate of the jammer when $P_a = 20$ dBm, $P_J = 5$ dBm, $P_b = 15$ dBm and $\mathcal{R}_s = 1$ bits/sec/Hz.

Figs. 5 and 6 show the SOP of our proposed scheme as a function of the x-coordinate of the relays and the x-coordinate of the cooperative jammer (John), denoted by x_J. These two figures demonstrate that, according to the John's location, there are two limited areas where the relays could compromise the secrecy of the system. These areas are the ones where the relays are located close to Alice and Bob. We observe that for when the x-coordinate of the relay's location $x_r \leq 0.3$ (i.e., the relay is closer to the source) the SOP increases as John moves far away from the source and toward to the destination (i.e., x_J grows). In fact, when John is far away from the untrusted relays, his jamming is less effective in improving the secrecy performance. For the RDHT mode, when x_r decreases, the SOP increases. This is because, relays are supposed to be cooperative in forwarding the information from Alice but they are not trusted. Hence, to have secure communications, the relays should be closer to the source. On the other hand, when relays are close to the destination, the first-hop becomes the bottleneck

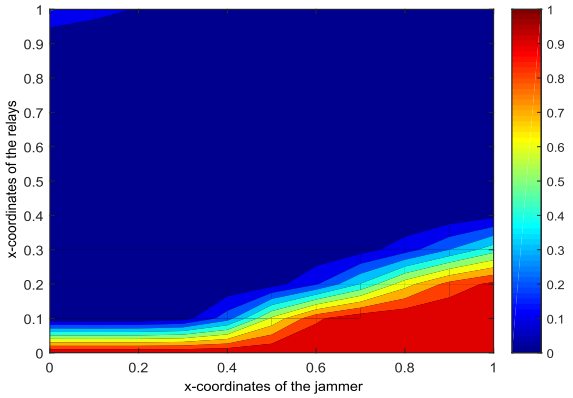

FIGURE 6. The SOP versus the x-coordinate of the relays and x-coordinate of the jammer when $P_a = 20$ dBm, $P_J = 15$ dBm, $P_b = 5$ dBm and $\mathcal{R}_s = 1$ bits/sec/Hz.

for the dual-hop communications since the performance gain achieved from the second-hop is significantly higher. Moreover, when the relays are located far away from the source, the harvested energy at the relays becomes limited since the distance is high.

V. CONCLUSION

We proposed a new AN-aided relay-selection scheme to secure a wireless-powered untrusted AF-relay network. We analyzed the systemâĂŹs secrecy rates and SOPs. We showed that our proposed scheme outperforms the benchmark schemes. We demonstrated that increasing the number of jamming nodes and jamming powers from the cooperative jammer or the destination node will increase the security of the transmissions as well as the amount of energy transferred to the relays; hence, they will be able to help the source's transmissions in more time slots. We showed that the security is more compromised when the relays are located close to Alice and Bob. That is, in the RDHT mode, when the relays are closer to Alice, the SOP increases since the relays are supposed to forward Alice's transmission but they are not trusted. Hence, to secure communications, the relays should be closer to Alice. On the other hand, when relays are close to Bob, the first-hop becomes the bottleneck for the dual-hop communications since the performance gain achieved from the second-hop is significantly higher. Moreover, when the relays are located far away from Alice, the harvested energy at the relays becomes limited due to the large distance. In addition, the SOP increases as John moves far away from Alice towards Bob. In fact, when John is far away from the untrusted relays, the impact of his jamming signal is low and less energy transfer occurs from John to the relays. Finally, we showed that for the RDHT-only scheme, there is an optimal transmit power level for Alice that minimizes the SOP.

REFERENCES

[1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[2] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104–110, Nov. 2014.
[3] S. Bi and R. Zhang, "Node placement optimization in wireless powered communication networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
[4] K.-H. Liu and P. Lin, "Toward self-sustainable cooperative relays: State of the art and the future," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 56–62, Jun. 2015.
[5] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.
[6] H. Chen, Y. Li, Y. Jiang, Y. Ma, and B. Vucetic, "Distributed power splitting for SWIPT in relay interference channels using game theory," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 410–420, Jan. 2015.
[7] A. A. Nasir, D. T. Ngo, X. Zhou, R. A. Kennedy, and S. Durrani, "Joint resource optimization for multicell networks with wireless energy harvesting relays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6168–6183, Aug. 2016.
[8] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607–1622, May 2015.
[9] I. Krikidis, S. Timotheou, and S. Sasaki, "RF energy transfer for cooperative networks: Data relaying or energy harvesting?" *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1772–1775, Nov. 2012.
[10] Z. Zhou, M. Peng, Z. Zhao, W. Wang, and R. S. Blum, "Wireless-powered cooperative communications: Power-splitting relaying with energy accumulation," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 969–982, Apr. 2016.
[11] J. Kang *et al.*, "Toward secure energy harvesting cooperative networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 114–121, Aug. 2015.
[12] K. Tourki and M.-S. Alouini, "Outage analysis of blind cooperative diversity," *Wireless Commun. Mobile Comput.*, vol. 13, no. 10, pp. 908–915, 2013.
[13] K. Tourki and M.-S. Alouini, "Toward distributed relay selection for opportunistic amplify-and-forward transmission," in *Proc. IEEE 73rd Veh. Technol. Conf. (VTC Spring)*, May 2011, pp. 1–5.
[14] K.-H. Liu, "Performance analysis of relay selection for cooperative relays based on wireless power transfer with finite energy storage," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5110–5121, Jul. 2016.
[15] Y. Gu, H. Chen, Y. Li, and B. Vucetic. (2016). "Distributed multi-relay selection in accumulate-then-forward energy harvesting relay networks." [Online]. Available: https://arxiv.org/abs/1602.00339
[16] Y. Gu, H. H. Chen, Y. Li, and B. Vucetic, "Distributed multi-relay selection in wireless-powered cooperative networks with energy accumulation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.
[17] I. Krikidis, "Relay selection in wireless powered cooperative networks with energy storage," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2596–2610, Dec. 2015.
[18] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.
[19] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.
[20] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Artificial-noise-aided secure MIMO full-duplex relay channels with fixed-power transmissions," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1591–1594, Aug. 2016.
[21] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.
[22] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616–6631, Dec. 2015.
[23] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in af multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.
[24] A. Mabrouk, K. Tourki, and N. Hamdi, "Transmission mode selection scheme for physical layer security in multi-user multi-relay systems," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.
[25] 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.
[26] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.
[27] D. J. Su, S. A. Mousavifar, and C. Leung, "Secrecy capacity and wireless energy harvesting in amplify-and-forward relay networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Aug. 2015, pp. 258–262.
[28] A. Mabrouk, A. El Shafie, K. Tourki, and N. Al-Dhahir, "Adaptive secure transmission for RF-EH untrusted relaying with alien eavesdropping," *IEEE Commun. Lett.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7987800/
[29] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861–1874, May 2016.
[30] M. Zhao, S. Feng, X. Wang, M. Zhang, Y. Liu, and H. Fu, "Joint power splitting and secure beamforming design in the wireless-powered untrusted relay networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
[31] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2703–2709, Jun. 2015.
[32] F. Yuan, Q. T. Zhang, S. Jin, and H. Zhu, "Optimal harvest-use-store strategy for energy harvesting wireless systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 698–710, Feb. 2015.
[33] H. Liu, K. J. Kim, K. S. Kwak, and H. V. Poor, "Power splitting-based SWIPT with decode-and-forward full-duplex relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7561–7577, Nov. 2016.
[34] A. Mabrouk, A. El Shafie, K. Tourki, and N. Al-Dhahir, "AN-aided relay-selection scheme for securing untrusted RF-EH relay systems," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 4, pp. 481–493, Dec. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8013067/
[35] V. N. Q. Bao and H. Van Cuu, "Secure distributed switch-and-stay combining networks: Secure outage probability analysis," in *Proc. 3rd Nat. Found. Sci. Technol. Develop. Conf. Inf. Comput. Sci. (NICS)*, Sep. 2016, pp. 101–106.
[36] Y. Gu, H. Chen, Y. Li, and B. Vucetic, "An adaptive transmission protocol for wireless-powered cooperative communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 4223–4228.
[37] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6–28, Dec. 2004.
[38] I. Krikidis, J. Thompson, S. Mclaughlin, and N. Goertz, "Amplify-and-forward with partial relay selection," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 235–237, Apr. 2008.
[39] D. B. D. Costa and S. Aissa, "Performance analysis of relay selection techniques with clustered fixed-gain relays," *IEEE Signal Process. Lett.*, vol. 17, no. 2, pp. 201–204, Feb. 2010.
[40] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Dec. 2009, Art. no. 305146.
[41] K. Itô, *Diffusion Processes*. Hoboken, NJ, USA: Wiley, 1974.
[42] R. Gallager, *Discrete Stochastic Processes*. Norwell, MA, USA: Kluwer, 1996.
[43] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, May 2012.

AHMED EL SHAFIE (M'10) received the B.Sc. degree (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2009, and the M.Sc. degree in communication and information technology from Nile University, Cairo, Egypt, in 2014. He is currently pursuing the Ph.D. degree with The University of Texas at Dallas, Richardson, TX, USA. He received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer 2015, the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer 2016, and the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer 2016.

ASMA MABROUK was born in Nabeul, Tunisia. She received the B.E. degree in computer science and network engineering from the National School of Computer Sciences, Université de la Manouba, Tunisia, in 2013, where she is currently pursuing the Ph.D. degree. Her research interests include wireless physical layer security, cooperative communications, energy harvesting, and simultaneous wireless information and power transfer.

KAMEL TOURKI (S'05–M'08–SM'13) was born in Antibes, France. He received the B.E. degree in telecommunications from the National School of Engineers of Tunis, Tunisia, in 2003, and the master's and Ph.D. degrees from the University of Nice Sophia-Antipolis, France, in 2004 and 2008, respectively. He was with Texas A&M University at Qatar (TAMUQ) from 2008 to 2014 as a Senior Researcher. He joined the Huawei France Research Center in 2014, where he is currently a Senior Research Engineer. His current research interests lie in the field of 4G/5G wireless communication systems, green cooperative and cognitive systems, PHY security, and energy harvesting. He received twice the Research Fellow Excellence Award from TAMUQ (2011 and 2014), the Best Poster Award at the IEEE DysPan 2012 Conference, and the Outstanding Young Researcher Award from the IEEE Communications Society for Europe - Middle East - Africa region in 2013. He has been elected by the Huawei France Research Staff as the Future Star of Huawei in 2015. He currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE COMMUNICATIONS LETTERS.

NAOFAL AL-DHAHIR (F'07) received the Ph.D. degree in electrical engineering from Stanford University. From 1994 to 2003, he was a Principal Member of the technical staff with GE Research and the AT&T Shannon Laboratory. He is the Erik Jonsson Distinguished Professor with The University of Texas at Dallas, Richardson, TX, USA. He is the co-inventor of 41 issued U.S. patents, co-author of over 325 papers with over 8700 citations, and co-recipient of four IEEE best paper awards, including the 2006 IEEE Donald G. Fink Award. He is the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS.

RIDHA HAMILA (SM'03) received the M.Sc. degree, the Lic. Tech. degree (Hons.), and the Dr.Tech. degree from the Department of Information Technology, Tampere University of Technology (TUT), Tampere, Finland, in 1996, 1999, and 2002, respectively. He is currently an Associate Professor with the Department of Electrical Engineering, Qatar University, Qatar. Also, he is an Adjunct Professor with the Department of Communications Engineering, TUT. From 1994 to 2002, he held various research and teaching positions with the Department of Information Technology, TUT. From 2002 to 2003, he was a System Specialist with the Nokia Research Center and Nokia Networks, Helsinki. From 2004 to 2009, he was with Etisalat University College, Emirates Telecommunications Corporation, United Arab Emirates. In his research areas, he has authored or co-authored over 60 journal and conference papers most of them in the peer-reviewed IEEE publications, filed two patents, and wrote numerous confidential industrial research reports. His current research interests include mobile and broadband wireless communication systems, cellular and satellites-based positioning technologies, synchronization and DSP algorithms for flexible radio transceivers. He has been involved in several past and current industrial projects Qtel, QNRF, Finnish Academy projects, TEKES, Nokia, and EU research and education programs. He supervised a large number of under/graduate students and post-doctoral fellows.