A Distributed Implementation Algorithm for Physical Layer Security Based on Untrusted Relay Cooperation and Artificial Noise

Xiangyu Li, Xueming Wang, Xiangyang Xu, and Liang Jin

In this letter, we consider a cooperation system with multiple untrusted relays (URs). To keep the transmitted information confidential, we obtain joint channel characteristics (JCCs) through combining the channels from the source to the destination. Then, in the null space of the JCCs, jammers construct artificial noise to confuse URs when the source node broadcasts its data. Through a distributed implementation algorithm, the weight of each node can be obtained from its own channel state information. Simulation results show that high-level security of the system can be achieved when internal and external eavesdroppers coexist.

Keywords: Physical layer security, untrusted relay, artificial noise, joint channel characteristics, secrecy rate.

I. Introduction

Recently, to take full advantage of spatial diversity and extend the network coverage, multi-node cooperation has attracted increasing interest in physical-layer security. Many approaches, including cooperative relaying [1] and cooperative jamming [2], have been proposed in the literature. However, when the relay nodes are "untrusted," it is more difficult to ensure system security.

The untrusted relay (UR) was first studied by Oohama in [3], wherein the relay node acted as both an eavesdropper and a transmission helper. In [4], to prevent the UR from wiretapping, the destination node created interference at the same time the source node transmitted information to relays. It was easy for the destination node to obtain original information, but its location limited the interference range. He and Yener also proposed a mechanism using an external interference node, but the same problem still existed [5]. In [6], an interference node was randomly selected from an intermediate node set, but the destination node was also disturbed. Based on this, Zhang and others [7] began to use multiple interference nodes to ensure security, but they assumed that the recipient had perfect knowledge of the jamming signals from friendly jammers.

Works [3] through [7] only selected one node as a relay, which does not take full advantage of multi-node cooperation. There are still many shortcomings in the study of multiple interference nodes. In [1], [8], a multiple relay node scenario was studied, but all the relay nodes were assumed to be credible. To solve these problems, we introduce the concept of joint channel characteristics (JCCs) into a scenario involving multiple jammers and UR nodes, as it is easier to construct artificial noise (AN) [9] in the null space of the JCCs and prevent URs from wiretapping. To reduce the operational complexity of global channel state information (CSI) exchange, a distributed implementation algorithm is proposed. Each individual relay and jammer node can derive its own transmission weight based on local CSI.

Notation. Bold upper and lower case letters denote matrices and vectors, respectively. The superscripts $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ respectively denote the conjugate, transpose, and conjugate transpose. The expectation is denoted by $E\{\cdot\}$. diag(a) stands for a diagonal matrix with a along its main diagonal. $[a]^+ = \max(a, 0)$.

Manuscript received Feb. 27, 2013; revised May 8, 2013; accepted June 3, 2013.

This work was supported by the National Natural Science Foundation of China under Grant (No. 6117118).

Xiangyu Li (phone: +86 0371 8163 2918, luckyxiangyu@gmail.com), Xueming Wang (13007602360@wo.com.cn), Xiangyang Xu (18637191889@163.com), and Liang Jin (liangjin@263.net) are with the Department of Wireless Communication, National Digital Switching System Engineering & Technological Research Center, Henan, China.

II. System Model

We consider an amplify-and-forward (AF) relay network, illustrated in Fig. 1, in which the source node, Alice, wants to send information to the destination node, Bob, under the existence of an external eavesdropper, Eve. There is no direct link between Alice and Bob, so we need to choose N relay nodes, $\mathbf{R}_n$, $n = 1, 2, ..., N$, from the intermediate node set. However, we assume that all the intermediate nodes are untrusted since they act as both internal wiretappers and transmission helpers. As a result, Alice needs other M jammers to cause interference to ensure the transmission security.

Each node in the network is equipped with a single antenna and influenced by white complex Gaussian noise with zero mean and variance σ^2. All the relay and jammer nodes can be randomly chosen from a set of appropriate intermediate nodes to improve the channel diversity. It is natural to choose the nodes near Eve as jammers to produce greater interference. However, when Eve's location is not known, the best choice is to select the nodes near Alice as jammers. Otherwise, secrecy of the area around Alice may be impaired.

Bob and relay nodes send training sequences of channel estimation periodically, so the global CSI except that of Eve is assumed to be available. The flat fading channel coefficients between all the nodes, $\mathbf{h}_{\mathrm{AR}}$, $\mathbf{h}_{\mathrm{RB}}$, $\mathbf{h}_{\mathrm{RE}}$, h_{AE}, $\mathbf{h}_{\mathrm{JE}}$, and $\mathbf{H}_{\mathrm{JR}}$, are shown in Fig. 1. $\mathbf{h}_{\mathrm{AR}} = \left[h_{\mathrm{AR}_1}, h_{\mathrm{AR}_2}, \cdots, h_{\mathrm{AR}_N}\right]$, $\mathbf{h}_{\mathrm{RB}} = \left[h_{\mathrm{R}_1\mathrm{B}}, h_{\mathrm{R}_2\mathrm{B}}, \cdots, h_{\mathrm{R}_N\mathrm{B}}\right]^T$ can be given for example. Since all the relay nodes are independent and untrusted, they can be treated as internal eavesdroppers. It should be guaranteed that both the relay nodes and Eve cannot get any information. If Alice has global CSI, a centralized algorithm (CA) based on JCCs can be given as follows. We ignore the details of the internal transmission and forwarding and combine the two channels, $\mathbf{H}_{\mathrm{JR}}$ and $\mathbf{h}_{\mathrm{RB}}$, into one to get JCCs.

$$\mathbf{h}_{\mathrm{JRB}} = \mathbf{H}_{\mathrm{JR}} \mathbf{W}^H \mathbf{h}_{\mathrm{RB}}, \tag{1}$$

where $\mathbf{W} = \mathrm{diag}[\omega_1, \omega_2, \cdots, \omega_N]$. The transmission process can be divided into two phases.

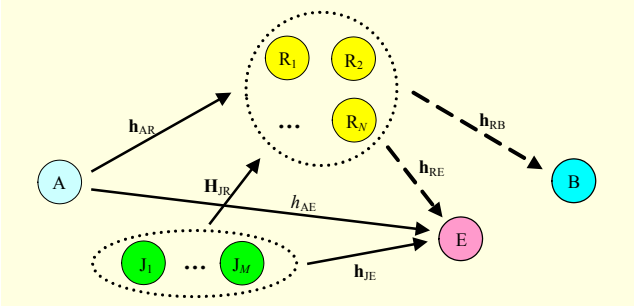

Fig. 1. AF relay network.

In the first phase, Alice broadcasts signal s to all the relay nodes. At the same time, the jammers send AN to cover the information transmission. Therefore, the received signals of the relays and Eve can be described as

$$\mathbf{y}_{\mathrm{R}} = \sqrt{P_{\mathrm{A}}}\mathbf{h}_{\mathrm{AR}}^H s + \sqrt{P_{\mathrm{J}}}\mathbf{H}_{\mathrm{JR}}^H \mathbf{g} z + \mathbf{n}_{\mathrm{R}}, \tag{2}$$

$$y_{\mathrm{E},1} = \sqrt{P_{\mathrm{A}}}h_{\mathrm{AE}}^* s + \sqrt{P_{\mathrm{J}}}\mathbf{h}_{\mathrm{JE}}^H \mathbf{g} z + n_{\mathrm{E},1}. \tag{3}$$

Here, P_{A} and P_{J} represent the transmission power of Alice and the jammers, respectively, z is a complex Gaussian random variable that is used as the jamming signal, and $E\{|s|^2\} = E\{|z|^2\} = 1$. $\mathbf{n}_{\mathrm{R}}$ and $n_{\mathrm{E},1}$ are white complex Gaussian noise. Projection vector $\mathbf{g}$, which is normalized to unity, makes the jamming signals lie in the null space of $\mathbf{h}_{\mathrm{JRB}}$. This can be described as $\mathbf{h}_{\mathrm{JRB}}^H \mathbf{g} = 0$. Since Eve's CSI is completely absent, the AN should be spatially isotropic and $\mathbf{g}$ should be constructed randomly after each packet's transmission.

In the second phase, relay nodes amplify and forward the received signals, $\mathbf{y}_{\mathrm{R}}$, by beamforming. As $\mathbf{y}_{\mathrm{R}}$ already contain AN, jammer nodes do not send any other noise in this phase to decrease the power consumption. The signals received by Bob and Eve are

$$y_{\mathrm{B}} = \mathbf{h}_{\mathrm{RB}}^H \mathbf{W}\mathbf{y}_{\mathrm{R}} + n_{\mathrm{B}} = \sqrt{P_{\mathrm{A}}}h_{\mathrm{ARB}}^* s + \mathbf{h}_{\mathrm{RB}}^H \mathbf{W}\mathbf{n}_{\mathrm{R}} + n_{\mathrm{B}}, \tag{4}$$

$$y_{\mathrm{E},2} = \sqrt{P_{\mathrm{A}}}h_{\mathrm{ARE}}^* s + \sqrt{P_{\mathrm{J}}}\mathbf{h}_{\mathrm{JRE}}^H \mathbf{g} z + \mathbf{h}_{\mathrm{RE}}^H \mathbf{W}\mathbf{n}_{\mathrm{R}} + n_{\mathrm{E},2}, \tag{5}$$

where both n_{B} and $n_{\mathrm{E},2}$ are white complex Gaussian noise. Equations (2) through (5) indicate that all the received signals of URs and Eve contain AN whereas the legitimate receiver, Bob, is not impacted.

III. Distributed Implementation Algorithm

The overall transmission mechanism can be performed at Alice, which involves all necessary system CSI. However, the requirement of global CSI may prevent the application of this mechanism if there is a large number of cooperation nodes or there are fast fading channels, since the overhead of CSI exchange could be extremely high. Thus, each relay and jammer node should better derive its own transmission weight based on local CSI. Herein, we propose such a distributed implementation algorithm (DA) to facilitate the system design.

The calculation of the jammers' projection vector $\mathbf{g}$ needs the full CSI of $\mathbf{h}_{\mathrm{JRB}}$, which is estimated by M jammers. The distributed calculation method can then be given as

$$\begin{aligned} &\mathbf{g} = k_g \left[z_{\mathrm{J}_1}(h_{\mathrm{J}_1\mathrm{RB}}^*)^{-1}, \cdots, z_{\mathrm{J}_M}(h_{\mathrm{J}_M\mathrm{RB}}^*)^{-1}\right]^T, \\ &s.t. \sum_{m=1}^{M} z_{\mathrm{J}_m} = 0, \; z_{\mathrm{J}_m} \in C, \; \left|h_{\mathrm{J}_m\mathrm{RB}}\right| \geq \beta_{\mathrm{J}}. \end{aligned} \tag{6}$$

ETRI Journal, Volume 36, Number 1, February 2014
http://dx.doi.org/10.4218/etrij.14.0213.0090

Here, k_g is the power adjustment coefficient, which is modified dynamically by Alice with some simple feedback information on whether each node's power consumption is beyond its constraint. β_{J} is a threshold by which the jammer node with appropriate CSI is chosen to decline the total power consumption. z_{J_m}, constructed randomly by Alice, can be broadcast to jammers without any CSI. For simplicity, we can make z_{J_m} randomly equal to ± 1 or 0. The m-th jammer is able to get the weight, g_m, only using its own CSI, $h_{\mathrm{J}_m\mathrm{RB}}$.

In spite of the above fact, each jammer still needs to know $\mathbf{W}$ and $\mathbf{h}_{\mathrm{RB}}$, as described in (1), to calculate $h_{\mathrm{J}_m\mathrm{RB}}$. At the same time, we expect that the construction of weight vector ω_n can be distributed in each relay node likewise. So, the distributed calculation method of ω_n can be given as

$$\omega_n = k_\omega (h^*_{\mathrm{R}_n\mathrm{B}})^{-1}, \ \text{when} \left| h_{\mathrm{R}_n\mathrm{B}} \right| \geq \beta_{\mathrm{R}}, \tag{7}$$

where k_ω is a power adjustment coefficient similar to k_g and is the same for all the relay nodes. β_{R} is a threshold that helps us choose a relay node with appropriate CSI. As the n-th relay R_n only needs to know its own CSI $h_{\mathrm{R}_n\mathrm{B}}$ to get ω_n, then

$$h_{\mathrm{J}_m\mathrm{RB}} = \mathbf{h}_{\mathrm{J}_m\mathrm{R}} \mathbf{W}^H \mathbf{h}_{\mathrm{RB}} = k_\omega \sum_{n=1}^{N} h_{\mathrm{J}_m\mathrm{R}_n}. \tag{8}$$

Equation (8) shows that the projection weight of the m-th jammer can be calculated based on its own CSI to the relay nodes $\mathbf{h}_{\mathrm{J}_m\mathrm{R}}$ by using DA.

IV. Secrecy Rate

The maximum achievable secrecy rate [1] is defined as

$$C_s = \max\left[I(y_{\mathrm{B}}, s) - I(y_{\mathrm{E}}, s) \right]^+, \tag{9}$$

where $I(\cdot,\cdot)$ is the mutual information.

$$I(y_{\mathrm{B}}, s) = \frac{1}{2}\log_2(1+\gamma_{\mathrm{B}}), \tag{10}$$

$$I(y_{\mathrm{E}}, s) = \frac{1}{2}\log_2(1+\gamma_{\mathrm{E}}), \tag{11}$$

where γ_{B} and γ_{E} represent the received signal-to-noise ratio (SNR) at Bob and Eve, respectively.

1. Secrecy Rate When Untrusted Relay Exists

The UR nodes can be discussed as internal eavesdroppers. Since Alice has added AN to its transmission signal, which affects relay nodes more seriously than Bob, Bob will get more information than relay nodes. As such, the SNR at Bob can be given as

$$\gamma_{\mathrm{B}} = \frac{P_{\mathrm{A}} \left| h_{\mathrm{ARB}} \right|^2}{\left| \mathbf{h}^H_{\mathrm{RB}} \mathbf{W} \mathbf{n}_{\mathrm{R}} \right|^2 + \sigma^2} = \frac{P_{\mathrm{A}} k_\omega^2 \left| \sum_{n=1}^{N} h_{\mathrm{AR}_n} \right|^2}{\left(N k_\omega^2 + 1 \right) \sigma^2}. \tag{12}$$

The SNR at the n-th relay node can be described as

$$\gamma_{\mathrm{R}_n} = \frac{P_{\mathrm{A}} \left| h_{\mathrm{AR}_n} \right|^2}{P_{\mathrm{J}} \left| \mathbf{h}^H_{\mathrm{JR}_n} \mathbf{g} \right|^2 + \sigma^2}. \tag{13}$$

For the n-th relay, the secrecy rate of the system at a high SNR is

$$\begin{aligned} C_{s,\mathrm{R}_n} \approx \max[& \frac{1}{2}\log(1 + \frac{P_{\mathrm{A}} \left| \sum_{n=1}^{N} h_{\mathrm{AR}_n} \right|^2}{N\sigma^2}) \\ & - \frac{1}{2}\log(1 + \frac{P_{\mathrm{A}} \left| h_{\mathrm{AR}_n} \right|^2}{P_{\mathrm{J}} \left| \mathbf{h}^H_{\mathrm{JR}_n} \mathbf{g} \right|^2})]^+. \end{aligned} \tag{14}$$

2. Secrecy Rate When Eve Exists

The information received by Eve can be divided into two parts: one from Alice and the other from the relay nodes. Due to the existence of extra interference, it is difficult for Eve to completely remove the AN. To maximize the signal-to-interference-plus-noise ratio (SINR) at Eve, the signals received in two phases can be combined as

$$y_e = \begin{bmatrix} h_{\mathrm{AE}} & h_{\mathrm{ARE}} \end{bmatrix} \begin{bmatrix} y_{\mathrm{E},1} & y_{\mathrm{E},2} \end{bmatrix}^T. \tag{15}$$

Therefore, at a high SNR, the SINR of Eve can be approximated more clearly as

$$\gamma_{\mathrm{E}} \approx \frac{P_{\mathrm{A}} \left(\left| h_{\mathrm{AE}} \right|^2 + \left| h_{\mathrm{ARE}} \right|^2 \right)^2}{P_{\mathrm{J}} \left(\left| h_{\mathrm{AE}} \right|^2 \left| \mathbf{h}^H_{\mathrm{JE}} \mathbf{g} \right|^2 + \left| h_{\mathrm{ARE}} \right|^2 \left| \mathbf{h}^H_{\mathrm{JRE}} \mathbf{g} \right|^2 \right)}. \tag{16}$$

Through (12) and (16), we can obtain the secrecy rate $C_{s,\mathrm{E}}$.

3. Secrecy Rate of Whole System

Considering the secrecy rate of the whole system, it should be guaranteed that all the relay nodes and Eve cannot get any information. If there is more than one eavesdropper in the system, the secrecy rate [10] is

$$C_s = \max \min_{j=1,2,\cdots,J} \left[I(y_{\mathrm{B}}, s) - I(y_{\mathrm{E}_j}, s) \right]^+. \tag{17}$$

Here, $I(y_{\mathrm{E}_j}, s)$ represents the information tapped by the j-th eavesdropper. As a result, the system secrecy rate can be described as

$$C_s = \min\left(C_{s,\mathrm{R}_1}, C_{s,\mathrm{R}_2}, \cdots, C_{s,\mathrm{R}_N}, C_{s,\mathrm{E}} \right). \tag{18}$$

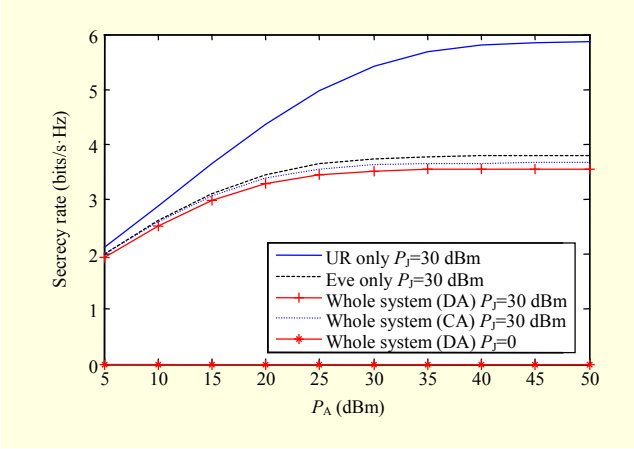

Fig. 2. Secrecy rate vs. P_A.

V. Simulation Results and Analysis

In this section, we carry out simulations to evaluate the achievable secrecy rate of the proposed algorithm. The channels can be expressed as $h = d^{-c/2}e^{j\theta}$, where d is the transmission distance, the path loss exponent c can be chosen as 3.5, and θ is uniformly distributed over $[0, 2\pi)$.

We assume that d_{AR}, that is, the distance between Alice and the n-th relay node, is uniformly distributed over $[80,120]$ m, the same as d_{R_nB}, $d_{J_mR_n}$, and d_{J_mE}. However, Eve always chooses a location near Alice or relay nodes to get information more easily, so it is assumed that d_{AE} and d_{R_nE} are uniformly distributed over $[20,60]$ m. The white noise power is –80 dBm and P_J is 30 dBm. P_A varies from 5 dBm to 50 dBm.

Figure 2 shows the secrecy rate versus P_A in different scripts. When jamming power P_J is 0, the total secrecy rate is very low since Eve can always get more information from Alice. When the jammer nodes begin to send AN, the information leakage is greatly reduced and the security can be improved significantly. As P_A increases, the secrecy rate of the system increases. However, when P_J is fixed and P_A is large enough, the achievable secrecy rate cannot benefit much from the increase of Alice's sending power, which helps both Bob and eavesdroppers to obtain more information.

In contrast to the optimal CA described in section II, the secrecy rate of the DA is a little lower but very close. In fact, their optimal solutions have the same maximum; however, without global CSI, DA cannot control the sending power as precisely as CA does. It requires a short-term convergence process with dynamic adjustment to achieve the optimal solution.

VI. Conclusion

In this letter, we proposed a distributed implementation algorithm for the physical-layer security in a UR system. A transmission mechanism based on JCCs and AN was discussed to prevent the intermediate nodes from wiretapping. Subject to the operational complexity of instantaneous CSI exchange, the projection weight of each jammer and relay node can be obtained only with its local CSI. Simulation results show that high-level security of the system can be achieved even when internal and external eavesdroppers coexist.

References

[1] L. Dong et al., "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, Mar. 2010, pp. 1875-1888.

[2] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, Mar. 2011, pp. 1317-1322.

[3] Y. Oohama, "Capacity Theorems for Relay Channels with Confidential Messages," *Proc. ISIT*, 2007, pp. 926-930.

[4] X. He and A. Yener, "Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming," *Proc. GLOBECOM*, 2008, pp. 1-5.

[5] X. He and A. Yener, "Two-Hop Secure Communication Using an Untrusted Relay," *EURASIP J. Wireless Commun. Netw.*, 2009.

[6] J. Chen et al., "Joint Relay and Jammer Selection for Secure Two-Way Relay Networks," *Proc. ICC*, 2011, pp. 1-5.

[7] R. Zhang et al., "Physical Layer Security for Two-Way Untrusted Relaying with Friendly Jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, Aug. 2012, pp. 3693-3704.

[8] H. Wang et al., "Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems with Individual Power Constraint and No Eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, Jan. 2013, pp. 39-42.

[9] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, June 2008, pp. 2180-2189.

[10] Y. Liang et al., "Compound Wiretap Channels," *EURASIP J. Wireless Commun. Netw.*, 2009.