[5] S. Noh, M. Zoltowski, Y. Sung, and D. Love, "Pilot beam pattern design for channel estimation in massive MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 781–801, Oct. 2014.

[6] J. Choi, D. Love, and P. Bidigare, "Downlink training techniques for FDD massive MIMO systems: Open-loop and closed-loop training with memory," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 802–814, Oct. 2014.

[7] D. Samardzija and N. Mandayam, "Unquantized and uncoded channel state information feedback in multiple-antenna multiuser systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1335–1345, Jul. 2006.

[8] G. Caire, N. Jindal, M. Kobayashi, and N. Ravindran, "Quantized vs. analog feedback for the MIMO broadcast channel: A comparison between zero-forcing based achievable rates," in *Proc. IEEE ISIT*, Jun. 2007, pp. 2046–2050.

[9] X. Zhu *et al.*, "Structured matching pursuit for reconstruction of dynamic sparse channels," in *Proc. IEEE GLOBECOM*, Dec. 2015, pp. 1–5.

[10] Y. Han, P. Zhao, L. Sui, and Z. Fan, "Time-varying channel estimation based on dynamic compressive sensing for OFDM systems," in *Proc. IEEE BMSB*, Jun. 2014, pp. 1–5.

[11] P. Kuo, H. Kung, and P. Ting, "Compressive sensing based channel feedback protocols for spatially-correlated massive antenna arrays," in *Proc. IEEE WCNC*, Apr. 2012, pp. 492–497.

[12] Z. Zhang, K. Teh, and K. Li, "Application of compressive sensing to limited feedback strategy in large-scale multiple-input single-output cellular networks," *IET Commun.*, vol. 8, no. 6, pp. 947–955, Apr. 2014.

[13] X. Rao and V. Lau, "Distributed compressive CSIT estimation and feedback for FDD multi-user massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 62, no. 12, pp. 3261–3271, Jun. 2014.

[14] Y. Barbotin, A. Hormati, S. Rangan, and M. Vetterli, "Estimation of sparse MIMO channels with common support," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3705–3716, Dec. 2012.

[15] J. Ziniel and P. Schniter, "Dynamic compressive sensing of time-varying signals via approximate message passing," *IEEE Trans. Signal Process.*, vol. 61, no. 21, pp. 5270–5284, Nov. 2013.

[16] C. Tan and N. Beaulieu, "On first-order Markov modeling for the Rayleigh fading channel," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2032–2040, Dec. 2000.

[17] K. Baddour and N. Beaulieu, "Autoregressive modeling for fading channel simulation," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1650–1662, Jul. 2005.

[18] H. Shirani-Mehr and G. Caire, "Channel state feedback scheme for multiuser MIMO-OFDM downlink," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2713–2723, Sep. 2009.

[19] M. Duarte and Y. Eldar, "Structured compressed sensing: From theory to applications," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4053–4085, Sep. 2011.

[20] Y. Eldar and G. Kutyniok, *Compressed Sensing: Theory and Applications*. Cambridge, U.K.: Cambridge Univ. Press, May 2012.

[21] Z. Gao, L. Dai, Z. Wang, and S. Chen, "Spatially common sparsity based adaptive channel estimation and feedback for FDD massive MIMO," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6169–6183, Dec. 2015.

Two Birds With One Stone: Towards Secure and Interference-Free D2D Transmissions via Constellation Rotation

Li Sun, Qinghe Du, Pinyi Ren, and Yichen Wang

***Abstract*—This paper studies the cooperative device-to-device (D2D) transmissions in cellular networks, where two D2D users communicate bidirectionally with each other and simultaneously serve as relays to assist the two-way transmissions between two cellular users. For this scenario, both cellular and D2D links share the same spectrum, thus creating mutual interference. In addition to that, a security problem also exists since the cellular users want to keep their messages secret from the D2D users and *vice versa*. To address these two issues, a security-embedded interference avoidance scheme is proposed in this paper. By exploiting the constellation rotation technique, the proposed scheme can create interference-free links for both D2D and cellular communications, thereby significantly improving the system error performance. Moreover, our scheme also provides an inherent secrecy protection at the physical layer, which makes the information exchange between cellular users and that between D2D users confidential from each other.**

***Index Terms*—Constellation rotation, device-to-device (D2D) communications, interference avoidance, physical-layer security.**

I. Introduction

With the explosive growth of the proximity-aware services such as media sharing, online gaming, and social networking, device-to-device (D2D) communications has emerged as an underlay approach to cellular network and has strongly appealed to both the academia and the industry [1], [2]. In cellular networks supporting D2D communications, both cellular and D2D links share the same radio resources, and the mutual interference between these two types of links severely hampers the system performance. Therefore, interference management plays a critically important role in enabling efficient D2D communications. To date, extensive research has been undertaken to investigate the avoidance, coordination, and cancellation of the interference between cellular and D2D transmissions [3]–[5].

The existing works regarding interference management mainly focuses on the use of power control, resource allocation, or signal processing approaches. By introducing the cooperation between cellular and D2D users, the mutual interference can also be suppressed, and the system performance can be further improved. The integration of cooperative relaying technique into D2D communications forms a new D2D networking paradigm: *cooperative D2D transmissions*.

Manuscript received March 21, 2015; revised August 12, 2015, October 26, 2015; accepted November 14, 2015. Date of publication December 4, 2015; date of current version October 13, 2016. This work was supported in part by the National Natural Science Foundation of China under Grant 61431011 and Grant 61201207 and in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, under Grant 2012D04. The review of this paper was coordinated by Prof. M. C. Gursoy.

L. Sun is with the Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: lisun@mail.xjtu.edu.cn).

Q. Du, P. Ren, and Y. Wang are with the Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: duqinghe@mail.xjtu.edu.cn; pyren@mail.xjtu.edu.cn; wangyichen0819@mail.xjtu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2505715

The key idea is to allow the D2D transmitter (DT) to act as a relay for the cellular link in exchange for the transmission opportunities. As an embodiment of this idea, a network-coding-aided cooperative strategy was developed in [6] for D2D-enabled cellular networks. In [7], a superposition-coding based scheme was proposed, for which DT sends the linear combination of its own information and the decoded information from CU. This scheme, however, suffers from the low spectrum utilization due to the half-duplex constraint of the nodes. To overcome this drawback, in [8], a spectrally efficient cooperative D2D transmission strategy was proposed, which allows two D2D users to communicate bidirectionally while assisting the two-way transmissions between cellular base station (BS) and cellular user (CU).

Although the cooperative strategy in [8] is spectrally efficient, it may give rise to two critical problems. First, every terminal has to detect its desired signal while being interfered by the signal intended for other nodes. This results in an irreducible error floor as the SNR grows and deteriorates the achievable symbol error probability (SEP) performance dramatically. Second, in practical systems, the cellular users may want to keep their messages secret from the D2D users and *vice versa*. However, the scheme in [8] allows every node to access the data transmitted from any other node, which violates the users' secrecy requirements.

To address these two issues, we in this paper propose a security-embedded interference avoidance scheme. This scheme is based on the concept of constellation rotation. Through rotating the signal constellation and exploiting the *intrinsic orthogonality* between the real and the imaginary components of the complex signal, the interuser interference is perfectly avoided, and the error floor can be completely eliminated. In addition to that, by using our scheme, the signals from the cellular users (D2D users) can be aligned in the same direction at the D2D users (cellular users), thereby enhancing the secrecy of data exchange at the physical layer.

It should be pointed out that securing transmissions at the physical layer (also known as physical-layer security) has already attracted considerable attention in recent years, and several physical-layer security protocols have been developed so far for various systems [9]–[12]. With respect to D2D-enabled cellular networks, in [13], it was shown that, in most scenarios, the D2D mode can offer a security advantage over the conventional two-hop messaging through the BS. The work in [14] proposed to exploit the interference generated by D2D communications to enhance the security of cellular links and simultaneously create extra transmission opportunities for D2D users. In [15], the robust secrecy rate optimizations were studied for multiuser multiple-input–single-output channel with D2D communications, where the D2D nodes help to improve the secrecy of information exchange between the legitimate user pairs. Common to the works [13]–[15] is that all of them assume that the eavesdropper(s) are *external* nodes in addition to the legitimate parties (including both the cellular and D2D users). In contrast, we consider a scenario where there is no external eavesdropper, and the security problem comes from the mutual distrust between cellular and D2D user pairs. Therefore, the addressed issue in this paper is totally different from the existing literature on D2D communications security.

The main contributions of this paper can be summarized as follows.

1) Based on the concept of constellation rotation, a security-embedded interference avoidance scheme is proposed. By using this scheme, the interference-free transmissions are realized for both the cellular and D2D users, and the secrecy requirements of these users can be guaranteed as well.
2) We propose two criteria of choosing the rotation angles. The first one aims to minimize the SEP upper bound for the intended messages, thus improving the communications reliability. The second one tries to balance the demands of reliability and security. By using this criterion, an error floor is *created* for detection of the *unintended* messages, and the transmission secrecy is improved.
3) We analyze the achievable SEP performance for both the cellular and D2D users. Specifically, the closed-form expressions for the upper bounds of the SEPs are derived. It is shown through the numerical simulations that the derived theoretical results match well with the simulated ones.

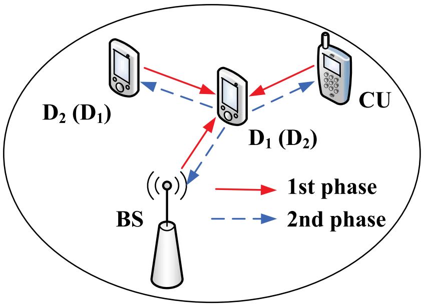

Fig. 1. System model.

II. System Model

As shown in Fig. 1, we consider a system consisting of one BS, one CU, and two D2D users (denoted by D_1 and D_2). The BS and CU need to establish a two-way communication, but the distance between them is too far to connect directly. Meanwhile, due to the proximity of D_1 and D_2, they want to communicate with each other bidirectionally to support local services. Thus, the BS may allow the D2D pair to reuse the cellular spectrum to exchange messages directly. In return, one of the D2D users acts as a relay to facilitate the communications between the BS and CU. We introduce d_{ij} to represent the distance between node i and j. Then, D_1 is selected if $\max\{d_{\mathrm{BS},D_1}, d_{\mathrm{CU},D_1}\} < \max\{d_{\mathrm{BS},D_2}, d_{\mathrm{CU},D_2}\}$, and D_2 is selected otherwise. For the ease of discussions, we assume that D_1 is selected as the relay node in what follows, and relay selection will be considered in the simulations in Section VI.

Every cooperation period is divided into two phases. During the first phase, the BS, CU, and D_2 transmit their individual messages to D_1. During the second phase, D_1 forwards the combination of BS and CU's signals to realize the two-way information exchange between the cellular users, and it simultaneously delivers its own message to D_2 as well.

All terminals are single-antenna devices and operative in a time-division duplex (TDD) mode. The channel coefficients between BS and D_1, CU and D_1, and D_1 and D_2, separately denoted by h_{B1}, h_{C1}, and h_{12}, are modeled as zero-mean complex Gaussian random variables with variances μ_{B1}, μ_{C1}, and μ_{12}, respectively. Here, we have already assumed all the links are reciprocal, i.e., $h_{ij} = h_{ji}$ for all i's and j's. We introduce $|h_{ij}|$ and $\angle h_{ij}$ to denote the amplitude and phase of h_{ij}, respectively. The channel coefficients remain constant within one cooperation period and vary independently among periods. We presume that each node only has the local channel state information (CSI), i.e., the channel coefficients of the links connecting this node and its neighboring nodes. We further assume that BS (CU) also has $h_{C1}(h_{B1})$. The transmit power of each node is constrained by P, and the additive noise at each receiver is represented by a zero-mean complex Gaussian variable with variance N_0. We denote the average SNR of the system by $\rho = P/N_0$. For the considered channel model, the received SNR of the $i \to j$ link can be expressed as $\gamma_{ij} = \rho|h_{ij}|^2$, which follows an exponential distribution with the rate parameter $\lambda_{ij} = (\rho\mu_{ij})^{-1}$. Throughout this paper, $\Pr(A)$ stands for the probability of event A, $E(\cdot)$ is the expectation operator, and $\Re\{x\}$, $\Im\{x\}$, and x^* are used to denote the real component, imaginary component, and the complex conjugate of x, respectively.

III. Security-Embedded Interference Avoidance Scheme

We now present the proposed security-embedded interference avoidance scheme. The basic idea is to rotate signal constellations, which was first proposed in [16] as a diversity approach over fading channels. We denote u as the original complex constellation, taking values from an alphabet $\mathcal{X}$. Then, the transmitted symbol is $x = e^{j\theta}u$, where θ is the rotation angle chosen in such a way that no two symbols have the same coordinate. That is, for any $i \neq k$, we have

$$\Re\{x^i\} \neq \Re\{x^k\},\ \Im\{x^i\} \neq \Im\{x^k\},\ \forall x^i, x^k \in e^{j\theta}\mathcal{X}. \tag{1}$$

In our scheme, constellation rotation is applied to every symbol prior to transmission.

In the first phase, the BS transmits $\sqrt{P}\Re\{x_B\}e^{-j\angle h_{B1}}$ with x_B being its information-bearing signal.[1] Similarly, CU and D_2 send $\sqrt{P}\Re\{x_C\}e^{-j\angle h_{C1}}$ and $j\sqrt{P}\Re\{x_{D_2}\}e^{-j\angle h_{12}}$, respectively. The received signal at D_1 is expressed as

$$y_{D_1}^{(1)} = \sqrt{P}\left(|h_{B1}|\Re\{x_B\} + |h_{C1}|\Re\{x_C\} + j|h_{12}|\Re\{x_{D_2}\}\right) + w_{D_1}^{(1)} \tag{2}$$

where $w_n^{(m)}$ stands for the noise at node n during phase m ($n \in \{\mathrm{BS}, \mathrm{CU}, D_1, D_2\}$, $m \in \{1, 2\}$). D_1 extracts the imaginary component of $y_{D_1}^{(1)}$ to estimate $\Re\{x_{D_2}\}$. According to (1), there is a one-to-one mapping between the rotated constellation and its real (or imaginary) part. Therefore, x_{D_2} can be determined from $\Re\{x_{D_2}\}$.

On the other hand, D_1 also acts as an eavesdropper and attempts to decode the messages from the BS and CU. To fulfill this, D_1 extracts the real part of $y_{D_1}^{(1)}$ to yield

$$\Re\left\{y_{D_1}^{(1)}\right\} = \sqrt{P}|h_{B1}|\Re\{x_B\} + \sqrt{P}|h_{C1}|\Re\{x_C\} + \Re\left\{w_{D_1}^{(1)}\right\} \tag{3}$$

based on which the joint decoding is performed to estimate $\Re\{x_B\}$ and $\Re\{x_C\}$ (equivalently, x_B and x_C).[2] However, these two signals are aligned in the same direction at D_1, thereby increasing the difficulty of decoding the cellular messages and making the BS ↔ CU transmission more secure.

During the second phase, D_1 needs to forward the messages of the BS and CU to complete the two-way communications between these two entities. Meanwhile, it also wants to deliver its own information *securely* to D_2. To accomplish the whole task at one stroke, D_1 transmits the following signal:

$$x_{D_1}^{(\mathrm{trans})} = \sqrt{\frac{P}{2}}\left[\alpha\Re\left\{y_{D_1}^{(1)}\right\} + j\left(\frac{1}{\sqrt{2}}\Re\{x_{D_1}\} + \frac{\beta}{\sqrt{2}}\Im\left\{y_{D_1}^{(1)}\right\}\right)\right] \tag{4}$$

where x_{D_1} is D_1's message intended for D_2. $\alpha = 1/\sqrt{P|h_{B1}|^2 + P|h_{C1}|^2 + N_0/2}$ and $\beta = 1/\sqrt{P|h_{12}|^2 + N_0/2}$ are normalization factors such that the transmit power at D_1 is P. The received signal at D_2 is given by $y_{D_2}^{(2)} = h_{12}x_{D_1}^{(\mathrm{trans})} + w_{D_2}^{(2)}$. By multiplying $y_{D_2}^{(2)}$ by $h_{12}^*/|h_{12}|^2$ and extracting the imaginary part, we can obtain the decision statistics as

$$\begin{aligned}
&\Im\left\{\frac{h_{12}^*}{|h_{12}|^2}y_{D_2}^{(2)}\right\}\\
&\quad= \sqrt{\frac{P}{2}}\left(\frac{1}{\sqrt{2}}\Re\{x_{D_1}\} + \frac{\beta}{\sqrt{2}}\Im\left\{y_{D_1}^{(1)}\right\}\right) + \Im\left\{\frac{h_{12}^*}{|h_{12}|^2}w_{D_2}^{(2)}\right\}\\
&\quad= \frac{\sqrt{P}}{2}\Re\{x_{D_1}\} + \frac{P}{2}\beta|h_{12}|\Re\{x_{D_2}\} + n_{e,D2}
\end{aligned} \tag{5}$$

where $n_{e,D2} = (\sqrt{P}/2)\beta\Im\{w_{D_1}^{(1)}\} + \Im\{(h_{12}^*/|h_{12}|^2)w_{D_2}^{(2)}\}$. Since $\Re\{x_{D_2}\}$ is the transmitted signal of D_2 during the previous phase, D_2 will first subtract $(P/2)\beta|h_{12}|\Re\{x_{D_2}\}$ from $\Im\{(h_{12}^*/|h_{12}|^2)y_{D_2}^{(2)}\}$ and then detect $\Re\{x_{D_1}\}$ (or equivalently x_{D_1}) based on the remainder. After some tedious calculations, we can derive the SNR expression for the $D_1 \to D_2$ link as

$$\gamma^{(\mathrm{D_1 \to D_2})} = \frac{\gamma_{12}(2\gamma_{12} + 1)}{5\gamma_{12} + 2}. \tag{6}$$

Like D_1, D_2 also wants to eavesdrop BS and CU's messages. Notice that the cellular users' information is contained only in the real component of D_1's transmitted signal. Hence, D_2 constructs the following decision statistics to complete eavesdropping:

$$\begin{aligned}
\Re\left\{\frac{h_{12}^*}{|h_{12}|^2}y_{D_2}^{(2)}\right\} &= \sqrt{\frac{P}{2}}\alpha\Re\left\{y_{D_1}^{(1)}\right\} + \Re\left\{\frac{h_{12}^*}{|h_{12}|^2}w_{D_2}^{(2)}\right\}\\
&= \alpha\frac{P}{\sqrt{2}}\left(|h_{B1}|\Re\{x_B\} + |h_{C1}|\Re\{x_C\}\right)\\
&\quad + \sqrt{\frac{P}{2}}\alpha\Re\left\{w_{D_1}^{(1)}\right\} + \Re\left\{\frac{h_{12}^*}{|h_{12}|^2}w_{D_2}^{(2)}\right\}.
\end{aligned} \tag{7}$$

It can be seen from (7) that the signals from the BS and CU (i.e., $\Re\{x_B\}$ and $\Re\{x_C\}$) are aligned at D_2. This makes it difficult for the joint decoding of these two signals and thus enhances the physical-layer security.

Now, attention is shifted to the signal reception and processing at the cellular users within the second phase. The received signal at the BS can be represented as $y_{\mathrm{BS}}^{(2)} = h_{B1}x_{D_1}^{(\mathrm{trans})} + w_{\mathrm{BS}}^{(2)}$. Similar to what D_2 does as mentioned earlier, the BS first multiplies $y_{\mathrm{BS}}^{(2)}$ by $h_{B1}^*/|h_{B1}|^2$ and then extracts the real part to obtain

$$\begin{aligned}
\Re\left\{\frac{h_{B1}^*}{|h_{B1}|^2}y_{\mathrm{BS}}^{(2)}\right\} &= \sqrt{\frac{P}{2}}\alpha\Re\left\{y_{D_1}^{(1)}\right\} + \Re\left\{\frac{h_{B1}^*}{|h_{B1}|^2}w_{\mathrm{BS}}^{(2)}\right\}\\
&= \frac{P}{\sqrt{2}}\alpha|h_{B1}|\Re\{x_B\} + \frac{P}{\sqrt{2}}\alpha|h_{C1}|\Re\{x_C\} + n_{e,\mathrm{BS}}
\end{aligned} \tag{8}$$

where $n_{e,\mathrm{BS}} = \sqrt{P/2}\alpha\Re\{w_{D_1}^{(1)}\} + \Re\{(h_{B1}^*/|h_{B1}|^2)w_{\mathrm{BS}}^{(2)}\}$. After canceling the self-interference term $(P/\sqrt{2})\alpha|h_{B1}|\Re\{x_B\}$, $\Re\{x_C\}$ (or equivalently x_C) can be decoded, using the ML method, from

$$\begin{aligned}
y_{\mathrm{BS}}^{(\mathrm{rem})} &\triangleq \Re\left\{\frac{h_{B1}^*}{|h_{B1}|^2}y_{\mathrm{BS}}^{(2)}\right\} - \frac{P}{\sqrt{2}}\alpha|h_{B1}|\Re\{x_B\}\\
&= \frac{P}{\sqrt{2}}\alpha|h_{C1}|\Re\{x_C\} + n_{e,\mathrm{BS}}
\end{aligned} \tag{9}$$

[1] Here, we have assumed that the real part of the transmitted signal is normalized such that $E[|\Re\{x\}|^2] = 1$. This assumption also holds in the following discussions.

[2] It is emphasized that the joint maximum likelihood (ML) detection (i.e., the multiuser detection) method is adopted at D_1 to decode the signals from BS and CU. Similar assumptions hold in (7), (11), and (12) as well. In the simulations in Section VI, we also adopt this assumption to generate the results.

and the resultant instantaneous SNR expression for the CU → BS transmission can be calculated as

$$\gamma^{(\mathrm{CU}\to\mathrm{BS})} = \frac{2\gamma_{B1}\gamma_{C1}}{3\gamma_{B1}+2\gamma_{C1}+1}. \tag{10}$$

From the secrecy perspective, we assume the BS as an eavesdropper for the data exchange between D_1 and D_2. By multiplying $y_{\mathrm{BS}}^{(2)}$ by $h_{B1}^*/|h_{B1}|^2$ and extracting the imaginary component, BS can obtain

$$\begin{aligned}\Im&\left\{\frac{h_{B1}^*}{|h_{B1}|^2}y_{\mathrm{BS}}^{(2)}\right\}\\ &= \sqrt{\frac{P}{2}}\left(\frac{1}{\sqrt{2}}\Re\{x_{D_1}\}+\frac{\beta}{\sqrt{2}}\Im\left\{y_{D_1}^{(1)}\right\}\right)+\Im\left\{\frac{h_{B1}^*}{|h_{B1}|^2}w_{\mathrm{BS}}^{(2)}\right\}\\ &= \frac{\sqrt{P}}{2}\Re\{x_{D_1}\}+\frac{P}{2}\beta|h_{12}|\Re\{x_{D_2}\}\\ &\quad+\frac{\sqrt{P}}{2}\beta\Im\left\{w_{D_1}^{(1)}\right\}+\Im\left\{\frac{h_{B1}^*}{|h_{B1}|^2}w_{\mathrm{BS}}^{(2)}\right\}\end{aligned} \tag{11}$$

from which BS tries to jointly decode x_{D_1} and x_{D_2}. However, the detection performance will be rather poor due to the alignment of these two signals, which protects the secrecy of $D_1 \leftrightarrow D_2$ transmission.

Due to the symmetry between the CU → D_1 → BS link and the BS → D_1 → CU link, the signal detection at CU is almost the same as that performed at BS. The eavesdropping procedure is also similar to that conducted at BS. Specifically, CU extracts the D2D information based on the following:

$$\begin{aligned}\Im\left\{\frac{h_{C1}^*}{|h_{C1}|^2}y_{\mathrm{CU}}^{(2)}\right\} &= \frac{\sqrt{P}}{2}\Re\{x_{D_1}\}+\frac{P}{2}\beta|h_{12}|\Re\{x_{D_2}\}\\ &\quad+\frac{\sqrt{P}}{2}\beta\Im\left\{w_{D_1}^{(1)}\right\}+\Im\left\{\frac{h_{C1}^*}{|h_{C1}|^2}w_{\mathrm{CU}}^{(2)}\right\}\end{aligned} \tag{12}$$

where $y_{\mathrm{CU}}^{(2)}$ and $w_{\mathrm{CU}}^{(2)}$ are the received signal and the additive noise at CU during the second phase, respectively.

Remark 1: From the given descriptions, we can find that the signal detections for the *intended* messages at all the terminals are free of interference, and the SEP error floor can be perfectly eliminated as a result. Moreover, the *unintended* messages are aligned in the same direction at each node, thus providing an inherent antieavesdropping capability.[3]

Remark 2: The considered system model in our paper can be thought of as a pairwise data exchange model, which is a special type of the multiway relay channel [17]. To the best of our knowledge, there are only two studies, i.e., [18] and [19], discussing the security issue for multiway relay systems with an untrusted relay. However, the work in [18] was based on the compute-and-forward framework, and the focus of [18] was on the achievable secrecy rate region analysis. On the other hand, the work in [19] allocated orthogonal transmission resources to different user pairs to avoid the interference and exploited a friendly jammer to send jamming signals to disturb the untrusted relay. Comparably, the proposed scheme in this paper utilizes signal design approach to prevent information leakage to the untrusted entities, which is completely different from these two papers.

IV. Choice of the Rotation Angles

Here, two criteria will be given to choose the rotation angles. To facilitate the presentations, we name these two criteria as the CSI-free criterion and the CSI-based criterion, respectively.

A. CSI-Free Criterion

The CSI-free criterion aims to optimize the system SEP. To formulate this criterion, the error performance of the CU → D_1 → BS link will be first dealt with. Making use of the union bound, the instantaneous SEP of this end-to-end transmission can be upper bounded by

$$\begin{aligned}&\Pr\{\mathrm{error}|h_{B1},h_{C1}\}\\ &\quad\le \sum_{x_C\in e^{j\theta}\mathcal{X}}\Pr(x_C)\sum_{\substack{\hat{x_C}\ne x_C\\ \hat{x_C}\in e^{j\theta}\mathcal{X}}}\Pr\{x_C\to\hat{x_C}|h_{B1},h_{C1}\}\\ &\quad=\frac{1}{|\mathcal{X}|}\sum_{\substack{x_C,\hat{x_C}\in e^{j\theta}\mathcal{X}\\ \hat{x_C}\ne x_C}}\Pr\{x_C\to\hat{x_C}|h_{B1},h_{C1}\}\end{aligned} \tag{13}$$

where $|\mathcal{X}|$ is the cardinality of $\mathcal{X}$, and $\Pr\{x_C\to\hat{x_C}|h_{B1},h_{C1}\}$ represents the conditional pairwise error probability (PEP) of confusing x_C with $\hat{x_C}$. In (13), we have assumed that each $x_C\in e^{j\theta}\mathcal{X}$ has the same prior probability. Based on (9), the conditional PEP in (13) can be derived as

$$\begin{aligned}\Pr\{x_C\to\hat{x_C}|h_{B1},h_{C1}\} &= Q\left(\frac{1}{2}\sqrt{d_{C,\hat{C}}^2\gamma^{(\mathrm{CU}\to\mathrm{BS})}}\right)\\ &\le Q\left(\frac{1}{2}\sqrt{d_{\min,C}^2\gamma^{(\mathrm{CU}\to\mathrm{BS})}}\right)\end{aligned} \tag{14}$$

where $d_{C,\hat{C}}=\Re\{x_C\}-\Re\{\hat{x_C}\}$, $d_{\min,C}^2=\min_{x_C,\hat{x_C}}|\Re\{x_C\}-\Re\{\hat{x_C}\}|^2$, $Q(x)\triangleq(1/\sqrt{2\pi})\int_x^\infty e^{-(t^2/2)}dt$ is the Gaussian-Q function, and $\gamma^{(\mathrm{CU}\to\mathrm{BS})}$ is the received SNR given by (10). By substituting (14) into (13), the instantaneous SEP of the CU → BS transmission can be obtained.

Following similar analysis as given, we can also derive the instantaneous SEP expressions for the BS → CU, $D_1\to D_2$, and $D_2\to D_1$ transmissions. All these results indicate that, to reduce the error probability of the $i\to j$ transmission, the transmitter (i.e., node i) should choose such an angle that can *maximize the minimum squared distance* among all the real parts of signal points in its rotated constellation set, i.e.,

$$\theta^* = \arg\max_{\theta\in(0,2\pi)} d_{\min}^2 \tag{15}$$

which does not rely on the CSI and only depends on the adopted modulation type (alphabet).[4] Therefore, the proposed criterion herein enjoys very low complexity. The rotation angles for some commonly used modulations, which are obtained based on (15), can be found in Table I.[5]

[3] The proposed scheme can also be applied to a multiuser scenario where multiple CUs are served by one BS. For this scenario, a single CU should be first selected out of all the CUs prior to each cooperation period. After that, the two-phase cooperative transmission starts, and the proposed scheme can be applied without any modifications.

[4] Since the adopted alphabets at different nodes may not be identical, the chosen rotation angles at these nodes can also be different.

[5] We emphasize that, although the rotation angles can be determined without knowing the CSI, the proposed scheme, as is described in Section III, relies on the availability of the CSI. Therefore, the CSI-free method can only avoid real-time calculating or updating the rotation angles but cannot make the whole scheme completely CSI free.

TABLE I
ROTATION ANGLES FOR SOME COMMONLY USED MODULATIONS (UNDER THE CSI-FREE CRITERION)

Modulation type	θ (degrees)
QPSK	26.56
8PSK	52.86
16QAM	75.96
64QAM	7.12

B. CSI-Based Criterion for Cellular Users

Unlike the CSI-free criterion which only targets at the SEP optimization, the CSI-based criterion aims at balancing the users' reliability and security requirements. To illuminate our ideas, let us first look at the secrecy performance improvement for the cellular users. From Section III, we have learned that the leakage of BS and CU's information happens within both the first and second phases. To be specific, D_1 and D_2 try to decode the cellular messages based on (3) and (7), respectively, where $\Re\{x_B\}$ and $\Re\{x_C\}$ are aligned in the same direction. The difficulty of eavesdropping can be further increased if the following condition is met for some $k \neq l$:

$$|h_{B1}|\Re\left\{u_B^{(k)}e^{j\theta_{\mathrm{BS}}}\right\}+|h_{C1}|\Re\left\{u_C^{(l)}e^{j\theta_{\mathrm{CU}}}\right\} = |h_{B1}|\Re\left\{u_B^{(l)}e^{j\theta_{\mathrm{BS}}}\right\}+|h_{C1}|\Re\left\{u_C^{(k)}e^{j\theta_{\mathrm{CU}}}\right\} \quad (16)$$

where $u_B^{(k)}, u_B^{(l)} \in \mathcal{X}_{\mathrm{BS}}$ and $u_C^{(k)}, u_C^{(l)} \in \mathcal{X}_{\mathrm{CU}}$. In (16), we have already used the relationship between the original constellation and the rotated constellation, i.e., $x = e^{j\theta}u$.

The constraint in (16) destroys the one-to-one correspondence between the aligned signal (i.e., $|h_{B1}|\Re\{x_B\}+|h_{C1}|\Re\{x_C\}$) and the two individual signals (i.e., $\Re\{x_B\}$ and $\Re\{x_C\}$). As a result, even if the system SNR goes to infinity such that the aligned signal can be perfectly eavesdropped by D_1 or D_2, the detection for the individual signals still suffers from high error rate, and an error floor can be created.

While (16) sheds light on the design of rotation angles toward enhanced security, it does not provide an explicit criterion. Aiming at this problem, we proceed to find a sufficient yet not necessary condition for (16). For simplicity, we assume that BS and CU adopt the same modulation format, i.e., $\mathcal{X}_{\mathrm{BS}} = \mathcal{X}_{\mathrm{CU}} = \mathcal{X}$. By exploiting this assumption and doing some simple manipulations, (16) can be rewritten as

$$\Re\left\{|h_{B1}|\left(u^{(k)}-u^{(l)}\right)e^{j\theta_{\mathrm{BS}}}\right\} = \Re\left\{|h_{C1}|\left(u^{(k)}-u^{(l)}\right)e^{j\theta_{\mathrm{CU}}}\right\}, \text{for some } k \neq l. \quad (17)$$

By Further imposing a constraint that $u^{(k)}-u^{(l)}$ is a real number, we can simplify (17) as

$$|h_{B1}|\cos\theta_{\mathrm{BS}} = |h_{C1}|\cos\theta_{\mathrm{CU}}. \quad (18)$$

It is obvious that the solution to (18), i.e., the $(\theta_{\mathrm{BS}}, \theta_{\mathrm{CU}})$ pair satisfying (18), is not unique. Among all these solutions, we would like to choose a single pair to optimize the system SEP performance, which yields the proposed criterion as

$$(\theta_{\mathrm{CU}}^*, \theta_{\mathrm{BS}}^*) = \underset{|h_{B1}|\cos\theta_{\mathrm{BS}}=|h_{C1}|\cos\theta_{\mathrm{CU}}}{\arg\max} \min\left\{d_{\min,B}^2, d_{\min,C}^2\right\} \quad (19)$$

where $d_{\min,B}^2 = \min_{x_B,\hat{x_B}} |\Re\{x_B\}-\Re\{\hat{x_B}\}|^2$ and $d_{\min,C}^2 = \min_{x_C,\hat{x_C}} |\Re\{x_C\}-\Re\{\hat{x_C}\}|^2$. Intuitively speaking, the chosen angles can optimize the error performance of the worse link between BS → CU and CU → BS transmissions, while guaranteeing the security of both links. The search operation in (19) can be performed at the BS and CU, distributively. It is also feasible to let the BS conduct the search and then broadcast the result to CU. Compared with (15), the implementation of the criterion in (19) requires real-time calculations based on the instantaneous CSI and incurs increased complexity correspondingly.

C. CSI-Based Criterion for D2D Users

D2D users' information is eavesdropped by BS and CU at the end of the second phase. To be specific, BS and CU extract D2D users' signals based on (11) and (12), respectively. Applying similar analysis as above, we can formulate the criterion of choosing the rotation angles at D_1 and D_2 (i.e., θ_{D_1} and θ_{D_2}) as

$$\left(\theta_{D_1}^*, \theta_{D_2}^*\right) = \underset{\cos\theta_{D_1}=\sqrt{P}\beta|h_{12}|\cos\theta_{D_2}}{\arg\max} \min\left\{d_{\min,D_1}^2, d_{\min,D_2}^2\right\} \quad (20)$$

where $d_{\min,D_1}^2 = \min_{x_{D_1},\hat{x_{D_1}}} |\Re\{x_{D_1}\}-\Re\{\hat{x_{D_1}}\}|^2$ and $d_{\min,D_2}^2 = \min_{x_{D_2},\hat{x_{D_2}}} |\Re\{x_{D_2}\}-\Re\{\hat{x_{D_2}}\}|^2$. Like (19), the angles chosen as per (20) not only provides an enhanced security performance but also minimizes the SEP upper bound of the worse link between $D_1 \to D_2$ and $D_2 \to D_1$ transmissions.

Remark 3: One may recall that (1) has to be satisfied to make the proposed scheme work. However, it can be easily seen that the minimum of the two squared distances in (20) will be zero if either of the two angles (i.e., θ_{D_1} or θ_{D_2}) violates the condition in (1). Therefore, it suffices to find θ_{D_1} and θ_{D_2} based on (20), and the constraint in (1) does not need to be explicitly mentioned. Similar conclusion applies to (15) and (19) as well.

V. SYMBOL ERROR PROBABILITY ANALYSIS

It is rather difficult, if not impossible, to analyze the SEP performance of our scheme with CSI-based rotation angle selection. Therefore, we only present the analytical results for the system SEP under the CSI-free criterion.

A. SEP for Cellular Users

The error performance for the cellular users will be first dealt with. By averaging (13) over the distributions of the channel gains, the end-to-end SEP of the CU → BS link can be upper bounded by

$$P_E^{(C)} \leq \frac{1}{|\mathcal{X}|}\sum_{\substack{x_C,\hat{x_C}\in e^{j\theta}\mathcal{X}\\ \hat{x_C}\neq x_C}} \Pr\{x_C \to \hat{x_C}\} \quad (21)$$

where $\Pr\{x_C \to \hat{x_C}\}$ is the unconditional PEP. In (14), the conditional PEP is derived as $\Pr\{x_C \to \hat{x_C}|h_{B1}, h_{C1}\} = Q\left((1/2)\sqrt{d_{C,\hat{C}}^2\gamma^{(\mathrm{CU}\to\mathrm{BS})}}\right)$. Through some manipulations, $\gamma^{(\mathrm{CU}\to\mathrm{BS})}$ can be rewritten and lower bounded by

$$\gamma^{(\mathrm{CU}\to\mathrm{BS})} = \frac{1}{3}\frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1} \overset{(a)}{\geq} \frac{1}{3}\left(\frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2}-\frac{1}{4}\right) \quad (22)$$

where $\gamma_1 = 2\gamma_{C1}$, $\gamma_2 = 3\gamma_{B1}$, and (a) is obtained by resorting to [20, Eq. (21)]. Therefore, the conditional PEP can be upper bounded by

$$\begin{aligned}\Pr\{x_C \to \hat{x_C} | h_{B1}, h_{C1}\} &\overset{(a)}{\leq} Q\left(\sqrt{\frac{d^2_{C,\hat{C}}\left(\frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2} - \frac{1}{4}\right)}{12}}\right)\\ &\overset{(b)}{\leq} \frac{1}{12}e^{\frac{d^2_{C,\hat{C}}}{96}}e^{-\frac{d^2_{C,\hat{C}}}{24}\gamma} + \frac{1}{4}e^{\frac{d^2_{C,\hat{C}}}{72}}e^{-\frac{d^2_{C,\hat{C}}}{18}\gamma}\end{aligned} \tag{23}$$

where $\gamma = \gamma_1\gamma_2/(\gamma_1 + \gamma_2)$. In (23), (a) comes from the fact the Gaussian-Q function is a monotonously decreasing function, and (b) is derived by exploiting the upper bound of Q-function $Q(x) \leq (1/12)e^{-(x^2/2)} + (1/4)e^{-(2x^2/3)}$ [21].

By averaging (23) over the distributions of γ, the unconditional PEP in (21) can be upper bounded by

$$\begin{aligned}\Pr\{x_C \to \hat{x_C}\} \leq & \underbrace{\int_0^\infty \frac{1}{12}e^{\frac{d^2_{C,\hat{C}}}{96}}e^{-\frac{d^2_{C,\hat{C}}}{24}t}f_\gamma(t)dt}_{I_1}\\ &+ \underbrace{\int_0^\infty \frac{1}{4}e^{\frac{d^2_{C,\hat{C}}}{72}}e^{-\frac{d^2_{C,\hat{C}}}{18}t}f_\gamma(t)dt}_{I_2}\end{aligned} \tag{24}$$

where $f_X(x)$ stands for the probability density function (pdf) of the random variable X. For the considered channel model, γ_1 and γ_2 are exponentially distributed with rate parameters $\lambda_1 = \lambda_{C1}/2$ and $\lambda_2 = \lambda_{B1}/3$, respectively. With the help of [22, Eq. (13)], the pdf of γ can be calculated as

$$\begin{aligned}f_\gamma(t) = & 2\sqrt{\lambda_1\lambda_2}te^{-(\lambda_1+\lambda_2)t}\\ & \times \left[2\sqrt{\lambda_1\lambda_2}K_0(2\sqrt{\lambda_1\lambda_2}t) + (\lambda_1+\lambda_2)K_1(2\sqrt{\lambda_1\lambda_2}t)\right]\end{aligned} \tag{25}$$

where $K_v(x)$ is the vth-order modified Bessel function of the second kind [23, Eq. (8.432.6)].

Substituting (25) into (24) and utilizing [23, Eq. (6.621.3)], I_1 and I_2 can be derived as (26), shown at the bottom of the page, with $\Lambda_1 \triangleq (d^2_{C,\hat{C}}/8) + 3\lambda_1 + 3\lambda_2$ and $\Lambda_2 \triangleq (d^2_{C,\hat{C}}/6) + 3\lambda_1 + 3\lambda_2$. In (26), $\Gamma(x)$ is the gamma function [23, Eq. (8.310.1)], and $F(\alpha, \beta; \gamma; z)$ is the Gauss hypergeometric function [23, Eq. (9.111)].

Combining (24)–(26) with (21) leads to the SEP upper bound of the CU → D_1 → BS link. However, we omit its explicit expression here due to page limit. The SEP of BS → D_1 → CU link can also be derived straightforwardly.

B. SEP for D2D Users

We now shift our attention to the error performance of the D2D users. Similar to the derivations in Section V-A, the SEP for the $D_1 \to D_2$ transmission can be upper bounded by

$$\begin{aligned}P_E^{(D)} &\leq \frac{1}{|\mathcal{X}|}\sum_{\substack{x_{\mathrm{D}}, \hat{x_D} \in e^{j\theta}\mathcal{X}\\ \hat{x_D} \neq x_D}} \Pr\{x_D \to \hat{x_D}\}\\ &\overset{(a)}{=} \frac{1}{|\mathcal{X}|}\sum_{\substack{x_D, \hat{x_D} \in e^{j\theta}\mathcal{X}\\ \hat{x_D} \neq x_D}} \int_0^\infty Q\left(\sqrt{\frac{d^2_{D,\hat{D}}t\frac{2t+1}{5t+2}}{4}}\right)f_{\gamma_{12}}(t)dt\\ &< \frac{1}{|\mathcal{X}|}\sum_{\substack{x_D, \hat{x_D} \in e^{j\theta}\mathcal{X}\\ \hat{x_D} \neq x_D}} \int_0^\infty Q\left(\sqrt{\frac{d^2_{D,\hat{D}}\frac{2}{5}t}{4}}\right)f_{\gamma_{12}}(t)dt\\ &= \frac{1}{|\mathcal{X}|}\sum_{\substack{x_D, \hat{x_D} \in e^{j\theta}\mathcal{X}\\ \hat{x_D} \neq x_D}} \frac{1}{2}\left[1 - \frac{1}{\sqrt{\frac{20\lambda_{12}}{d^2_{D,\hat{D}}} + 1}}\right]\end{aligned} \tag{27}$$

where $d_{D,\hat{D}} = \Re\{x_D\} - \Re\{\hat{x_D}\}$, and (a) is obtained by referring to (6). The SEP upper bound for $D_2 \to D_1$ link can be attained with the same procedure as earlier, and we thus omit its detailed derivations.

VI. Simulation Results and Discussions

Here, computer simulations are carried out to validate the proposed schemes. All nodes are distributed in a 2-D plane. Without loss of generality, we locate BS and CU at (0, 0) and (1, 1), respectively. D_1 is randomly generated in the first quadrant of the 1×1 rectangular coordinate system. For any position of D_1, the other device D_2 is restricted to be at most L from D_1. The value of L should be much less than the distance between the BS and CU, thus making the D2D communications feasible. In our simulations, we set $L = 0.4$. Prior to data transmissions, relay selection (according to the policy given in Section II) is first conducted to determine whether D_1 or D_2 is selected as the relay to assist the cellular communications. The channel model follows the descriptions in Section II, i.e., $h_{ij} \sim \mathcal{CN}(0, \mu_{ij})$. We assume $\mu_{ij} = d_{ij}^{-\eta}$, where d_{ij} is the distance between node i and j, and $\eta = 3$ is the path-loss exponent. Unless otherwise stated, QPSK modulation is adopted at all nodes. In the following figures, the notation "SNR" represents the ratio of P to N_0, i.e., ρ in Section II. For the purpose of comparisons, we consider two benchmark schemes: "superposition coding" and "two-way overlay", where the former is the cooperative relaying scheme 1 devised in [7], and the latter is the scheme proposed in [8].[6]

$$\begin{cases} I_1 = \dfrac{3\lambda_1\lambda_2\sqrt{\pi}e^{\frac{d^2_{C,\hat{C}}}{96}}F\left(2, \frac{1}{2}; \frac{5}{2}; \frac{\Lambda_1 - 6\sqrt{\lambda_1\lambda_2}}{\Lambda_1 + 6\sqrt{\lambda_1\lambda_2}}\right)}{\Gamma\left(\frac{5}{2}\right)(\Lambda_1 + 6\sqrt{\lambda_1\lambda_2})^2} + \dfrac{36\lambda_1\lambda_2(\lambda_1+\lambda_2)\sqrt{\pi}e^{\frac{d^2_{C,\hat{C}}}{96}}F\left(3, \frac{3}{2}; \frac{5}{2}; \frac{\Lambda_1 - 6\sqrt{\lambda_1\lambda_2}}{\Lambda_1 + 6\sqrt{\lambda_1\lambda_2}}\right)}{\Gamma\left(\frac{5}{2}\right)(\Lambda_1 + 6\sqrt{\lambda_1\lambda_2})^3}\\ I_2 = \dfrac{9\lambda_1\lambda_2\sqrt{\pi}e^{\frac{d^2_{C,\hat{C}}}{72}}F\left(2, \frac{1}{2}; \frac{5}{2}; \frac{\Lambda_2 - 6\sqrt{\lambda_1\lambda_2}}{\Lambda_2 + 6\sqrt{\lambda_1\lambda_2}}\right)}{\Gamma\left(\frac{5}{2}\right)(\Lambda_2 + 6\sqrt{\lambda_1\lambda_2})^2} + \dfrac{108\lambda_1\lambda_2(\lambda_1+\lambda_2)\sqrt{\pi}e^{\frac{d^2_{C,\hat{C}}}{72}}F\left(3, \frac{3}{2}; \frac{5}{2}; \frac{\Lambda_2 - 6\sqrt{\lambda_1\lambda_2}}{\Lambda_2 + 6\sqrt{\lambda_1\lambda_2}}\right)}{\Gamma\left(\frac{5}{2}\right)(\Lambda_2 + 6\sqrt{\lambda_1\lambda_2})^3}. \end{cases} \tag{26}$$

[6] It should be pointed out that, "superposition coding" is a one-way transmission scheme, whereas "two-way overlay" and our proposed one are both two-way transmission schemes. Hence, 16-QAM is adopted for the "superposition coding" scheme to make the comparison fair.

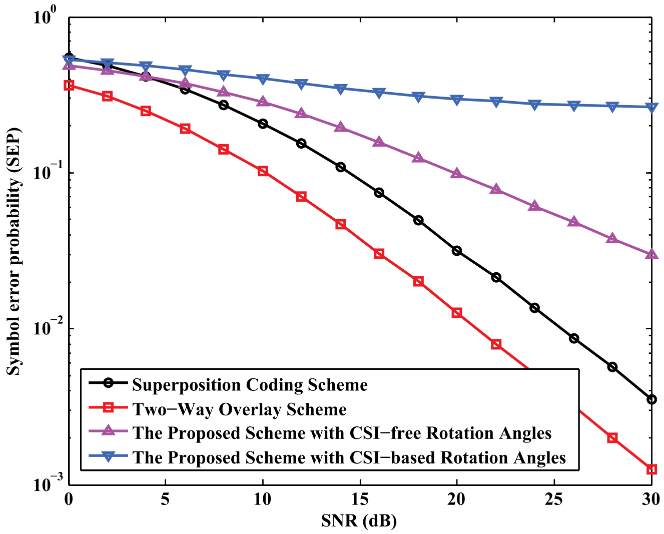

Fig. 2. SEP for the detection of CU's message at D_1.

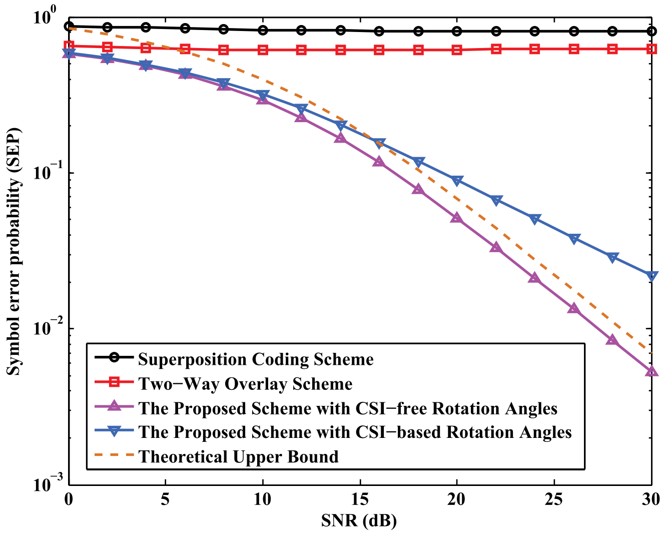

Fig. 3. SEP of the CU → BS transmission.

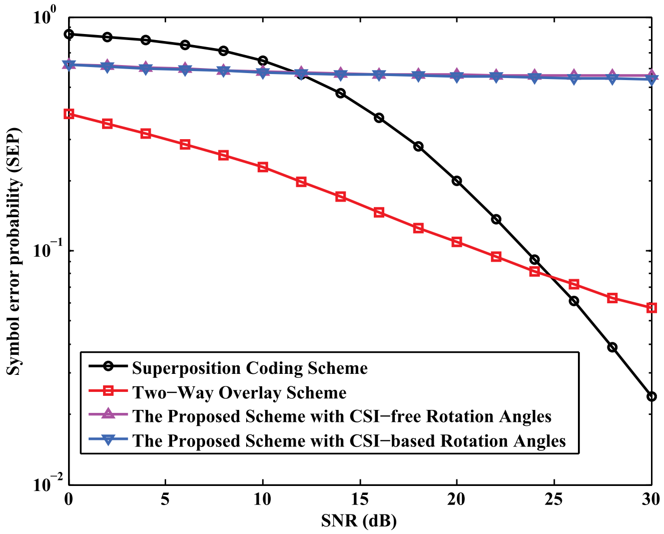

Fig. 4. SEP for the detection of D_1's message at BS.

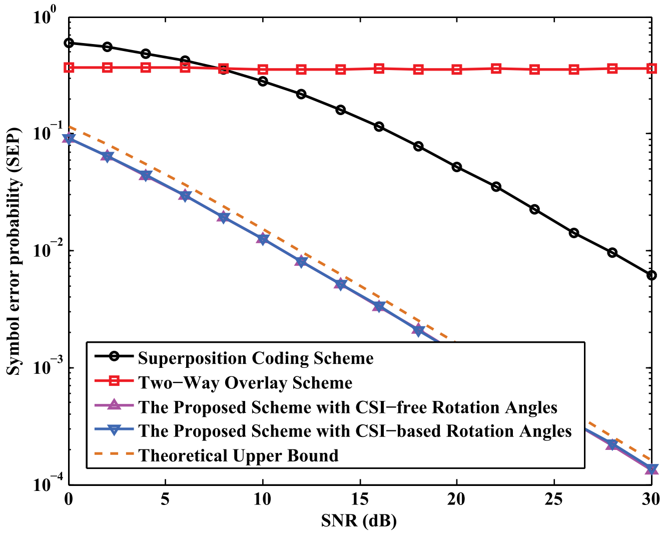

Fig. 5. SEP of the $D_1 \rightarrow D_2$ transmission.

The security performance of the cellular users is first examined. Specifically, we in Fig. 2 plot the SEP curves for the detection of CU's message at D_1 for different schemes. As observed, the SEPs obtained by "superposition coding" and "two-way overlay" strategies decrease with the increased SNR. Therefore, these schemes cannot effectively protect the secrecy of cellular users. By using our scheme with CSI-free rotation angles, the SEP is deteriorated due to the inherent signal alignment mechanism provided by this scheme. Further, via CSI-based rotation angle design, an error floor is created for detection of the unintended message, as exhibited by the blue curve in Fig. 2.

The SEPs for the CU → BS transmission are shown in Fig. 3. It is shown from this figure that the two benchmark schemes both exhibit a significant error floor, which is attributed to their interference-limited characteristics. Compared with these counterparts, our schemes can perfectly avoid the interference, and the achieved SEP falls off with SNR as a waterfall shape. Moreover, the derived bound correctly reflects how the SEP varies when SNR grows, validating our theoretical analysis. A final observation in Fig. 3 is that the proposed scheme with the CSI-based rotation angles performs worse than that with the CSI-free rotation angles. This is because that the CSI-based criterion takes both the reliability and security requirements into account, which yields a significant SEP degradation. However, it still outperforms the competing alternatives, without adding much overhead.

Fig. 4 shows the SEP for the detection of D_1's message at BS. As expected, "superposition coding" and "two-way overlay" strategies cannot guarantee a satisfactory secrecy performance. In comparison, the SEPs achieved by the proposed schemes stay above 10^{-1} even when the system SNR tends to infinity. This indicates that the BS cannot extract any information from D_1, and the $D_1 \rightarrow D_2$ transmission is thus secured.

We consider the reliability of $D_1 \rightarrow D_2$ data transfer in Fig. 5. The red curve shows that the SEP performance of the "two-way overlay" scheme cannot be improved when SNR increases. Comparably, by allowing the D2D receiver to decode CU's signal in the first phase, the "superposition coding" scheme can mitigate the effect of interference from the cellular user, yielding a notable gain for medium-to-high SNRs. However, in contrast to our proposed schemes, the "superposition coding" strategy suffers nonnegligible performance degradation. This is because the interference mitigation at the D2D receiver may not be successful due to possible decoding errors in the first phase. In contrast, our schemes can perfectly avoid the interference due to the use of constellation rotation technique. Finally, we would like to comment that the performance of the CSI-based design and that of the CSI-free design are undistinguishable in terms of both the security and reliability. Therefore, from the perspective of D2D users, the CSI-free scheme is preferred due to its low complexity.

VII. Conclusion

In this paper, a security-embedded interference avoidance scheme has been proposed for cooperative D2D communications in cellular systems. By rotating the signal constellations, the interference-free transmissions are realized for both the cellular and D2D users, and the secrecy of these users can be significantly enhanced as well. We present two criteria of choosing the rotation angles, namely the CSI-free criterion and the CSI-based criterion. The former targets at system SEP optimization and has low implementation complexity, whereas the latter balances the performances between the security and reliability with increased complexity. The closed-form expressions for the SEP upper bounds are derived for the proposed scheme with the CSI-free rotation angle design. There are some issues that are worthy of further investigations. For example, it is of practical significance to extend the proposed idea to the scenarios where there are multiple CUs and (or) multiple D2D pairs. Moreover, it is interesting to evaluate the performance of the proposed schemes by considering the channel estimation errors.

References

[1] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, “Device-to-device communication in 5G cellular networks: challenges, solutions and future directions,” *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, May 2014.

[2] J. Huang *et al.*, “A game-theoretic resource allocation approach for intercell device-to-device communications in cellular networks,” *IEEE Trans. Emerging Topics Comput.*, DOI: 10.1109/TETC.2014.2384372, to be published.

[3] H. Min, J. Lee, S. Park, and D. Hong, “Capacity enhancement using an interference limited area for device-to-device uplink underlaying cellular networks,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 3995–4000, Dec. 2011.

[4] B. Kaufman, J. Lilleberg, and B. Aazhang, “Spectrum sharing scheme between cellular users and ad-hoc device-to-device users,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1038–1049, Mar. 2013.

[5] C.-H. Yu and O. Tirkkonen, “Device-to-device underlay cellular network based on rate spliting,” in *Proc. IEEE WCNC*, Shanghai, China, Apr. 2012, pp. 262–266.

[6] Y. Zhao, Y. Li, X. Chen, and N. Ge, “Joint optimization of resource allocation and relay selection for network coding aided device-to-device communications,” *IEEE Commun. Lett.*, vol. 19, no. 5, pp. 807–810, May 2015.

[7] C. Ma *et al.*, “Cooperative relaying schemes for device-to-device communication underlaying celluar networks,” in *Proc. IEEE GLOBECOM*, Atlanta, GA, USA, Dec. 2013, pp. 3890–3895.

[8] Y. Pei and Y.-C. Liang, “Resource allocation for device-to-device communications overlaying two-way cellular networks,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3611–3621, Jul. 2013.

[9] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, “Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks,” in *Proc. IEEE GLOBECOM*, Austin, TX, USA, Dec. 2014, pp. 3145–3150.

[10] M. C. Gursoy, “Secure communication in the low-SNR regime,” *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 1114–1123, Apr. 2012.

[11] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, “Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone,” *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

[12] P. Baracca, N. Laurenti, and S. Tomasin, “Physical layer authentication over MIMO fading wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.

[13] D. Zhu, A. L. Swindlehurst, S. A. Fakoorian, W. Xu, and C. Zhao, “Device-to-device communications: The physical layer security advantage,” in *Proc. IEEE ICASSP*, Florence, Italy, May 2014, pp. 1606–1610.

[14] C. Ma *et al.*, “Interference exploitation in D2D-enabled cellular networks: A secrecy perspective,” *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[15] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, “Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications,” *IET Commun.*, vol. 9, no. 3, pp. 396–403, Feb. 2015.

[16] J. Boutros and E. Viterbo, “Signal space diversity: A power—and bandwidth-efficient diversity technique for the rayleigh fading channel,” *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1453–1467, Jul. 1998.

[17] D. Gündüz, A. Yener, A. Goldsmith, and H. V. Poor, “The multiway relay channel,” *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 51–63, Jan. 2013.

[18] J. Richter, C. Scheunert, S. Engelmann, and E. A. Jorswieck, “Weak secrecy in the multiway untrusted relay channel with compute-and-forward,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1262–1273, Jun. 2015.

[19] A. Wang, Y. Cai, X. Guan, and S. Wang, “Physical layer security for multi-user two-way relay using distributed auction game,” in *Proc. IEEE 3rd Int. Conf. Inf. Sci. Technol.*, Yangzhou, China, Mar. 2013, pp. 1202–1207.

[20] A. Behnad, R. Parseh, and H. Khodakarami, “Upper bound for the performance metrics of amplify-and-forward cooperative networks based on harmonic mean approximation,” in *Proc. IEEE 18th ICT*, Ayia Napa, Cyprus, May 2011, pp. 157–161.

[21] M. Chiani, D. Dardari, and M. K. Simon, “New exponential bounds and approximations for the computation of error probability in fading channels,” *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 840–845, Jul. 2003.

[22] M. O. Hasna and M.-S. Alouini, “End-to-end performance of transmission systems with relays over rayleigh-fading channels,” *IEEE Trans. Wireless Commun.*, vol. 2, no. 6, pp. 1126–1131, Nov. 2003.

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