Abstract—This paper presents a secure beamforming design to prevent eavesdropping on multiple-input multiple-output (MIMO) device-to-device (D2D) communication. The devices communicate via a trusted relay which performs physical layer network coding (PNC), and multiple eavesdroppers are trying to intercept the device information. The beamforming design is based on minimizing mean square error of the D2D communication while employing signal-to-interference-plus-noise ratio (SINR) threshold constraints to prevent possible eavesdropping. The channel state information of the device-to-eavesdropper and relay-to-eavesdropper channels is imperfect at the devices and relay. The channel estimation errors are assumed with Gaussian Markov uncertainty model. Consequently, robust optimization problems are formulated considering the multiple access and broadcasting stages of the D2D communication. These problems are non-convex, and two algorithms are proposed to solve them. In the numerical analysis, we discuss the convergence of the proposed algorithms, impact of the number of eavesdroppers on the performance, and the SINR distributions at eavesdroppers.

I. INTRODUCTION

Numerous modern technological applications require various advances in wireless systems such as higher data rates, larger coverage areas, more reliable communication, smaller latency, and less complex designs with lower power and processing. In particular for mobile technology, it is predicted that the number of mobile devices will exceed the world population over the next few years [1]. This is already one of the primary contributors of global wireless traffic growth. Traffic will further increase as future mobile devices will possess more sophisticated features compared to early generation devices. With the higher number of mobile devices, there is a strong possibility they are located nearby and engage in communication with each other. The device-to-device (D2D) communication has attracted considerable attention recently in this context [2], [3].

Ongoing Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) [4] has also identified D2D communication as a potential technique to increase the spectral efficiency, enhance the end-user experience and improve the energy efficiency. In particular, it requires only half of the resources compared to the cellular communication mode, thus offering better spectral efficiency. Most of the previous studies on D2D consider direct D2D mode and discuss the advantages over the cellular communication mode [2], [3], [5]–[7]. A relay placed in between D2D pair can extend the coverage area with less transmit power. This also allows longer distance communication through the D2D mode. However, the half-duplexing issue of the relay should be avoided to maintain the higher spectral efficiency promised by the D2D mode. Physical layer network coding (PNC) based two-way relaying [8]–[11] is recognized as spectrally efficient technique to mitigate half-duplexing issue, where it requires only two time slots to exchange information between two nodes as opposed to four in a conventional relaying system. In particular, the PNC considers interference as useful information and improves the capacity of the system. In [12], we proposed PNC based D2D communication underlaying cellular communication. The proposed scheme extends the D2D coverage area and provides more flexibility without loss of the spectral efficiency. As D2D communication offloading traffic from the base station (BS), the involvement of the BS is limited once the D2D communication is established. Therefore, the possibilities of eavesdropping on the D2D communications can be high.

Recent studies on physical layer security [13]–[18] have shown advantages of using security features at the physical layer. These features can be used to prevent eavesdropping on the D2D communications. The authors in [13] considered multiple users communicating with a common receiver in the presence of an eavesdropper. They provided an optimal transmit power allocation policy to maximize the secrecy sum-rate. The quality-of-service (QoS) oriented optimal secure beamforming schemes were discussed in [14] for one-way transmission. Secrecy-rate maximization problem in the presence of multiple eavesdroppers with imperfect channel state information (CSI) was investigated in [15]. Furthermore, the authors in [16]–[18] studied various cooperative relay networks in unsecure environments. In [16], AF relaying was used. Many other relay protocols were considered in [17], where different scenarios were investigated to maximize the secrecy-rate subject to transmit power constraint and minimize the total transmit power subject to a secrecy-rate constraint. Moreover, the authors in [18] studied bi-directional communication options with eavesdroppers and proposed a secrecy transmission protocol.

In PNC based D2D communication, both devices transmit symbols during the multiple access (MA) stage. When an eavesdropper attempts to intercept one symbol, it experiences interference from other one. During the broadcasting (BC) stage, the relay transmits XOR symbol which is an encrypted symbol to the eavesdropper unless it already knows one symbol. This provides added security for the D2D communication. Additionally, in many situations, the devices do not receive any feedbacks from eavesdropping nodes. Therefore, the channel state information (CSI) of the device-to-eavesdropper channels is imperfect at the devices. In this paper, in part presented in [19], we apply aforementioned features and propose a robust beamforming scheme to prevent the eavesdropping in multiple-input multiple-output (MIMO) PNC based D2D communication system.

The rest of the paper is organized as follows. In Section II, we describe the system model. Section III presents the secure
beamforming designs for both MA and BC stages. Section IV gives the numerical results. Finally, conclusions are given in Section V.

Notations: \( \mathbb{C}^{m \times n} \) denotes an \( m \times n \) matrix with elements in the complex field. Capital bold, simple bold, and simple letters represent matrices, vectors and scalar variables, respectively. \( \text{Tr}(), (\cdot)^T, (\cdot)^* \) and \( (\cdot)^H \) indicate trace, transpose, conjugate and hermitian of a matrix. \( \mathcal{E}\{\cdot\} \) and \( \mathbb{H}(\cdot) \) denote the expectation of a random variable and real part of \( z \). \( \mathcal{C}\mathcal{N}(x,y) \) denotes a complex Gaussian random variable with mean \( x \) and variance \( y \).

II. SYSTEM MODEL

We consider two devices communicating in an unsecured environment using a trusted relay node as shown in the Fig. 1. The relay performs PNC mapping, and bi-directional communication of the devices is provided with time division duplex (TDD) mode. Multiple eavesdroppers (\( K \)) attempt to intercept information of the D2D communication. All nodes are equipped with multiple antennas. \( N_i, N_r \) and \( N_k \) are the number of antennas at the \( i \)th device (denoted \( D_i \) with \( i = 1, 2 \)), relay and \( k \)th eavesdropper (denoted \( E_k \) with \( k = 1, 2, \ldots, K \)), respectively. We consider channels to be frequency-flat and quasi-static. Single stream transmissions are assumed with perfect synchronization at the relay node.

A. Multiple access (MA) stage

During the MA stage, both devices transmit their modulated information \( s_i \in \mathbb{C} \) beamformed by \( w_i \in \mathbb{C}^{N_i \times 1} \) (\( i = 1, 2 \)). The relay estimates the sum of two transmitted symbols after going through a receive beamforming vector \( w_r \in \mathbb{C}^{N_r \times 1} \). The post-processed signal at the relay is given by,

\[
y_r = w_r^H H_{1r} w_1 s_1 + w_r^H H_{2r} w_2 s_2 + w_r^H n_r,
\]

where \( H_{ir} \in \mathbb{C}^{N_r \times N_i} \) (\( i = 1, 2 \)) is the channel between the \( D_i \) and relay, and \( n_r \sim \mathcal{C}\mathcal{N}(0, \sigma_r^2) \). The eavesdropper \( E_k \) uses receive beamforming vector \( w_{rk} \in \mathbb{C}^{N_r \times 1} \). The post-processed signal at the \( E_k \) is

\[
y_{rk} = w_{rk}^H H_{1k} w_1 s_1 + w_{rk}^H H_{2k} w_2 s_2 + w_{rk}^H n_{rk}, \quad k \in \{1, \ldots, K\},
\]

where \( H_{1k} \in \mathbb{C}^{N_k \times N_i} \) is the channel between the \( D_1 \) and \( E_k \) with entries assumed to be \( \sim \mathcal{C}\mathcal{N}(0, \sigma_k^2) \), and \( n_{rk} \) is an additive Gaussian noise vector at the \( E_k \) with zero-mean and covariance matrix \( \mathcal{E}\{n_{rk} n_{rk}^H\} = \sigma_k^2 I_{N_k} \). The post-processed signal at the \( E_k \) is

\[
y_{rk} = w_{rk}^H H_{1k} w_1 s_1 + w_{rk}^H H_{2k} w_2 s_2 + w_{rk}^H n_{rk}, \quad k \in \{1, \ldots, K\},
\]

where \( \mathbb{H}(\cdot) \) denotes the Hermitian of a matrix. \( \mathcal{E}\{\cdot\} \) denotes the expectation of a random variable and real part of \( z \). \( \mathcal{C}\mathcal{N}(x,y) \) denotes a complex Gaussian random variable with mean \( x \) and variance \( y \).

B. Physical layer network coding (PNC)

The post-processed signal \( y_r \) can be used to obtain the estimate corresponding to \( s_1 + s_2 \). Two categories of PNC mapping are possible at the relay. In the first method, the estimation is mapped to XOR of two transmitted unmodulated information \[8\]. This is possible for simple modulation schemes like QPSK. Then, the modulated version of the XOR (denoted by \( s_r \in \mathbb{C} \)) is broadcast during the next time slot. Each device estimates the \( s_r \) and uses that to find the desired symbol which is transmitted by other device. The second method is appropriate for many modulation schemes, where the estimate corresponding to \( s_1 + s_2 \) can be broadcast during the second slot \[10, 11\]. In this paper, we adopt first PNC scheme.

C. Broadcasting (BC) stage

During the second time slot, the relay broadcasts \( s_r \) beamformed by \( v_r \in \mathbb{C}^{N_r \times 1} \). The \( D_i \) estimates \( s_r \) after going through a receive beamforming vector \( w_i \in \mathbb{C}^{N_i \times 1} \) (\( i = 1, 2 \)). The post-processed signal at the \( D_i \) is given by,

\[
y_i = v_i^H H_{1i} v_r s_r + v_i^H n_i, \quad i = 1, 2,
\]

where \( n_i \) is an additive Gaussian noise vector at the \( D_i \) with zero-mean and covariance matrix \( \mathcal{E}\{n_i n_i^H\} = \sigma_i^2 I_{N_i} \). The CSI of \( H_{1k} \) is imperfect at the relay.

III. SECURE BEAMFORMING DESIGN

The beamforming vectors are designed to provide secrecy of the D2D communication. The physical layer security during the MA stage is more important to prevent eavesdropping, because at least one message from \( s_1 \) or \( s_2 \) is required for decoding \( s_r \). However, the secrecy can be further improved by beamforming design during the BC stage. Thus, we consider both MA and BC stages in the beamforming design.

A. Beamforming design for MA stage

The proposed secure beamforming design is based on minimizing mean square error (MSE) at the relay. This is necessary to facilitate an accurate PNC operation. The error
at the relay is \( e_r = y_r - (s_1 + s_2) \), and the MSE at the relay is \( M_{SE_r} = E_s \| e_r \|^2 \). This can be further expanded into

\[
M_{SE_r} = \sum_{i=1}^{2} (w_i^H H_{ir} w_i w_i^H H_{ir} w_r - 2R(w_i^H H_{ir} w_i)) + \sigma_r^2 w_i^H w_r.
\]

We assume statistical properties \( E_{s,n} \{s_1 s_1^*\} = 1, E_{s,n} \{s_1 s_2^*\} = 0, E_{s,n} \{s_1 n_i^*\} = \sigma_r^2 I_{N_r} \) with \( i = 1, 2 \) to obtain (5).

The transmit powers at the devices are limited to \( P_{max} \). The physical layer security of D2D communication is provided by limiting the signal-to-interference-plus-noise ratio (SINR) at all eavesdroppers. An eavesdropper intends to decode one symbol during first time slot, and use that to decode the other symbol during the next time slot. In such cases, one symbol acts as an interference to the other one. Therefore, the received SINR of \( s_i \) \( (i = 1, 2) \) at \( E_k \) \( (k \in \{1, \ldots, K\}) \) is given by,

\[
\text{SINR}^i_k = \frac{h_{ik}^H w_i w_i^H h_{ik}}{h_{ik}^H w_i w_i^H h_{ik} + \sigma_r^2}, \quad (i, j) \in \{i \neq j \mid 1, 2\},
\]

where \( h_{ik} = \sqrt{\gamma_k} H_{ik} \). Both SINR values at \( E_k \) should be less than a certain threshold \( \gamma_k \) to prevent the eavesdropping. Considering all these, the following optimization problem is formulated to find transmit and receive beamforming vectors:

\[
\begin{align*}
\min_{w_1, w_2, w_r} & \quad M_{SE_r} \\
\text{subject to} & \quad w_i^H w_i \leq P_{max} \quad \forall i \\
& \quad \text{SINR}^i_k \leq \gamma_k \quad \forall i \text{ and } k.
\end{align*}
\]

### B. Gaussian Markov Uncertainty (GMU) model

We assume Gaussian Markov uncertainty model (GMU) for the \( D_{1} \)-to-\( E_k \) channel as

\[
H_{ik} = \sqrt{1 - \beta_{ik}^2} h_{ik} + \beta_{ik} e_{ik},
\]

where \( H_{ik} \in \mathbb{C}^{N_i \times N_r} \) is the estimated channel component with entries assumed to be \( \sim \mathcal{CN}(0, \sigma^2) \), \( E_{ik} \in \mathbb{C}^{N_i \times N_r} \) is the error component with entries assumed to be \( \sim \mathcal{CN}(0, \sigma^2) \), and \( \beta_{ik} \in [0, 1] \) controls the amount of uncertainty in the CSI. We rewrite this by received the receiver beamforming vector at \( E_k \), and obtain \( h_{ik} = \sqrt{1 - \beta_{ik}^2} h_{ik} + \beta_{ik} e_{ik} \), where all random entries are \( \sim \mathcal{CN}(0, \sigma^2) \).

Now, the SINR constraints of the optimization problem (7) consist of error components. These error components have a known Gaussian distribution, therefore, a robust beamforming design can be considered by taking expectation in terms of error variables. After some algebraic manipulations on (7), the robust optimization problem is reformulated as in (9). This is a non-convex optimization problem and we use an iterative method to solve this. The problem is divided into following two sub-problems.

1) **Sub-problem I**: Here, the transmit beamforming vectors \( w_1 \) and \( w_2 \) are considered fixed. The receiver beamforming vector \( w_r \) is only associated with the objective function. Therefore, taking the derivative with respect to \( w_r \) and equating that to zero gives the optimal solution,

\[
w_r = \left( \sum_{i=1}^{2} (H_{ir} w_i w_i^H H_{ir}^H) + \sigma_r^2 I_{N_r} \right)^{-1} \left( \sum_{i=1}^{2} H_{ir} w_i \right).
\]

2) **Sub-problem II**: When \( w_r \) is fixed, the problem (9) can be reformulated by taking \( w = [w_1; w_2] \in \mathbb{C}^{N_1+N_2} \). Then, the problem becomes a quadratic optimization problem as

\[
\begin{align*}
\min_{w} & \quad w^H A_0 w - 2R(b_0^H w) + c_0 \\
\text{subject to} & \quad w^H P_i w - P_{max} \leq 0 \quad \forall i \\
& \quad w^H A_k w - \gamma_k \sigma_r^2 \leq 0 \quad \forall i \text{ and } k,
\end{align*}
\]

where \( A_0 = [H_{ir}^H w_i w_i^H H_{ir}; 0_{N_1 \times N_2}; 0_{N_2 \times N_1} H_{ir}^H w_i w_i^H H_{ir}], b_0 = [H_{ir}^H w_i w_i^H H_{ir}; A_k \text{ (given in (12))}, P_1 = [I_{N_1} 0_{N_1 \times N_2}; 0_{N_1 \times N_2} 0_{N_2 \times N_1}], \text{ and } P_2 = [0_{N_1 \times N_1} 0_{N_1 \times N_2}; 0_{N_2 \times N_1} 0_{N_2 \times N_1}], \text{ and } c_0 = \sigma_r^2 w_r^H w_r + 2. \) This is not a convex optimization problem. However, according to [20], p.654, Ap. B.1], this can be solved by semi-definite programming (SDP) relaxation. The SDP relaxation can be obtained as in (13).

\[
\begin{align*}
\min & \quad \text{Tr}(A_0 W) - 2R(b_0^H w) + c_0 \\
\text{subject to} & \quad \text{Tr}(P_i W) - P_{max} \leq 0 \quad \forall i \\
& \quad \text{Tr}(A_k W) - \gamma_k \sigma_r^2 \leq 0 \quad \forall i \text{ and } k
\end{align*}
\]

\[
\left[ \begin{array}{cc}
W & w \\
-w^H & 1
\end{array} \right] \succeq 0.
\]

Now, the problem (13) is convex, and can be solved with the interior point method. In general, rank-one solution of \( W \) is required to find the optimal \( w \) of the original problem. The procedure to obtain the rank-one solution is described in [21], [22]. Both sub-problems are iteratively solved till the MSE-
is converged. The algorithm to obtain beamforming vectors is provided as Algorithm 1.

Algorithm 1 Secure Beamforming design for MA stage

Information about $K$, $P_{\text{max}}$, $\gamma_k$, $\sigma^2_k$, $\sigma^2_r$, $N_i$, $\beta_k$, $H_{ir}$, $h_{ik}(\forall i, \forall k)$ is available at the devices.

1: initialize : Beamforming vectors $w_i = \sqrt{\frac{P_{\text{max}}}{N_i}}$.
2: repeat
3: Fix $w_1$ and $w_2$ obtained from step 4 (Or step 1 at initial point). Find optimum $w_r$ from (10).
4: Fix $w_r$ obtained from step 3. Solve problem (13) to find optimum $W$. Obtain optimal rank-one solution of $W$ to find $w_1$ and $w_2$.
5: until MSE, converge.
6: Update $w_r$, $\text{MSE}$, converge.

We assume that the devices share CSI knowledge of device-to-eavesdropper channels. Since modern wireless devices have higher processing powers, Algorithm 1 can be used at the devices without any difficulty. The beamforming vector $w_r$ is sent to the relay prior to data transmission.

C. Beamforming design for BC stage

During the BC stage, the secrecy of the D2D communication can be further improved by employing beamforming vectors at the nodes. A similar method as in the MA stage is used to find the optimal beamforming vectors. Both devices estimate $s_r$, and the MSE at the $D_1$ (denoted by MSE$_1$) can be obtained as

$$\text{MSE}_1 = \rho \bar{v}_r^H H^*_{ir} v_r + \rho \bar{H}_{ir}^H H^*_{ir} v_r - 2\rho \bar{v}_r^H H^*_{ir} v_r + \sigma^2_r$$ \hspace{1cm} (14)

where, $E[s_r, s_r^*] = \rho$, and $\rho$ represents the average normalized power of symbol $s_r$ (compared to $s_i$). Both MSE$_1$ and MSE$_2$ are considered together by taking the sum-MSE as the objective function. The received SNR of $s_r$, at $E_k$ is $\text{SNR}_r = \rho h_{ir}^H v_r v_r^H H_{rk} / \sigma^2_k$, where $h_{rk}^H = \frac{\sqrt{\gamma_k}}{\gamma_k} \sqrt{R_k}$. The received SNR should be less than a certain threshold $\gamma_k$ to prevent decoding $s_r$ at $E_k$. Then, the optimal transmit and receive beamforming vectors can be obtained by solving the following optimization problem:

$$\min_{v_r, v_r^*} \quad 0.5 \text{MSE}_1 + 0.5 \text{MSE}_2$$
$$\text{subject to} \quad v_r^H v_r \leq P_{\text{max}} / \rho$$
$$\text{SNR}_r \geq \gamma_k$$ \hspace{1cm} (15)

The CSI of $H_{rk}$ ($\forall k$) at the relay is also assumed to follow GMU model. Considering post-processing at $E_k$, we have $h_{rk} = \sqrt{1 - \beta_k^2} h_r + \beta_k e_r$, where all entries of $h_{rk}$ and $e_r$ are $\sim \mathcal{CN}(0, \sigma^2)$. All nodes are equipped with two antennas. The parameter $\beta_k$ and $\beta_k$ control the amount of uncertainty in the CSI. All are assumed to be $\beta$ to simplify the discussion. Moreover, the SNR threshold levels at all eavesdroppers are equal to $\gamma$. Monte Carlo simulations are used find the average performances, where algorithms are applied to find beamforming vectors for each channel realization. Furthermore, the device symbols are created with binary phase-shift keying (BPSK) modulation with unit power. The relay

is obtained as

$$\min_{v_1, v_2, v_r} \sum_{i=1}^2 0.5 (\rho v_i^H H_{ik}^H v_r v_r^H H_{ik}^* v_i - 2\rho \Re(v_i^H H_{ik}^* v_i)$$
$$+ \sigma^2_i v_i^H v_i + \rho)$$
$$\text{s.t.} \quad v_r^H v_r \leq P_{\text{max}} / \rho$$
$$\frac{1}{2} - \beta_k^2 v_r^H H_{rk}^* v_r + \beta_k^2 \sigma^2 v_r^H v_r \leq \gamma_k \sigma^2 / \rho \quad \forall k.$$  \hspace{1cm} (16)

This is also a non-convex combination optimization problem, and the problem is divided into following sub-problems.

1) Sub-problem I: Here, the transmit beamforming vector $v_r$ at the relay is considered fixed. Two receive beamforming vectors $v_1$ and $v_2$ appear only in the objective function. Therefore, taking the derivative with respect to $v_i$ ($i = 1, 2$) and setting it equal to zero leads to the optimal solutions,

$$v_i = (H_{ik}^* v_r v_r^H H_{ik}^* + \sigma^2_i I_{N_i})^{-1} H_{ik}^* v_r \quad (i = 1, 2).$$  \hspace{1cm} (17)

2) Sub-problem II: The receive beamforming vectors $v_1$ and $v_2$ are considered fixed. Then, the modified problem (16) becomes convex quadratic constrained quadratic program (QCQP) of the variable $v_r$. This can be easily solved with the interior point method. Finally, the iterative method used in the BC stage is given as Algorithm 2.

Algorithm 2 Secure Beamforming design for BC stage

Information about $K$, $P_{\text{max}}$, $\gamma_k$, $\sigma^2_k$, $\sigma^2_r$, $N_i$, $\beta_k$, $H_{ir}$, $h_{ik}(\forall i, \forall k)$ is available at the relay.

1: initialize : Beamforming vector $v_r = \sqrt{\frac{P_{\text{max}}}{N_k}}$.
2: repeat
3: Fix $v_r$ obtained from step 4 (step 1 at initial point). Find optimum $v_1$ and $v_2$ from (17).
4: Fix $v_1$ and $v_2$ obtained from step 3. Solve modified problem (16) only with variable $v_r$.
5: until $0.5 \text{MSE}_1 + 0.5 \text{MSE}_2$ converge.
6: Update $v_1$ and $v_2$ at the devices.

The relay computes the beamforming vectors during the BC stage. Beamforming vectors $v_1$ and $v_2$ are sent to the devices prior to data transmission. This is more practical as relay-eavesdropper channels $h_{rk}$ can only be estimated at the relay, not at the devices.

IV. NUMERICAL RESULTS

In this section, we investigate the convergence of the proposed algorithms, impact of the number of eavesdroppers on the D2D communication, and SINR distributions at a given eavesdropper. All channels are assumed to undergo Rayleigh fading with entries $\sim \mathcal{CN}(0, 1)$, and the noise variances are considered equal ($\sigma^2$). All nodes are equipped with two antennas. The parameter $\beta_k$ and $\beta_k$ control the amount of uncertainty in the CSI. All are assumed to be $\beta$ to simplify the discussion. Moreover, the SNR threshold levels at all eavesdroppers are equal to $\gamma$. Monte Carlo simulations are used find the average performances, where algorithms are applied to find beamforming vectors for each channel realization. Furthermore, the device symbols are created with binary phase-shift keying (BPSK) modulation with unit power. The relay
performs maximum likelihood estimation to obtain the XOR of transmitted messages.

In Fig. 2, the convergence of Algorithm 1 is illustrated with the number of iterations. Different $\beta$ and $\gamma/\sigma^2$ values are considered when $P_{\text{max}}/\sigma^2 = 10$ dB. For all cases, the algorithm converges with a small number of iterations. The average MSE (AMSE) improves with both $\gamma/\sigma^2$ and $\beta$. Since the convergence of the algorithm is fast, this is suitable for practical deployments. The Algorithm 2 has a similar convergence pattern. Therefore, it is not illustrated.

Fig. 3 shows the AMSE at the relay verses the number of eavesdroppers. The AMSE increases with the number of eavesdroppers $K$. When $K$ is high, the optimization problem has more constraints. Then the feasibility set becomes smaller. Therefore, the AMSE increases with $K$. However, when $\beta$ increases, the AMSE decreases. This is possible as the robust optimization problem is formulated by taking the expectation of SINR constraints.

The SINR distributions at $E_1$ during both MA and BC stages are illustrated in Fig. 4 and Fig. 5. During the MA stage, the cumulative distribution function (c.d.f.) of the SINR of symbol $s_1$ and maximum SINR of symbols $s_1$ and $s_2$ are shown in Fig. 4. There we assume four eavesdroppers, $P_{\text{max}}/\sigma^2 = 10$ dB, and $\gamma/\sigma^2 = 0$ dB. The maximum SINR always has a certain gap with the SINR of $s_1$. In a near perfect CSI scenario, i.e., $\beta = 0.1$, the maximum SINR at $E_1$ is almost limited at the desired level (0 dB in this simulation). When $\beta$ is higher, the maximum SINR at the eavesdropper exceeds the desired level. Eavesdroppers can intercept device information in such scenarios. This can be avoided by reducing $\gamma$ in the optimization problem.

Fig. 5 shows the c.d.f. of the received SNR of symbol $s_r$ at $E_1$ during the BC stage. We assume the same simulation parameters except for $\rho = 1$. For all $\beta$ values, the received SNR at the eavesdropper is almost limited at the desired level. Therefore, the eavesdropper is prevented from decoding $s_r$. Even though the eavesdropper succeeds in decoding one symbol during the MA stage, it cannot decode the other symbol during the BC stage.

Finally, Fig.6 shows the average bit error rate (ABER) for bi-directional communication. Bit errors at both devices are considered, and plotted with $P_{\text{max}}/\sigma^2$. Similar simulation parameters are used as with the Fig. 4 and Fig. 5. There is a maximum error performance level that the secure optimal beamforming designs can achieve. Error performance is better when the $\gamma/\sigma^2$ is high. Moreover, the error performance degrades when $\beta$ increases.

V. CONCLUSIONS

In this paper, a robust secure beamforming design has been proposed to prevent eavesdropping on the relay assisted D2D communication. The relay performed PNC mapping, that has an added security feature compared to other relaying schemes. The performance of the D2D communication was enhanced via minimizing MSE during both MA and BC stages while considering SINR constraints to prevent eavesdropping. The CSI of the device-to-eavesdropper and relay-to-eavesdropper channels was imperfect at devices and relay. The CSI error was assumed to follow Gauss Markov uncertainty model,
Fig. 5: c.d.f. of the received SNR of $s_r$ at $E_1$. $K$ = 4, and $P_{\text{max}}/\sigma^2 = 10$ dB.

![Graph showing the c.d.f. of the received SNR of $s_r$ at $E_1$.](image)

Fig. 6: Average BER versus $P_{\text{max}}/\sigma^2$ for different $\beta$ and $\gamma/\sigma^2$.

![Graph showing the average BER versus $P_{\text{max}}/\sigma^2$ for different $\beta$ and $\gamma/\sigma^2$.](image)

and we considered Gaussian nature of the error to propose robust optimization algorithms. Proposed algorithms were used to analyze the performance of the D2D communication and investigate the SINR distribution at a given eavesdropper. Numerical examples revealed that the proposed algorithm converged fast and the D2D performance degraded with number of eavesdroppers. Moreover, SINR distributions during both MA and BC stages verified that the proposed beamforming scheme provided higher secrecy for the D2D communication.

VI. ACKNOWLEDGEMENT

The authors would like to acknowledge the support of the European Commission by partially funding this work, under FP7 project ICT-317669 METIS, Finnish Funding Agency for Technology and Innovation (Tekes), Nokia Networks, and Elektrobit.

REFERENCES


