A Joint Optimization Scheme for Artificial Noise and Transmit Filter for Half and Full Duplex Wireless Cyber Physical Systems

Özge Cepheli, Guido Dartmann, Güneş Karabulut Kurt, *Senior Member, IEEE*, and Gerd Ascheid, *Senior Member, IEEE*

Abstract—While half and full duplex wireless enabled cyber physical systems (CPSs) are gaining more importance and research attention, maintaining the security of CPS systems remains a vital challenge. The broadcast nature of wireless channels makes it possible for unauthorized receivers, called eavesdroppers, to capture the information signal. Wireless physical layer security techniques aim to harden the secrecy characteristics of wireless systems, decreasing the signal quality of a prospective eavesdropper. This paper considers a joint optimization of artificial noise (AN) signal and transmit filter for the information signals in order to achieve a target secrecy level. As eavesdropping attacks are very critical threats in CPS networks, and the need for high secrecy techniques remains valid. The proposed framework includes a scenario with two multi-antenna legitimate parties and a multi-antenna eavesdropper node (or multiple cooperating eavesdroppers). The transmit filter and AN signal are jointly optimized by the transmitters, where receiver nodes can make use of optimal transmit filters. The problem is derived for the cases where the legitimate CPS nodes perform full duplex and half duplex transmissions. The impact of channel estimation errors and self interference are also discussed.

Index Terms—Artificial noise, transmit filter, power optimization, secrecy, physical layer security, PHY, CPS

1 Introduction

Cyber physical systems (CPSs) are one of the most prevalent technologies in today's communication world. As a tool, wireless communication systems are a strong candidate to take part in CPS networks, especially for the automated mobile scenarios such as autonomous vehicular systems, medical monitoring, and robotics systems. However, compared to their wired counterparts, information security in wireless systems is a greater challenge due to the broadcast nature of the wireless medium.

Modular and layered structure of communication networks led to the absence of relation between traditional security systems and physical layer transmission techniques. In other words, traditional security systems handle the information security regardless of the used transmission technology in the physical signal level. [1] This phenomena resulted in adaptable-but-non-optimal security techniques to be used in the production systems, where interoperability and decreased complexity are very critical. However, as the wireless systems evolve, there is increasing need of more efficient methods to maintain security while reducing the consumption of system resources such as power and bandwidth.

With the evaluation of Industry 4.0, CPSs and wireless control devices are designed to be a part of industrial automation [2]. The eavesdropping attacks may be used as a first step for manipulating sensors and actors or even sabotaging the overall system. In Fig. 1, an exemplary use case with wireless tagged production is shown. Due to the unlimited possible use cases, which may also require mobility, transmit speed and reliability has become crucial requirements. As the transmit power is often limited in mobile devices, technologies that will be deployed in CPSs should aim minimizing the power consumption and maximizing speed. In order to achieve a better performance than the previous systems, new technologies make use of diversity techniques with multiple-input-multiple-output (MIMO) and even full duplex communication. Using full duplex communication, the throughput can be almost doubled by enabling simultaneous transmission and reception, which makes it bandwidth efficient and very suitable for machine to machine communications.

This paper provides a artificial noise (AN) and transmit filter optimization problem to minimize transmission power while guarantying the quality of service (QoS) and secrecy constraints in a one way transmission between two legitimate nodes in the presence of an eavesdropper. In the second part, the problem is extended to full duplex case and the analysis is repeated in comparison to the half duplex system. We show that the full duplex communication

- *Ö. Cepheli and G. Karabulut Kurt are with the Wireless Communications Research Laboratory, Istanbul Technical University, Istanbul 34467, Turkey. E-mail: {irmakoz, gkurt}@itu.edu.tr.*
- *G. Dartmann is with the University of Applied Sciences Trier, Trier 54296, Germany. E-mail: g.dartmann@umwelt-campus.de.*
- *G. Ascheid is with the Chair for Integrated Signal Processing Systems, RWTH Aachen University, Aachen 52062, Germany. E-mail: ascheid@ice.rwth-aachen.de.*

Manuscript received 15 Nov. 2016; revised 10 Apr. 2017; accepted 23 May 2017. Date of publication 20 July 2017; date of current version 6 June 2018. (Corresponding author: Özge Cepheli.)
Recommended for acceptance by S. Hu, B. Yu, and H. Yu.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TSUSC.2017.2729515

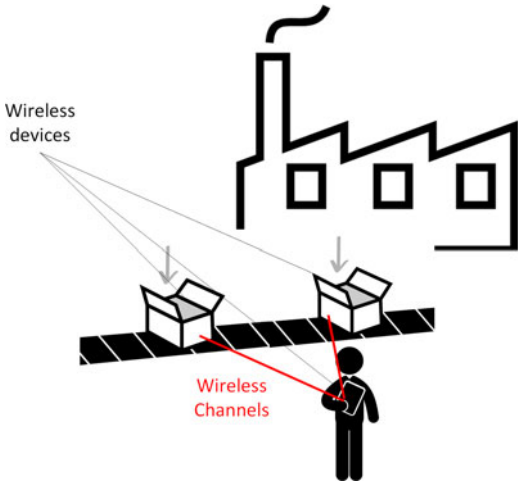

Fig. 1. A possible use case with CPS in industry.

technique does not only provide increased throughput, but also has efficient results when analyzed from a security perspective, due to its multi-user nature. The problem is further analyzed under the existence of channel estimation error and the performance gap is modeled. As the channel estimation error affects the performance of the legitimate communication drastically, estimation of the resultant performance decrease is useful for practical concerns.

The main contributions of this paper are the following:

// MIMO gaussian channels

1) The problem statement provided in Section 3 embodies an extensive class of wireless networks by the use of parallel MIMO Gaussian channels, representing a number of practical channels for both half duplex and full duplex communications. These include MIMO - orthogonal frequency division multiplexing (MIMO-OFDM) and orthogonal frequency division multiple access (OFDMA). Especially for the full duplex transmission the self interference is shown to be an advantage against the eavesdropper.
2) A framework is proposed in Section 4 for the joint optimization of transmit/receive filters of legitimate users and artificial noise, which results in optimal artificial noise calculation by taking the effect of the adopted receive filters into account. This approach is distinguished from the literature, where most of the work do not consider the effect of the designated receive filters.
3) The effects of channel estimation errors and the self interference on the performance of the system are also considered and explained in Section 5. The resilience against these errors are very important for such techniques especially for practical implementations.

Notation: In this paper, $\mathbf{I}_n$ refers to a $n \times n$ identity matrix. The set of n-dimensional complex vectors is denoted by $\mathbb{C}^n$ and $n \times n$ Hermitian matrix is defined by $\mathbb{H}^n$. $\mathbf{x} \sim CN(\mu, \Sigma)$ refers to a random vector $\mathbf{x}$ which follows a complex circular Gaussian distribution with mean μ and covariance Σ. Boldface lowercase letters donate vectors and boldface uppercase letters donate matrices. The trace operator and euclidean norm are denoted by $\mathrm{Tr}(\cdot)$ and $\|\cdot\|$, respectively. $\mathbf{A}^H$ represents the conjugate transpose of $\mathbf{A}$. $\mathbf{B} \succeq 0$ refers that $\mathbf{B}$ is a positive semi-definite (PSD) matrix.

2 Literature Review

Security in CPS systems has lately attracted many researchers' attraction [1], [3], [4]. A physical layer key generation method based on the reciprocity and high spatial and temporal variation properties of the automotive wireless communication channel was proposed in [3]. In [4], the authors proposed a cooperative beamforming schema for secure communications in wireless CPSs, where two legitimate devices communicate with the help of amplify-and-forward (AF) relays. In fact, physical layer security has been a popular topic among researchers for the last decade, as the preservation of the secrecy is a challenge due to the broadcast nature of the wireless channels. After Wyner introduced the wiretap channel in his pioneer study [5], the literature for physical layer security has been expanding with an increasing pace. The wiretap channel in [5] was a special channel scheme where the eavesdropper's channel is a degraded version of the channel of the legitimate user. In the study [6], this was extended to a general independent channel condition. Note that the studies were not considering wireless channels directly, however became fundamental studies in physical layer security in wireless networks as channel definitions do not only comply with wireless channel models but also cover eavesdropping in wireless channels perfectly. Since multi-antenna technologies are now frequently used, many studies have been conducted with various antenna configurations, as single-input-multiple-output (SIMO) [7], multiple-input-single-output (MISO) [8], [9], [10] and MIMO [11], [12], [13], [14] channels.

In [7], [9], [15], [16], [17], various aspects of secure communications over interference channels have been examined from an information theoretical perspective. Although information theoretical metrics as secrecy rate and a performance metric is a key indicator of fundamental limits for secure communications, it should be complemented with low-complexity approaches in order to obtain practical secure systems. This is the driver of improving the security performance of communication systems via QoS framework which adopts signal-to-noise ratio (SNR) or mean-square error based metrics as performance criteria that has been recently used by many researchers [18], [19], [20], [21]. Minimum mean square error (MMSE) based filter optimization framework is adopted in numerous Gaussian interference channel scenarios in [19], [20]. In [22], the authors formulated the problem of minimizing the total weighted MMSE at the legitimate receivers while keeping the MMSE at the eavesdroppers above target levels.

2.1 Artificial Noise

Artificial noise, which refers to the deliberately transmitted noise signals to the eavesdropper, is commonly used for improving physical layer security by degrading eavesdroppers' channel condition [18], [23]. Also called as artificial interference (AI), this technique is proven to be an effective solution to the problem of secrecy in broadcast channels. AN will be used in our proposed framework, for increased efficiency.

2.2 Full Duplex Systems

Full duplex communications has been also a popular topic recently. Full duplex systems allow transmitting and

TABLE 1
Literature Summary

Scenario	Studies	Secrecy Concern	Transmit-Receive Filter Design
Half duplex	[18], [19], [20], [21], [22], [23]	Yes	No
Half duplex	[19], [20], [33], [34], [35]	No	Yes
Half duplex	[36]	Yes	Yes
Full duplex	[31], [32]	Yes	No
Full duplex	[37], [38]	No	Yes

receiving data at the same time and frequency slots, possibly doubling the spectral efficiency [24], [25]. Besides the spectral efficiency advantage, they have not been frequently used due to the generated self-interference [24]. However, recent studies target to alleviate the performance degradation observed due to self-interference by using self-interference cancellation (SIC) techniques [26], [27]. Full duplex beamforming is proposed in [28] to increase the total ergodic capacity at multihop wireless relay networks. In [29], bipolar-beamforming was proposed to jointly design transmitting signals. In [30], a high data rate framework is designed to optimize the beamforming coefficients of a full duplex system, which use the interference to satisfy secrecy constraints. Communication with a single antenna is studied in [31] and the AN is emitted by a full duplex receiver that acts as a base station. With this approach, the full duplex gain of the system is sacrificed to improve the uplink secrecy rate. More recently, a full duplex artificial noise scheme which uses a FD base station combined with the AN approach to improve both the uplink and downlink secrecy rates is proposed [32]. In our proposed framework, full duplex case and and effect of SI are considered.

MIMO filter: MF, ZF, MMSE

2.3 Filter Optimization

Optimization of MIMO linear precoding schemes are discussed in [33], [34], [35] by using transmit matched filter (MF), zero forcing (ZF) filter, and minimum mean square error (MMSE) filter. Authors in [33] show that different transmit filters can be obtained with the same optimization as the respective receive filters by changing transmit power constraints. Both the transmit and receive Wiener (MMSE) filters converge to the matched filter for low SNR and to the ZF filter for high SNR. It is also shown that the matched filter gives the optimal results under noise limited scenarios, whereas for interference limited scenarios one should use ZF filter. Various schemes for filter optimization without artificial noise has been proposed in [19], [20], [36], [37], [38]. In [37], the authors focus on a full-duplex multi-user MIMO system and propose a transceiver design to maximize the weighted sum data rate subject to maximum power constraints. In [38], a multi-link full duplex scenario is considered, where the transmit and receive filters are designed with weighted sum-rate (WSR) maximization problem, using both individual and sum power constraints. The studies regarding the filter optimization are summarized in Table 1.

To the best of our knowledge, the effect of receive filters in a full duplex scenario with an eavesdropper channel has not been considered yet. In this paper the problem of joint optimization of transmit and receive filters of legitimate users, along with the artificial noise is derived and solved for both half and full duplex systems.

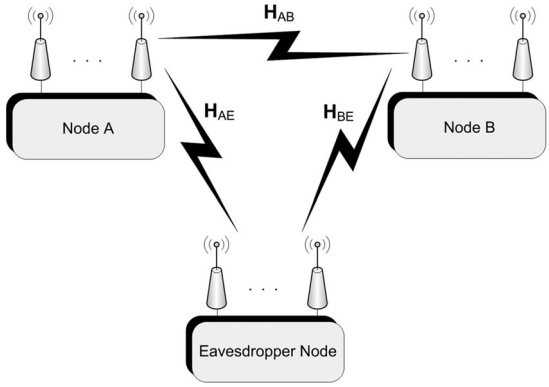

Fig. 2. Full duplex high level system model.

3 System Model & Problem Statement

The system model consists of two legitimate nodes (node A and node B) communicating through a parallel MIMO Gaussian channel having K sub-channels where an eavesdropper node (node E) is trying to gather the information signal, as shown in Fig. 2. Note that the parallel MIMO Gaussian channels represent a number of practical channels such as MIMO-OFDM and OFDMA. All three nodes are equipped with antenna arrays. The number of antenna elements in the arrays are N_A, N_B and N_E for A, B and the eavesdropper, respectively. As proposed in [24], in the full duplex technique, the transmit and receive antenna arrays are separated for each node. Hence the two legitimate nodes have both $2N_A$ and $2N_B$ antennas in total. The MIMO channel between any two nodes for the subchannel k is shown with the notation of $\mathbf{H}_{ij}(k)$, where $i \in \{A, B, E\}$, showing node i is the transmitter and node j is the receiver. Following this notation, $\mathbf{H}_{ij}(k)$ has the dimensions of $N_i \times N_j$.

The channels are assumed to be reciprocal throughout the paper, hence $\mathbf{H}_{ij}(k) = \mathbf{H}_{ji}(k), \forall i, j, k$. Unless stated otherwise, we assume that all channels are accurately estimated by node B and are also known by eavesdropper node, using a noise-free feedback link. The high quality feedback link could be achieved by using a low-rate transmission with high quantization. While the design of a such feedback link and the effect of noisy feedback are beyond the scope of this paper, we will investigate the effect of imperfect channel knowledge in Section 4, to give an insight on the effect of the practical channel estimation errors.

As both half duplex and full duplex scenarios will be investigated in this paper, both legitimate nodes are capable of sending and receiving wireless signals. However, in the half duplex mode the direction of the information flow is assumed to be from node A to node B. Please note that as the channels are assumed to be symmetric, the validity of the system model is preserved when node B is the transmitter and node A is the receiver. In this case, only the notation should be changed to cover the reverse information flow.

3.1 Adversary Model

The adversary considered in this paper is a passive eavesdropper that has a multiantenna receiver. The location of the eavesdropper node can be static or dynamic (mobile eavesdropper) and can be chosen freely. Moreover, the antenna locations can be scattered. This also corresponds to collaborating eavesdropper nodes.

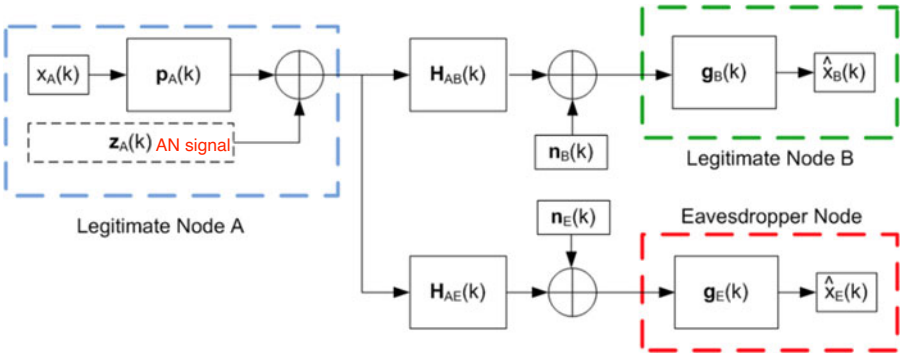

Fig. 3. Half duplex system model: Legitimate node A sends information signal along with artificial noise. Both signals go through wireless parallel Gaussian channels before they are received by legitimate receiver node B and the eavesdropper node E. As the transmit filter $\mathbf{p}_A(k)$ and the artificial noise $\mathbf{z}_A(k)$ is optimized using the knowledge of wireless channels between the nodes, legitimate receiver gets a higher signal quality and get affected from the artificial noise less, while the eavesdropper gets poor signal quality and more artificial noise.

The mobility of the adversary effects the stationarity of the wireless channel. In [39], the achievable performance is given for inter-cell interference-limited networks with single user detection and different beamforming techniques for slow and fast fading channels. Higher mobility levels can have negative effects on the performance of the system. However the stationarity of the channel is assumed to have no negative effect on the channel estimation in the scope of this study.

The effects of hardware components of the nodes are not considered in this study.

3.2 Half Duplex Communication Signal Model

The system model regarding the half duplex case is given in Fig. 3. Suppose node A sends the unit energy signal $x_A(k)$ to node B. The information bearing part of the transmitted signals of A is defined as

$$\mathbf{s}_A(k) = \mathbf{p}_A(k)x_A(k), \tag{1}$$

where $\mathbf{p}_A(k)$ is the $N_A(k) \times 1$ transmit filter of $x_A(k)$.

The AN component of the transmitted signal $\mathbf{z}_A(k)$ is an $N_A(k)$ length vector with covariance matrix $\mathbf{\Phi}(k)$. The power invested in the transmission of information signal is denoted by $\mathcal{P}_i$ and calculated as

$$\mathcal{P}_i = \sum_{k=1}^{K} \mathrm{Tr}\Big(\mathbf{s}_A(k)\mathbf{s}_A(k)^H(k)\Big) = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{P}_A(k)), \tag{2}$$

where $\mathbf{P}_A(k) = \mathbf{p}_A(k)\mathbf{p}_A^H(k)$. Similarly, power invested in artificial noise transmission $\mathcal{P}_{AN}$ is calculated as

$$\mathcal{P}_{AN} = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{\Phi}(k)). \tag{3}$$

The received signals of B and E are represented by $\mathbf{r}_B(k)$ and $\mathbf{r}_E(k)$, respectively. The signals can be modeled as

$$\begin{aligned} \mathbf{r}_B(k) &= \mathbf{H}_{AB}^H(k)(\mathbf{s}_A(k) + \mathbf{z}_A(k)) + \mathbf{n}_B(k) \\ \mathbf{r}_E(k) &= \mathbf{H}_{AE}^H(k)(\mathbf{s}_A(k) + \mathbf{z}_A(k)) + \mathbf{n}_B(k), \end{aligned} \tag{4}$$

where $\mathbf{n}_B(k)$ and $\mathbf{n}_E(k)$ are independent and identically distributed (i.i.d.) complex circular Gaussian noise vectors following $\mathbf{n}_i \sim CN(0, \sigma_{n_i}^2 \mathbf{I}_{N_i}), \forall i \in \{B, E\}$. The estimated signals transmitted by node i at the receiver j is given by the notation $\hat{x}_i^j$. The estimated signals are

$$\begin{aligned} \hat{x}_A^B(k) &= \mathbf{g}_B(k)\mathbf{r}_B(k) \\ \hat{x}_A^E(k) &= \mathbf{g}_E(k)\mathbf{r}_E(k), \end{aligned} \tag{5}$$

where $\mathbf{g}_B(k)$ and $\mathbf{g}_E(k)$ have dimensions of $1 \times N_B(k)$ and $1 \times N_E(k)$ and represent the receive filters of the corresponding nodes. The SINR expressions at the receivers can be obtained as,

$$\begin{aligned} \gamma^B(k) &= \frac{\mathrm{E}\Big\{|\mathbf{g}_B(k)\mathbf{H}_{AB}^H(k)\mathbf{p}_A(k)x_A(k)|^2\Big\}}{\mathrm{E}\Big\{|\mathbf{g}_B(k)\mathbf{H}_{AB}^H(k)\mathbf{z}_A(k)|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_B(k)\mathbf{n}_B(k)|^2\Big\}} \\ \gamma^E(k) &= \frac{\mathrm{E}\Big\{|\mathbf{g}_E(k)\mathbf{H}_{AE}^H(k)\mathbf{p}_A(k)x_A(k)|^2\Big\}}{\mathrm{E}\Big\{|\mathbf{g}_E(k)\mathbf{H}_{AE}^H(k)\mathbf{z}_A(k)|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_E(k)\mathbf{n}_E(k)|^2\Big\}}. \end{aligned} \tag{6}$$

The average SINR can be calculated for each node by taking average of all the channel SINRs. In this paper, we consider SINR constraints on each subchannel, hence all the calculations constraints and relations will be given per subchannel. It is important to note that the subchannel constraints may be chosen according to the desired system model. For example, the same SNR constraint can be used for each subchannel to force the system to predistortion mode, while it is also possible to force the system for different modes, e.g., to use a set of subchannels, by choosing specific SNR constraints.

The mean square error between the estimate of the transmitted information signal and the received signal given by,

$$\mathrm{MSE}_i(k) = \mathrm{E}\Big\{|\hat{x}_A^i(k) - x_A^i(k)|^2\Big\}. \tag{7}$$

3.3 Receive Filter

The receive filters $\mathbf{g}_B(k)$ and $\mathbf{g}_E(k)$ are calculated at the corresponding node maximize the signal reception performance. If the transmit filter $\mathbf{p}_A(k)$ and the channel $\mathbf{H}_{Ai}^H(k), i \in \{B, E\}$ are known at the node i, the optimum receive filter can be used in order to gather the transmitted information signal $x_A(k)$. Note that even in this case, the noise components (both AN and thermal noise) still affects the error performance. However, as AN can be controlled by the legitimate transmitter who has the channel information, its effects can be maximized on the receiver. The ideal scenario, which is not easy to achieve in practical systems,

Design of AN not in Bob null space since they consider that Hb and He can be correlated. In general it is not the case since it should require than Eve is less than a wavelength apart from Bob —> In the case channels are correlated: pseudo random noise is generated

would be that the channels between legitimate users and the one between transmitter and the eavesdropper is uncorrelated. In this case, it is possible to send AN only to the eavesdropper E, which is in the null space of the legitimate receiver channel.

In order to make sure that the legitimate receiver is able to remove all the effects of AN from the signal even when the channels are correlated, pseudo random noise can be used as AN. In this case, legitimate receiver can also know the AN component $\mathbf{z}_A(k)$ and is able to eliminate AN from the received signal.

In this section, we will introduce three commonly used linear receive filters. The optimization problem and numerical results will be given for different scenarios.

1) *Receive matched filter:* The receive matched filter is optimum for noise limited scenarios as it maximizes the SNR at the filter output

$$\mathbf{g}_{MF}(k) = \lambda \mathbf{p}_A^H(k)\mathbf{H}_{AB}(k), \tag{8}$$

where λ is a scalar that can be chosen freely. Note that the receive matched filter does not take the interference into account. SINR expression for node $i \in \{B, E\}$ adopting the receive matched filter can be given as

$$\gamma_{MF}^i = \frac{\mathbf{p}_A^H(k)\mathbf{R}_{Ai}(k)\mathbf{p}_A(k)}{\mathrm{Tr}(\mathbf{P}_A(k)\mathbf{\Phi}(k)) + \sigma_{n_i}^2}, \tag{9}$$

where $\mathbf{R}_{Ai}(k) = \mathbf{H}_{Ai}(k)\mathbf{H}_{Ai}^H(k)$.

2) *Receive zero-forcing (ZF) filter:* The zero forcing filter aims to achieve the interference free information component of the received signal, fulfilling

$$\mathbf{g}_{ZF}(k)\mathbf{H}_{Ai}^H(k)\mathbf{p}_A(k)x_A(k) = x_A(k), \tag{10}$$

which implies

$$\mathbf{g}_{ZF}(k)\mathbf{H}_{Ai}^H(k)\mathbf{p}_A(k) = 1. \tag{11}$$

Thus, the ZF filter can be obtained as

$$\mathbf{g}_{ZF} = (\mathbf{p}_A^H(k)\mathbf{H}_{Ai}(k)\mathbf{H}_{Ai}^H(k)\mathbf{p}_A(k))^{-1}\mathbf{p}_A^H(k)\mathbf{H}_{Ai}(k). \tag{12}$$

The ZF filter is similar to the matched filter solution in (7). In fact, (11) can be obtained from (7) by setting $\lambda = (\mathbf{p}_A^H(k)\mathbf{H}_{Ai}(k)\mathbf{H}_{Ai}^H(k)\mathbf{p}_A(k))^{-1}$. This means that the SNR obtained for matched filter in (8) is valid for ZF filter, as

$$\gamma_{MF}^i = \gamma_{ZF}^i = \frac{\mathbf{p}_A^H(k)\mathbf{R}_{Ai}(k)\mathbf{p}_A(k)}{\mathrm{Tr}(\mathbf{P}_A(k)\mathbf{\Phi}(k)) + \sigma_{n_i}^2}. \tag{13}$$

3) *The optimum receive filter:* The optimal linear receive filter is obtained by minimizing the MSE defined as

$$\mathbf{g}_{OF} = \mathrm{argmin}_g E\left\{|\hat{x}_A^i(k) - x_A(k)|^2\right\}. \tag{14}$$

The optimum filter achieves a trade-off between the noise and the interference cancellation, maximizing the error performance. The filter can be obtained as

$$\mathbf{g}_{OF}(k) = \alpha \mathbf{R}_i^{-1}(k)\mathbf{p}_A^H(k)\mathbf{H}_{Ai}(k), \tag{15}$$

where $\alpha > 0$ is a scaling factor and $\mathbf{R}_i(k) = \mathbf{H}_{Ai}(k)\mathbf{\Phi}(k)\mathbf{H}_{Ai}^H(k) + \sigma_{n_i}\mathbf{I}_{N_i}$ is the autocorrelation matrix of the effective interference plus noise on the receiver node i. At the output of the optimal filter the SINR can be expressed as

$$\gamma_{OF}^i(k) = \mathbf{p}_A^H(k)\mathbf{H}_{Ai}(k)(\mathbf{R}_i(k))^{-1}\mathbf{H}_{Ai}^H(k)\mathbf{p}_A(k). \tag{16}$$

Please note that we restrict our study with the above-mentioned three well-known receiver designs in order to show the effect of the use of different filters.

transmit filter designed to ensure a given SR and a given QoS for the legitimate link

3.4 Transmit Filter

The transmit filter $\mathbf{p}_A(k)$ can be optimized on the transmitter side in order to maintain a QoS level for the legitimate communication while ensuring a predefined secrecy capacity.

The power minimization problem can be expressed as follows:

$$\begin{cases} \min\limits_{\mathbf{p}_A(k),\mathbf{\Phi}(k)} & \mathcal{P}_i + \mathcal{P}_{AN} \\ \text{s.t.} & \gamma^b \geq \beta_b \\ & \gamma^e \leq \beta_e \\ & \mathbf{\Phi}(k) \succeq 0, \end{cases} \tag{17}$$

where $\beta_B(k)$ and $\beta_E(k)$ are the SINR constraints for nodes B and E, respectively. The problem aims to jointly optimize the transmit filter $\mathbf{p}_A(k)$ and the AN correlation matrix $\mathbf{\Phi}(k)$ with respect to the QoS constraint on legitimate receiver and secrecy constraint on the eavesdropper.

3.5 Full-Duplex Communication Signal Model

In the FD case, both legitimate nodes A and B are actively sending and receiving information signals at the same time. Additionally they are able to send AN signals to the eavesdropper. The system model is shown in Fig. 4. Hence the eavesdropper node E receives the information signals from both A and B along with the transmitted AN. We consider for E to listen both A and B, as in [26] and derive the optimization problem to jointly optimize $\mathbf{p}_A(k)$, $\mathbf{p}_B(k)$, $\mathbf{\Phi}_A(k)$ and $\mathbf{\Phi}_B(k)$. The QoS constraints are defined for the received SINR of A and B. Similarly, the secrecy constraints are extended to cover the cases where E is trying to gather $x_A(k)$ and $x_B(k)$.

In this section, the signal model regarding the full duplex case is given. The transmitted information signals after the transmit filter of A and B are

$$\mathbf{s}_A(k) = \mathbf{p}_A(k)x_A(k), \mathbf{s}_B(k) = \mathbf{p}_B(k)x_B(k). \tag{18}$$

The power invested in the transmission of information signal and artificial noise are denoted by $\mathcal{P}_i$ and $\mathcal{P}_{AN}$, and calculated as

$$\mathcal{P}_i^A = \sum_{k=1}^{K} \mathrm{Tr}\left(\mathbf{s}_A(k)\mathbf{s}_A(k)^H\right) = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{P}_A(k)), \tag{19}$$

$$\mathcal{P}_{AN}^A = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{\Phi}_A(k)) \tag{20}$$

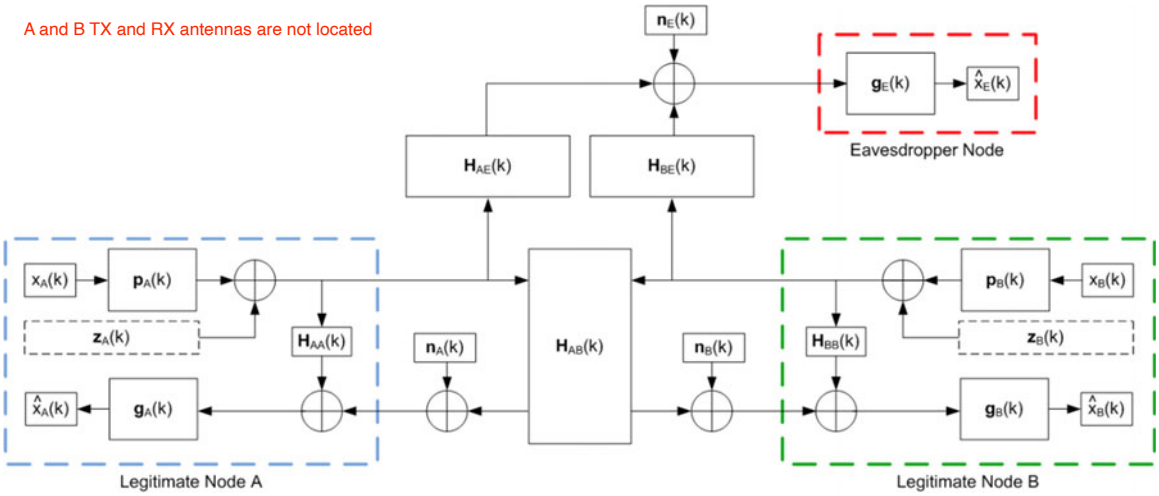

Fig. 4. Full duplex case. Legitimate nodes A and B send information signal along with artificial noise. All signals go through wireless parallel Gaussian channels before they are received by the other legitimate node and the eavesdropper node E. The eavesdropper node gets affected by the interference caused by simultaneous transmission along with the artificial noise.

$$\mathcal{P}_i^B = \sum_{k=1}^{K} \mathrm{Tr}\Big(\mathbf{s}_B(k)\mathbf{s}_B(k)^H\Big) = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{P}_B(k)), \tag{21}$$

$$\mathcal{P}_{AN}^B = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{\Phi}_B(k)) \tag{22}$$

where $\mathbf{P}_B(k) = \mathbf{p}_B(k)\mathbf{p}_B(k)^H$. The received signals can be modeled as

$$\begin{aligned} r_A(k) = {} & \mathbf{H}_{BA}^H(\mathbf{s}_B(k) + \mathbf{z}_B(k)) \\ & + \kappa_A(k)\mathbf{H}_{AA}(\mathbf{s}_A(k) + \mathbf{z}_A(k)) + \mathbf{n}_A(k) \end{aligned} \tag{23}$$

$$\begin{aligned} r_B(k) = {} & \mathbf{H}_{AB}^H(k)(\mathbf{s}_A(k) + \mathbf{z}_A(k)) \\ & + \kappa_B(k)\mathbf{H}_{BB}(\mathbf{s}_B(k) + \mathbf{z}_B(k)) + \mathbf{n}_B(k) \end{aligned} \tag{24}$$

$$\begin{aligned} r_E(k) = {} & \mathbf{H}_{AE}^H(\mathbf{s}_A(k) + \mathbf{z}_A(k)) \\ & + \mathbf{H}_{BE}^H(\mathbf{s}_B(k) + \mathbf{z}_B(k)) + \mathbf{n}_E(k), \end{aligned} \tag{25}$$

where $\mathbf{n}_A(k)$, $\mathbf{n}_B(k)$ and $\mathbf{n}_E(k)$ are independent and identically distributed (i.i.d.) complex circular Gaussian noise vectors following $\mathbf{n}_i \sim CN(0, \sigma_{n_i}^2 \mathbf{I}_{N_i}), \forall i \in \{A, B, E\}$. $\kappa_A(k)$ and $\kappa_B(k)$ are the SIC factor of A and B, which control the non-canceled self-interference component of FD operating nodes. As this part is usually very small and dependent on SIC cancellation technique, the exact value is disregarded and $\kappa_A(k) = \kappa_B(k) = \kappa$ will be used throughout the rest of the paper.

Self Interference Cancellation := SIC

The estimated signals for each receiver can be expressed as

$$\hat{x}_B^A(k) = \mathbf{g}_A(k)\mathbf{r}_A(k) \tag{26}$$

$$\hat{x}_A^B(k) = \mathbf{g}_B(k)\mathbf{r}_B(k) \tag{27}$$

$$\hat{x}_A^E(k) = \mathbf{g}_{E_A(k)}\mathbf{r}_E(k) \tag{28}$$

$$\hat{x}_B^E(k) = \mathbf{g}_{E_B(k)}\mathbf{r}_E(k), \tag{29}$$

where $\mathbf{g}_A(k)$ and $\mathbf{g}_B(k)$ have dimensions of $1 \times N_A$ and $1 \times N_B$ and represent the receive filters of the corresponding nodes. $\mathbf{g}_{E_i}, i \in \{A, B\}$ represents the receive filter of E, when listening to node i. The SINR expressions at the receivers can be obtained as,

$$\gamma^A = \frac{\mathrm{E}\Big\{|\mathbf{g}_A(k)\mathbf{H}_{BA}^H\mathbf{p}_B(k)x_B(k)|^2\Big\}}{\mathrm{E}\Big\{|\mathbf{g}_A(k)\mathbf{H}_{BA}^H\mathbf{z}_B(k)|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_A(k)\kappa|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_A(k)\mathbf{n}_A(k)|^2\Big\}} \tag{30}$$

$$\gamma^B = \frac{\mathrm{E}\Big\{|\mathbf{g}_B(k)\mathbf{H}_{AB}^H(k)\mathbf{p}_A(k)x_A(k)|^2\Big\}}{\mathrm{E}\Big\{|\mathbf{g}_B(k)\mathbf{H}_{AB}^H(k)\mathbf{z}_A(k)|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_B(k)\kappa|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_B(k)\mathbf{n}_B(k)|^2\Big\}} \tag{31}$$

$$\gamma_A^E(k) = \frac{\mathrm{E}\Big\{|\mathbf{g}_{E_A(k)}\mathbf{H}_{AE}^H\mathbf{p}_A(k)x_A(k)|^2\Big\}}{\mathrm{E}\Big\{|\mathbf{g}_{E_A(k)}\mathbf{H}_{AE}^H\mathbf{z}_A(k)|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_{E_A(k)}\mathbf{H}_{BE}^H(\mathbf{s}_B(k) + \mathbf{z}_B(k))\Big\} + \mathrm{E}\Big\{|\mathbf{g}_{E_A(k)}\mathbf{n}_E(k)|^2\Big\}} \tag{32}$$

$$\gamma_B^E(k) = \frac{\mathrm{E}\Big\{|\mathbf{g}_{E_B(k)}\mathbf{H}_{BE}^H\mathbf{p}_B(k)x_B(k)|^2\Big\}}{\mathrm{E}\Big\{|\mathbf{g}_{E_B(k)}\mathbf{H}_{BE}^H\mathbf{z}_B(k)|^2\Big\} + \mathrm{E}\Big\{|\mathbf{g}_{E_B(k)}\mathbf{H}_{AE}^H(\mathbf{s}_A(k) + \mathbf{z}_A(k))\Big\} + \mathrm{E}\Big\{|\mathbf{g}_{E_B(k)}\mathbf{n}_E(k)|^2\Big\}}. \tag{33}$$

TABLE 2
Simulation Parameters

Parameter	Value	Effect
# of Monte-Carlo runs	1,000	improves convergence
Eavesdropping node	E	-
Target node	A	-
$N_A = N_B = N_E$	4	improves tx/rx performance
β_B	10 dB	QoS constraint, increases the required power
β_E	0 dB	Secrecy constraint, decreases the required power
$\sigma^2_{n_A} = \sigma^2_{n_B}$	0 dB	Noise variance of legitimate channels
Channels	Normalized power Rayleigh fading	-

The matched filter and ZF filter does not change for the full duplex case, therefore the above-mentioned half duplex case derivations can be used. However, as the interference changes for each node, the optimal filter also changes. By updating the interference covariance matrices as

$$\mathbf{R}_i = \mathbf{H}_{Ai}(k)\mathbf{\Phi}(k)\mathbf{H}^H_{Ai}(k) + \kappa^2\mathbf{I}_N + \sigma^2_{n_i}\mathbf{I}_N, i \in \{A, B\}$$

$$\begin{aligned}\mathbf{R}^A_E(k) = {} & \mathbf{H}_{AE}(k)\mathbf{\Phi}_A(k)\mathbf{H}^H_{AE}(k) + \mathbf{H}_{BE}(k)\mathbf{\Phi}_B(k)\mathbf{H}^H_{BE}(k) \\ & + \mathbf{H}_{BE}(k)\mathbf{p}_B(k)\mathbf{p}_B(k)^H\mathbf{H}^H_{BE}(k) + \sigma^2_e\mathbf{I}_N\end{aligned}$$

$$\begin{aligned}\mathbf{R}^B_E(k) = {} & \mathbf{H}_{AE}(k)\mathbf{\Phi}_A(k)\mathbf{H}^H_{AE}(k) + \mathbf{H}_{BE}(k)\mathbf{\Phi}_B(k)\mathbf{H}^H_{BE}(k) \\ & + \mathbf{H}_{AE}(k)\mathbf{p}_A(k)\mathbf{p}^H_A(k)\mathbf{H}^H_{AE}(k) + \sigma^2_e\mathbf{I}_N.\end{aligned} \tag{34}$$

Afterwards the final SINR of $j-i$ link can be expressed as

$$\gamma^i_j(k) = \mathbf{p}_j(k)\mathbf{H}^H_{ji}(k)\mathbf{R}_i(k)^{-1}\mathbf{p}^H_j(k)\mathbf{H}_{ji}(k), \tag{35}$$

where $i \in \{A, B, E\}$ and $j \in \{A, B\}, i \neq j$.

Finally, our proposed FD power optimization problem is defined as

$$\begin{cases} \min\limits_{\mathbf{p}_A(k),\mathbf{\Phi}_A(k),\mathbf{p}_B(k),\mathbf{\Phi}_B(k)} & \mathcal{P}^A_i + \mathcal{P}^B_i + \mathcal{P}^A_{AN} + \mathcal{P}^B_{AN} \\ \text{s.t.} & \gamma_{AB}(k) \geq \beta_A(k) \\ & \gamma_{BA}(k) \geq \beta_B(k) \\ & \gamma_{EA}(k) \leq \beta_E(k) \\ & \gamma_{EA}(k) \leq \beta_E(k) \\ & \mathbf{\Phi}_A(k) \succeq 0 \\ & \mathbf{\Phi}_B(k) \succeq 0, \end{cases} \tag{36}$$

where $\beta_A(k)$, $\beta_B(k)$ and $\beta_E(k)$ are the SINR constraints for A, B and E respectively. The formulation in (36) is our proposed optimization method which ensures a QoS and secrecy level with minimum power consumption possible. The SINR constraints of A and B given in (36) define the QoS requirements of the system, while SINR constraints on E imply the secrecy level for the legitimate nodes A and B. Note that use of different modulation schemes, coding techniques, antenna arrays or joint detection performance of eavesdropper do not change our problem defined on SINR. However, these variations affect the error performance and the required SINR level corresponding to a certain bit error rate (BER) may change. Hence, SINR constraints should be chosen according to the expected error performance.

Lemma 1. *SINR constraints in (36) can be stated as a semi-definite program (SDP) for both zero forcing and optimal filter methods.*

Proof. Please refer to Appendix A. □

4 Effect of Channel Estimation Error and Residual Self Interference

AN and beamforming methods are usually based on using channel modeling and estimation to optimize related network parameters. Noting that an ideal CSI is difficult to obtain [40], analysis of the effects of the channel estimation error is very important especially for channel estimation based optimizations. There exist many studies about how to model channel estimation errors [41], [42], [43]. In order to include channel estimation error in the problem definition provided above, we define the estimated channel as $\hat{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{H}_{i_e}$, where $\mathbf{H}_{i_e} \sim CN(0, \sigma^2_{H_{error}}\mathbf{I}_{N_i})$. Estimation error covariance $\sigma^2_{H_{error}}$ is defined by,

$$\sigma^2_{H_{error}} = \frac{\xi\mathbf{I}_{N_i}}{N_i}, i \in \{AB, BA, AE, BE\}, \tag{37}$$

where ξ is channel estimation error factor. This formulation is based on the estimation error model given in [36]. After inclusion of channel estimation error, we assume that the CSI is obtained with an error depending on a statistical error rate. After the calculations, data is sent by the transmitter using parameters which are mistakenly considered to be optimal by the system. With this assumption, we can determine the real and erroneous SINRs of the system. The beamforming coefficients calculated using the channel estimates will be non-optimal and a difference between required and erroneous SINRs is expected.

The self interference component is also very crucial when analyzing the FD system's ergodic capacity performance because of its destructive effects on received signal and transmission power. To observe the effects of SIC, we operate different values of κ in the numerical results to show the effect of the SI in the performance.

5 Numerical Results

We used the MATLAB as the simulation platform and SeDuMi [44] as convex optimization engine. The simulation parameters are given in Table 2.

The results of the simulations are given in Fig. 5, where we consider improving channel conditions for E (i.e., decreasing σ^2_v). The doubled values of power levels regarding the half duplex systems are also given to make a fair comparison with full duplex systems by equalizing throughput. We conclude from Fig. 5 that the full duplex systems outperforms the half duplex systems in all receiver cases. However optimum filter satisfies the constraints with lower transmit power consumption than the other filters, as expected.

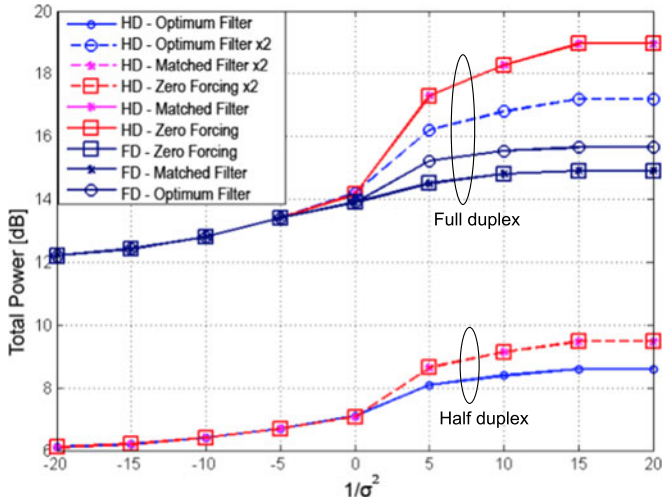

Fig. 5. Half duplex and full duplex results with different receivers.

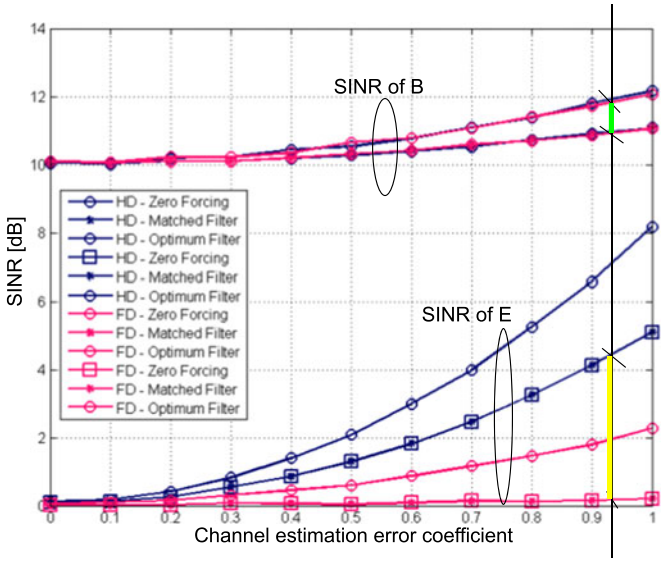

Fig. 6. The impact of channel estimation error.

In order to compare the performance of our proposed framework with the baseline studies [18] and [30] the simulations are run for each method with the same parameters. σ_v^2 is set to 10 dB for all scenarios. The results are given in Table 3. From the table, it can be seen that the full duplex systems outperforms the half duplex one, which is an expected result. It is shown that as our system is considers the receive filters during the optimization, it is more efficient than the previous full duplex scenario.

The real and erroneous SINR values on B and E under varying channel estimation error factor can be seen in Fig. 6. As the figure clearly shows, the lowest Δ_{SINR} is achieved by the full duplex system. Notice that lower Δ_{SINR} values mean lower SINR on E. This is a result of the FD communication systems, as two nodes communicate in the same time and frequency blocks and all other channels also are affected by either of them. Endorsed by the simulation results, we can conclude that FDB is more resilient to channel estimation errors. Also, the receive filter choice effects the system performance under the presence of channel estimation errors. We can see that ZF and matched filter performs better than the optimum filter. However in all cases, as the channel estimation errors still results in unmet constraints, they are definitely an important aspect to consider especially when designing a practical system.

In Fig. 7, it can be seen that while the residual self interference coefficient κ is increasing, the total transmit power of system also increases. When the SIC performance is closer to perfect, the system requires less transmit power to communicate at FD mode. The optimum filter outperforms the other receive filters on the resiliency to uncanceled self interference. We can conclude from the results that if the self interference cancellation process is not very successful, the total power needed to satisfy the constraints may increase. In this case, it may be more power efficient to use half duplex mode instead of full duplex.

TABLE 3
Performance Comparison with Baseline Works [18] and [30]

Method	Total Power [dB]
Half duplex optimized-AN QoS beamforming [18]	18.05 dB
Full duplex optimized AN-beamforming [30]	14.96 dB
Proposed full duplex tx/rx filter optimization	14.23 dB

6 Practical Considerations

The framework proposed in this paper has a high potential for practical implementation on the CPSs due to the power efficient nature. Power consumption is a critical aspect for mobile CPSs due to the limited battery power of multiple wireless sensor devices and also the possible interference problems in industrial scenarios.

6.1 Complexity

One of the most important implementation concerns would be the calculation complexity of the solution. The computational resources should be sufficient to compute the system parameters within an acceptable delay window and re-calculate the system parameters when the channel conditions are changed. The acceptable delay window can vary regarding the application and the optimization frequency is

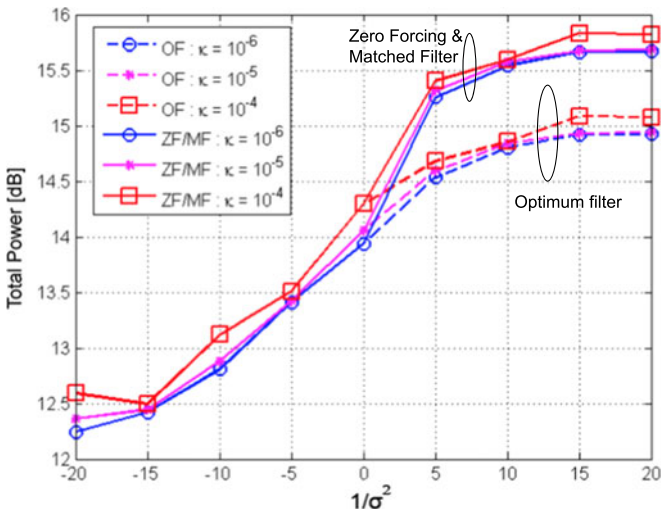

Fig. 7. The impact of self-interference coefficient.

directly bounded to the channel stationarity. However note that industry environments are usually not very dynamic and/or are repetitive. Hence, it may be possible to calculate and reuse the results in an industry application, as the conditions are likely to repeat themselves, e.g., the products follow the same path in a factory.

The optimization frequency should be higher on rapidly time-varying channels, as in vehicular networks where the nodes have high speeds, leading to higher utilization computational resources. As proposed in [45], the process of the increasing difference between the channel estimate and the actual channel coefficients can be modeled as a function of the time between the channel estimations. The required frequency changes by the MIMO setup, modulation and coherence time. However, it is possible to calculate the time needed between channel estimates. For example, the authors state in [45] that for an 8×2 MIMO system with 4-QAM modulation, the time between estimates would be about 17 ms where the coherence channel is 35 ms. Whereas an 8×8 MIMO system needs a new estimation every 0.086 ms with the same modulation.

6.2 Mobility

Mobility of the nodes may affect the system. Assume the location of Alice is fixed (e.g., base station), and Bob is mobile (e.g., a robot in production). Here, if Eve has a stationary location, she may be able to get a better channel than Bob's. With AN, the constraints may still be met with additional power, if the problem is not infeasible. If the possible locations of the eavesdropper are known (e.g., public areas), additional AN sources may be implemented to further disturb the potential eavesdropper.

7 Conclusion

In this paper we have proposed a joint transmit filter and AN optimization framework for the wireless full duplex and half duplex communication systems. We have analyzed the systems using different linear filters in parallel MIMO Gaussian channels. The results are extended by the addition of channel estimation errors and the self interference. The proposed framework was implemented and evaluated through simulations. It has been concluded that the full duplex AN system has better performance than the other systems when there is successful SIC. We also assert that channel estimation errors should be considered in added power optimization models as they have a significant influence on the performance, especially for practical implementations.

Appendix A
Proof of Lemma 1

In order to achieve the optimal solution we use the coordinate descent method, where $\mathbf{p}_A(k)$ and $\mathbf{p}_A(k)$ and and $\mathbf{\Phi}_A(k)$ and $\mathbf{\Phi}_B(k)$ are optimized step-by-step in an iterative fashion, by setting an initial value to $\mathbf{\Phi}_A(k)$ and $\mathbf{\Phi}_B(k)$. We define $\mathbf{Q}_i(k) = \mathbf{H}_{ji}^H(k)\mathbf{R}_i^{-1}(k)\mathbf{H}_{ji}(k)$, which become PSD matrices. Hence, we may make use of semi-definite relaxation (SDR) techniques, as they are a common approach to obtain a convex problem that approximate the original solution by relaxing the non-convex constraints. For the optimal receive filters, (36) becomes a nonconvex quadratically constrained quadratic problem. SINR constraints in (36) can be expressed for optimum filter scheme as

$$\begin{aligned} &\mathbf{p}_j(k)\mathbf{H}_{ji}^H(k)\mathbf{R}_i^{-1}(k)\mathbf{H}_{ji}(k)\mathbf{p}_j^H(k) \geq \beta_i(k) \\ &\mathbf{p}_j(k)\mathbf{Q}_j(k)\mathbf{p}_j^H(k)\beta_i(k), \end{aligned} \tag{38}$$

where $i, j \in \{A, B\}, j \neq i$.

The first step in deriving an SDR is to observe that

$$\mathbf{p}\mathbf{Q}\mathbf{p}^H = \mathrm{Tr}\{\mathbf{p}\mathbf{Q}\mathbf{p}^H\} = \mathrm{Tr}\{\mathbf{Q}\mathbf{p}\mathbf{p}^H\} = \mathrm{Tr}\{\mathbf{Q}\mathbf{P}\}, \forall \mathbf{Q} \succeq 0. \tag{39}$$

Notice that defining new variable $\mathbf{P}(k) = \mathbf{p}(k)\mathbf{p}^H(k)$ is equivalent to $\mathbf{P}(k)$ being a rank one symmetric PSD matrix which adds the constraints $\mathbf{P}(k) \succeq 0$, $\mathrm{rank}(\mathbf{P}(k)) = 1$. However, the problem is still considered as hard to solve, due to the non-convex $\mathrm{rank}(\mathbf{P}(k)) = 1$ constraint. Applying SDR approach to make the problem convex, we relax it by neglecting this constraint and we achieve the convex SDR problem for optimum filter receiver case as

$$\begin{cases} \min\limits_{\mathbf{P}_A(k), \mathbf{P}_B(k)} & \mathrm{Tr}\{\mathbf{P}_A(k)\} + \mathrm{Tr}\{\mathbf{P}_B(k)\} \\ \text{s.t.} & \mathrm{Tr}\{\mathbf{Q}_A(k)\mathbf{P}_A(k)\} \geq \beta_A(k) \\ & \mathrm{Tr}\{\mathbf{Q}_B(k)\mathbf{P}_B(k)\} \geq \beta_B(k) \\ & \mathrm{Tr}\{\mathbf{Q}_E(k)\mathbf{P}_A(k)\} \leq \beta_E(k) \\ & \mathrm{Tr}\{\mathbf{Q}_E(k)\mathbf{P}_B(k)\} \leq \beta_E(k) \end{cases} \tag{40}$$

The problem (40) is an SDP. As the next iteration, we perform the identical procedure to obtain $\mathbf{\Phi}_A(k)$ and $\mathbf{\Phi}_B(k)$ and repeat until convergence. As we omitted the non-convex rank-1 constraints on $\mathbf{P}_A(k)$ and $\mathbf{P}_B(k)$, the SDP problem in (40) is not actually equal to the original problem in (36), however the solution of (40) yields to the our original problem in (36), which can be derived with the same approach presented in [30].

Acknowledgments

This work is supported in part by TUBITAK under Grant 115E827.

References

[1] J. Wurm, et al., "Introduction to cyber-physical system security: A cross-layer perspective," *IEEE Trans. Multi-Scale Comput. Syst.*, to be published, doi: 10.1109/TMSCS.2016.2569446.
[2] C. C. Lin, D. J. Deng, Z. Y. Chen, and K. C. Chen, "Key design of driving industry 4.0: Joint energy-efficient deployment and scheduling in group-based industrial wireless sensor networks," *IEEE Commun. Mag.*, vol. 54, no. 10, pp. 46–52, Oct. 2016.
[3] J. Wan, A. B. Lopez, and M. A. A. Faruque, "Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security," in *Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst.*, Apr. 2016, pp. 1–10.
[4] Y. Zhang, G. Li, Q. Du, G. Lyu, and G. Zhang, "High-rate cooperative beamforming for physical-layer security in wireless cyber-physical systems," in *Proc. IEEE Int. Conf. Commun. Workshop*, Jun. 2015, pp. 2622–2626.
[5] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1334–1387, 1975.
[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[7] M. Sarkar and T. Ratnarajah, "Secrecy capacity and secure outage performance for Rayleigh fading SIMO channel," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, 2011, pp. 1900–1903.

[8] S. Yang, P. Piantanida, M. Kobayashi, and S. Shamai, "On the secrecy degrees of freedom of multi-antenna wiretap channels with delayed CSIT," in *Proc. IEEE Int. Symp. Inf. Theory Proc.*, 2011, pp. 2866–2870.
[9] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[10] J. Huang and A. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
[11] X. Yang and A. Swindlehurst, "On the use of artificial interference for secrecy with imperfect CSI," in *Proc. IEEE 12th Int. Workshop Signal Process. Advances Wireless Commun.*, 2011, pp. 476–480.
[12] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
[13] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.
[14] A. Mukherjee and A. Swindlehurst, "Ensuring secrecy in MIMO wiretap channels with imperfect CSIT: A beamforming approach," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.
[15] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
[16] J. Yang, I. M. Kim, and D. I. Kim, "Joint design of optimal cooperative jamming and power allocation for linear precoding," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3285–3298, Sep. 2014.
[17] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.
[18] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
[19] M. R. D. Rodrigues and P. D. M. Almeida, "Filter design with secrecy constraints: The degraded parallel Gaussian wiretap channel," in *Proc. IEEE Global Telecommun. Conf.*, Nov. 2008, pp. 1–5.
[20] H. Reboredo, M. Ara, M. R. D. Rodrigues, and J. Xavier, "Filter design with secrecy constraints: The degraded multiple-input multiple-output gaussian wiretap channel," in *Proc. IEEE 73rd Veh. Technol. Conf.*, May 2011, pp. 1–5.
[21] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
[22] A. Ozcelikkale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2234–2238, Dec. 2015.
[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[24] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, 2010, pp. 1–12.
[25] M. Jain, et al., "Practical, real-time, full duplex wireless," in *Proc. 17th Annu. Int. Conf. Mobile Comput. Netw.*, 2011, pp. 301–312.
[26] P. Lioliou, M. Viberg, M. Coldrey, and F. Athley, "Self-interference suppression in full-duplex MIMO relays," in *Proc. Conf. Rec. 44th Asilomar Conf. Signals Syst. Comput.*, Nov. 2010, pp. 658–662.
[27] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex bidirectional MIMO: Achievable rates under limited dynamic range," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3702–3713, Jul. 2012.
[28] H. Ju, S. Lim, D. Kim, H. V. Poor, and D. Hong, "Full duplexity in beamforming-based multi-hop relay networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1554–1565, Sep. 2012.
[29] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.
[30] O. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1075–1078, Jun. 2014.
[31] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[32] X. Ji, X. Kang, K. Huang, N. Li, and M. Yi, "The full-duplex artificial noise scheme for security of a cellular system," *China Commun.*, vol. 12, pp. 150–156, Dec. 2015.
[33] M. Joham, W. Utschick, and J. A. Nossek, "Linear transmit processing in MIMO communications systems," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 2700–2712, Aug. 2005.
[34] B. R. Vojcic and W. M. Jang, "Transmitter precoding in synchronous multiuser communications," *IEEE Trans. Commun.*, vol. 46, no. 10, pp. 1346–1355, Oct. 1998.
[35] R. L.-U. Choi and R. D. Murch, "New transmit schemes and simplified receivers for MIMO wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 2, no. 6, pp. 1217–1230, Nov. 2003.
[36] G. Dartmann, V. Lucken, O. Cepheli, G. K. Kurt, and G. Ascheid, "Filter optimization aided interference management with improved secrecy," in *Proc. IEEE 80th Veh. Technol. Conf.*, Sep. 2014, pp. 1–6.
[37] S. Li, R. D. Murch, and V. K. N. Lau, "Linear transceiver design for full-duplex multi-user MIMO system," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 4921–4926.
[38] A. C. Cirik, O. Taghizadeh, L. Lampe, R. Mathar, and Y. Hua, "Linear transceiver design for full-duplex multi-cell MIMO Systems," *IEEE Access*, vol. 4, pp. 4678–4689, 2016.
[39] A. Ispas, C. Schneider, G. Dartmann, X. Gong, G. Ascheid, and R. Thomä, "Analysis of mismatched downlink beamforming over non-stationary channels with interference," in *Proc. 30th URSI General Assembly Sci. Symp.*, Aug. 2011, pp. 1–4.
[40] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2007–2019, Sep. 1999.
[41] L. Berriche, K. Abed-Meraim, and J. C. Belfiore, "Effect of imperfect channel knowledge on the MIMO channel outage capacity," in *Proc. IEEE 7th Workshop Signal Process. Advances Wireless Commun.*, Jul. 2006, pp. 1–5.
[42] T. Yoo and A. Goldsmith, "Capacity of fading MIMO channels with channel estimation error," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2004, pp. 808–813.
[43] W. Junxuan, "Effect of channel estimation error on MIMO-OFDM systems capacity," in *Proc. Int. Conf. Wireless Commun. Netw. Mobile Comput.*, 2010, pp. 1–3.
[44] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods Softw.*, vol. 11, pp. 625–653, 1999.
[45] V. Pohl, P. H. Nguyen, V. Jungnickel, and C. von Helmolt, "How often channel estimation is needed in MIMO systems," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2003, pp. 814–818.

Özge Cepheli received the BSc degree in electronics engineering, in 2009 and the MSc degree in telecommunications engineering from Istanbul Technical University, Turkey, in 2011. She is now working toward the PhD degree working on wireless physical layer security within the Wireless Communications Research Laboratory, Istanbul Technical University. She also works as a consultant in the Technical and Scientific Support Department, EUMETSAT. Her research interests include wireless communications, physical layer security, and multi-layer security techniques in communication networks.

Guido Dartmann received the diploma degree in computer engineering and the PhD degree in electrical engineering from RWTH Aachen University, Germany. From 2012 to 2015, he was a chief engineer in the Institute for Integrated Signal Processing Systems, RWTH Aachen University. Since 2016, he has been a professor of distributed systems with the University of Applied Sciences Trier. His main areas of research interests include distributed systems, secrecy in wireless communication, and communication aspects of real-time cyber-physical systems and machine learning and data analytics in engineering.

Güneş Karabulut Kurt (M'06-SM'15) received the BS degree (high Hons.) in electronics and electrical engineering from Bogazici University, Istanbul, Turkey, in 2000 and the MASc and PhD degrees in electrical engineering from the University of Ottawa, ON, Canada, in 2002 and 2006, respectively. From 2000 to 2005, she was a research assistant with the CASP Group, University of Ottawa. Betweeen 2005 and 2006, she was with TenXc Wireless, where she worked on location estimation and radio-frequency identification (RFID) systems. From 2006 to 2008, she was with Edgewater Computer Systems Inc., where she worked on high-bandwidth networking in aircraft and priority based signaling methodologies. From 2008 to 2010, she was with Turkcell Research and Development Applied Research and Technology, Istanbul. Since 2010, she has been an associate professor with Istanbul Technical University. Her research interests include sparse signal decomposition algorithms, multicarrier networks, traffic analysis, and network planning/management. She is a fellow of the Marie Curie and a senior member of the IEEE.

Gerd Ascheid (SM'08) received the diploma and PhD (Dr-Ing) degrees in electrical engineering (communication eng.) from RWTH Aachen University. In 1988, he started as a co-founder and managing director of a start-up which was acquired by Synopsys Inc., a California-based EDA market leader. During his nine years as director/senior director at Synopsys, he was responsible for IC design projects for advanced digital communication systems. In 2003, he joined RWTH Aachen University as a full professor in the Institute for Communication Technologies and Embedded Systems. His research interests is in wireless communication algorithms, application specific integrated platforms, in particular, for mobile terminals and wireless IoT devices. He has co-authored three books, published numerous papers in the domain of digital communication algorithms and ASIC implementation and is founder of several successful start-up companies. He is a senior member of the IEEE.