Physical Communication 27 (2018) 143–149

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

How to manage resources to provide physical layer security: Active versus passive adversary?

Mohammad Reza Abedi, Nader Mokari *, Hamid Saeedi

Tarbiat Modares University, Islamic Republic of Iran

ARTICLE INFO

Article history:
Received 26 August 2017
Received in revised form 8 January 2018
Accepted 1 February 2018
Available online 6 February 2018

Keywords:
Cooperative jamming
Imperfect channel state information
Physical layer security
Active and passive adversary
Semi-definite programming

ABSTRACT

This paper studies the required physical (e.g. relays and jammers) and radio resources (e.g. power) to provide physical layer security for relay and friendly jammer assisted multiple-input and single-output transmissions in the presence of multiple active and passive adversaries. The passive adversaries are half duplex and only able to overhear the transmissions from the legitimate transmitter to the legitimate receiver, while the active adversaries are full duplex and able to jam and eavesdrop simultaneously. Since the channel information between adversaries and other nodes are uncertain, robust optimization methods are considered. In this regard, the main aim is to maximize the worst case secrecy rate subject to the normalized transmit power constraints of legitimate transmitter, friendly jammer and relay, and channel state information uncertainty constraints. Through several examples, we then investigate the required increase in physical and radio resources to maintain secure communication when passive adversaries upgrades themselves to active adversaries.

1. Introduction

There has been a growing interest to provide security at the physical layer against potential adversary. The theoretical basis of physical layer security (PLS) was initiated by Wyner [1]. Accordingly, secrecy rate is defined as the achievable rate between the transmitter and receiver minus the rate from the transmitter to the eavesdropper. If the former rate is greater than the latter rate, the secrecy rate will be zero. Controlled interference, or artificial noise can be used to increase the secrecy rate and degrade the decoding ability of the adversaries. This is achieved with transmitters having multiple antennas [2–4]. On the other hand, the jamming signals of external relays can be used to degrade the adversary abilities [5–11]. In these works, it is assumed that the channels state information (CSI) between all nodes, including the CSI between adversaries and legitimate nodes, are perfectly known at which might not be a practical assumption. Accordingly, CSI uncertainty in PLS systems has been considered in [12–15]. It has to be mentioned that majority of the works on PLS assume a passive eavesdropper or adversary (PA) where the eavesdropper can only intercept the transmitted data. However, the adversary can upgrade itself to be able to also send jamming signals to destroy the transmitted data as in [16,17] or as in our prior works [18,19]. This case of active adversary (AA) will significantly degrade the secrecy rate and usually the secrecy rate will become zero.[1]

In this paper, we first assess the effect of such an upgrade on the adversary side on the secrecy rate. More importantly, in case of such an upgrade in the adversary side, we want to answer the following important question: Is it possible to maintain the secrecy rate at the level of the PA case at all and if so, what will be the required physical (i.e., number of friendly jammers and relays) and radio (i.e., the normalized transmit power) resources?

To answer this question, a system model including a single legitimate transmitter (LT) (source), a single legitimate receiver (LR) (destination), multiple adversaries, jammers, and decode-and-forward (DF) relays is assumed. To reduce the total throughput of network, AA can act as a jammer. This can create unfavorable conditions for secure communication. We then consider two scenarios. In the first one referred to as PA, the adversaries are eavesdropping the transmitted data from the LT to the LR. In the second one referred to as AA, the adversaries are eavesdropping the transmitted data from the LT to the LR while also sending jamming signals over it. In this paper, the CSI values between legitimate and adversary nodes are assumed to be uncertain and to take this issue

* Corresponding author.
E-mail addresses: mra@aut.ac.ir (M.R. Abedi), nader.mokari@modares.ac.ir (N. Mokari), hsaeedi@sce.carleton.ca (H. Saeedi).

https://doi.org/10.1016/j.phycom.2018.02.004
1874-4907/

[1] It is important to note that when the adversary becomes active, it can simultaneously overhear and jam the signal through its full duplex transceiver. In particular, we assume that the FD transceiver of the eavesdropper is equipped with an ideal self-interference canceler such that it can overhear the signal with the same quality as the PA case despite transmitting jamming signals towards the legitimate receiver.

into account, robust resource allocation based on the worst-case approach are proposed.

This paper is organized as follows. We present the notation and assumptions in the next section. In Sections 3 and 4, the corresponding optimization problems for the two proposed scenarios are provided. In Section 5, the simulation results of the two proposed scenarios are studied and we conclude the paper in Section 6.

2. Notations and assumptions

In this paper, $\mathbb{E}\{\cdot\}$ represents expectation. $(\cdot)^H$ and $\|\cdot\|$ are the Hermitian transpose and the Euclidean norm, respectively. $(\cdot)^\dagger$ is the pseudo-inverse. $\mathrm{tr}(\cdot)$ denotes the trace operator. $\mathbf{I}$ denotes an identity matrix. $\mathbb{H}^N$ represents an $N \times N$ Hermitian matrix set. $\mathbb{C}^{M\times N}$ denotes an $M \times N$ complex matrix set. In addition, $\mathbf{A} \succ 0$ denotes the positive definiteness of $\mathbf{A}$. We let $\mathcal{J}$, $\mathcal{K}$ and $\mathcal{Q}$ denote the set of jammers, relays and adversaries, respectively. The LT, jammer $j \in \mathcal{J}$, relay $k \in \mathcal{K}$ and adversary $q \in \mathcal{Q}$ are equipped with N_s, N_j, N_k and N_q transmit antennas, respectively.

For both AA and PA scenarios, we let $\mathbf{h}_{sd} \in \mathbb{C}^{1\times N_s}$ and $\mathbf{h}_{sq} \in \mathbb{C}^{1\times N_s}$ represent the channel vectors from the LT to the destination and the qth adversary, respectively. In addition, $\mathbf{h}_{jd} \in \mathbb{C}^{1\times N_j}$ and $\mathbf{h}_{jq} \in \mathbb{C}^{1\times N_j}$ denote the channel vectors from the jth jammer to the LR and the qth adversary, respectively. Accordingly, $\mathbf{h}_{kd} \in \mathbb{C}^{1\times N_k}$ and $\mathbf{h}_{kq} \in \mathbb{C}^{1\times N_k}$ denote the channel vectors from the kth relay to the LR and the qth adversary, respectively.

For the AA scenario, $\mathbf{h}_{qd} \in \mathbb{C}^{1\times N_q}$ and $\mathbf{h}_{qk} \in \mathbb{C}^{1\times N_q}$ represent the channel vectors from the qth AA to the LR and kth relay, respectively. $\mathbf{g}_q \in \mathbb{C}^{1\times N_q}$ denote the loop interference channel at the qth AA. The received noise at the LR, the kth relay and the qth adversary are assumed to be circular complex Gaussian random variables with zero-mean and ζ_d^2, ζ_k^2 and ζ_q^2 variances, respectively. For the sake of simplicity, it is assumed that $\zeta_d^2 = \zeta_k^2 = \zeta_q^2 = \zeta^2$.

We model the channel vectors $\mathbf{h}_{sq}$, $\mathbf{h}_{jq}$, $\mathbf{h}_{kq}$, $\mathbf{h}_{qk}$ and $\mathbf{h}_{qd}$ as

$$\mathbf{h}_{sq} = \tilde{\mathbf{h}}_{sq} + \mathbf{e}_{\mathbf{h}_{sq}}, \tag{1}$$

$$\mathbf{h}_{jq} = \tilde{\mathbf{h}}_{jq} + \mathbf{e}_{\mathbf{h}_{jq}}, \tag{2}$$

$$\mathbf{h}_{kq} = \tilde{\mathbf{h}}_{kq} + \mathbf{e}_{\mathbf{h}_{kq}}, \tag{3}$$

$$\mathbf{h}_{qk} = \tilde{\mathbf{h}}_{qk} + \mathbf{e}_{\mathbf{h}_{qk}}, \tag{4}$$

$$\mathbf{h}_{qd} = \tilde{\mathbf{h}}_{qd} + \mathbf{e}_{\mathbf{h}_{qd}}, \tag{5}$$

where $\tilde{\mathbf{h}}_{sq}$, $\tilde{\mathbf{h}}_{jq}$, $\tilde{\mathbf{h}}_{kq}$, $\tilde{\mathbf{h}}_{qk}$ and $\tilde{\mathbf{h}}_{qd}$ represent the estimated value of the channels and $\mathbf{e}_{\mathbf{h}_{sq}}$, $\mathbf{e}_{\mathbf{h}_{jq}}$, $\mathbf{e}_{\mathbf{h}_{kq}}$, $\mathbf{e}_{\mathbf{h}_{qk}}$ and $\mathbf{e}_{\mathbf{h}_{qd}}$ denote the corresponding CSI errors, respectively. It is assumed that the channel mismatches lie in a bounded set [12], i.e., $\mathcal{E}_{\mathbf{h}_{sq}} = \{\mathbf{e}_{\mathbf{h}_{sq}} : \|\mathbf{e}_{\mathbf{h}_{sq}}\|^2 \le \epsilon^2_{\mathbf{h}_{sq}}\}$, $\mathcal{E}_{\mathbf{h}_{jq}} = \{\mathbf{e}_{\mathbf{h}_{jq}} : \|\mathbf{e}_{\mathbf{h}_{jq}}\|^2 \le \epsilon^2_{\mathbf{h}_{jq}}\}$, $\mathcal{E}_{\mathbf{h}_{kq}} = \{\mathbf{e}_{\mathbf{h}_{kq}} : \|\mathbf{e}_{\mathbf{h}_{kq}}\|^2 \le \epsilon^2_{\mathbf{h}_{kq}}\}$, $\mathcal{E}_{\mathbf{h}_{qk}} = \{\mathbf{e}_{\mathbf{h}_{qk}} : \|\mathbf{e}_{\mathbf{h}_{qk}}\|^2 \le \epsilon^2_{\mathbf{h}_{qk}}\}$, $\mathcal{E}_{\mathbf{h}_{qd}} = \{\mathbf{e}_{\mathbf{h}_{qd}} : \|\mathbf{e}_{\mathbf{h}_{qd}}\|^2 \le \epsilon^2_{\mathbf{h}_{qd}}\}$, where $\epsilon^2_{\mathbf{h}_{sq}}$, $\epsilon^2_{\mathbf{h}_{kq}}$, $\epsilon^2_{\mathbf{h}_{qk}}$, $\epsilon^2_{\mathbf{h}_{jq}}$ and $\epsilon^2_{\mathbf{h}_{qd}}$ are known constants.

3. The PA scenario

In this section, we consider a multiple-input and single-output (MISO) communication system with an LT, a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of $J = |\mathcal{J}|$ jammers, a set $\mathcal{K} = \{1, 2, \ldots, K\}$ of $K = |\mathcal{K}|$ DF relays, an LR, and a set $\mathcal{Q} = \{1, 2, \ldots, Q\}$ of $Q = |\mathcal{Q}|$ PAs. In this scenario, adversaries are only able to overhear the link between LT and LR. The data rate through the kth DF relay link assisted by friendly jammer j can be written as [20]

$$R^{\mathrm{D}}_{kj} = \frac{1}{2}\left[\min\left\{\log_2\left(1 + \frac{\mathbf{h}_{sk}\mathbf{G}_s\mathbf{h}^H_{sk}}{\zeta^2 + \mathbf{h}_{jk}\mathbf{G}_j\mathbf{h}^H_{jk}}\right), \log_2\left(1 + \frac{\mathbf{h}_{kd}\mathbf{G}_k\mathbf{h}^H_{kd} + \mathbf{h}_{sd}\mathbf{G}_s\mathbf{h}^H_{sd}}{\zeta^2 + \mathbf{h}_{jd}\mathbf{G}_j\mathbf{h}^H_{jd}}\right)\right\}\right], \tag{6}$$

where factor $\frac{1}{2}$ appears because the relay transmission is divided into two stages. The transmitted signal by LT and its covariance matrix are denoted by $\mathbf{z}_s$ and $\mathbf{G}_s = \mathbb{E}\{\mathbf{z}_s\mathbf{z}_s^H\}$, respectively. The normalized transmit power constraint set for LT is represented by $\mathcal{G}_s = \{\mathbf{G}_s : \mathbf{G}_s \succeq \mathbf{0}, \mathrm{tr}(\mathbf{G}_s) \le P_s\}$ where P_s is the maximum predefined normalized transmit power for it. The transmitted signal by jammer j and its covariance matrix are denoted by $\mathbf{z}_j$ and $\mathbf{G}_j = \mathbb{E}\{\mathbf{z}_j\mathbf{z}_j^H\}$, respectively. The normalized transmit power constraint set for jammer j is represented by $\mathcal{G}_j = \{\mathbf{G}_j : \mathbf{G}_j \succeq \mathbf{0}, \mathrm{tr}(\mathbf{G}_j) \le P_j\}$ where P_j is the maximum predefined normalized transmit power for it. $\mathbf{G}_k$ is the covariance matrix of the signal transmitted by the kth relay, $\mathbf{z}_k$, which is given by $\mathbf{G}_k = \mathbb{E}\{\mathbf{z}_k\mathbf{z}_k^H\}$. The power constraint is imposed such that $\mathbf{G}_k \in \mathcal{G}_k = \{\mathbf{G}_k : \mathbf{G}_k \succeq \mathbf{0}, \mathrm{tr}(\mathbf{G}_k) \le P_k\}$ where P_k is the maximum allowable transmission power for the kth relay. The qth PA overhears both hops, and its data rate is written as

$$R^{\mathrm{E}}_{kjq} = \frac{1}{2}\log_2\left(1 + \frac{\Theta(\mathbf{G}_s, \mathbf{e}_{\mathbf{h}_{sq}}) + \Theta(\mathbf{G}_k, \mathbf{e}_{\mathbf{h}_{kq}})}{\zeta^2 + \Theta(\mathbf{G}_j, \mathbf{e}_{\mathbf{h}_{jq}})}\right). \tag{7}$$

where $\Theta(\mathbf{G}_s, \mathbf{e}_{\mathbf{h}_{sq}}) = (\tilde{\mathbf{h}}_{sq} + \mathbf{e}_{\mathbf{h}_{sq}})\mathbf{G}_s(\tilde{\mathbf{h}}_{sq} + \mathbf{e}_{\mathbf{h}_{sq}})^H$, $\Theta(\mathbf{G}_k, \mathbf{e}_{\mathbf{h}_{kq}}) = (\tilde{\mathbf{h}}_{kq} + \mathbf{e}_{\mathbf{h}_{kq}})\mathbf{G}_k(\tilde{\mathbf{h}}_{kq} + \mathbf{e}_{\mathbf{h}_{kq}})^H$ and $\Theta(\mathbf{G}_j, \mathbf{e}_{\mathbf{h}_{jq}}) = (\tilde{\mathbf{h}}_{jq} + \mathbf{e}_{\mathbf{h}_{jq}})\mathbf{G}_j(\tilde{\mathbf{h}}_{jq} + \mathbf{e}_{\mathbf{h}_{jq}})^H$. Accordingly, by exploiting relay k and friendly jammer j, the secrecy rate between LT and LR overheard by PA q can be obtained as

$$R^{\mathrm{S}}_{kjq} = \max\left\{0, R^{\mathrm{D}}_{kj} - R^{\mathrm{E}}_{kjq}\right\}. \tag{8}$$

Therefore, the optimization problem can be formulated as follows

Problem $\mathcal{O}^{PA}$:

$$\max_{\substack{\mathbf{G}_s\in\mathcal{G}_s;\\ \mathbf{G}_k\in\mathcal{G}_k;\\ \mathbf{G}_j\in\mathcal{G}_j}} \quad \min_{\substack{\mathbf{e}_{\mathbf{h}_{sq}}\in\mathcal{E}_{\mathbf{h}_{sq}};\\ \mathbf{e}_{\mathbf{h}_{kq}}\in\mathcal{E}_{\mathbf{h}_{kq}};\\ \mathbf{e}_{\mathbf{h}_{jq}}\in\mathcal{E}_{\mathbf{h}_{jq}}}} \tilde{R}^S, \tag{9a}$$

$$\text{s.t. } \frac{\mathbf{h}_{sk}\mathbf{G}_s\mathbf{h}^H_{sk}}{\zeta^2 + \mathbf{h}_{jk}\mathbf{G}_j\mathbf{h}^H_{jk}} \le \frac{\mathbf{h}_{kd}\mathbf{G}_k\mathbf{h}^H_{kd} + \mathbf{h}_{sd}\mathbf{G}_s\mathbf{h}^H_{sd}}{\zeta^2 + \mathbf{h}_{jd}\mathbf{G}_j\mathbf{h}^H_{jd}}, \forall k, j, \tag{9b}$$

$$\mathrm{tr}(\mathbf{G}_s) \le P_s, \tag{9c}$$

$$\mathrm{tr}(\mathbf{G}_j) \le P_j, \forall j, \tag{9d}$$

$$\mathrm{tr}(\mathbf{G}_k) \le P_k, \forall k, \tag{9e}$$

$$\|\mathbf{e}_{\mathbf{h}_{sq}}\|^2 \le \epsilon^2_{\mathbf{h}_{sq}}, \forall q, \tag{9f}$$

$$\|\mathbf{e}_{\mathbf{h}_{jq}}\|^2 \le \epsilon^2_{\mathbf{h}_{jq}}, \forall j, q, \tag{9g}$$

$$\|\mathbf{e}_{\mathbf{h}_{kq}}\|^2 \le \epsilon^2_{\mathbf{h}_{kq}}, \forall k, q, \tag{9h}$$

$$\mathbf{G}_s \succeq 0, \tag{9i}$$

$$\mathbf{G}_j \succeq 0, \forall j, \tag{9j}$$

$$\mathbf{G}_k \succeq 0, \forall k. \tag{9k}$$

where $\tilde{R}^S = \arg\max_{k\in\mathcal{K}} \arg\max_{j\in\mathcal{J}} \arg\min_{q\in\mathcal{Q}} R^S_{kjq}$. We remind that the difficulty in solving problem $\mathcal{O}^{PA}$ comes from the inner minimization over $\mathbf{e}_{\mathbf{h}_{sq}}$, $\mathbf{e}_{\mathbf{h}_{kq}}$, and $\mathbf{e}_{\mathbf{h}_{jq}}$ where it is a non-convex problem due to the non-convexity of the objective function and constraints. However, as shown in [12,18], through a proper transformation, problem $\mathcal{O}^{PA}$ can be converted to a solvable quasi-convex optimization problem. Then, the conventional bisection method can be used to solve the problem. On the other hand, one can also use the Charnes–Cooper transformation [21] to transform