Peer-reviewed version available at *Sensors* **2018**, *18*, 3914; doi:10.3390/s18113914

Article

Iterative Distributed Minimum Total MSE Algorithm for Secure Communications in the Internet of Things Using Relays

Zhengmin Kong [1], Die Wang [2], Yunjuan Li [3,*], Chao Wang [4]

[1] Wuhan University, 430072, China; zmkong@whu.edu.cn
[2] Wuhan University, 430072, China; wangdie1995@whu.edu.cn
[3] Kunming University, 650118, China; linda220603@126.com
[4] Space Engineering University, 430072, China; drchaowang@126.com
* Correspondence: linda220603@126.com; Tel.: +86-13888220603

Abstract: In this paper, we first investigate secure communications for a two-hop interference relay system in the wireless Internet of Things (IoT), where K source-destination pairs communicate in the presence of an eavesdropper. Explicitly, we jointly design source, relay and destination matrices upon minimizing total mean-squared error (MSE) of all legitimate destinations while keeping the MSE at eavesdropper above a certain threshold. We illuminate that the joint design of the source, relay and destination matrices subject to both secrecy and transmit power constraints. More specifically, we proposed an efficient iterative distributed algorithm to simplify the process of the joint design for optimal source, relay and destination matrices. Furthermore, the convergence of the iterative distributed algorithm is described. Additionally, the performances of the proposed algorithm, including both its secrecy rate and MSE, are characterized with the aid of simulation results. We demonstrate that our proposed algorithm outperforms the traditional approach. As a benefit, secure communications can be guaranteed by using the proposed algorithm for the multiple input multiple output (MIMO) interference relay IoT network in the presence of an eavesdropper.

Keywords: physical layer security; MIMO interference channel; relay; total MSE; IoT

1. Introduction

Future Internet of Things networks integrate the existing and evolving network with developments in communication and sensing fields, such as multi-hop, self-configuration and enhance the security of the communications with proper management to create an intelligent network that can be sensed. Recently, with the rapid technological advancements of relay networks, wireless multi-hop relay networks (such as wireless sensor network) have become a popular technology for the future IoT networks. Due to the proliferation of wireless communication and hardware technology, wireless multi-hop relay networks are considered as major applications in IoT [1].

As the application scenarios in wireless IoT, the multi-hop relay networks consist of spatially distributed sensors or nodes, which enable IoT devices to collect and exchange data in relay manner. Since the broadcasting nature of wireless communications, this wireless IoT is more prone to eavesdropping [2]. Therefore, security is required, which can be accomplished by security approaches. Most of the security approaches for the wireless multi-hop IoT are deployed in the upper layers of the networks. However, nearly all upper-layer security approaches for IoT believe that the opponent or eavesdropper can obtain entirely control over a sensor or node by way of decode cryptographic scheme [3]. Physical layer security technology,

Peer-reviewed version available at Sensors 2018, 18, 3914; doi:10.3390/s18113914

which develops from the information theoretic perspective to obtain perfect security [4-6], is found to be more robust than upper-layer security approaches for the IoT with multi-hop relay connectivity [2].

Physical layer security has been focused for multi-hop relay networks to combat eavesdropping for IoT [7-12]. In [2], both channel aware encryption and precoding strategies are discussed in multi-hop IoT for sensing and communication confidentiality under resource constraints. In [7,8], joint relay and jammer selection schemes are proposed to improve the security， where only one node is selected as relay, which may not take full use of the multiple nodes. In [9], secure resource allocation problem for a two-way single relay wireless sensor network is investigated, which is designed under scenarios of applying and not applying cooperative jamming in the case of an eavesdropper. Security enhancement algorithm for IoT communication exposed to eavesdroppers has been forced on transmission design [10]. The authors in [11] study the problem of improving security for the important data collection in IoT, where eavesdroppers can combine their observations to decode the signal extremely. The precoding matrices are optimized in such a situation that the MSEs at legitimate receivers are at a lower value and the MSE at eavesdropper is large in a relay aided IoT system in the presence of cellular interference [12].

Although physical layer security for multi-hop relay networks has studied well, when the relay networks are faced interferences, the resultant physical layer security problem remains a significant challenge. Some literatures consider physical layer security problem just in interference channels. In [13], a joint power control and beamforming algorithm is proposed to minimize the total transmission power while keeping the signal-to-interference-plus-noise ratio (SINR) at each receiver above an expected threshold. An iterative distributed algorithm is used to jointly design the transmit precoding matrices and receive filter matrices for secure communications over the MIMO interference channels with an eavesdropper [14].

To the best of our knowledge, there is no open literature addressing the interference relay networks analysis and design for secure communications in the presence of an eavesdropper. Motivated by this challenge, in this paper, we aim to provide secure communications for a two-hop relay system in future IoT with power supply strategy, where multiple source-destination pairs communicate simultaneously over the interference channels in the presence of an active eavesdropper. To ensure secure communications in the above system, we design an optimization scheme in order to minimize the total MSE of the signal waveform estimation at legitimate destinations and keep the MSE at eavesdropper above an expected threshold, which subjects to the transmission power constrains at source nodes and relay nodes. To implement this optimization scheme, the source, relay and destination matrices must be jointly designed. Nevertheless, there exists a huge problem to design these matrices mentioned above, because of the optimization scheme is too complicated to achieve the closed form solution or numerical solution of the matrices.

To conquer the above problem, we proposed an iterative distributed algorithm to simplify the optimization scheme. Specifically, for the sake of achieving the source, relay and destination matrices, we circularly calculate one of them by using the other two matrix variables obtained from previous iterations. Furthermore, Kronecker product is employed to facilitate the process of solving these matrix variables. Consequently, the acquisition of the numerical solution of the source, relay and destination matrices are much easier. Additionally, our numerical results show that the proposed iterative distributed algorithm converges after a few iterations to a constant. We demonstrate that our proposed algorithm outperforms the traditional approach.

The remainder of the paper is organized as follows. In Section 2, we describe the system model and propose the optimization problem. In Section 3, we propose an iterative distributed algorithm for dividing the non-convex optimization problem into three sub-problems. In Section 4, the simulation results are provided. In Section 5, the conclusions are summarized.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 October 2018 doi:10.20944/preprints201810.0038.v1

Peer-reviewed version available at *Sensors* **2018**, *18*, 3914; doi:10.3390/s18113914

Notation: Throughout this paper, we use $(.)^H$ to represent Hermitian transpose, Tr(.) to represent the trace of a matrix, E{.} to represent the expectation, **I** to represent the identity matrix, **0** to represent a matrix or vector whose all element are zeros, $bd(.)$ to represent a block-diagonal matrix, $vec(.)$ to represent stack columns of a matrix on top of each other into a single vector, $\otimes$ to represent Kronecker product, $\|.\|$ to represent 2-norm of a vector and $\mathbb{C}$ to represent the complex field.

2. System Model and Methods

We consider a two-hop interference MIMO relay communication system in the wireless IoT. As shown in Figure 1, K source nodes try to transmit data to corresponding destination nodes with the help of M IoT relay nodes. Meanwhile, an eavesdropper node attempts to overhear the data from source. Considering the path loss and transmission power constrains, the direct links between source and destination are negligible. According to previous related study [15,16], we assume that the eavesdropper is close to the relay and is far away from the source. Because it is difficult for the eavesdropper to overhear the signals from both the source and the relay when they are far away, we only consider the links from relay to the eavesdropper and ignore the links from source to the eavesdropper. The interference channels exist in the system when one of the source nodes transmits signal to corresponding destination while the others source nodes transmit signals synchronously.

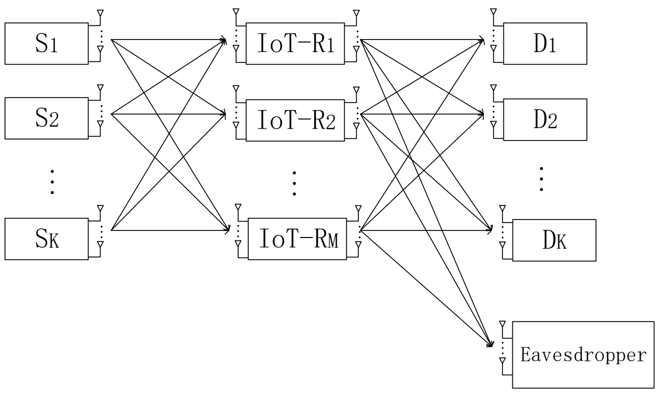

Figure 1. two-hop interference MIMO relay communication system in the wireless IoT

In the system model, the sets of source nodes, relay nodes, corresponding destination nodes and the source-destination pairs are denoted as $\{S_k\}$, $\{R_m\}$, $\{D_k\}$ and $\{(S_k, D_k)\}$, where $k = 1, \ldots, K, m = 1, \ldots, M$. More generally, the eavesdropper is denoted as E. Furthermore, the source S_k, the relay R_m, the destination D_k and the eavesdropper are equipped with T_k, Q_m, N_k and N_e antennas. The channels between nodes are set to undergo slow varying flat Rayleigh fading and assume that additive white Gaussian noise (AWGN) with zero mean and variance σ^2 is appended to all receiving nodes [17]. We denote $\mathbf{H}_{km}$, $\mathbf{G}_{mk}$ and $\mathbf{G}_{me}$ as the channel matrices of $S_k - R_m$, $R_m - D_k$ and $R_m - E$ links.

We assume that the relay nodes work in half-duplex model with amplify and forward (AF) strategy. So there needs two time slots to complete the communication between source and destination. In the first time slot, the source S_k transmits data $\boldsymbol{s}_k$ to relay R_m, then the relay R_m receives the incoming signal with its receiving antennas and transmits $\boldsymbol{y}_{r_m}$ to the destination D_k and the eavesdropper in the second time slot. The received signals at R_m, D_k and the eavesdropper can be denoted as follows

$$\mathbf{y}_{r_m} = \sum_{k=1}^{K} \mathbf{H}_{km}\mathbf{s}_k + \mathbf{n}_{r_m}, m = 1, \ldots, M, \quad (1)$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 October 2018 doi:10.20944/preprints201810.0038.v1

Peer-reviewed version available at Sensors 2018, 18, 3914; doi:10.3390/s18113914

$$\mathbf{y}_{d_k} = \sum_{m=1}^{M} \mathbf{G}_{mk}\mathbf{y}_{r_m} + \mathbf{n}_{d_k}, k = 1, \dots, K, \tag{2}$$

$$\mathbf{y}_e = \sum_{m=1}^{M} \mathbf{G}_{me}\mathbf{y}_{r_m} + \mathbf{n}_e, \tag{3}$$

where $\boldsymbol{y}_{r_m} \in \mathbb{C}^{Q_m\times 1}$ is the received signal vector at relay R_m; $\boldsymbol{y}_{d_k} \in \mathbb{C}^{N_k\times 1}$ is the received signal vector at destination D_k; $\boldsymbol{y}_e \in \mathbb{C}^{N_e\times 1}$ is the received signal vector at the eavesdropper E; $\mathbf{H}_{km} \in \mathbb{C}^{Q_m\times T_k}$ is the matrix of channel coefficients between source S_k and relay R_m; $\mathbf{G}_{mk} \in \mathbb{C}^{N_k\times Q_m}$ is the matrix of channel coefficients between relay R_m and destination D_k; $\mathbf{G}_{me} \in \mathbb{C}^{N_e\times Q_m}$ is the matrix of channel coefficients between relay R_m and the eavesdropper E; $\boldsymbol{s}_k \in \mathbb{C}^{T_k\times 1}$ is the transmitted signal vector at source S_k; $\boldsymbol{n}_{r_m} \in \mathbb{C}^{Q_m\times 1}$, $\boldsymbol{n}_{d_k} \in \mathbb{C}^{N_k\times 1}$ and $\boldsymbol{n}_e \in \mathbb{C}^{N_e\times 1}$ are the additive white Gaussian noise (AWGN) vectors at R_m, D_k and eavesdropper with zero mean and covariance matrix $\sigma_{r_m}^2\mathbf{I}_{Q_m}$, $\sigma_{d_k}^2\mathbf{I}_{N_k}$ and $\sigma_e^2\mathbf{I}_{N_e}$.

To minimize total MSE at destinations and achieve secure communication, we jointly design transmit precoding matrices at source and relay, and liner receive matrices at destinations and eavesdropper, which subject to transmission power constrains at the source nodes and relay nodes. For the sake of seeking optimum solution about above matrices, we propose an iterative distributed algorithm.

Before transmitting the data $\boldsymbol{s}_k$, we use transmit precoding matrix $\mathbf{U}_k$ to encode the data $\boldsymbol{s}_k$ at source S_k. Similarly, we use transmit precoding matrix $\mathbf{V}_m$ to encode the data $\boldsymbol{y}_{r_m}$ at relay R_m. We can rewrite the received signals at R_m, D_k and the eavesdropper as follows

$$\mathbf{y}_{r_m} = \sum_{k=1}^{K} \mathbf{H}_{km}\mathbf{U}_k\mathbf{s}_k + \mathbf{n}_{r_m}, m = 1, \dots, M, \tag{4}$$

$$\mathbf{y}_{d_k} = \sum_{m=1}^{M} \mathbf{G}_{mk}\mathbf{V}_m\mathbf{y}_{r_m} + \mathbf{n}_{d_k}, k = 1, \dots, K, \tag{5}$$

$$\mathbf{y}_e = \sum_{m=1}^{M} \mathbf{G}_{me}\mathbf{V}_m\mathbf{y}_{r_m} + \mathbf{n}_e, \tag{6}$$

Finally, we use liner receive matrix $\mathbf{W}_k$ at destination D_k and $\mathbf{W}_{e,k}$ at eavesdropper to receive the transmitted signals. The estimate of the data $\boldsymbol{s}_k$ at D_k and the eavesdropper can be denoted as follows

$$\hat{\mathbf{s}}_k = \mathbf{W}_k^H\mathbf{y}_{d_k} = \mathbf{W}_k^H\left(\sum_{m=1}^{M}\sum_{l=1}^{K} \mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{s}_l + \sum_{m=1}^{M} \mathbf{G}_{mk}\mathbf{V}_m\mathbf{n}_{r_m} + \mathbf{n}_{d_k}\right) \tag{7}$$

$$\hat{\mathbf{s}}_{ek} = \mathbf{W}_{e,k}^H\mathbf{y}_e = \mathbf{W}_{e,k}^H\left(\sum_{m=1}^{M}\sum_{l=1}^{K} \mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{s}_l + \sum_{m=1}^{M} \mathbf{G}_{me}\mathbf{V}_m\mathbf{n}_{r_m} + \mathbf{n}_e\right), \tag{8}$$

where $\mathbf{W}_k$ and $\mathbf{W}_{e,k}$ are the $\boldsymbol{T}_k \times \boldsymbol{N}_k$ and $\boldsymbol{T}_k \times \boldsymbol{N}_{e,k}$ receive weight matrices. We assume that $\mathrm{E}\{\boldsymbol{s}_k\boldsymbol{s}_k^H\} = \mathbf{I}_{T_k}$ is the covariance matrix of the information-carrying symbol vector at S_k. From (7), the MSE of estimating $\boldsymbol{s}_k$ at D_k can be calculated as

$$\begin{aligned}\mathrm{MSE}_k = tr(E\{(\hat{\mathbf{s}}_k - \mathbf{s}_k)(\hat{\mathbf{s}}_k - \mathbf{s}_k)^H\}) = tr\Big(\big(\textstyle\sum_{m=1}^{M} \mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k - \\ \mathbf{I}_{T_k}\big)\big(\textstyle\sum_{m=1}^{M} \mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k - \mathbf{I}_{T_k}\big)^H + \textstyle\sum_{m=1}^{M} \sigma_{r_m}^2\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k + \\ \textstyle\sum_{m=1}^{M}\sum_{l=1,l\neq k}^{K} \mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{U}_l^H\mathbf{H}_{lm}^H\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k + \sigma_{d_k}^2\mathbf{W}_k^H\mathbf{W}_k\Big).\end{aligned} \tag{9}$$

Similarly, we can get the MSE of estimating $\boldsymbol{s}_k$ at eavesdropper as follows

$$\begin{aligned}\mathrm{MSE}_{e,k} = tr(E\{(\hat{\mathbf{s}}_{ek} - \mathbf{s}_k)(\hat{\mathbf{s}}_{ek} - \mathbf{s}_k)^H\}) = tr\Big(\big(\textstyle\sum_{m=1}^{M} \mathbf{W}_{e,k}^H\mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k - \\ \mathbf{I}_{T_k}\big)\big(\textstyle\sum_{m=1}^{M} \mathbf{W}_{e,k}^H\mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k - \mathbf{I}_{T_k}\big)^H + \textstyle\sum_{m=1}^{M} \sigma_{r_m}^2\mathbf{W}_{e,k}^H\mathbf{G}_{me}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{me}^H\mathbf{W}_{e,k} + \\ \textstyle\sum_{m=1}^{M}\sum_{l=1,l\neq k}^{K} \mathbf{W}_{e,k}^H\mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{U}_l^H\mathbf{H}_{lm}^H\mathbf{V}_m^H\mathbf{G}_{me}^H\mathbf{W}_{e,k} + \sigma_e^2\mathbf{W}_{e,k}^H\mathbf{W}_{e,k}\Big).\end{aligned} \tag{10}$$

The transmission power constraints at source nodes and relay nodes are as follows

$$tr(\mathbf{U}_k E\{\mathbf{s}_k\mathbf{s}_k^H\}\mathbf{U}_k^H) \le P_{sk}, k = 1, \dots, K, \tag{11}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 October 2018 doi:10.20944/preprints201810.0038.v1

Peer-reviewed version available at Sensors 2018, 18, 3914; doi:10.3390/s18113914

$$tr\left(\mathbf{V}_m E\left\{\mathbf{y}_{r_m}\mathbf{y}_{r_m}^H\right\}\mathbf{V}_m^H\right) \le P_{rm}, m = 1, \dots, M, \tag{12}$$

where P_{sk} and P_{rm} denote the maximum transmission power at S_k and R_m.

Without eavesdropper, the K legitimate communication pairs can achieve their maximum communication rates, and the transmission is secure and reliable. However, in the presence of an eavesdropper, the signals from source may be leaked out to the eavesdropper. Considering the worst situation, we assume that the eavesdropper can calculate the liner receive matrix $\mathbf{W}_{e,k}$ to minimize its own $\mathrm{MSE}_{e,k}$ and it knows all channel state information. The solution of the source matrices $\{\mathbf{U}_k\}$, relay matrices $\{\mathbf{V}_m\}$, destination matrices $\{\mathbf{W}_k\}$ and the eavesdropper matrices $\{\mathbf{W}_{e,k}\}$ is vital. The solution of the problem is to utilize the source, relay and destination matrices to minimize the total MSE of all legitimate destination nodes and keep the $\mathrm{MSE}_{e,k}$ above an expected threshold ε_k $(k = 1, \dots, K)$, while subjecting to the transmission power constrains at source and relay nodes. The solution can be denoted as follows

$$\begin{aligned} \min_{\{\mathbf{U}_k\},\{\mathbf{V}_m\},\{\mathbf{W}_k\},\{\mathbf{W}_{e,k}\}} &: \sum_{k=1}^{K} \mathrm{MSE}_k \\ s.t. &: \mathrm{MSE}_{e,k} \ge \varepsilon_k, \\ & tr(\mathbf{U}_k E\{\mathbf{s}_k\mathbf{s}_k^H\}\mathbf{U}_k^H) \le P_{sk}, \\ & tr\left(\mathbf{V}_m E\left\{\mathbf{y}_{r_m}\mathbf{y}_{r_m}^H\right\}\mathbf{V}_m^H\right) \le P_{rm}, \end{aligned} \tag{13}$$

where $\{\mathbf{U}_k\},\{\mathbf{V}_m\},\{\mathbf{W}_k\}$ and $\{\mathbf{W}_{e,k}\}$ are the solution obtained.

3. The Iterative Distributed Algorithm of Solving source, relay, destination and eavesdropper matrices

Due to the non-convex problem (13) with matrix variables, so we are facing an uphill battle to obtain the optimum solution of the joint design matrices. To deal with the problem, we propose an iterative distributed algorithm to jointly design the optimal solution of the source matrices $\{\mathbf{U}_k\}$, relay matrices $\{\mathbf{V}_m\}$ and destination matrices $\{\mathbf{W}_k\}$. The whole solving process of the three matrix variables is divided into three steps. We circularly calculate one of them by using the other two matrix variables obtained from previous iterations, the non-convex problem (13) is transformed into three sub-problems in each step.

The objective function of (13) can be denoted by total MSE (TMSE) as follows

$$\mathrm{TMSE} = \textstyle\sum_{k=1}^{K} \mathrm{MSE}_k. \tag{14}$$

3.1. Solution of destination matrices $\{\boldsymbol{W}_k\}$ and eavesdropper matrices $\{\boldsymbol{W}_{e,k}\}$

In the first iteration of our proposed algorithm, we set the initial value of $\{\mathbf{U}_k\}$ and $\{\mathbf{V}_m\}$, then calculate the optimal solution of $\{\mathbf{W}_k\}$. Thus, at the following iteration of the algorithm, we calculate the optimal $\{\mathbf{W}_k\}$ by utilizing previously obtained $\{\mathbf{U}_k\}$ and $\{\mathbf{V}_m\}$.

It is obvious from (13) that $\{\mathbf{W}_k\}$ and $\{\mathbf{W}_{e,k}\}$ are independent with transmission power constrains at source and relay. We can obtain the optimal liner receive matrices $\{\mathbf{W}_k\}$ to minimize the total MSE at destination by the well-known liner MMSE receiver [18], which can be formulated as

$$\begin{aligned} \mathbf{W}_k = \Big(&\textstyle\sum_{m=1}^{M}\sum_{l=1}^{K} \mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{U}_l^H\mathbf{H}_{lm}^H\mathbf{V}_m^H\mathbf{G}_{mk}^H + \sum_{m=1}^{M}\sigma_{r_m}^2\mathbf{G}_{mk}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{mk}^H + \\ &\sigma_{d_k}^2\mathbf{I}_{N_k}\Big)^{-1}\left(\textstyle\sum_{m=1}^{M}\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k\right). \end{aligned} \tag{15}$$

The matrices $\{\mathbf{W}_{e,k}\}$ can be calculated in the same way, which can be formulated as

Peer-reviewed version available at Sensors 2018, 18, 3914; doi:10.3390/s18113914

$$\mathbf{W}_{e,k} = \left(\sum_{m=1}^{M}\sum_{l=1}^{K}\mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{U}_l^H\mathbf{H}_{lm}^H\mathbf{V}_m^H\mathbf{G}_{me}^H + \sum_{m=1}^{M}\sigma_{r_m}^2\mathbf{G}_{me}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{me}^H + \sigma_e^2\mathbf{I}_{N_e}\right)^{-1}\left(\sum_{m=1}^{M}\mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k\right). \quad (16)$$

3.2. Solution of source matrices $\{\boldsymbol{U}_k\}$

After obtaining the optimal matrices $\{\mathbf{W}_k\}$ and $\{\mathbf{W}_{e,k}\}$, we can calculate the transmit precoding matrices $\{\mathbf{U}_k\}$ by using $\{\mathbf{W}_k\}$ and $\{\mathbf{W}_{e,k}\}$ obtained from current iteration and $\{\mathbf{V}_m\}$ obtained from the previous iteration.

For further analysis, the TMSE of (14) can be specifically written as

$$\begin{aligned}\mathrm{TMSE} = &\sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\sum_{l=1}^{K}\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{lm}\mathbf{U}_l\mathbf{U}_l^H\mathbf{H}_{lm}^H\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k\right) - \\ &\sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{km}\mathbf{U}_k\right) - \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\mathbf{U}_k^H\mathbf{H}_{km}^H\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k\right) + \\ &\sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\sigma_{r_m}^2\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k + \sigma_{d_k}^2\mathbf{W}_k^H\mathbf{W}_k + \mathbf{I}_{T_k}\right).\end{aligned} \quad (17)$$

Define $\mathbf{P}_{k,m,l} = \mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{H}_{lm}$, so (17) can be written as

$$\begin{aligned}\mathrm{TMSE} = &\sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\sum_{l=1}^{K}\mathbf{P}_{k,m,l}\mathbf{U}_l\mathbf{U}_l^H\mathbf{P}_{k,m,l}^H\right) - \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\mathbf{P}_{k,m,k}\mathbf{U}_k\right) - \\ &\sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\mathbf{U}_k^H\mathbf{P}_{k,m,k}^H\right) + \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\sigma_{r_m}^2\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k + \sigma_{d_k}^2\mathbf{W}_k^H\mathbf{W}_k + \mathbf{I}_{T_k}\right).\end{aligned} \quad (18)$$

Define $\mathbf{P}_{k,m} = [\mathbf{P}_{k,m,1}, \mathbf{P}_{k,m,2}, \dots, \mathbf{P}_{k,m,K}]$, $\widehat{\mathbf{P}}_{k,k} = \sum_{m=1}^{M}\mathbf{P}_{k,m,k}$, $\mathbf{U} = bd(\mathbf{U}_1, \mathbf{U}_2, \dots, \mathbf{U}_K)$.

$$\mathrm{TMSE} = \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\mathbf{P}_{k,m}\mathbf{U}\mathbf{U}^H\mathbf{P}_{k,m}^H\right) - \sum_{k=1}^{K} tr\left(\widehat{\mathbf{P}}_{k,k}\mathbf{U}_k\right) - \sum_{k=1}^{K} tr\left(\mathbf{U}_k^H\widehat{\mathbf{P}}_{k,k}^H\right) + \boldsymbol{\gamma}, \quad (19)$$

where $\boldsymbol{\gamma} = \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\sigma_{r_m}^2\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{mk}^H\mathbf{W}_k + \sigma_{d_k}^2\mathbf{W}_k^H\mathbf{W}_k + \mathbf{I}_{T_k}\right)$. $\boldsymbol{\gamma}$ is independent with $\{\mathbf{U}_k\}$, so it can be ignored in the solving process. Let $\widehat{\mathbf{P}} = bd[\widehat{\mathbf{P}}_{1,1}, \widehat{\mathbf{P}}_{2,2}, \dots, \widehat{\mathbf{P}}_{K,K}]$, from (19) we can get

$$\mathrm{TMSE} = \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M}\mathbf{P}_{k,m}\mathbf{U}\mathbf{U}^H\mathbf{P}_{k,m}^H\right) - tr\left(\widehat{\mathbf{P}}\mathbf{U}\right) - tr\left(\mathbf{U}^H\widehat{\mathbf{P}}^H\right) + \boldsymbol{\gamma}. \quad (20)$$

To solve the above problems simplistically, we introduce some important formulas of [19]

$$\mathrm{tr}(\mathbf{A}^H\mathbf{B}) = \left(vec(\mathbf{A})\right)^H vec(\mathbf{B}),$$

$$\mathrm{tr}(\mathbf{A}^H\mathbf{B}\mathbf{A}\mathbf{C}) = \left(vec(\mathbf{A})\right)^H(\mathbf{C}^H\otimes\mathbf{B})vec(\mathbf{A}),$$

$$vec(\mathbf{A}\mathbf{B}\mathbf{C}) = (\mathbf{C}^H\otimes\mathbf{A})vec(\mathbf{B}).$$

And define $\mathbf{u} \triangleq vec(\mathbf{U})$ and $\mathbf{U}_k = \mathbf{t}_k\mathbf{U}\mathbf{t}_k^H$, where $\mathbf{t}_k = [\mathbf{0}_{T_k\times\sum_{l=1}^{k-1}T_l}\ \mathbf{I}_{T_k\times T_k}\ \mathbf{0}_{T_k\times\sum_{l=k+1}^{K}T_l}]$. we can further simplify formula (20) as follows

$$\mathrm{TMSE} = \mathbf{u}^H\boldsymbol{\omega}\mathbf{u} - \boldsymbol{\psi}\mathbf{u} - \mathbf{u}^H\boldsymbol{\psi}^H + \boldsymbol{\gamma}, \quad (21)$$

where $\boldsymbol{\tau} = blkdiag\left(\mathbf{I}_{T_1}, \mathbf{I}_{T_2}, \dots, \mathbf{I}_{T_K}\right)$, $\boldsymbol{\omega} = \sum_{k=1}^{K}\sum_{m=1}^{M}\boldsymbol{\tau}\otimes\boldsymbol{P}_{k,m}^H\mathbf{P}_{k,m}$, $\boldsymbol{\psi} = \left(vec\left(\widehat{\mathbf{P}}^H\right)\right)^H$.

In the same way, we can obtain the simplified formula of $\mathrm{MSE}_{e,k}$ as follows

$$\mathrm{MSE}_{e,k} = \mathbf{u}^H\boldsymbol{\omega}_{e,k}\mathbf{u} - \boldsymbol{\psi}_{e,k}\mathbf{u} - \mathbf{u}^H\boldsymbol{\psi}_{e,k}^H + \boldsymbol{\gamma}_e, \quad (22)$$

where $\mathbf{P}_{e,k,m,l} = \mathbf{W}_{e,k}^H\mathbf{G}_{me}\mathbf{V}_m\mathbf{H}_{lm}$, $\mathbf{P}_{e,k,m} = [\mathbf{P}_{e,k,m,1}, \mathbf{P}_{e,k,m,2}, \dots, \mathbf{P}_{e,k,m,K}]$, $\widehat{\mathbf{P}}_{e,k,k} = \sum_{m=1}^{M}\mathbf{P}_{e,k,m,k}$, $\boldsymbol{\omega}_{e,k} = \sum_{m=1}^{M}\boldsymbol{\tau}\otimes\boldsymbol{P}_{e,k,m}^H\mathbf{P}_{e,k,m}$, $\boldsymbol{\gamma}_e = tr\left(\sum_{m=1}^{M}\sigma_{r_m}^2\mathbf{W}_{e,k}^H\mathbf{G}_{me}\mathbf{V}_m\mathbf{V}_m^H\mathbf{G}_{me}^H\mathbf{W}_{e,k} + \sigma_{e,k}^2\mathbf{W}_{e,k}^H\mathbf{W}_{e,k} + \mathbf{I}_{T_k}\right)$ and $\boldsymbol{\psi}_{e,k} = \left(vec\left(\widehat{\mathbf{P}}_{e,k,k}^H\right)\right)^H(\mathbf{t}_k\otimes\mathbf{t}_k)$.

Because of $\mathrm{E}\{\mathbf{s}_k\mathbf{s}_k^H\} = \mathbf{I}_{T_k}$, the transmission power constrains (11) can be rewritten as

$$tr\left(\mathbf{t}_k\mathbf{U}\mathbf{t}_k^H(\mathbf{t}_k\mathbf{U}\mathbf{t}_k^H)^H\right) \le P_{sk}, k = 1, \dots, K, \quad (23)$$

Then we obtain (24)

$$u^H\boldsymbol{\rho}u \le P_{sk}, k = 1, \dots, K, \quad (24)$$

where $\boldsymbol{\rho} = (\mathbf{t}_k^H \mathbf{t}_k) \otimes (\mathbf{t}_k^H \mathbf{t}_k)$.

From (21), (22) and (24), the source matrices optimization problem can be written as

$$\begin{aligned} &\min_{\{\mathbf{U}_k\}} : \text{TMSE} \\ &s.t.: \ \text{MSE}_{e,k} \geq \varepsilon_k \\ &u^H \boldsymbol{\rho} u \leq P_{sk} \end{aligned} \tag{25}$$

The source matrices optimization problem (25) is a quadratic constrained quadratic programming (QCQP) problem [20]. Compared with the non-convex problem (13), the problem (25) can be solved by the CVX of MATLAB toolbox [21].

3.3. Solution of relay matrices $\{\boldsymbol{V}_m\}$

Since $\{\mathbf{W}_k\}$, $\{\mathbf{W}_{e,k}\}$ and $\{\mathbf{U}_k\}$ are already obtained, the TMSE can be rewritten as

$$\begin{aligned} \text{TMSE} = &\textstyle\sum_{k=1}^{K} tr(\sum_{m=1}^{M}\sum_{l=1}^{K} \bar{\mathbf{G}}_{mk} \mathbf{V}_m \bar{\mathbf{H}}_{lm} \bar{\mathbf{H}}_{lm}^H \mathbf{V}_m^H \bar{\mathbf{G}}_{mk}^H) - \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \bar{\mathbf{G}}_{mk} \mathbf{V}_m \bar{\mathbf{H}}_{km}) - \\ &\textstyle\sum_{k=1}^{K} tr(\sum_{m=1}^{M} \bar{\mathbf{H}}_{km}^H \mathbf{V}_m^H \bar{\mathbf{G}}_{mk}^H) + \sum_{k=1}^{K} tr\left(\sum_{m=1}^{M} \sigma_{r_m}^2 \bar{\mathbf{G}}_{mk} \mathbf{V}_m \mathbf{V}_m^H \bar{\mathbf{G}}_{mk}^H + \sigma_{d_k}^2 \mathbf{W}_k^H \mathbf{W}_k + \mathbf{I}_{T_k}\right), \end{aligned} \tag{26}$$

where $\bar{\mathbf{G}}_{mk} = \mathbf{W}_k^H \mathbf{G}_{mk}$, $\bar{\mathbf{H}}_{km} = \mathbf{H}_{km} \mathbf{U}_k$. Define $\mathbf{V} = bd(\mathbf{V}_1, \mathbf{V}_2, \dots, \mathbf{V}_M)$, $\bar{\mathbf{G}}_k = bd[\bar{\mathbf{G}}_{1k}, \bar{\mathbf{G}}_{2k}, \dots, \bar{\mathbf{G}}_{Mk}]$, $\boldsymbol{\eta} = bd[\sigma_{r_1}^2 \mathbf{I}_{Q_1}, \sigma_{r_2}^2 \mathbf{I}_{Q_2}, \dots, \sigma_{r_M}^2 \mathbf{I}_{Q_M}]$, $\bar{\mathbf{H}}_k = bd[\bar{\mathbf{H}}_{k1}, \bar{\mathbf{H}}_{k2}, \dots, \bar{\mathbf{H}}_{kM}]$, $\boldsymbol{\beta} = \sum_{k=1}^{K}\left(\sigma_{d_k}^2 \mathbf{W}_k^H \mathbf{W}_k + \mathbf{I}_{T_k}\right)$. Then the TMSE can be simplified as

$$\begin{aligned} \text{TMSE} = &\textstyle\sum_{k=1}^{K} tr(\bar{\mathbf{G}}_k \mathbf{V}(\sum_{l=1}^{K} \bar{\mathbf{H}}_l \bar{\mathbf{H}}_l^H) \mathbf{V}^H \bar{\mathbf{G}}_k^H) - \sum_{k=1}^{K} tr(\bar{\mathbf{G}}_k \mathbf{V} \bar{\mathbf{H}}_k) - \sum_{k=1}^{K} tr(\bar{\mathbf{H}}_k^H \mathbf{V}^H \bar{\mathbf{G}}_k^H) + \\ &\textstyle\sum_{k=1}^{K} tr(\bar{\mathbf{G}}_k \mathbf{V} \boldsymbol{\eta} \mathbf{V}^H \bar{\mathbf{G}}_k^H) + \boldsymbol{\beta}. \end{aligned} \tag{27}$$

Let us introduce $\mathbf{v} = vec(\mathbf{V})$, then we obtain the TMSE as

$$\text{TMSE} = \mathbf{v}^H \boldsymbol{\Omega} \mathbf{v} - \boldsymbol{O}\mathbf{v} - \mathbf{v}^H \boldsymbol{O}^H + \mathbf{v}^H \boldsymbol{\mu} \mathbf{v} + \boldsymbol{\beta}, \tag{28}$$

where $\boldsymbol{\Omega} = \sum_{k=1}^{K}\left((\sum_{l=1}^{K} \bar{\mathbf{H}}_l \bar{\mathbf{H}}_l^H) \otimes (\bar{\mathbf{G}}_k^H \bar{\mathbf{G}}_k)\right)$, $\mathbf{O} = \sum_{k=1}^{K}\left(vec(\bar{\mathbf{G}}_k^H \bar{\mathbf{H}}_k^H)\right)^H$, $\boldsymbol{\mu} = \sum_{k=1}^{K}\left(\boldsymbol{\eta} \otimes (\bar{\mathbf{G}}_k^H \bar{\mathbf{G}}_k)\right)$.

In the same way, we can obtain the simplified formula of $\text{MSE}_{e,k}$ as follows

$$\text{MSE}_{e,k} = \mathbf{v}^H \boldsymbol{\Omega}_{e,k} \mathbf{v} - \mathbf{O}_{e,k} \mathbf{v} - \mathbf{v}^H \mathbf{O}_{e,k}^H + \mathbf{v}^H \boldsymbol{\mu}_{e,k} \mathbf{v} + \boldsymbol{\beta}_{e,k}, \tag{29}$$

where $\bar{\mathbf{G}}_{e,k,m} = \mathbf{W}_{e,k}^H \mathbf{G}_{me}$, $\boldsymbol{\Omega}_{e,k} = (\sum_{l=1}^{K} \bar{\mathbf{H}}_l \bar{\mathbf{H}}_l^H) \otimes \left(\bar{\mathbf{G}}_{e,k}^H \bar{\mathbf{G}}_{e,k}\right)$, $\mathbf{O}_{e,k} = \left(vec\left(\bar{\mathbf{G}}_{e,k}^H \bar{\mathbf{H}}_k^H\right)\right)^H$, $\boldsymbol{\mu}_{e,k} = \boldsymbol{\eta} \otimes \left(\bar{\mathbf{G}}_{e,k}^H \bar{\mathbf{G}}_{e,k}\right)$, $\boldsymbol{\beta}_{e,k} = \sigma_e^2 \mathbf{W}_{e,k}^H \mathbf{W}_{e,k} + \mathbf{I}_{T_k}$, $\bar{\mathbf{G}}_{e,k} = bd[\bar{\mathbf{G}}_{e,k,1}, \bar{\mathbf{G}}_{e,k,2}, \dots, \bar{\mathbf{G}}_{e,k,M}]$.

Because of $E\left\{\mathbf{y}_{r_m} \mathbf{y}_{r_m}^H\right\} = \sum_{k=1}^{K} \mathbf{H}_{km} \mathbf{U}_k \mathbf{U}_{km}^H \mathbf{H}_{km}^H + \sigma_{r_m}^2 \mathbf{I}_{Q_m}$ and $\mathbf{V}_m = \mathbf{d}_m \mathbf{V} \mathbf{d}_m^H$, $\mathbf{d}_m = [\mathbf{0}_{Q_m \times \sum_{l=1}^{m-1} Q_l}\ \mathbf{I}_{Q_m \times Q_m}\ \mathbf{0}_{Q_m \times \sum_{l=m+1}^{M} Q_l}]$. The transmission power constrains at relay nodes can be written as

$$\mathbf{v}^H \boldsymbol{\lambda} \mathbf{v} \leq P_{rm}, m = 1, \dots, M, \tag{30}$$

where $\boldsymbol{\lambda} = \left(\mathbf{d}_m^H \left(\sum_{k=1}^{K} \mathbf{H}_{km} \mathbf{U}_k \mathbf{U}_{km}^H \mathbf{H}_{km}^H + \sigma_{rm}^2 \mathbf{I}_{Q_m}\right) \mathbf{d}_m\right)^H \otimes (\mathbf{d}_m^H \mathbf{d}_m)$.

From (28), (29) and (30), the relay matrices optimization problem can be written as

$$\begin{aligned} &\min_{\{\mathbf{V}_m\}} : \text{TMSE} \\ &s.t. : \ \text{MSE}_{e,k} \geq \varepsilon_k \\ &\mathbf{v}^H \boldsymbol{\lambda} \mathbf{v} \leq P_{rm}, m = 1, \dots, M, \end{aligned} \tag{31}$$

The relay matrices optimization problem (31) is a quadratic constrained quadratic programming (QCQP) problem [20]. Compared with the non-convex problem (13), the problem (31) can be solved by the CVX of MATLAB toolbox [21].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 October 2018 doi:10.20944/preprints201810.0038.v1

Peer-reviewed version available at *Sensors* **2018**, *18*, 3914; doi:10.3390/s18113914

The solving process of optimization matrices $\{\mathbf{W}_k\}$, $\{\mathbf{U}_k\}$ and $\{\mathbf{V}_m\}$ by employing iterative distributed algorithm is summarized in table 1, where variable n denotes the nth iteration.

Table 1. The proposed iterative distributed algorithm for problem (13)

Steps	Specific Progress
Step 1	Set $n=0$, $\text{TMSE}^{(n)}=0$, and initialize the $\{\mathbf{U}_k^{(0)}\}$ and $\{\mathbf{V}_k^{(0)}\}$ satisfying power constrains (11) and (12).
Step 2	Calculate $\{\mathbf{W}_k^{(n+1)}\}$ and $\{\mathbf{W}_{e,k}^{(n+1)}\}$ with $\{\mathbf{U}_k^{(n)}\}$ and $\{\mathbf{V}_m^{(n)}\}$ obtained from previous iteration.
Step 3	Update $\{\mathbf{U}_k^{(n+1)}\}$ by solving the problem (25) with obtained $\{\mathbf{W}_k^{(n+1)}\}$, $\{\mathbf{W}_{e,k}^{(n+1)}\}$ and $\{\mathbf{V}_m^{(n)}\}$.
Step 4	Update $\{\mathbf{V}_m^{(n+1)}\}$ by solving the problem (31) with obtained $\{\mathbf{W}_k^{(n+1)}\}$, $\{\mathbf{W}_{e,k}^{(n+1)}\}$ and $\{\mathbf{U}_k^{(n+1)}\}$, then calculate $\text{TMSE}^{(n+1)}$.
Step 5	If $\text{TMSE}^{(n+1)}-\text{TMSE}^{(n)}\le\xi$, then end; otherwise set $n=n+1$ and go to step 2.

At last, we introduce the communication rate and secrecy rate in above scenario. The communication rate at destinations and eavesdropper are as follows [22],

$$\text{com}D_k=\log_2\left(1+\sum_{m=1}^{M}\frac{\|\mathbf{W}_k^H\mathbf{G}_{mk}\mathbf{V}_m\|^2}{\|\mathbf{W}_k^H\mathbf{W}_k\|}\right),k=1,\dots,K, \tag{32}$$

$$\text{com}E=\log_2\left(1+\sum_{m=1}^{M}\frac{\|\mathbf{W}_{e,m}^H\mathbf{G}_{me}\mathbf{V}_m\|^2}{\|\mathbf{W}_{e,m}^H\mathbf{W}_{e,m}\|}\right), \tag{33}$$

The secrecy rate at each destination can be obtained [23].

$$\text{Rate}D_k=max(0,\text{com}D_k)-max(0,\text{com}E),k=1,\dots,K. \tag{34}$$

4. Numerical Results

In this section, we present numerical results to examine the effectiveness of the optimization iterative distributed algorithm for secure transmission in multi-user interference MIMO relay systems with eavesdropping. Assuming all nodes are equipped with the same number of antennas, $T_k=Q_m=N_k=N_e=3$, and all channel matrices are independent and identically distributed Gaussian channel matrices with zero mean and unit variance. The noises at all receiving nodes are assumed as AWGN with zero mean and unit variance, i.e., $\sigma_{d_k}^2=\sigma_{r_m}^2=\sigma_e^2=1$. The transmission power constrains at sources and relays are assumed as $P_{s_k}=P_{r_m}=20\text{dB}$. Assuming the eavesdropper knows the channel state information of the links between relay and itself. In addition, set the threshold of eavesdropper's MSE $\varepsilon_k=2.2,k=1,\dots,K$. All simulation results are averaged over 1000 independent channel realizations.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 October 2018 doi:10.20944/preprints201810.0038.v1

Peer-reviewed version available at Sensors 2018, 18, 3914; doi:10.3390/s18113914

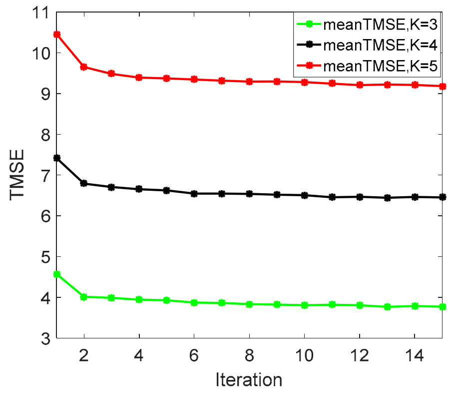

Figure 2. TMSE versus the number of iterations

Figure 2 illustrates the convergence behavior of proposed iterative distributed algorithm, where we have $K = 3, 4, 5$, $M = 3$, as well as $P_{s_k} = P_{r_m} = 20$dB. As can be seen in Figure 2, TMSE decreases gradually until convergence when the number of iterations increases. The plot shows that the TMSE always converges within about 2~4 iterations. As the number of legitimate source-destination pairs increases, the convergence speed decreases and TMSE increases. This is because more legitimate source-destination pairs increase both the system complexity and the interferences between each legitimate source-destination pair, and they lead to more iterations to approximate convergence and the increasement of TMSE.

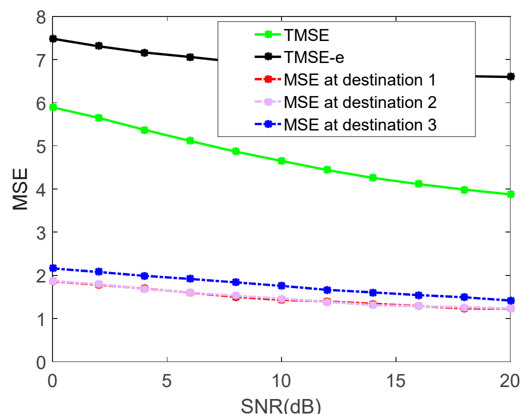

Figure 3. the MSE at destination versus SNR

Figure 3 shows the changes of TMSE and MSEs at different destinations versus signal to noise ratio (SNR), where we have $K = 3$, $M = 3$, TMSE-e denotes the $\sum_{k=1}^{K} \mathrm{MSE}_{e,k}$. As shown in Figure 3, both TMSE of all destinations and MSE at different destinations decrease gradually as the SNR increases. It can also be observed that MSEs at different destinations are very similar, statistically there is the nearly the same of the three legitimate links. Obviously, the TMSE of all legitimate destinations is much lower than the TMSE-e. It means that the system can be achieved a better transmission performance by employing our proposed algorithm against the eavesdropper.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 October 2018 doi:10.20944/preprints201810.0038.v1

Peer-reviewed version available at Sensors 2018, 18, 3914; doi:10.3390/s18113914

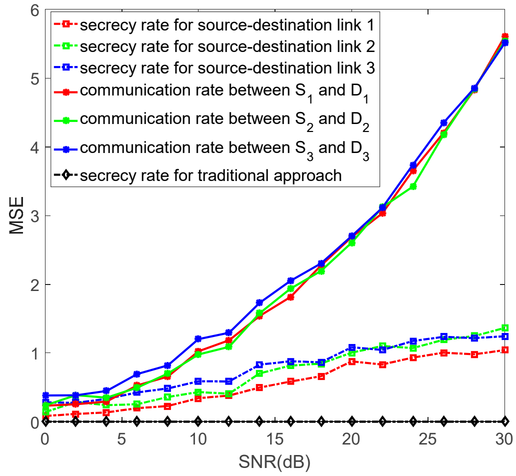

Figure 4. the communication rate and secrecy rate versus SNR

Figure 4 depicts the values of the secrecy rate and communication rate versus the transmission power constrains, when $K = 3$, $M = 3$, which is in the same background with Figure 3. As shown in Figure 4, compared to the traditional approach, the proposed algorithm can support a useful positive secrecy rate that increases as the SNR increases. In other word, our proposed algorithm guarantees secure communications for all source-destination pairs. It can also be observed in Figure 4 that communication rates of three links are similar, the situation of the secrecy rates is the same. Statistically, there is no difference among the three legitimate links. Additionally, the achievable secrecy rates are lower than communication rates, because the proposed algorithm sacrifices a part of communication rate for the sake of achieving a useful positive secrecy rate of data transmission.

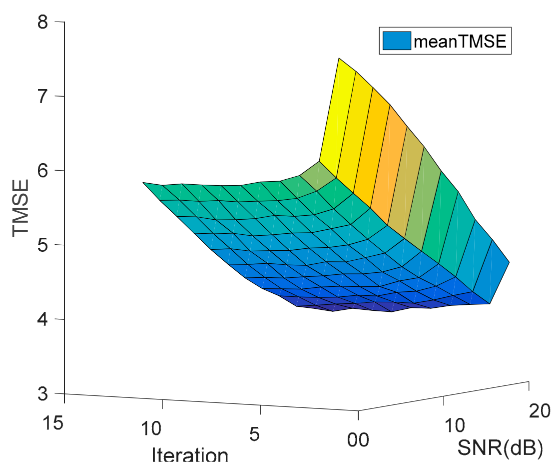

Figure 5. the TMSE versus the number of iterations and SNR

Furthermore, in Figure 5 we depict the variation of the TMSE as a function of the number of iterations and the transmission power constrains, where we have $K = 3, M = 3$. As shown in Figure 5, the TMSE of all destinations decreases as the SNR or the number of iterations increases. It can also be observed in Figure 5 that the TMSE decreases quickly at the beginning of the iteration process. And that means the proposed algorithm converges quickly.

Peer-reviewed version available at *Sensors* **2018**, *18*, 3914; doi:10.3390/s18113914

5. Conclusion

In this paper, we first investigate secure communication in MIMO interference relay IoT network with an active eavesdropper. An iterative distributed algorithm which jointly optimizes the source, relay and destination matrices has been proposed. It aims to minimize the TMSE of all legitimate destinations subjecting to transmission power constrains while keeping MSE at eavesdropper above a certain threshold. The convergence of the proposed algorithm has also been proved. Furthermore, the performances of the proposed algorithm, including both its secrecy rate and MSE, are characterized with the aid of simulation results. We demonstrate that our proposed algorithm outperforms the traditional approach. In other word, secure communications can be guaranteed by using the proposed algorithm for the MIMO interference relay IoT network in the presence of an eavesdropper.

Funding: This research was funded by National Natural Science Foundation of China (61801518) and Hubei Provincial Natural Science Foundation of China (2017CFB661).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, and interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Li, J.L.; Chang, S.; Fu, X.M. A Coalitional Formation Game for Physical Layer Security of Cooperative Compressive Sensing Multi-Relay Networks. *Sensors* 2018, 18(9), 2942, DOI:10.3390/s18092942.
2. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proceedings of the IEEE*, Oct. 2015, *Vol. 103, no. 10*, pp. 1747-1761, DOI: 10.1109/JPROC.2015.2466548.
3. Albashier, M. A. M.; Abdaziz, A.; Ghani, H. A. Performance analysis of physical layer security over different error correcting codes in wireless sensor networks. *2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Bali, 2017, pp. 191-195, DOI: 10.1109/WPMC.2017.8301806.
4. Bloch, M.; Barros, J. Physical-Layer Security: From Information Theory to Security Engineering[M]. Cambridge University Press, 2011, ISBN:0521817951 9780521516501.
5. Mukherjee, A.; Fakoorian, S. A. A.; Huang, J. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials*, Third Quarter 2014, *Vol. 16, no. 3*, pp. 1550-1573, DOI: 10.1109/SURV.2014.012314.00178.
6. Bloch, M.; Barros, J.; Rodrigues, M.R.D. Wireless Information-Theoretic Security. *IEEE Transactions on Information Theory*, June 2008, *Vol. 54, no. 6*, pp. 2515-2534, DOI: 10.1109/TIT.2008.921908.
7. Krikidis, I.; Thompson, J.; Mclaughlin, S. Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*, Oct. 2009, *Vol. 8, no. 10*, pp. 5003–5011, DOI: 10.1109/TWC.2009.090323.
8. Chen, J.; Zhang, R.; Song, L. Joint relay and jammer selection for secure two-way relay networks. Proc. *IEEE Transactions on Information Forensics and Security*, Feb. 2012, *Vol. 7, no. 1*, pp. 310-320, DOI: 10.1109/TIFS.2011.2166386.
9. Zhang, H.J.; Xing, H.; Cheng, J.L. Secure Resource Allocation for OFDMA Two-Way Relay Wireless Sensor Networks Without and With Cooperative Jamming. *IEEE Transactions on Industrial Informatics*, Oct. 2016, *Vol. 12, no. 5*, pp. 1714-1725, DOI: 10.1109/TII.2015.2489610.
10. Xu, Q.; Ren, P.Y.; Song, H.B. Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations. *IEEE Access*, 2016, *Vol. 4*, pp. 2840-2853, DOI: 10.1109/ACCESS.2016.2575863.
11. Zhang, Y.Y.; Shen, Y.L.; Wang, H. On Secure Wireless Communications for IoT Under Eavesdropper Collusion. *IEEE Transactions on Automation Science and Engineering*, July 2016, *Vol. 13, no. 3*, pp. 1281-1293, DOI: 10.1109/TASE.2015.2497663.

12. Islam, S. N.; Mahmud, M. A. Secured Communication among IoT Devices in the Presence of Cellular Interference. *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, *Sydney, NSW*, 2017, pp. 1-6, DOI: 10.1109/VTCSpring.2017.8108673.
13. Khandaker, M. R. A.; Rong, Y. Interference MIMO Relay Channel: Joint Power Control and Transceiver-Relay Beamforming. *IEEE Transactions on Signal Processing*, Dec. 2012, *Vol. 60, no. 12*, pp. 6509-6518, DOI: 10.1109/TSP.2012.2217135.
14. Kong, Z.M.; Yang, S.S; Wu, F.L. Iterative Distributed Minimum Total MSE Approach for Secure Communications in MIMO Interference Channels. *IEEE Transactions on Information Forensics and Security*, March 2016, *Vol. 11, no. 3*, pp. 594-608, DOI: 10.1109/TIFS.2015.2493888.
15. Zou, Y.L.; Wang, X.B.; Shen, W.M. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications*, Oct 2013, *Vol. 31, no. 10*, pp. 2099-2111, DOI: 10.1109/JSAC.2013.131011.
16. Park, K. H.; Wang, T.; Alouini, M.S. On the Jamming Power Allocation for Secure Amplify-and-Forward Relaying via Cooperative Jamming. *IEEE Journal on Selected Areas in Communications*, September 2013, *Vol. 31, no. 9*, pp. 1741-1750, DOI: 10.1109/JSAC.2013.130908.
17. Xu, Z.Y.; Zhong, J.; Chen, G.J. Novel joint secure resource allocation optimization for full-duplex relay networks with cooperative jamming. *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, 2016, pp. 1-6, DOI: 10.1109/PIMRC.2016.7794706.
18. Yang, S.S.; Hanzo, L. Fifty Years of MIMO Detection: The Road to Large-Scale MIMOs. *IEEE Communications Surveys & Tutorials*, Fourth-quarter 2015, *Vol. 17, no. 4*, pp. 1941-1988, DOI: 10.1109/COMST.2015.2475242.
19. Horn, R. A.; Johnson, C. R. *Topics in Matrix Analysis,* 1st ed.; Cambridge, U.K.: Cambridge Univ. Press, 1994.
20. Boyd, S.; Vandenberghe, L. *Convex Optimization.* Cambridge, U.K.: Cambridge Univ. Press, 2004.
21. Grant, M.; Boyd, S. *Cvx: MATLAB Software for Disciplined Convex Programming (Webpage and Software).* Apr. 2010, Available Online: http://cvxr.com/cvx.
22. Fang, H.; Xu, L. Coordinated Multiple-Relays Based Physical-Layer Security Improvement: A Single-Leader Multiple-Followers Stackelberg Game Scheme. *IEEE Transactions on Information Forensics and Security*, Jan. 2018, *Vol. 13, no. 1*, pp. 197-209, DOI: 10.1109/TIFS.2017.2746001.
23. Al-jamali, M.; Al-nahari, A.; AlKhawlani, M. M. Relay selection scheme for Improving the physical layer security in cognitive radio networks. *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, Malatya, 2015, pp. 495-498, DOI: 10.1109/SIU.2015.7129868.