sensors

MDPI

Article

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

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

1 School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China; zmkong@whu.edu.cn (Z.K.); wangdie1995@whu.edu.cn (D.W.)
2 School of Automation and Mechanical Engineering, Kunming University, Kunming 650118, China
3 School of Information Engineering, Space Engineering University, Beijing 101400, China; drchaowang@126.com
* Correspondence: linda220603@126.com; Tel.: +86-138-8822-0603

Received: 29 September 2018; Accepted: 2 November 2018; Published: 13 November 2018

Abstract: In this article, we first investigate secure communications for a two-hop interference channel relay system with imperfect channel estimation in the wireless Internet of Things (IoT), where K source-destination pairs communicate simultaneously when an eavesdropper exists. We jointly conceive source, relay and destination matrices upon minimizing total mean-squared error (MSE) of all legitimate destinations while keeping the MSE at eavesdropper above a given threshold. We illuminate that the design of the source, relay and destination matrices is subject to both transmit power constraints and secrecy requirements. More specifically, we propose an efficient robust 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 our proposed algorithm, such as its secrecy rate and MSE, are characterized in the form of simulation results. The simulation results reveal that the proposed algorithm is superior to the traditional approach. As a benefit, secure communications can be ensured 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; imperfect channel estimation

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 [1–6]. 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 [7–11]. Along with the enormous development in the field of wireless communication and hardware technology, wireless multi-hop relay networks are considered as major applications in IoT [12].

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 [13]. 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 decoding cryptographic scheme [14]. Physical layer security technology, which comes from information theory to achieve perfect security [15–17], is found to be more robust than upper-layer security approaches for the IoT with multi-hop relay connectivity [13].

The physical layer security of the traditional close-range wireless systems mainly considers that the eavesdropper wiretaps the messages between sources and legitimate destinations. However, the security of long-range relays system considers that the eavesdropper wiretaps not only the messages between sources and relays but also the messages between relays and legitimate destinations. Therefore, the security of long-range relays system become more complexity than that of traditional wireless systems for close-range communication [18,19].

Physical layer security has been focused for multi-hop relay networks to combat eavesdropping for IoT [20–25]. In Reference [13], both channel aware encryption and precoding strategies are discussed in multi-hop IoT to achieve secrecy communication subject to resource constraints. In References [20,21], the authors select the optimal relay to improve security by joint relay and jammer selection algorithm, which may not fully take advantage of all relay nodes. In Reference [22], the problem of secure resource allocation for a two-way single relay wireless network is investigated, which is designed under schemes 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 [23]. The authors in Reference [24] study the problem of improving security for the important data collection in IoT, where eavesdroppers can decode the signal extremely by combining their observations. The precoding matrices are optimized to satisfy that the MSEs at legitimate receivers are small and the MSE at eavesdropper is large in a relay aided cellular interference IoT system [25]. There are also some other schemes of achieving security, which are worth investigating. For instance, artificial noise has played an important role in enhancing the wireless communication physical layer secrecy in a two-hop relay network [26]. Furthermore, transmit beamforming is employed in an Amplify-and-Forward MIMO relay system, in order to obtain the maximum secrecy rate [27].

Although physical layer security for multi-hop relay IoT networks has been studied well, the resultant problem for secure communications still remains a significant challenge when the relay networks are faced with interferences and imperfect channel estimation. Some literature considers physical layer security problem just in interference channels. In Reference [28], a joint power control and beamforming algorithm is proposed for minimizing the total transmitted power, while keeping the signal-to-interference-plus-noise ratio (SINR) at each receiver over an expected threshold. An iterative distributed algorithm is used to design transmit precoding matrices and receive filter matrices for secure communications over the MIMO interference channels with an eavesdropper [29]. Other literatures just consider imperfect channel estimation. In Reference [30], an efficient beamforming approach has been proposed to combat eavesdropper with imperfect channel estimation. Secrecy outage analysis over a multiplicative composite channel model has been investigated with imperfect channel estimation [31].

To the best of our knowledge, the works on interference relay networks analysis and design for physical layer security in IoT system under imperfect channel estimation are still absent. Motivated by this challenge, we aim to provide secure communications for a two-hop relay system in future IoT with power supply strategy in this paper, where multiple source-destination pairs communicate simultaneously over the relay-interference channel in the presence of an active eavesdropper. In our article, we use MSE as the main performance metric. The system-wide minimum MSE (MMSE) has been considered in many works. In Reference [32], MMSE performance metric has been considered in a multiuser MIMO system where a distributed iterative algorithm and interference alignment are presented. In Reference [33], a weighted-MMSE method is proposed to apply in the optimization problems of sum-rate maximization, sum-MSE minimization and sum SINR maximization, respectively. However, the security problem of relays system is not considered in References [32,33].

To guarantee security in the relays system for IoT, we design an optimization scheme in order to minimize the total MSE estimated at legitimate destinations and keep the MSE at eavesdropper above an expected threshold, which is subject to the transmission power constrains at relay nodes and source 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 the optimization scheme is too complicated to achieve the closed form solution or numerical solution of these 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 simulation results demonstrate that the proposed iterative distributed algorithm will converge to a constant after several iterations. We also reveal that our proposed algorithm is superior to the traditional approach.

The remainder of the article 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, we demonstrate the convergence of the proposed algorithm. In Section 5, the simulation results are presented. In Section 6, the conclusions are summarized.

Notation: In this article, 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, $Y \sim \mathcal{CN}(\mu, \sigma^2)$ to represent Y following the complex normal distribution with mean μ and variance σ^2. $bd(.)$ to represent a block-diagonal matrix, $vec(.)$ to represent stack columns of a matrix on top of each other into a single vector, $\|.\|$ to represent 2-norm of a vector, $\otimes$ to represent Kronecker product and $\mathbb{C}$ to represent the complex field.

2. System Model and Methods

In this article, we investigate secrecy communication over the MIMO interference channels in two-hop relay system for the wireless IoT [34,35]. As shown in Figure 1, K source nodes transmit data to corresponding destination nodes by employing M IoT relay nodes. Meanwhile, an eavesdropper tries to wiretap the data from source. Assuming that the sophisticated eavesdropper can calculate its optimal receive matrix relying on minimizing its own total MSE [36]. Considering the path loss and transmission power constrains, the direct links between sources and destinations are negligible. According to previous related study [18,19], we assume that the eavesdropper is near by the relay and far away from the source. Therefore, the eavesdropper wiretapping the messages from both the sources and the relays simultaneously is difficult. Hence, we only consider the links from relay to eavesdropper and ignore the links from source to 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.

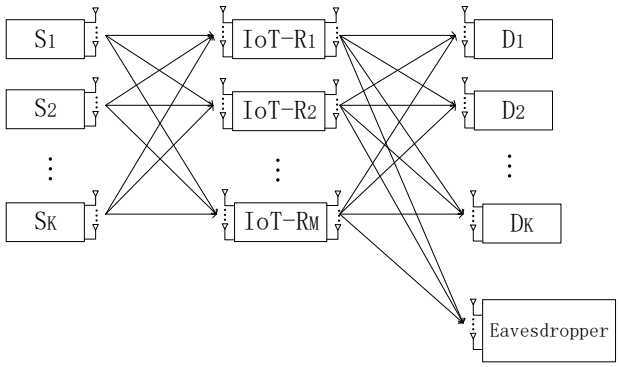


Figure 1. Two-hop multiple input multiple output (MIMO) interference relay system model in the wireless Internet of Things (IoT).

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, S_k, R_m, D_k and eavesdropper are equipped with T_k, Q_m, N_k and N_e antennas. We consider that the channels undergo slow varying flat Rayleigh fading. We also assume that the noise at all receiving nodes is additive white Gaussian noise (AWGN) with zero mean and variance σ^2 [37]. We denote $\mathbf{H}_{km}$, $\mathbf{G}_{mk}$ and $\mathbf{G}_{me}$ as the actual channel matrices of $S_k - R_m$, $R_m - D_k$ and $R_m - E$ links.

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

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

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

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

where $\mathbf{y}_{r_m} \in \mathbb{C}^{Q_m \times 1}$ is the received signal vector at relay R_m; $\mathbf{y}_{d_k} \in \mathbb{C}^{N_k \times 1}$ is the received signal vector at destination D_k; $\mathbf{y}_e \in \mathbb{C}^{N_e \times 1}$ is the received signal vector at the eavesdropper E; $\mathbf{H}_{km} \in \mathbb{C}^{Q_m \times T_k}$ is denoted as channel gain between source S_k and relay R_m; $\mathbf{G}_{mk} \in \mathbb{C}^{N_k \times Q_m}$ is denoted as channel gain between relay R_m and destination D_k; $\mathbf{G}_{me} \in \mathbb{C}^{N_e \times Q_m}$ is denoted as channel gain between relay R_m and eavesdropper E; $\mathbf{s}_k \in \mathbb{C}^{T_k \times 1}$ is the transmitted data vector at source S_k; $\mathbf{n}_{r_m} \in \mathbb{C}^{Q_m \times 1}$, $\mathbf{n}_{d_k} \in \mathbb{C}^{N_k \times 1}$ and $\mathbf{n}_e \in \mathbb{C}^{N_e \times 1}$ are 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 linear receive matrices at destinations and eavesdropper, which are subject to transmission power constrains at source and relay. For the sake of seeking optimum solution about above matrices, we scheme an iterative distributed algorithm.

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

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

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

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

In most scenarios, perfect channel estimation is considered. However, channel estimation is far from being perfect in realistic practical system. Hence, we assume imperfect channel estimation in our article. Here, P_{sk} and P_{rm} denote the maximum transmission power at S_k and R_m. N_p denotes the number of channel estimation pilot symbols. Considering $\hat{\mathbf{H}}_{km}$, $\hat{\mathbf{G}}_{mk}$ and $\hat{\mathbf{G}}_{me}$ as the estimated channel matrices and $\mathbf{E}_{h,km}$, $\mathbf{E}_{r,mk}$, and $\mathbf{E}_{e,me}$ as the MMSE estimation error matrices, respectively, we obtain the relationship of the estimated and actual channel matrices as $\mathbf{H}_{km} = \hat{\mathbf{H}}_{km} + \mathbf{E}_{h,km}$, $\mathbf{G}_{mk} = \hat{\mathbf{G}}_{mk} + \mathbf{E}_{r,mk}$, $\mathbf{G}_{me} = \hat{\mathbf{G}}_{me} + \mathbf{E}_{e,me}$, where $\mathbf{E}_{h,km} \in \mathbb{C}^{Q_m \times T_k} \sim \mathcal{CN}\left(0,\ (1+\rho_h \mathrm{SNR}_h)^{-1}\right)$ with $\rho_h = N_p/T_k$ and $\mathrm{SNR}_h = P_{sk}/\sigma_{r_m}^2$, $\mathbf{E}_{r,mk} \in \mathbb{C}^{N_k \times Q_m} \sim \mathcal{CN}\left(0,\ (1+\rho_r \mathrm{SNR}_r)^{-1}\right)$ with $\rho_r = N_p/Q_m$ and $\mathrm{SNR}_r = P_{rm}/\sigma_{d_k}^2$, and $\mathbf{E}_{e,me} \in \mathbb{C}^{N_e \times Q_m} \sim \mathcal{CN}\left(0,\ (1+\rho_e \mathrm{SNR}_e)^{-1}\right)$ with $\rho_e = N_p/Q_m$ and $\mathrm{SNR}_e = P_{rm}/\sigma_e^2$.

Finally, both destination D_k and the eavesdropper employ linear receive matrix $\mathbf{W}_k$ and $\mathbf{W}_{e,k}$ respectively to receive the transmitted signals. Assuming imperfect channel estimation above mention, the estimate of the data $\mathbf{s}_k$ at D_k and the eavesdropper can be denoted as follows

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

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

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

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

Similarly, we can get the MSE of estimating s_k at eavesdropper as follows

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

The transmission power constraints at source S_k and relay R_m are as follows

$$tr\left(\mathbf{U}_k E\left\{\mathbf{s}_k\mathbf{s}_k^H\right\}\mathbf{U}_k^H\right) \leq P_{sk}, k = 1,\ldots,K, \tag{11}$$

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

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, when there exists an eavesdropper, the signals from source may be leaked out to the eavesdropper.

In order to elaborate more specifically and clearly, we assume a worst-case situation, namely in the presence of a sophisticated eavesdropper which can obtain the channel state information and our proposed algorithm, the eavesdropper calculates its linear receive matrix $\mathbf{W}_{e,k}$ to minimize its own

$\mathrm{MSE}_{e,k}$. To prevent this, we exploit the assumption to conceive the precoding/receive matrices for legitimate system at source or relay.

The solution of the source matrices $\{\mathbf{U}_k\}$, relay matrices $\{\mathbf{V}_m\}$ and destination matrices $\{\mathbf{W}_k\}$ 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 $(k = 1, \ldots, K)$, while subjecting to the transmission power constrains at source and relay. The solution is denoted as follows

$$\begin{array}{c} \underset{\{\mathbf{U}_k\},\{\mathbf{V}_m\},\{\mathbf{W}_k\}}{min} \quad : \sum_{k=1}^{K} \mathrm{MSE}_k \\ s.t. \quad : \mathrm{MSE}_{e,k} \geq \varepsilon_k, \\ tr\left(\mathbf{U}_k E\left\{\mathbf{s}_k \mathbf{s}_k^H\right\} \mathbf{U}_k^H\right) \leq P_{sk}, \\ tr\left(\mathbf{V}_m E\left\{\mathbf{y}_{r_m} \mathbf{y}_{r_m}^H\right\} \mathbf{V}_m^H\right) \leq P_{rm}, \end{array} \tag{13}$$

where $\{\mathbf{U}_k\}$, $\{\mathbf{V}_m\}$ and $\{\mathbf{W}_k\}$ 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 solution, we design 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

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

3.1. Solution of Destination Matrices $\{W_k\}$

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 $\{\mathbf{W}_k\}$ are independent with transmission power constrains of source and relay. Therefore, we can obtain the optimal linear receive matrices $\{\mathbf{W}_k\}$ to minimize the total MSE at destination by the well-known linear MMSE receiver [38], which can be formulated as

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

Assuming that the eavesdropper employs the above well-known linear MMSE method to calculate its linear receive matrix $\mathbf{W}_{e,k}$., which can be formulated as

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

3.2. Solution of Source Matrices $\{U_k\}$

After obtaining the optimal matrices $\{\mathbf{W}_k\}$, we can calculate the transmit precoding matrices $\{\mathbf{U}_k\}$ with $\{\mathbf{W}_k\}$ 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

$$\begin{array}{c}\text{TMSE} = \sum_{k=1}^{K} tr(\sum_{m=1}^{M}\sum_{l=1}^{K} \mathbf{W}_k^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})\mathbf{V}_m(\mathbf{H}_{lm}-\mathbf{E}_{h,lm})\mathbf{U}_l\mathbf{U}_l^H(\mathbf{H}_{lm}-\mathbf{E}_{h,lm})^H \\ \mathbf{V}_m^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})^H\mathbf{W}_k) - \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \mathbf{W}_k^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})\mathbf{V}_m(\mathbf{H}_{km}-\mathbf{E}_{h,km})\mathbf{U}_k) \\ + \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \mathbf{U}_k^H(\mathbf{H}_{lm}-\mathbf{E}_{h,lm})^H\mathbf{V}_m^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})^H\mathbf{W}_k) + \\ \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \sigma_{r_m}^2\mathbf{W}_k^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})\mathbf{V}_m\mathbf{V}_m^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})^H\mathbf{W}_k + \sigma_{d_k}^2\mathbf{W}_k^H\mathbf{W}_k + \mathbf{I}_{T_k})\end{array} \tag{17}$$

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

$$\begin{array}{c}\text{TMSE} = \sum_{k=1}^{K} tr(\sum_{m=1}^{M}\sum_{l=1}^{K} \mathbf{P}_{k,m,l}\mathbf{U}_l\mathbf{U}_l^H\mathbf{P}_{k,m,l}^H) - \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \mathbf{P}_{k,m,k}\mathbf{U}_k) - \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \mathbf{U}_k^H\mathbf{P}_{k,m,k}^H) \\ + \sum_{k=1}^{K} tr(\sum_{m=1}^{M} \sigma_{r_m}^2\mathbf{W}_k^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})\mathbf{V}_m\mathbf{V}_m^H(\mathbf{G}_{mk}-\mathbf{E}_{r,mk})^H\mathbf{W}_k + \sigma_{d_k}^2\mathbf{W}_k^H\mathbf{W}_k + \mathbf{I}_{T_k})\end{array} \tag{18}$$

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

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

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

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

To solve the above problems simplistically, we introduce some important formulas of Reference [39]

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

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

$$\text{TMSE} = \mathbf{u}^H\boldsymbol{\omega}\mathbf{u} - \boldsymbol{\psi}\mathbf{u} - \mathbf{u}^H\boldsymbol{\psi}^H + \boldsymbol{\gamma}, \tag{21}$$

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

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

$$\text{MSE}_{e,k} = \mathbf{u}^H\boldsymbol{\omega}_{e,k}\mathbf{u} - \boldsymbol{\psi}_{e,k}\mathbf{u} - \mathbf{u}^H\boldsymbol{\psi}_{e,k}^H + \boldsymbol{\gamma}_e, \tag{22}$$

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

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

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

Then we obtain (24)

$$u^H\boldsymbol{\rho}u \le P_{sk}, k = 1,\ldots,K, \tag{24}$$

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

From (21), (22) and (24), the source matrices optimization problem is denoted as

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

The source matrices optimization problem (25) is a quadratic constrained quadratic programming (QCQP) problem [40]. Compared with the non-convex problem (13), the (25) will be solved by the CVX of MATLAB toolbox [41].

3.3. Solution of Relay Matrices $\{V_m\}$

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

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

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

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

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

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

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

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

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

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

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

From (28), (29) and (30), the relay matrices optimization problem is denoted as

$$\underset{\{\mathbf{V}_m\}}{min} \ : \text{TMSE} \ s.t. : \ \text{MSE}_{e,k} \geq \varepsilon_k \ \mathbf{v}^H \boldsymbol{\lambda} \mathbf{v} \leq P_{rm}, m = 1, \ldots, M, \tag{31}$$

The relay matrices optimization problem (31) is a QCQP problem [40]. Compared with the non-convex problem (13), the (31) will be solved by utilizing the CVX of MATLAB toolbox [41].

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 and variable n denotes the nth iteration.

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

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

At last, we introduce the communication rate and secrecy rate in this system model. The communication rate at destinations and eavesdropper are as follows [42],

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

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

The secrecy rate at each destination can be obtained [43].

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

4. The Convergence of the Proposed Algorithm

In this part, the convergence of our proposed algorithm is proved [44]. Since the $\{\mathbf{U}_k\}$ and $\{\mathbf{V}_m\}$ are updated at each iteration by minimizing the TMSE, the TMSE is reduced gradually after each iteration. Furthermore, it is obvious that the TMSE has a lower limit which is at least greater than 0. This implies that the proposed algorithm is convergence. The convergence of the proposed algorithm can be proved exactly as follows. According to Section 3, we can obtain the objective function is

$$\min_{\{\mathbf{U}_k\}, \{\mathbf{V}_m\}, \{\mathbf{W}_k\}} : \sum_{k=1}^{K} \mathrm{MSE}_k \tag{35}$$

The solution of $\{\mathbf{W}_k\}$ can be ignored in the proof of convergence, because it is calculated by obtained $\{\mathbf{U}_k\}$ and $\{\mathbf{V}_m\}$ rather than utilize optimal scheme. For the obtained $\{\mathbf{V}_m\}$, the optimal solution can be denoted as follows.

$$\min_{\{\mathbf{U}_k\}} : \sum_{k=1}^{K} \mathrm{MSE}_k \tag{36}$$

Therefore, we can get $\sum_{k=1}^{K} \mathrm{MSE}_k(\mathbf{U}_k(n+1), \mathbf{V}_m(n)) \leq \sum_{k=1}^{K} \mathrm{MSE}_k(\mathbf{U}_k(n), \mathbf{V}_m(n))$.
Similarly, for the obtained $\{\mathbf{U}_k\}$, the optimal solution can be denoted as follows.

$$\min_{\{\mathbf{V}_m\}} : \sum_{k=1}^{K} \mathrm{MSE}_k \tag{37}$$

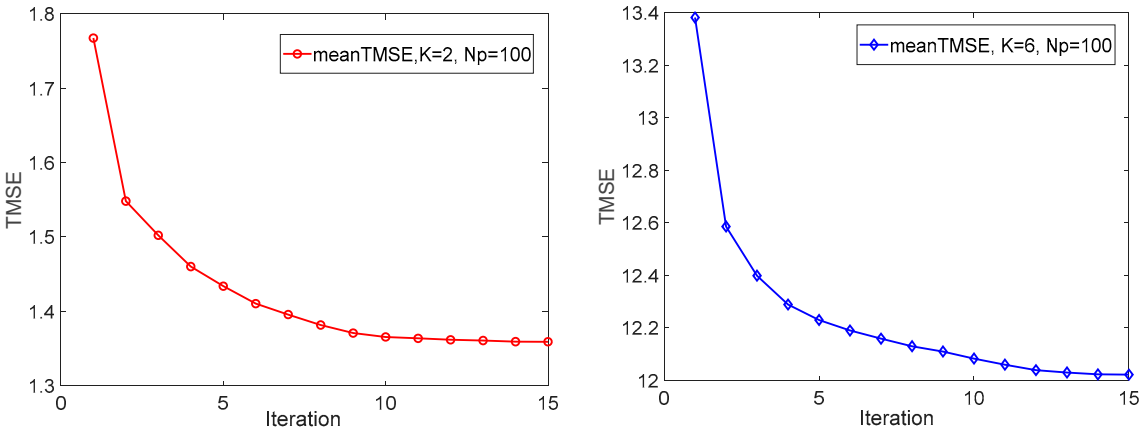
Hence, we can deduce $\sum_{k=1}^{K} \mathrm{MSE}_k(\mathbf{U}_k(n+1), \mathbf{V}_m(n+1)) \leq \sum_{k=1}^{K} \mathrm{MSE}_k(\mathbf{U}_k(n+1), \mathbf{V}_m(n))$. Furthermore, we get $\sum_{k=1}^{K} \mathrm{MSE}_k(\mathbf{U}_k(n+1), \mathbf{V}_m(n+1)) \leq \sum_{k=1}^{K} \mathrm{MSE}_k(\mathbf{U}_k(n), \mathbf{V}_m(n))$.

According to the mentioned above, we conclude that the TMSE is decreasing gradually with the updated $\{\mathbf{U}_k\}$ and $\{\mathbf{V}_m\}$ after each iteration. The TMSE converges to a constant after several iterations, which is also demonstrated by the Figure 2 of the Numerical Results part.

5. Numerical Results

In this part, we provide numerical results to examine the effectiveness of the optimization iterative distributed algorithm for secure transmission in interference channels MIMO relay system with eavesdropping. Assuming that all nodes have the same antennas, $T_k = Q_m = N_k = N_e = 3$ and all channel matrices are independently distributed Gaussian channel matrices with zero mean and unit variance. The noises at all receiving nodes are assumed as AWGN with $\sigma_{d_k}^2 = \sigma_{r_m}^2 = \sigma_e^2 = 1$. The transmission power constrains at sources and relays are assumed as $P_{s_k} = P_{r_m} = 20$ dB. Assuming that the eavesdropper knows the channel state information of the links between relay and itself. In addition, the threshold of eavesdropper's MSE are $\varepsilon_k = 2.2,\ k = 1, \ldots, K$. All figures are averaged over 1000 independent test.

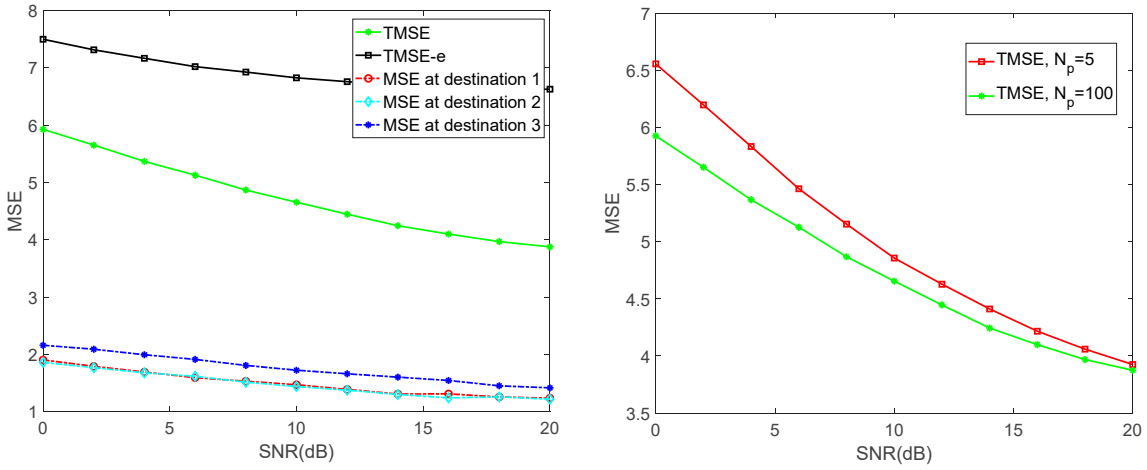
Figure 2 depicts the convergence of proposed iterative distributed algorithm, where we have $K = 2$ or 6, $M = 3$, $N_p = 100$, as well as $P_{s_k} = P_{r_m} = 20$ dB. As can be seen in Figure 2, TMSE decreases gradually until convergence when the number of iterations increases. It can be observed in both Figure 2a,b, as the system scale increases (i.e., increasing K), 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.



(**a**) $K = 2$ (**b**) $K = 6$

Figure 2. Total mean square error (TMSE) versus the number of iterations.

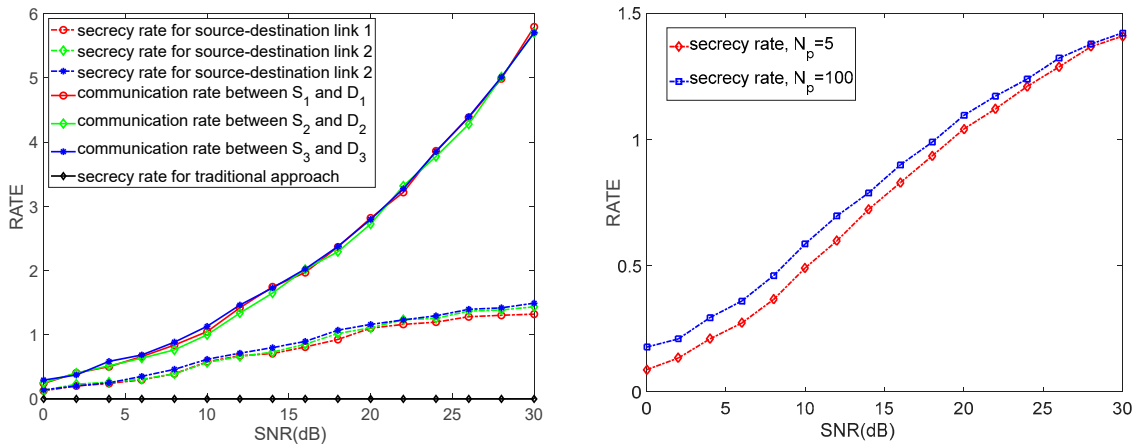
Figure 3 shows the changes of TMSE and MSEs at different destinations versus signal to noise ratio (SNR) with different N_p, where we have $K = 3$, $M = 3$, TMSE-e denotes the $\sum_{k=1}^{K} \mathrm{MSE}_{e,k}$. As shown in Figure 3a, both TMSE of all destinations and MSE at different destinations decrease gradually as the SNR increases. It can also be observed in Figure 3a 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. Additionally, Figure 3b shows that the TMSE of all destinations decreases when N_p increases. The reason is that the reduction of N_p causes the increasement of channel estimation errors, which in turn leads to the increasement of the TMSE.



(**a**) $N_p = 100$ (**b**) different N_p

Figure 3. The TMSE and MSE versus signal to noise ratio (SNR).

Figure 4 depicts the values of secrecy rate and communication rate versus transmission power constrains with different N_p, when $K = 3$, $M = 3$, which is in the same background with Figure 3. As shown in Figure 4a, compared to the traditional approach, the proposed algorithm can support a positive secrecy rate and secrecy rate gradually improves with the SNR increasing. In other word, our proposed algorithm guarantees secure communications for the system. According to Reference [45], when the communication rate of legitimate transmitter-receiver link is lower than that of the transmitter-eavesdropper link, we define the secrecy rate as "0"; when the communication rate of legitimate transmitter-receiver link is larger than that of the transmitter-eavesdropper link, we define secrecy rate as the difference between the communication rate of legitimate transmitter-receiver link and that of the transmitter-eavesdropper link (as shown in (32)). The traditional approach does not consider the eavesdropper and the eavesdropper is so "sophisticated" (it knows our security algorithm) that the communication rate of legitimate transmitter-receiver link is lower than that of the transmitter-eavesdropper link. Consequently, no matter how large the SNR is, the secrecy rate is always zero. That communication rates of three links are similar, the situation of the secrecy rates is the same. Moreover, the achievable secrecy rates are lower than communication rates, because the proposed algorithm sacrifices a part of communication rate to realize a positive secrecy rate. Additionally, it can be observed in Figure 4b that the secrecy rate improves with the increasing of N_p. This is because the increasement of N_p causes the reduction of channel estimation errors, which in turn leads to the increasement of secrecy rates.



(**a**) $N_p = 100$ (**b**) different N_p

Figure 4. The communication rate and secrecy rate versus 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 $K = 3, M = 3$ and $N_p = 100$ As shown in Figure 5, the TMSE of all destinations decreases when the SNR or the number of iterations increases. In addition, it also be depicted in Figure 5 that the TMSE decreases quickly at the beginning of the iteration process. And that means the proposed algorithm converges quickly.

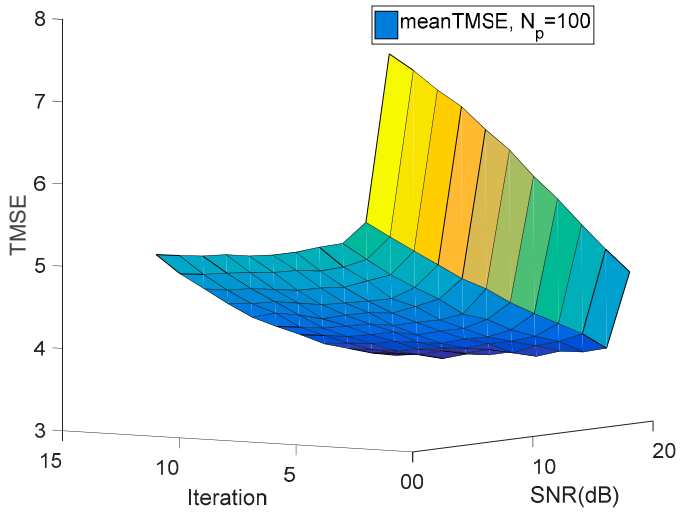


Figure 5. The TMSE versus the number of iterations and SNR.

6. Conclusions

In this article, we first investigate secure communication in MIMO interference relay IoT network in the presence of an active eavesdropper. A robust iterative distributed algorithm which jointly optimizes the source, relay and destination matrices has been proposed under the imperfect channel estimation. It aims to minimize the TMSE of all legitimate destinations subject to transmission power constrains while keeping MSE at eavesdropper above a certain threshold. The convergence of the proposed algorithm has also been proved. In addition, the performances of our proposed algorithm, such as its secrecy rate and MSE, are characterized in the form of simulation results. The simulation results reveal that our proposed algorithm is superior to the traditional approach. In other word, security can be ensured by using the proposed algorithm in the interference channel MIMO relay IoT network when there exists an eavesdropper.

Author Contributions: Conceptualization, Z.K. and D.W.; Methodology, Z.K.; Software, D.W.; Validation, Z.K., D.W. and Y.L.; Formal Analysis, C.W.; Investigation, C.W.; Resources, Z.K.; Data Curation, D.W.; Writing-Original Draft Preparation, Z.K. and D.W.; Writing-Review & Editing, Y.L.

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.

References

1. Zhu, C.; Wang, H.; Liu, X.; Shu, L.; Yang, L.T.; Leung, V.C.M. A novel sensory data processing framework to integrate sensor networks with mobile cloud. *IEEE Syst. J.* **2016**, *10*, 1125–1136. [CrossRef]
2. Liu, H.; Ning, H.; Zhang, Y.; Xiong, Q.; Yang, L.T. Role-dependent privacy preservation for secure V2G networks in the smart grid. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 208–220. [CrossRef]
3. Jiang, P.; Winkley, J.; Zhao, C.; Munnoch, R.; Min, G.; Yang, L.T. An intelligent information forwarder for healthcare big data systems with distributed wearable sensors. *IEEE Syst. J.* **2016**, *10*, 1147–1159. [CrossRef]
4. Liu, H.; Ning, H.; Zhang, Y.; Yang, L.T. Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid. *IEEE Trans. Smart Grid* **2012**, *3*, 1722–1733. [CrossRef]
5. Xiong, W.; Hu, H.; Xiong, N.; Yang, L.T.; Peng, W.-C.; Wang, X.; Qu, Y. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. *Inf. Sci.* **2014**, *258*, 403–415. [CrossRef]
6. Naik, V.K.; Liu, C.; Yang, L.T.; Wagner, J. Online resource matching for heterogeneous grid environments. In Proceedings of the IEEE International Symposium on Cluster Computing and the Grid, Cardiff, UK, 9–12 May 2005; pp. 607–614. [CrossRef]
7. Deng, X.J.; Tang, Z.J.; Yang, L.T.; Lin, M.; Wang, B. Confident Information Coverage Hole Healing in Hybrid Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2220–2229. [CrossRef]
8. Deng, X.J.; Tang, Z.J.; Yi, L.Z.; Yang, L.T. Healing Multimodal Confident Information Coverage Holes in NB-IoT-Enabled Networks. *IEEE Internet Things J.* **2018**, *5*, 1463–1473. [CrossRef]
9. Deng, X.J.; Yang, L.T.; Yi, L.Z.; Wang, M.; Zhu, Z. Detecting Confident Information Coverage Hole in Industrial Internet of Things: An Energy-Efficient Perspective. *IEEE Commun. Mag.* **2018**, *56*, 68–73. [CrossRef]
10. Yi, L.Z.; Deng, X.J.; Wang, M.H.; Ding, D.; Wang, Y. Localized Confident Information Coverage Hole Detection in Internet of Things for Radioactive Pollution Monitoring. *IEEE Access* **2017**, *5*, 18665–18674. [CrossRef]
11. Zou, Z.H.; Deng, X.J.; Yi, L.Z.; Tang, Z.; Wang, M.; Gong, X. A Novel Confident Information Coverage Hole Detection Algorithm in Sensor Networks. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data, Chengdu, China, 15–18 December 2016; pp. 199–204.
12. Li, J.L.; Chang, S.; Fu, X.M.; Zhang, L.; Su, Y.; Jin, Z. A Coalitional Formation Game for Physical Layer Security of Cooperative Compressive Sensing Multi-Relay Networks. *Sensors* **2018**, *18*, 2942. [CrossRef] [PubMed]
13. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
14. Albashier, M.A.M.; Abdaziz, A.; Ghani, H.A. Performance analysis of physical layer security over different error correcting codes in wireless sensor networks. In Proceedings of the 2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC), Bali, Indonesia, 17–20 December 2017; pp. 191–195. [CrossRef]
15. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011; ISBN 9780521516501.
16. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [CrossRef]
17. Bloch, M.; Barros, J.; Rodrigues, M.R.D. Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]

18. Zou, Y.L.; Wang, X.B.; Shen, W.M. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2099–2111. [CrossRef]
19. Park, K.H.; Wang, T.; Alouini, M.S. On the Jamming Power Allocation for Secure Amplify-and-Forward Relaying via Cooperative Jamming. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1741–1750. [CrossRef]
20. Krikidis, I.; Thompson, J.; Mclaughlin, S. Relay selection for secure cooperative networks with jamming. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 5003–5011. [CrossRef]
21. Chen, J.; Zhang, R.; Song, L. Joint relay and jammer selection for secure two-way relay networks. *Proc. IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 310–320. [CrossRef]
22. 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 Trans. Ind. Inform.* **2016**, *12*, 1714–1725. [CrossRef]
23. Xu, Q.; Ren, P.Y.; Song, H.B. Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations. *IEEE Access* **2016**, *4*, 2840–2853. [CrossRef]
24. Zhang, Y.Y.; Shen, Y.L.; Wang, H. On Secure Wireless Communications for IoT under Eavesdropper Collusion. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 1281–1293. [CrossRef]
25. Islam, S.N.; Mahmud, M.A. Secured Communication among IoT Devices in the Presence of Cellular Interference. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–7 June 2017; pp. 1–6. [CrossRef]
26. Ying, L.; Liang, L.; Alexandropoulos, G.C. Securing Relay Networks with Artificial Noise: An Error Performance Based Approach. *Entropy* **2017**, *19*, 384.
27. Jeong, C.; Kim, I.; Kim, D.I. Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System. *IEEE Trans. Signal Process.* **2012**, *60*, 310–325. [CrossRef]
28. Khandaker, M.R.A.; Rong, Y. Interference MIMO Relay Channel: Joint Power Control and Transceiver-Relay Beamforming. *IEEE Trans. Signal Process.* **2012**, *60*, 6509–6518. [CrossRef]
29. Kong, Z.M.; Yang, S.S.; Wu, F.L. Iterative Distributed Minimum Total MSE Approach for Secure Communications in MIMO Interference Channels. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 594–608. [CrossRef]
30. Badra, N.; Yang, J.X.; Psaromiligkos, I.; Champagne, B. Robust and secure beamformer design for MIMO relaying with imperfect eavesdropper CSI. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 442–449. [CrossRef]
31. Alexandropoulos, G.C.; Peppas, K.P. Secrecy Outage Analysis Over Correlated Composite Nakagami-m/Gamma Fading Channels. *IEEE Commun. Lett.* **2018**, *22*, 77–80. [CrossRef]
32. Alexandropoulos, G.C.; Papadias, C.B. A reconfigurable distributed algorithm for K-user MIMO interference networks. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013; pp. 3063–3067. [CrossRef]
33. Shi, Q.; Razaviyayn, M.; Luo, Z. An Iteratively Weighted MMSE Approach to Distributed Sum-Utility Maximization for a MIMO Interfering Broadcast Channel. *IEEE Trans. Signal Process.* **2011**, *59*, 4331–4340. [CrossRef]
34. Alexandropoulos, G.C.; Ferrand, P.; Papadias, C.B. On the Robustness of Coordinated Beamforming to Uncoordinated Interference and CSI Uncertainty. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6. [CrossRef]
35. Alexandropoulos, G.C.; Barousis, V.I.; Papadias, C.B. Precoding for multiuser MIMO systems with single-fed parasitic antenna arrays. In Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM), Austin, TX, USA, 8–12 December 2014; pp. 3897–3902. [CrossRef]
36. Xu, D.; Ren, P.; Ritcey, J.A. Optimal Grassmann Manifold Eavesdropping: A Huge Security Disaster for M-1-2 Wiretap Channels. In Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM), Singapore, 4–8 December 2017; pp. 1–6. [CrossRef]
37. Xu, Z.Y.; Zhong, J.; Chen, G.J. Novel joint secure resource allocation optimization for full-duplex relay networks with cooperative jamming. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; pp. 1–6. [CrossRef]
38. Yang, S.S.; Hanzo, L. Fifty Years of MIMO Detection: The Road to Large-Scale MIMOs. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1941–1988. [CrossRef]

39. Horn, R.A.; Johnson, C.R. *Topics in Matrix Analysis*, 1st ed.; Cambridge University Press: Cambridge, UK, 1994.
40. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.
41. Grant, M.; Boyd, S. Cvx: MATLAB Software for Disciplined Convex Programming (Webpage and Software). Available online: http://cvxr.com/cvx (accessed on 1 April 2010).
42. Fang, H.; Xu, L. Coordinated Multiple-Relays Based Physical-Layer Security Improvement: A Single-Leader Multiple-Followers Stackelberg Game Scheme. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 197–209. [CrossRef]
43. Al-jamali, M.; Al-nahari, A.; AlKhawlani, M.M. Relay selection scheme for improving the physical layer security in cognitive radio networks. In Proceedings of the 2015 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16–19 May 2015; pp. 495–498. [CrossRef]
44. Shen, H.; Li, B.; Tao, M. MSE-Based Transceiver Designs for the MIMO Interference Channel. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 3480–3489. [CrossRef]
45. Zheng, C.; Kanapathippillai, C.; Ding, Z.G. Robust outage secrecy rate optimizations for a MIMO secrecy channel. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 86–89. [CrossRef]