Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6626355, 17 pages
https://doi.org/10.1155/2021/6626355

Research Article

Trustworthy Jammer Selection with Truth-Telling for Wireless Cooperative Systems

Yingkun Wen, Tao Jing, and Qinghe Gao

School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China

Correspondence should be addressed to Yingkun Wen; 16111024@bjtu.edu.cn

Received 9 November 2020; Revised 23 December 2020; Accepted 9 January 2021; Published 8 February 2021

Academic Editor: Zhuojun Duan

In this paper, we propose a trustworthy friendly jammer selection scheme with truth-telling for wireless cooperative systems. We first utilize the reverse auction scheme to enforce truth-telling as the dominant strategy for each candidate friendly jammer. Specifically, we consider two auction cases: (1) constant power (CP) case and (2) the utility of the BS maximization (UBM) case. In both cases, the reverse auction scheme enforces truth-telling as the dominant strategy. Next, we introduce the *trust category* and *trust degree* to evaluate the trustworthiness of each Helper transmitter (Helper-Tx). Specifically, an edge controller calculates the reputation value of each Helper-Tx periodically using an additive-increase multiplicative-decrease algorithm by observing its jamming behavior. With the historical reputation values, the edge controller (EC) classifies a Helper-Tx into one of four trust categories and calculates its trust degree. Then, the EC selects the best Helper-Tx based on the trust category and trust degree. Lastly, we present numerical results to demonstrate the performance of our proposed jammer selection scheme.

1. Introduction

Cooperative jamming enables two wireless nodes to exchange secret messages in the presence of an eavesdropper without encryption [1, 2]. It is an information-theoretic security approach that exploits the physical characteristics of the wireless channel, which does not depend on the assumption of computational hardness. In cooperative jamming, a selected friendly jammer sends out artificial noise (i.e., jamming signal) at the same time when a sender transmits a message to a receiver [3, 4]. The artificial noise is aimed at creating intentional interference at the eavesdropper. If the channel condition between the sender-receiver is better than that of the channel between the sender-eavesdropper, the sender and receiver can exchange secure messages at a certain rate.

Friendly jammer selection plays a fundamental role in maximizing the secure message exchange rate (i.e., secrecy rate) in cooperative jamming [5, 6]. In general, there are two phases in a jammer selection scheme. In the first phase, each candidate jammer reports its private information (e.g., battery state) to the sender (also known as the source node or mechanism designer) through a common control channel [7, 8]. According to the reported private information, the sender selects a suitable candidate as the jammer. In the second phase, the selected jammer sends out sufficient jamming signals to create desired interference at the eavesdropper (Eve).

There are challenges that need to address in both phases. In the first phase, since each candidate wants to be selected to get payment, it may not be telling the truth in reporting its private information so as to increase the chance of being selected. A candidate without truth-telling can cause unfairness and degrade the secrecy performance of the entire network. Therefore, it is necessary to develop a mechanism to ensure truth-telling for each candidate. In the second phase, a selected jammer may transmit a partial (or even none) jamming signal due to various reasons. We call it an *untrusted* friendly jammer. An untrusted jammer can also lead to unfairness and a decrease in the secrecy rate. Hence, it is important to avoid untrusted jammers.

To address the aforementioned challenges, we propose a trustworthy friendly jammer selection scheme with truth-telling for a wireless cooperative system (WCS). Firstly, we utilize the reverse auction scheme to enforce truth-telling under two cases: (1) constant power (CP) case and (2) utility of the BS maximization (UBM) case. In these two cases, we enforce truth-telling as the dominant strategy of each candidate jammer. In the auction scheme, helper transmitters (Helper-Txs) are edge devices that function as candidate jammers. Spectrum resources of a base station (BS) are revenues for Helper-Txs. In the CP case, the BS assigns a fixed transmission power to the jammer. In the UBM case, the utility of the BS is approximately maximized.

Secondly, we introduce *trust categories* and *trust degree* to evaluate the trustworthiness of each Helper-Tx. Specifically, an edge controller (EC) is introduced to calculate the reputation value of each Helper-Tx periodically using an additive-increase multiplicative-decrease (AIMD) algorithm by observing its jamming behavior. Subsequently, the EC classifies each Helper-Tx into one of four trust categories based on its historical reputation values. The trust degree of each Helper-Tx is obtained by averaging its reputation values over time. If a Helper-Tx belongs to a certain trust category and meets the trust degree requirement, it can be regarded as a trustworthy jammer.

The main contributions of this paper are summarized as follows:

(i) We prove that the BS can achieve the highest secrecy rate by selecting a one best Helper-Tx as the jammer. More than one jammer can lead to a decreased secrecy performance

(ii) We utilize the reverse auction scheme to stimulate truth-telling of Helper-Txs. In the reverse auction scheme, we consider two cases: (1) CP case and (2) UBM case. In both cases, the reverse auction scheme can guarantee incentive compatible (IC) and individual rationality (IR). In both cases, we show numerical results that the reverse auction scheme outperforms the widely used Vickrey auction scheme

(iii) We propose two metrics (i.e., trust category and degree) to measure the trustworthiness of a selected jammer. We adopt the AIMD algorithm to promote trustworthy behavior and penalize selfish conducts

The rest of the paper is organized as follows. Related work is given in Section 2. In Section 3, an overview of the network model and some preliminaries are presented. In Section 4, we give out the auction scheme and related solutions. In Section 5, the trust management process and the jammer selection scheme are described. Numerical results are given in Section 6, and conclusions are drawn in Section 7.

Notations: $(\cdot)^H$ and $|\cdot|$ denote the Hermitian transpose and the absolute value, respectively. $\mathrm{Tr}(\cdot)$ denotes the trace operator. $\mathbf{I}_N$ is the $N \times 1$ vector of all ones. The normal distribution with the mean μ and the variance σ^2 is denoted as $\mathcal{N}(\mu, \sigma^2)$. $[x]^+ = \max\{x, 0\}$. $\mathbf{A} \pm 0$ ($\mathbf{A} \succ 0$) means that $\mathbf{A}$ is a Hermitian positive semidefinite (definite) matrix.

2. Related Work

Conventional cryptographic-based methods at the upper layer are of high complexity due to the expensive operations such as the encryption and decryption [9–11]. Physical layer security approaches with the advantages of low complexity and resource savings have been explored both as an alternative and a complementary to conventional cryptographic-based methods [12–14]. Physical layer security approaches with the cooperation of helping nodes (cooperative relaying and jamming) have been extensively investigated [15–18]. Recently, some new physical layer security technologies have been proposed for secure communication, e.g., unmanned aerial vehicle- (UAV-) aided jamming [19], intelligent reflecting surfaces- (IRS-) assisted jamming [20], and learning-aided cooperative relays [21, 22].

Considering that the helping nodes consume energy during cooperation, it is necessary to investigate how to incentivize users to cooperate for security enhancement [23–25]. Therefore, game theory is employed in physical layer security to study the interactions between the source and helping nodes, where helping nodes would gain some payoffs [26, 27]. However, in most of the current cooperative networks, the helping nodes are assumed honest and ready to disclose their true private information, which is usually not realistic [28, 29]. In practice, helping nodes may exaggerate their private information to maximize their payoffs, which is a key issue in cooperative networks.

To address this issue, a mechanism designer aims to motivate the helping nodes to disclose their private information by designing the payoff structure [30–33]. Authors of [31] designed different "transfer payment" functions to the payoff of each relay and proved that each relay gains its maximum payoff when it truthfully reports its private information. In [33], the author proposed a truth-telling based mechanism, where the selected relays' energy harvesting requirements would be fulfilled if they tell the truth. Otherwise, the relays are penalized by the transfer payment.

Besides cooperative relays, cooperative jammers are also important helping nodes for physical layer security in cooperative networks [6, 34, 35]. In [6], the authors investigated the physical layer security of amplify-and-forward (AF) relaying networks with the aid of the joint relay and jammer selection. Authors in [34] proposed three categories of relay and jammer selection for a two-way cooperative communication scenario. In [35], the authors proposed a joint relay and jammer selection scheme and derived a closed-form suboptimal solution to maximize the secrecy rate.

In addition, untrusted jammers were investigated in [5, 36]. Specifically, the authors of [36] investigated a social-tie-based jammer selection scheme, allocating power appropriately to the source node and the cooperative jammer node to maximize the worst-case ergodic secrecy rate. In [5], the authors investigated how to select jammers for device to device users to thwart eavesdroppers by exploiting social relationship with the help of full CSI and partial CSI, respectively.

In the above literatures, the jammers are assumed honest, and the private information are perfectly known at the source

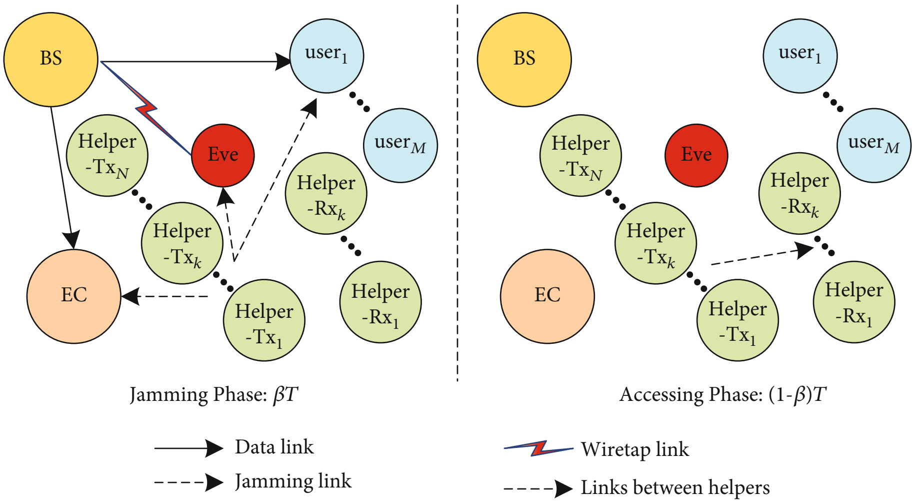


Figure 1: Network components.

node. However, the optimal solutions in these works would not hold if the jammers report their private information untruthfully. In addition, the trust degree of a jammer was only considered to be one of the parameters to analyze the secrecy performance. To the best of our knowledge, how to incentive cooperative jammers to report their private information and do trustworthiness analysis for a jammer has never been investigated, which motivates the study of this paper.

3. An Overview

In this paper, we consider a WCS that consists of a BS, M users, an Eve, an EC, and N pairs of Helper-Tx/Rx as shown in Figure 1. The BS is a type of edge device that functions as a user data entry point to the primary network. Helper-Tx/Rxs are another type of edge device that protects user data from being intercepted by Eve. Both types of edge devices are managed by the EC that is a controller that can be configured to match multiple specific requirements.

3.1. Transmission Phases. In the WCS, from the perspective of the jammer, there are two transmission phases (the jamming phase and the accessing phase) with a duration of length T.

3.1.1. Jamming Phase. In the jamming phase of length βT, the BS wants to send a message to a user (e.g., user$_1$) on the data link. Meanwhile, there is an Eve that wants to intercept and decode the message on the wiretap link. To protect the transmitted message from being eavesdropped, the BS selects $K \leq N$ Helper-Txs as friendly jammers to interfere with Eve on the jamming link.

In the WCS, the selected Helper-Tx (the jammer) is an edge device of user$_1$; thus, it is assumed that the jamming signal cannot be known previously by user$_1$. It means that user$_1$ cannot remove the jamming signal from the received signal. Instead, the beamforming vector of the jammer ($\mathbf{w}_j$) needs to be designed to ensure that the interference imposed at user$_1$ is lower than a temperature limit. In the WCS, we would first analyze the secrecy performance of the BS through cooperative jamming and then select the appropriate Helper-Txs. In what follows, we would calculate the secrecy rate to measure the secrecy performance of the BS.

It is assumed that the BS is able to acquire the CSI of the data link through pilot sequences [37]. Each Helper-Tx measures its CSI between itself and user$_1$, i.e., $\mathbf{h}_{j_n,u}$, and reports the CSI to the EC. The EC would share the CSI of Helper-Txs with the BS via a secure channel, such as a common control channel [38]. Finally, the CSI of users and Helper-Txs are both available at the BS. Thus, we assume that the perfect CSI of the data link is available. For the CSI of wiretap link, there are two cases:

(i) *Perfect CSI Case.* In some special cases, one of the legitimate users (e.g., untrusted relays) may be considered to be a potential Eve [39]. In other words, Eve is one of the legitimate users; thus, we can obtain the perfect CSI of the wiretap link. Specifically, the instantaneous CSI of $\mathbf{h}_{b,e}$ and $\mathbf{h}_{j_k,e}$ is known.

(ii) *Statistical CSI Case.* In most cases, accurate CSI for passive Eve cannot be acquired. However, the statistical CSI for wiretap links can be obtained by some measurement methods. Therefore, it is assumed that we can obtain the statistical CSI of the wiretap link. Specifically, the covariance matrices of $\mathbf{h}_{b,e}$ and $\mathbf{h}_{j_k,e}$ are known, i.e., $\mathbf{h}_{b,e} \sim \mathscr{C}\mathscr{N}(0, \sigma_{b,e}^2 \mathbf{I}_{N_b})$ and $\mathbf{h}_{j_k,e} \sim \mathscr{C}\mathscr{N}(0, \sigma_{j_k,e}^2 \mathbf{I}_{N_j})$.

In this paper, we only consider the perfect CSI case. In the case with statistical CSI, the design and analysis for reverse auction and trust management can be treated similarly in our previous work [40], which is omitted for brevity.

In the WCS, the BS is equipped with N_b antennas, and Helper-Txs are equipped with N_j antennas. All users, Eve, the EC, and Helper-Rxs are all equipped with a single antenna. The transmit beamforming vectors of the BS ($\mathbf{w}_b$) and Helper-Tx$_k$ ($\mathbf{w}_{j_k}$) are both designed at the BS. Next, the

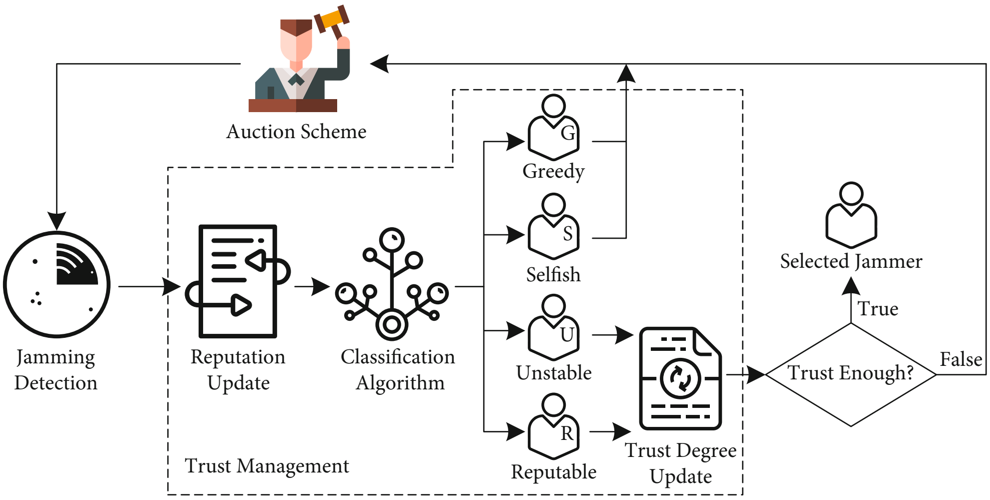


Figure 2: A framework for trustworthy jammer selection with truth-telling.

BS delivers the related beamforming vector ($\mathbf{w}_{j_k}$) to the EC, and the EC applies the beamforming vector ($\mathbf{w}_{j_k}$) to Helper-Tx$_k$.

With the CSI and beamforming vectors, the received signals at user$_1$, the EC, and Eve at time index t can be expressed as

$$y_q(t) = \mathbf{h}_{b,q}^H \mathbf{w}_b x_b(t) + \sum_{k=1}^{K} \mathbf{h}_{j_k,q}^H \mathbf{w}_{j_k} x_{j_k}(t) + n_q(t), \qquad (1)$$

respectively, where $\mathbf{h}_{p,q}$, $p \in \{b, j_k\}$, $q \in \{u, c, e\}$ are the links from the transmitters (the BS, Helper-Tx$_k$) to the receivers (user$_1$, the EC, and Eve). $\mathbf{h}_{p,q} = \bar{\mathbf{h}}_{p,q}\sqrt{\theta_{p,q}}$ with $\bar{\mathbf{h}}_{p,q}$ and $\theta_{p,q}$ denoting the $N_b(N_j) \times 1$ complex link vectors and the corresponding path loss from p to q link, respectively. The path loss can be expressed as $10\log_{10}(\theta_{p,q}) = -34.5 - 38\log_{10}(d_{p,q}[\mathrm{m}])$, where $d_{p,q}$ is the distances between transmitters and receivers. $\mathbf{w}_b \in \mathbb{C}^{N_b \times 1}$ and $\mathbf{w}_{j_k} \in \mathbb{C}^{N_j \times 1}$ are beamforming vectors of the BS and Helper-Tx$_k$, respectively. x_b is the message signal transmitted from the BS. x_{j_k} is the jamming signal transmitted from Helper-Tx$_k$, where $x_{j_k} \sim \mathcal{N}(0, 1)$. n_q is the additive white Gaussian noise (AWGN) with two-sided power spectral density N_{02}. It is assumed that $n_q \sim \mathcal{N}(0, \delta_q^2)$, where $\delta_q^2 = 2N_{02}B$ and B is the link bandwidth. All links are assumed to be subject to independent Rayleigh fading.

3.1.2. Accessing Phase. In the accessing phase of length $(1-\beta)T$, the selected Helper-Txs are allowed to access the data link when the data link is idle so that they can transmit their messages to intended Helper-Rxs.

3.2. Trustworthy and Truth-Telling Challenges. In the WCS, note that the secrecy rate is provided by a Helper-Tx; the selection of an appropriate Helper-Tx as the cooperative jammer plays a critical role in improving the secrecy rate. Specifically, the selection of an appropriate Helper-Tx faces two challenges as follows:

(i) *Truth-Telling Challenge*. Since the selected Helper-Txs may have greater opportunity to access the data link, all the Helper-Txs will be naturally interested in participating in the WCS. However, there is no guarantee that they would report its private information (the battery state) to the BS honestly. In practice, the issue is that Helper-Txs may exaggerate their private information to enhance their chance to be selected, hoping to maximize their transmission time in the data link.

(ii) *Trustworthy Challenge*. A selected jammer may transmit a partial (or even none) jamming signal due to various reasons. We call it an *untrusted* friendly jammer. An untrusted jammer cannot improve the secrecy performance of the WCS. In addition, an untrusted jammer can obtain undeserved utility, leading to unfairness to other trustworthy jammers.

To address these challenges, we propose a framework as shown in Figure 2, consisting of *Auction Scheme*, *Jamming Detection*, and *Trust Management*. The auction scheme is introduced in Section 4 to prevent Helper-Txs from cheating so that Helper-Txs are self-enforced to reveal the truth. Jamming detection is investigated in our previous work [40], where the EC is adopted to detect whether the artificial noise is absent or present by using an energy detection method. In Section 5, we adopt trust management to evaluate the trustworthiness of Helper-Tx and select a trustworthy jammer.

4. Auction Scheme

In this section, we utilize the reverse auction scheme to incentivize Helper-Txs to report their private information truthfully. In the reverse auction scheme, the number of jammers (K) is a critical parameter for the jammer selection. Therefore, we first investigate the optimal number of K so that the BS can select an appropriate number of Helper-Txs as jammers. Next, we consider the utility design of the reverse auction scheme in the CP case and UBM case. In both two cases, we prove that the reverse auction scheme satisfies IC and IR.

4.1. Optimal Number of Jammers. In this paper, it is assumed that Helper-Txs are independent and competing with each other. Therefore, we do not consider that there is cooperation between K jammers. Furthermore, if there is cooperation between multiple Helper-Txs, then we consider these cooperative Helper-Txs as a more powerful Helper-Tx that is competing with other Helper-Txs. It can be obtained that different K can lead to different results in the total secrecy rate. In this paper, we only investigate the optimal number of jammers in the case with perfect CSI, provided that the result is no difference from the case with statistical CSI. Specifically, in the case with perfect CSI, we can obtain the achieved SINRs of Helper-Tx$_n$ at user$_1$ and Eve as

$$\gamma_{u,n} = \frac{\mathrm{Tr}(\mathbf{W}_b \mathbf{H}_{b,u})}{\mathrm{Tr}\left(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}\right) + \delta_u^2}, \qquad \gamma_{e,n} = \frac{\mathrm{Tr}(\mathbf{W}_b \mathbf{H}_{b,e})}{\mathrm{Tr}\left(\mathbf{W}_{j_n} \mathbf{H}_{j_n,e}\right) + \delta_e^2}, \tag{2}$$

where $\mathbf{H}_{b,u} = \mathbf{h}_{b,u}\mathbf{h}_{b,u}^H$, $\mathbf{H}_{b,e} = \mathbf{h}_{b,e}\mathbf{h}_{b,e}^H$, $\mathbf{H}_{j_n,u} = \mathbf{h}_{j_n,u}\mathbf{h}_{j_n,u}^H$, $\mathbf{H}_{j_n,e} = \mathbf{h}_{j_n,e}\mathbf{h}_{j_n,e}^H$, $\mathbf{W}_b = \mathbf{w}_b\mathbf{w}_b^H$, and $\mathbf{W}_{j_n} = \mathbf{w}_{j_n}\mathbf{w}_{j_n}^H$.

The achievable secrecy rate is defined as the transmission rate at which Eve is unable to decode the transmitted message [41]. It is equal to the capacity difference between the data link and the wiretap link. Thus, the secrecy rate achieved by Helper-Tx$_n$ can be calculated as

$$R_{s,n} = \left[\log_2\left(1 + \gamma_{u,n}\right) - \log_2\left(1 + \gamma_{e,n}\right)\right]^+. \tag{3}$$

Let $q_n = \gamma_{u,n}/\gamma_{e,n}$. Sort q_n in a descending order, and get $q_1 \geq q_2 \cdots \geq q_N$, $q_n \in \{q_1, q_2, \cdots q_N\}$. Based on (3), we can obtain that the Helper-Tx which has a larger q_n also has a larger $R_{s,n}$. It is assumed that Helper-Tx$_1$ is the best jammer which has the largest secrecy rate, Helper-Tx$_2$ is the second best, and so forth. Thus, the jammer selection scheme is designed as follows:

Step 1. Select Helper-Tx$_1$ as a jammer. Let $n = 1$ and calculate $\Psi_1 = (1 + \gamma_{u,1})/(1 + \gamma_{e,1})$.

Step 2. For $1 \leq n \leq N - 1$, calculate $\Psi_{n+1} = (1 + \gamma_{u,\{1,2\cdots n+1\}})/(1 + \gamma_{e,\{1,2,\cdots n+1\}})$, where

$$\gamma_{u,\{1,2\cdots n+1\}} = \frac{\mathrm{Tr}(\mathbf{W}_b \mathbf{H}_{b,u})}{\sum_{k=1}^{n+1}\mathrm{Tr}\left(\mathbf{W}_{j_k} \mathbf{H}_{j_k,u}\right) + \delta_u^2}, \qquad \gamma_{e,\{1,2\cdots n+1\}} = \frac{\mathrm{Tr}(\mathbf{W}_b \mathbf{H}_{b,e})}{\sum_{k=1}^{n+1}\mathrm{Tr}\left(\mathbf{W}_{j_k} \mathbf{H}_{j_k,e}\right) + \delta_e^2}. \tag{4}$$

If $\Psi_n < \Psi_{n+1}$, proceed to Step 3, and if $\Psi_n \geq \Psi_{n+1}$, skip to Step 4.

Step 3. Select Helper-Tx$_{n+1}$ as jammer, then let $n = n + 1$ and go back to Step 2.

Step 4. Let $K = n$ and stop.

Proposition 1. *The optimal secrecy rate can be achieved by selecting $K = 1$ Helper-Tx as jammer, where $K = 1$ is decided by the process above.*

Proof. See the appendix.

From the Proposition 1, we can obtain that the BS may only select a single best Helper-Tx as jammer. More than one jammer would lead to a reduction in the secrecy rate of the WCS.

4.2. Utility Design and Objective

4.2.1. Utility of the BS with Perfect CSI. For each Helper-Tx$_n$, the utility of the BS can be characterized as:

$$U_{B,n} = aR_{s,n} - \pi_n R_{s,n} - C_n\left(P_{j_n}\right), \tag{5}$$

where a is the revenue per unit secrecy rate obtained by the BS from a user. π_n is the payment per unit secrecy rate for the jammer. $C_k(P_{j_n})$ is the monetary cost incurred due to the interference caused by the jammer.

4.2.2. Utility of the BS with Statistical CSI. In this section, we focus on the utility design in the case with statistical CSI. As we only know statistical CSI of the wiretap link, the beamforming vectors of the BS and the jammer are both designed as homogeneous isotropic. The CSI of Helper-Tx$_n$ is denoted as $g_n = \{\mathbf{h}_{j_n,u}, \delta_{j_n,e}^2\}$. Specifically, it means that $\mathbf{h}_{j_n,e}$ have the covariance matrices $\delta_{j_n,e}^2\mathbf{I}_{N_j}$ i.e., $\mathbf{h}_{j_n,e} \sim \mathscr{CN}(0, \delta_{j_n,e}^2\mathbf{I}_{N_j})$. $\mathbf{h}_{b,e}$ have the covariance matrices $\delta_{b,e}^2\mathbf{I}_{N_b}$, i.e., $\mathbf{h}_{b,e} \sim \mathscr{CN}(0, \delta_{b,e}^2 \mathbf{I}_{N_b})$. In this case, the accurate secrecy rate cannot be calculated. Instead, we calculate the probabilities of the transmission and secrecy outage events. On the basis of the probabilities, the utility of the BS is defined as efficient transmission throughput (ETT), which can be found in our previous work [40].

When Helper-Tx$_n$ is selected as a jammer, the instantaneous output SINRs at user$_1$ and Eve are calculated as follows

$$\zeta_{u,n} = \frac{P_b\|\mathbf{h}_{b,u}\|^2}{P_{j_n}\|\mathbf{h}_{j_n,u}\|^2 + \delta_u^2} = \frac{\psi_{b,u}}{\psi_{j_n,u} + 1}, \qquad \zeta_{e,n} = \frac{P_b\|\mathbf{h}_{b,e}\|^2}{P_{j_n}\|\mathbf{h}_{j_n,e}\|^2 + \delta_e^2} = \frac{\psi_{b,e}}{\psi_{j_n,e} + 1}, \tag{6}$$

where

$$\psi_{p,q} = \frac{P_b \|\mathbf{h}_{p,q}\|^2}{\delta_q^2}, p \in \{b, j_n\}, q \in \{u, e\}. \quad (7)$$

In (7), $P_p = \mathbf{w}_p^H \mathbf{w}_p$ are the transmit powers of the BS and the jammer. $\psi_{p,q}$ represents the instantaneous signal to noise ratios (SNRs) from node p to node q. As the CSI $\{\mathbf{h}_{b,u}, \mathbf{h}_{j_n,u}\}$ are perfectly known, we can calculate the transmission rate of BS as $R_{u,n} = \log_2(1 + \zeta_{u,n})$. For the statistical CSI $\{\mathbf{h}_{b,e}, \mathbf{h}_{j_n,e}\}$, according to equation (26) in our previous work [40], we can obtain the probability density function of $\zeta_{e,n}$ expressed as $f_{\zeta_{e,n}}(w)$.

To evaluate the secrecy performance, we adopt Wyner's encoding scheme with the target transmission rate $\bar{R}_u$ and the target secrecy rate $\bar{R}_s$ [42]. The difference between $\bar{R}_u$ and $\bar{R}_s$ is used as a redundancy rate against eavesdropping. Therefore, the user can decode the received signal with arbitrarily low error rate only if the instantaneous capacity of the user is larger than the transmission rate, i.e., $R_{u,n} > \bar{R}_u$; otherwise, a transmission outage event occurs. Besides, secrecy outage may occur when the instantaneous capacity of Eve is larger than the redundance rate, i.e., $R_{e,n} = \log_2(1 + \zeta_{e,n}) > \bar{R}_u - \bar{R}_s$. The probabilities of the transmission and secrecy outage events provided by Helper-Tx$_n$ are denoted as P_{st}^n and P_{out}^n, respectively. We can obtain the probability of transmission event as

$$P_{\text{st}}^n = \Pr\left(R_{u,n} > \bar{R}_u\right) = \begin{cases} 1, & R_{u,n} > \bar{R}_u, \\ 0, & R_{u,n} \le \bar{R}_u. \end{cases} \quad (8)$$

The secrecy outage probability can be derived as

$$P_{\text{out}}^n = \Pr\left(\zeta_{e,n} > \xi_e\right) = \int_{\xi_e}^{+\infty} f_{\zeta_{e,n}}(w)\,dw, \quad (9)$$

where $\xi_e = 2^{\bar{R}_u - \bar{R}_s} - 1$. Thus, the ETT that Helper-Tx$_n$ can provide is expressed as

$$T_n = R_{u,n} P_{st}^n (1 - P_{\text{out}}^n) = \begin{cases} R_{u,n}(1 - P_{\text{out}}^n), & R_{u,n} > \bar{R}_u, \\ 0, & R_{u,n} \le \bar{R}_u. \end{cases} \quad (10)$$

4.2.3. Utility of the Jammer. In the perfect CSI case, when Helper-Tx$_n$ is selected as a jammer, its utility is given by:

$$U_{b_n,n} = \pi_n R_{s,n} - E_n, \quad (11)$$

where $\pi_n R_{s,n}$ is the payment made by the BS to the jammer. E_n is the energy cost incurred by the jammer. In the statistical CSI case, the only difference in the utility of jammer is to replace the secrecy rate with ETT. Let P_{j_n} denotes the transmission power of Helper-Tx$_n$; we assume that the energy cost is a linear function of P_{j_n} and is expressed as:

$$U_{b_n,n} = \pi_n R_{s,n} - b_n P_{j_n}, \quad (12)$$

where b_n is the cost per unit power, i.e., the valuation that Helper-Tx$_n$ has for its power. In general, Helper-Tx$_n$ with a lower battery power would value its power highly and assign a higher b_n.

4.2.4. Objective. In this subsection, our objective is to design reverse auctions for the BS to select a jammer. Specifically, the auction has to satisfy IR and IC. IR means that each Helper-Tx gets a positive utility under any outcome of the auction. An auction satisfies IC if revealing its true valuation (b_n) is the dominant strategy for each Helper-Tx. To design reverse auctions that satisfy IC and IR, we consider two cases:

(a) *CP Case*. In this case, the BS assigns a fixed transmission power (P_j^c) to each Helper-Tx. In general, the BS needs to do secrecy rate maximization to design an optimal transmission power of a selected jammer. Although the optimal transmission power design leads to a higher secrecy performance, there is higher computational complexity when the number of Helper-Tx increases. In the process of auction scheme, it is necessary to evaluate the secrecy performance that each Helper-Tx can achieve and selects a suitable one as candidate. In fact, the optimal transmission power design needs to be completed on all Helper-Txs. Therefore, for the optimal power allocation design, there is higher computational complexity when the number of Helper-Tx increases. For the constant power case, we can allocate a fixed power to each Helper-Tx and evaluate the secrecy performance of all Helper-Txs. As an alternative, the constant power allocation with lower computational complexity is easier to implement, and the loss in performance is acceptable.

(b) *UBM Case*. In this case, we aim to design a reverse auction scheme to approximately maximize the utility of the BS.

4.3. Auction Scheme. In this section, we present the reverse auction scheme for the CP case and UBM case.

4.3.1. CP Case. In the CP case, the Vickrey auction selects a Helper-Tx with the lowest price $b_n P_j^c$. However, the Vickrey auction has several limitations shown as follows:

Secrecy performance: the Vickrey auction scheme ignores the secrecy performance achieved by a jammer.

Utility: from (5), the utility of the BS is an increasing function of the secrecy rate, which means that the Vickrey auction scheme also ignores the utility of the BS.

Interference: the Vickrey scheme does not consider the interference cost to the BS.

To avoid the above limitations, we utilize the reverse auction scheme in the CP case to select a Helper-Tx as a jammer.

Lemma 2. *The utility of the auction winner Helper-Tx$_i$ can be given by:*

$$U_{b_i,i} = W^{\setminus i}_{w_{\min}} R^c_{s,i} - b_i P^c_j, \tag{13}$$

Proof. The utility of a selected Helper-Tx$_n$ is expressed as:

$$U_{b_n,n} = \pi_n R_{s,n} - b_n P^c_j. \tag{14}$$

Each Helper-Tx reports its valuation b_n, and we calculate the weight of each Helper-Tx as:

$$W_n = \frac{b_n P^c_j}{R^c_{s,n}}, \tag{15}$$

where $R^c_{s,n}$ is calculated for each Helper-Tx with a fixed transmission power P^c_j. We denote that

$$w_{\min} = \arg \min_{n \in N} W_n, \tag{16}$$

we select Helper-Tx$_{w_{\min}}$ as the auction winner that is functioned as a jammer. For a Helper-Tx$_i$, it is assumed that

$$w^{\setminus i}_{\min} = \arg \min_{n \in N, n \neq i} W_n, \tag{17}$$

where $w^{\setminus i}_{\min}$ represents the auction winner when Helper-Tx$_i$ does not participate in the auction. We define that for the auction winner Helper-Tx$_i$, the payment is given by:

$$p_i = W^{\setminus i}_{w_{\min}} R^c_{s,i}, \tag{18}$$

thus the utility of the auction winner Helper-Tx$_i$ is calculated as:

$$U_{b_i,i} = W^{\setminus i}_{w_{\min}} R^c_{s,i} - b_i P^c_j. \tag{19}$$

Proposition 3. *The reverse auction in the CP case satisfies IR and IC.*

Proof. When Helper-Tx$_i$ is the auction winner, from (19), we can obtain that

$$U_{b_i,i} = W^{\setminus i}_{w_{\min}} R^c_{s,i} - b_i P^c_j \geq W_{w_{\min}} R^c_{s,i} - b_i P^c_j = W_i R^c_{s,i} - b_i P^c_j = 0. \tag{20}$$

We can obtain that $U_{b_n,n} \geq 0$ for Helper-Tx$_n$ so that participating in the reverse auction is the optimal choice for each Helper-Tx$_n$. Thus, the reverse auction in the constant case satisfies IR.

If Helper-Tx$_i$ is the auction winner whether reporting true valuation b_i or false valuation $\widehat{b}_i < b_i$, we can obtain from (19) that Helper-Tx$_i$ cannot change its utility. In addition, let us consider the case that Helper-Tx$_i$ is not the auction winner when it reports its true valuation b_i. We assume that Helper-Tx$_i$ is the auction winner when it reports a false valuation $\widehat{b}_i < b_i$. In this case, we can obtain that

$$\widehat{W}_{w_{\min}} < W_{w_{\min}} = W^{\setminus i}_{w_{\min}}, \tag{21}$$

then, the utility of Helper-Tx$_i$ is calculated as

$$\widehat{U}_{b_i,i} = W^{\setminus i}_{w_{\min}} R^c_{s,i} - b_i P^c_j = W_{w_{\min}} R^c_{s,i} - b_i P^c_j < 0. \tag{22}$$

Therefore, reporting the true valuation $\widehat{b}_n = b_n$ is the dominant strategy for each Helper-Tx$_n$, which means that the reverse auction satisfies IC in the CP case.

In this paper, the utility of the jammer is converted into spectrum resources, i.e., the transmission time in the primary channel. Therefore, we can obtain that

$$\nu U_{b_i,i} = (1 - \beta_i) T, \tag{23}$$

where ν is the transmission time per utility of the jammer. Therefore, we can obtain the transmission time fraction of Helper-Tx$_i$ expressed as:

$$\beta_i = 1 - \frac{\nu U_{b_i,i}}{T} = 1 - \frac{\nu \left(W^{\setminus i}_{w_{\min}} R^c_{s,i} - b_i P^c_j \right)}{T}. \tag{24}$$

4.3.2. UBM Case. In the UBM case, we aim to approximately maximize the BS's utility. As the Vickrey auction does not specify how the transmit power of the jammer, it is not applicable in this case. Therefore, in this subsection, we utilize the reverse auction scheme in the case that BS requests a jammer to transmit at a power that approximately maximize the BS's utility.

Let P_{j_n} denote the power at which the BS requires Helper-Tx$_n$ to transmit. The utility of Helper-Tx$_n$ can be expressed as:

$$U_{b_n,n} = \pi_n R_{s,n} - b_n P_{j_n}. \tag{25}$$

The utility of the BS can be calculated as:

$$U_{B,n} = (a - \pi_n) R_{s,n} - C_n \left(P_{j_n} \right). \tag{26}$$

As the reverse auction satisfies IR, we can obtain that $U_{b_n,n} \geq 0$, i.e., $\pi_n R_{s,n} \geq b_n P_{j_n}$. From (26), the utility of the BS is maximized when $\pi_n R_{s,n} = b_n P_{j_n}$; thus, the maximum contribution to the utility of the BS when Helper-Tx$_n$ is selected as a jammer and transmits at power P_{j_n} can be expressed as:

$$U_{B,n} = a R_{s,n} - b_n P_{j_n} - C_n \left(P_{j_n} \right). \tag{27}$$

In (34), the only variable is P_{j_n}; thus, we aim to find the optimal transmit power to maximizes $U_{B,n}$. Specifically, we focus the secrecy rate maximization to obtain the optimal transmit power to approximately maximize the utility of the BS. To obtain the optimal secrecy rate, we formulate an optimal beamforming design problem, which is divided into a two-part optimization problem. By solving this two-part optimization problem, we can obtain the optimal beamforming vectors of the BS and the jammer.

When a Helper-Tx (e.g., Helper-Tx$_n$) is selected as a jammer, the achievable secrecy rate can be calculated as

$$R_{s,n} = \left[\log_2\left(1+\gamma_{u,n}\right) - \log_2\left(1+\gamma_{e,n}\right)\right]^+. \tag{28}$$

where

$$\begin{aligned} \gamma_{u,n} &= \frac{\mathrm{Tr}(\mathbf{W}_b\mathbf{H}_{b,u})}{\mathrm{Tr}\left(\mathbf{W}_{j_n}\mathbf{H}_{j_n,u}\right)+\delta_u^2}, \\ \gamma_{e,n} &= \frac{\mathrm{Tr}(\mathbf{W}_b\mathbf{H}_{b,e})}{\mathrm{Tr}\left(\mathbf{W}_{j_n}\mathbf{H}_{j_n,e}\right)+\delta_e^2}, \end{aligned} \tag{29}$$

where $\mathbf{H}_{j_n,u} = \mathbf{h}_{j_n,u}\mathbf{h}_{j_n,u}^H$ and $\mathbf{H}_{j_n,e} = \mathbf{h}_{j_n,e}\mathbf{h}_{j_n,e}^H$.

To obtain the optimal beamforming vectors of the BS and Helper-Tx$_n$, the secrecy rate maximization problem is mathematically characterized as

$$2 \max_{\mathbf{W}_b,\mathbf{W}_{jn}} \quad R_{s,n}, \tag{30a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\mathbf{W}_{jn}\mathbf{H}_{j_n,u}\right) \le \Gamma, \tag{30b}$$

$$\mathrm{Tr}(\mathbf{W}_b) \le P_b^m, \tag{30c}$$

$$\mathrm{Tr}\left(\mathbf{W}_{jn}\right) \le P_j^m, \tag{30d}$$

$$\mathrm{rank}\ (\mathbf{W}_b) = 1, \tag{30e}$$

$$\mathrm{rank}\ \left(\mathbf{W}_{jn}\right) = 1, \tag{30f}$$

where (30b) is the interference temperature limit (Γ) imposed at user$_1$ from the jammer. (30c) and (30d) are the transmit power limits of the BS and Helper-Tx$_n$, respectively. (30e) and (30f) are rank-one constraints of beamforming vectors $\mathbf{W}_b$ and $\mathbf{W}_{jn}$, respectively. Actually, the nulling beamformer designed at Helper-Txs is a suboptimal solution that cannot achieve the optimal secrecy performance, which has been demonstrated in the literature. Specifically, based on (30b), the optimal beamforming vector of artificial noise can guarantee that the resulting interference power at the legitimate user is kept below the interference temperature limit, which can achieve a similar effect to nulling beamformer.

In this subsection, we come up with a solution to the secrecy rate maximization problem. Due to fractional forms in the objective function, problem (30) is nonconvex and difficult to solve. First, we introduce a slack variable $\tau = \gamma_{e,n}$, and problem (30) can be equivalently transformed into

$$2 \max_{\mathbf{W}_b,\mathbf{W}_{jn},\tau} \quad \frac{1+\gamma_{u,n}}{1+\tau}, \tag{31a}$$

$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{W}_b\mathbf{H}_{b,e}) \le \tau\left(\mathrm{Tr}\left(\mathbf{W}_{jn}\mathbf{H}_{j_n,e}\right)+\delta_e^2\right), \tag{31b}$$

$$\mathrm{Tr}\left(\mathbf{W}_{jn}\mathbf{H}_{j_n,u}\right) \le \Gamma, \tag{31c}$$

$$\mathrm{Tr}(\mathbf{W}_b) \le P_b^m, \tag{31d}$$

$$\mathrm{Tr}\left(\mathbf{W}_{jn}\right) \le P_j^m, \tag{31e}$$

$$\mathrm{rank}\ (\mathbf{W}_b) = 1, \tag{31f}$$

$$\mathrm{rank}\ \left(\mathbf{W}_{jn}\right) = 1. \tag{31g}$$

Based on [39], problem (31) can be solved optimally by reformulating it into a two-part optimization problem. The outer part is a one-dimensional line search problem with τ, i.e.,

$$\begin{aligned} f(\tau) &= \max_{\tau} \quad \frac{1+\mathrm{G}(\tau)}{1+\tau}, \\ &\text{s.t.} \quad 0 \le \tau \le \mathrm{Tr}(\mathbf{H}_{b,u})P_b^m, \end{aligned} \tag{32a}$$

where $G(\tau)$ is the objective function of the inner part optimization problem to be described below. The lower bound about τ can be obtained directly from (31b), i.e., $0 \le \mathrm{Tr}(\mathbf{W}_b \mathbf{H}_{b,e})/(\mathrm{Tr}(\mathbf{W}_{jn}\mathbf{H}_{j_n,e})+\delta_e^2) \le \tau$. The upper bound is derived from the fact that the secrecy rate is greater than or equal to zero, i.e., $\tau \le \mathrm{Tr}(\mathbf{W}_b\mathbf{H}_{b,u})/(\mathrm{Tr}(\mathbf{W}_{jn}\mathbf{H}_{j_n,u})+\delta_u^2) \le \mathrm{Tr}(\mathbf{H}_{b,u}) P_b^m$. For a fixed τ, the inner part can be expressed as

$$\begin{aligned} G(\tau) &\triangleq \max_{\mathbf{W}_b,\mathbf{W}_{jn}} \quad \frac{\mathrm{Tr}(\mathbf{W}_b\mathbf{H}_{b,u})}{\mathrm{Tr}\left(\mathbf{W}_{jn}\mathbf{H}_{j_n,u}\right)+\delta_u^2}, \\ &\text{s.t.} \quad (36\text{b}) - (36\text{g}). \end{aligned} \tag{33a}$$

Suppose that we can obtain $G(\tau)$ by solving problem (33) for any fixed τ. Then, we can solve problem (32) by applying the one-dimensional line search method, e.g., Golden Section Search to the interval $[0, \mathrm{Tr}(\mathbf{H}_{b,u})P_b^m]$. Therefore, the key step lies in computing $\mathrm{G}(\tau)$ for a fixed τ, which requires solving the nonconvex problem (33). Applying the semidefinite relaxation (SDR) technique, problem (33) can be solved by dropping two rank-one constraints [43]. When the problem (33) is solved, we can obtain the optimal solution of problem (30), i.e., $(\mathbf{W}_b^\star, \mathbf{W}_{j_n}^\star)$.

Therefore, the optimal transmit power of jammer is $P_{j_n}^\star$ $=\mathrm{Tr}(\mathbf{W}_{j_n}^\star)$. Then, the maximum contribution to the utility of the BS from the jammer is:

$$U_{B,n}^\star = aR_{s,n}^\star - b_nP_{j_n}^\star - C_n\left(P_{j_n}^\star\right). \tag{34}$$

In the reverse auction, each Helper-Tx$_n$ reports its valuation b_n to the BS. Then, we calculate the approximately maximized utility of the BS $U_{B,n}^\star$. We denote that

$$w_{\max} = \arg\ \max_{n\in N} U_{B,n}^\star. \tag{35}$$

In this case, we select Helper-Tx$_{w_{\max}}$ as the auction winner. For Helper-Tx$_i$, we assume that

$$w_{\max}^{\backslash i} = \arg \max_{n \in N, n \neq i} U_{B,n}^{\star}. \tag{36}$$

When Helper-Tx$_i$ is the auction winner, the payment is given by:

$$p_i = U_{B,i}^{\star} - U_{B,w_{\max}}^{\backslash i\star} + b_i P_{j_i}^{\star}, \tag{37}$$

Then, the utility of Helper-Tx$_i$ can be calculated as:

$$U_{b_i,i} = U_{B,i}^{\star} - U_{B,w_{\max}}^{\backslash i\star}. \tag{38}$$

In the UBM case, the reverse auction scheme also satisfies IR and IC. The proof is similar to Proposition 3, which is omitted here.

Similarly, in the UBM case, we can obtain the transmission time fraction of Helper-Tx$_i$ expressed as:

$$\beta_i = 1 - \frac{\nu\left(U_{B,i}^{\star} - U_{B,w_{\max}}^{\backslash i\star}\right)}{T}. \tag{39}$$

To ensure that the selected Helper-Tx$_w$ (auction winner) is trustworthy as a jammer, we would evaluate the Helper-Tx's trustworthiness in the next section.

5. Trust Management and Jammer Selection

In this framework, we apply two trustworthiness metrics, i.e., the trust category and the trust degree to evaluate the trustworthiness of Helper-Tx$_w$. Based on these two trustworthiness metrics, we can select a trustworthy Helper-Tx as a jammer.

5.1. Trust Category. Helper-Tx$_w$ is given an initial reputation r_0. In general, the value of r_0 is half less than the maximum value of the reputation, i.e., $0 \leq r_0 \leq 0.5$. The reason is that a high value may bring selfish behavior while a low value may be unfair to a newly joined Helper-Tx.

According to detection results, some policies can be adopted to encourage Helper-Tx$_w$ to cooperate. Specifically, the EC takes an additive increase/multiplicative decrease (AIMD) mechanism to update Helper-Tx$_w$'s reputation based on the energy detection results [44]. The AIMD mechanism consists of reward and penalty; then, Helper-Tx$_w$'s reputation can be updated as

$$\begin{aligned} r_{l,w} &= \left[\rho_1 r_{l-1,w} + \rho_2 (1 - e_{l,w}) - e_{l,w}(\rho_2 p r_{l-1,w})\right]^+, \\ &= \left[\rho_1 r_{l-1,w} + \rho_2 (1 - e_{l,w} - e_{l,w} p r_{l-1,w})\right]^+, \end{aligned} \tag{40}$$

where $l = 1, 2, 3 \cdots R$, ρ_1 and ρ_2 are weight factors that satisfy $\rho_1 + \rho_2 = 1$. They can be changed based on the requirement of the WCS. When the long term of the reputation plays a more important role, we increase ρ_1. On the contrary, when the demand for the sensitivity of reputation collection is higher, we increase ρ_2. R is the detection round during the detection duration τ. $r_{l-1,w}$ is the historical reputation of Helper-Tx$_w$, and $r_{l,w}$ is the updated reputation of Helper-T x$_w$. As shown below, $e_{l,w} \in \{0, 1\}$ is the reputation evidence of Helper-Tx$_w$, which depends on the detection result at round l. This reputation evidence can determine whether the AIMD mechanism is reward or penalty. When the detection result shows that there is artificial noise ($\mathscr{H}_1$): $e_{l,w} = 0$, then an additive increase ($\rho_2 * 1$) for the value of the reputation is used. When the detection result shows there is no artificial noise ($\mathscr{H}_0$): $e_{l,w} = 1$, then a multiplicative decrease ($\rho_2 * p * r_{l,w}$) for the value of the reputation is used.

```
Input:$r_0$, $R$;
Output:$\alpha_w$, $C_w$;
Initialize $p = 2$, $\rho_1 = 0.8$, $\rho_2 = 0.2$;
Set $k = 0$, $l = 1$;
The reputation evidence of $l$ round is $e_{l,w}$;
repeat
    $r_l = [\rho_1 r_{l-1,w} + \rho_2 (1 - e_{l,w} - e_{l,w} p r_{l-1,w})]^+$;
    $\hat{e} = e_{l,w} \oplus e_{l+1}$;
    if$\hat{e} = 1$then
        $k = k + 1$;
    end if
      Set $l = l + 1$;
      until$l \geq R$;
      if ($k = 0 \& e_{1,w} = 0$) then
          $C_w = 1$, A reputable user;
else if ($k = 1 \& e_{1,w} = 1$)||($k = 2 \& e_{1,w} = 0$)then
          $C_w = 2$, an unstable user;
else if ($k > 2 \& e_{R,w} = 0$) then
          $C_w = 3$, A selfish user;
else if ($e_{R,w} = 1$) then
      $C_w = 4$, A greedy user;
end if
$\alpha_w = 1/R \sum_{l=1}^{R} r_{l,w}$;
Return $\alpha_w$, $C_w$.
```

Algorithm 1. Classification algorithm.

The value of p is the degree of penalty, which determines how severe is the penalty imposed on Helper-Tx$_w$. The basic setting principle of the AIMD mechanism is to slow down the increasing rate and speed up the decreasing rate of the value of reputation.

Based on the number of inflection points of the reputation update curve and the initial reputation evidence, we propose a classification algorithm as shown in Algorithm 1. Then, Helper-Tx$_w$ can be classified into one of the following four trust categories.

(i) *A Reputable User.* As shown in Figure 3, if the detection results show that Helper-Tx$_w$ continuously sends out the artificial noise, the value of its reputation increases gradually to 1. Then, Helper-Tx$_w$ is considered to be a reputable user.

(ii) *A Selfish User.* As shown in Figure 4, Helper-Tx$_w$'s reputation update curve is serrated, which means that Helper-Tx$_w$ intermittently sends out the

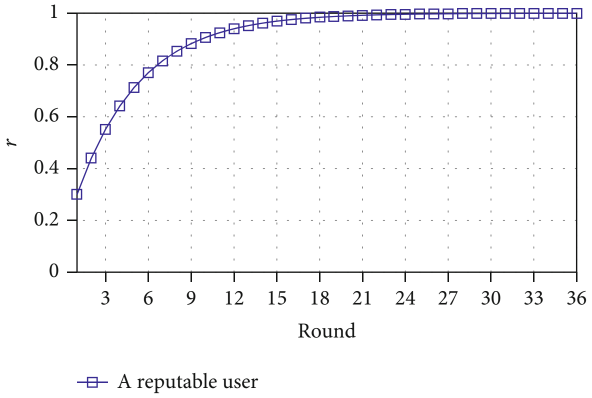


Figure 3: A reputable user.

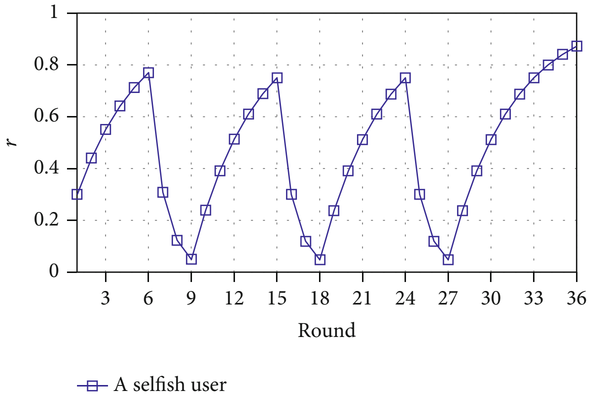


Figure 4: A selfish user.

artificial noise. Then, Helper-Tx$_w$ is considered to be a selfish user.

(iii) *An Unstable User*. As shown in Figure 5, Helper-Tx$_w$ does not send the artificial noise for a while, but it recovers quickly and continues sending the artificial noise. It is assumed that the situation is caused by hardware damage or mobility, and Helper-Tx$_w$ is considered to be an unstable user.

(iv) *A Greedy User*. As shown in Figure 6, we consider Helper-Tx$_w$ as a greedy user if it never sends the artificial noise, or it stops sending out the artificial noise in the middle time and never recovers.

5.2. Trust Degree. To evaluate the trustworthiness of Helper-Tx$_w$, we adopt the concept of trust degree α. The trust degree of Helper-Tx$_w$ is calculated by averaging the reputation, shown as

$$\alpha_w = \frac{1}{R}\sum_{l=1}^{R} r_{l,w}. \tag{41}$$

In the case with perfect CSI, we have to guarantee that Helper-Tx$_w$ is trustworthy enough to reach the target secrecy performance threshold R_s^{th}. In the case with statistical CSI, the target ETT performance threshold is defined as T^{th}. The calculation process of trust degree provides no different from the case with perfect CSI. It means that there is a target trust degree threshold α^{th}. Next, we investigate how to calculate this threshold.

We adopt the concept of expected secrecy rate to evaluate the secrecy performance. When Helper-Tx$_w$ is trusted (the artificial noise is present), the secrecy rate can be expressed as

$$R^t_{s,w} = [\log_2(1+\gamma^t_{u,w})) - \log_2(1+\gamma^t_{e,w})]^+, \tag{42}$$

where the SINRs are expressed as

$$\begin{aligned}\gamma^t_{u,w} &= \frac{\mathrm{Tr}(\mathbf{W}^\star_b \mathbf{H}_{b,u})}{\mathrm{Tr}\left(\mathbf{W}^\star_{j_w}\widehat{\mathbf{H}}_{j_n,u}\right)+\delta_p^2},\\ \gamma^t_{e,w} &= \frac{\mathrm{Tr}(\mathbf{W}^\star_b \mathbf{H}_{b,e})}{\mathrm{Tr}\left(\mathbf{W}^\star_{j_w}\widehat{\mathbf{H}}_{j_n,e}\right)+\delta_e^2}.\end{aligned} \tag{43}$$

When Helper-Tx$_w$ is untrusted (artificial noise is absent), the secrecy rate can be expressed as

$$R^u_{s,w} = [\log_2(1+\gamma^u_{u,w})) - \log_2(1+\gamma^u_{e,w})]^+, \tag{44}$$

where the SINRs are expressed as

$$\begin{aligned}\gamma^u_{u,w} &= \frac{\mathrm{Tr}(\mathbf{W}^\star_b \mathbf{H}_{b,u})}{\delta_p^2},\\ \gamma^u_{e,w} &= \frac{\mathrm{Tr}(\mathbf{W}^\star_b \mathbf{H}_{b,e})}{\delta_e^2}.\end{aligned} \tag{45}$$

In this paper, it is assumed that the trust degree α_w represents the probability that a Helper-Tx sends the artificial noise. Thus, we can obtain the expected secrecy rate as

$$\bar{R}_{s,w} = \alpha_w R^t_{s,w} + (1-\alpha_w)R^u_{s,w}. \tag{46}$$

For the given target secrecy performance threshold R_s^{th}, the expected secrecy rate has to satisfy that

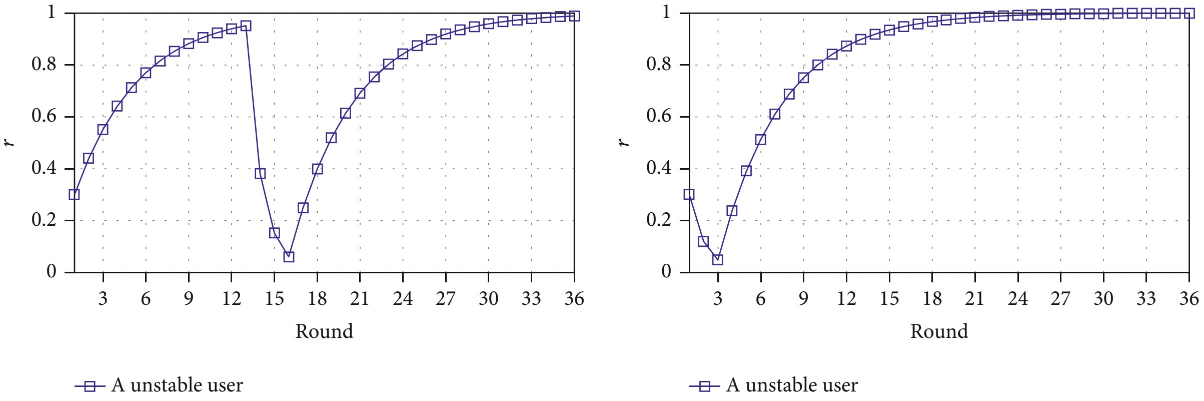
$$\beta_w \bar{R}_{s,w} \geq R_s^{\text{th}}, \tag{47}$$

then we can calculate the target trust degree threshold as

$$\alpha_w \geq \alpha^{\text{th}} = \frac{R_s^{\text{th}} - \beta_w R_s^u}{\beta_w R_s^t - \beta_w R_s^u}. \tag{48}$$

5.3. Jammer Selection. According to the classification algorithm, the trust degree of Helper-Tx$_w$ is updated, and Helper-Tx$_w$ is classified into one of four trust categories. As shown in Figure 2, Helper-Tx$_w$ would be selected as a cooperative friendly jammer if the following conditions are achieved at the same time:

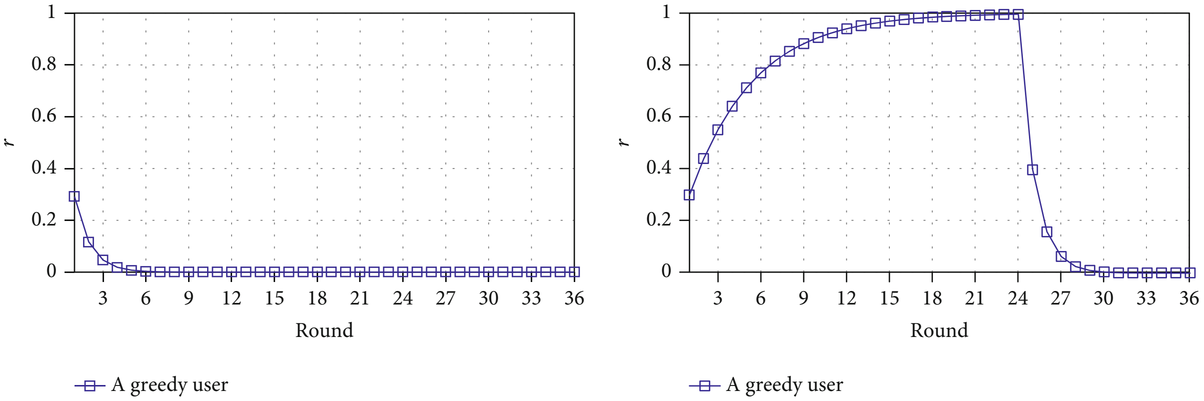
(i) Helper-Tx$_w$'s trust degree satisfies that $\alpha_w \geq \alpha^{\text{th}}$



(a)

(b)

Figure 5: An unstable user.



(a)

(b)

Figure 6: A greedy user.

Table 1: Simulation parameters.

Simulation parameter	Value
The maximum power of the BS P_b^m (dBm)	30
The maximum power of Helper-Tx$_n P_j^m$ (dBm)	30
The number of antennas of the BS	4
The number of antennas of Helper-Tx$_n$	4
The interference temperature limit imposed at user $_1\Gamma$	0.1
The distances between the BS to user $_1$ and Eve $d_{b,u}(d_{b,e})$ (m)	120
The distance between Helper-Tx$_n$ and user $_1 d_{j_n,u}$ (m)	150
The distance between Helper-Tx$_n$ and Eve $d_{j_n,e}$ (m)	100
Noise power spectral density N$_{02}$ (dBm/Hz)	-127
Transmission bandwidth B (MHz)	10

(ii) Helper-Tx$_w$ is classified as a reputable user or an unstable user

Otherwise, Helper-Tx$_w$ would be kicked out of the network, and we go back to the auction scheme to select another Helper-Tx.

6. Numerical Results

In this section, we present some numerical results of the reverse auction and the AIMD algorithm. In this paper, we consider that the WCS is static at a certain time duration. Therefore, it is assumed that the distances between users

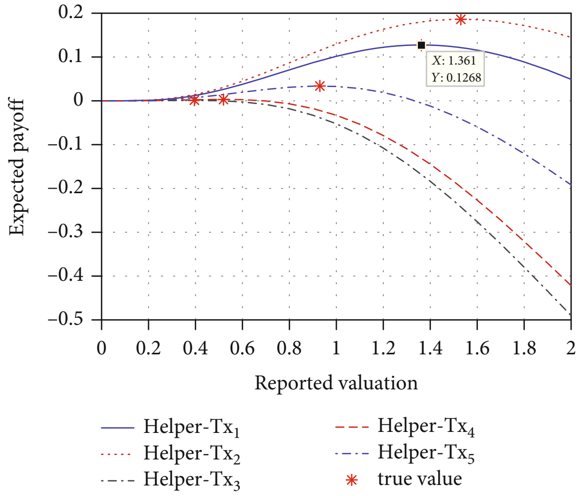


Figure 7: The expected payoff versus the reported valuation.

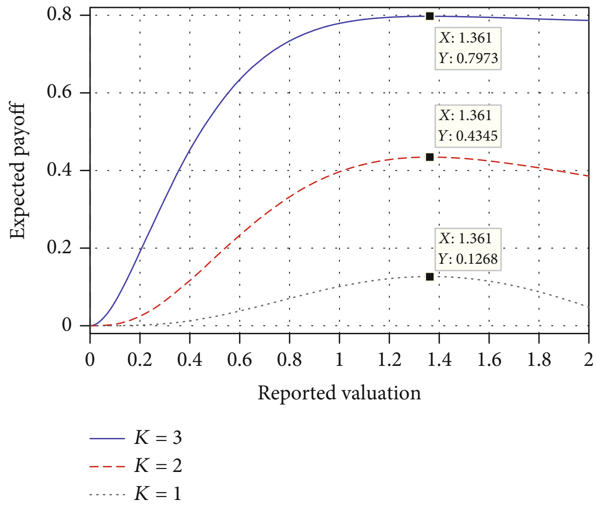


Figure 8: Expected payoff versus the reported valuation of Helper -Tx$_1$ with $K = 1, 2, 3$.

are fixed in this time duration, while the results of a static WCS can be well applied to a dynamic WCS. The simulation parameters are shown in Table 1. The values of these parameters are set according to the general guidelines in the existing literatures.

6.1. Auction Scheme Evaluation. In the WCS, each Helper-Tx reports its private information to the BS. It is assumed that each Helper-Tx does not know the reported valuation of other Helper-Txs. The reported valuation of each Helper-Tx obeys the probability density function: e^{-x_n}, where the random variable $x_n \triangleq v_{-n}(g_{-n})$ ($x_n \in [0,+\infty]$ and $\int_0^{+\infty} e^{-x_n} dn = 1$). In the simulation, we adopt random variable x_k instead of calculating $\pi_n R_{s,n}(n = 1, 2, \cdots N)$. This randomly generated variable does not affect the outcome of the mechanism. For simplicity, we assume that the price paid per unit of secrecy rate is $\pi_n = 1, \forall n$.

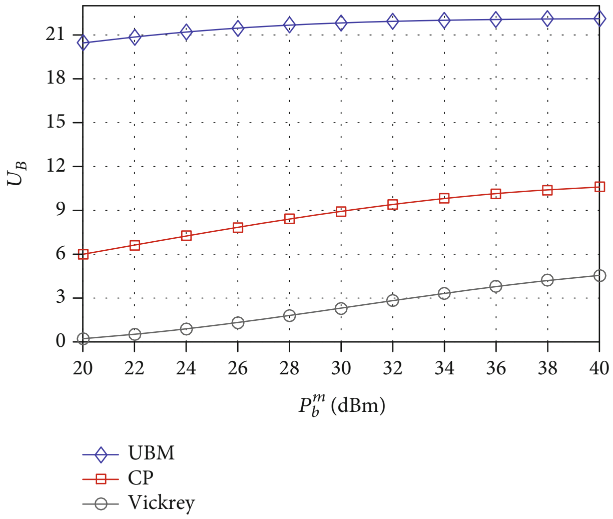


Figure 9: The BS utility under the reverse auction scheme and Vickrey auction.

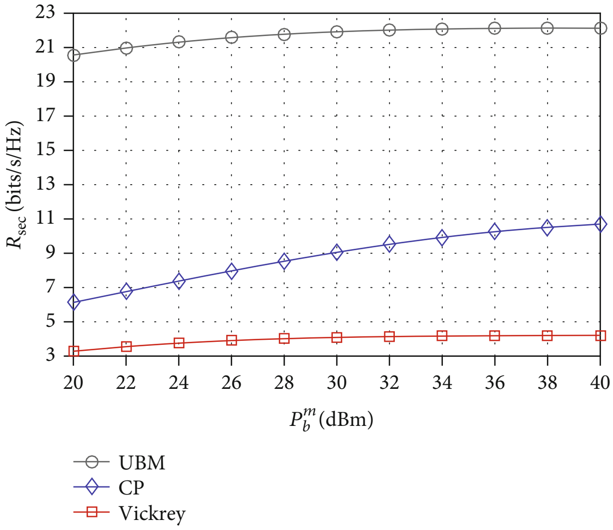


Figure 10: The secrecy performance under the reverse auction scheme for CP case and Vickrey auction.

Specifically, we consider a system with $N = 5$ Helper-Txs, and the BS would select $K = 1$ jammer. A random sample of these jammers' secrecy rates is obtained as [1.3610, 0.5184, 0.3954, 1.5313, 0.9302]. Figure 7 shows the expected payoff of each Helper-Tx versus the reported valuation. Specifically, the payoff of each Helper-Tx is the transmission time to access the data link. At each reported valuation, a large number (10^6) of sample values is randomly generated to calculate the utility of each Helper-Tx. We can obtain that truth-telling is the dominant strategy in the reverse auction. Each Helper-Tx can expect its maximum payoff when reporting its valuation truthfully. For example, the true valuation of Helper-Tx$_2$ is 1.3610, and as we can see in Figure 7, Helper-Tx$_2$ gets the maximum utility 0.1268 when it reports its true valuation. Furthermore, a Helper-Tx with a lager valuation can gain a larger utility. As each selected Helper-Tx$_n$ has to pay a

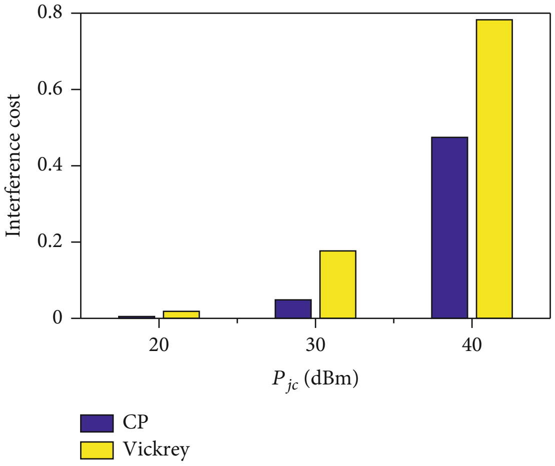


FIGURE 11: The interference cost under the reverse auction scheme for CP case and Vickrey auction.

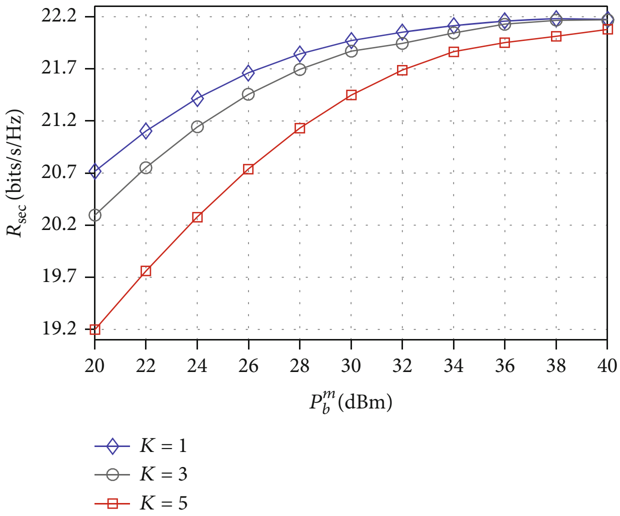


FIGURE 12: Secrecy performance with different number of jammers at the same location.

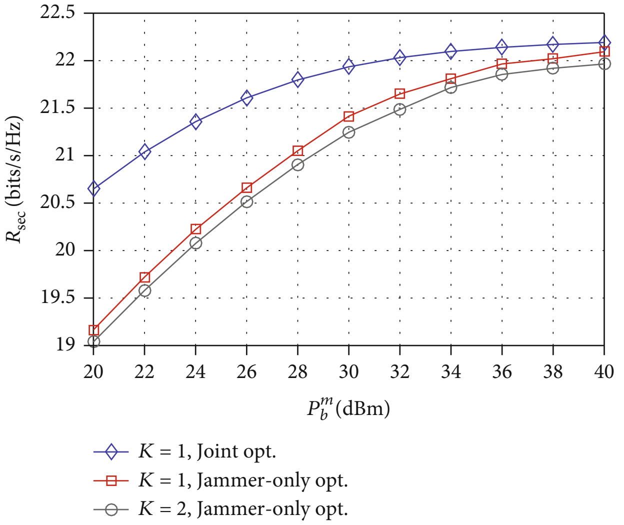


FIGURE 13: Joint beamforming design of the BS and jammers with $K = 1, 2$.

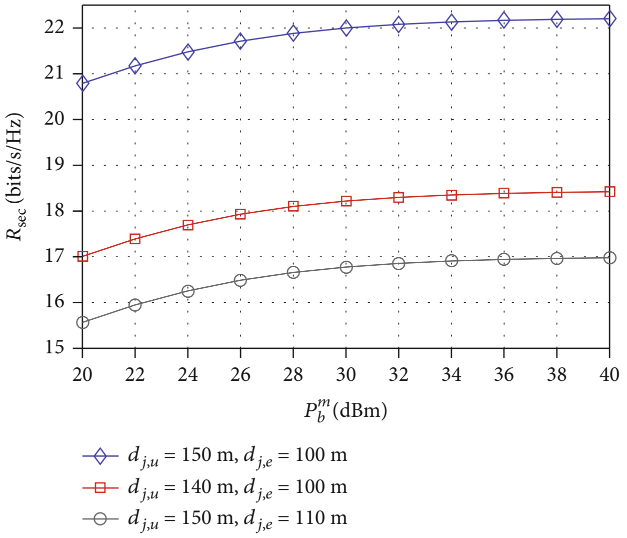


FIGURE 14: Secrecy performance with jammers at different locations.

transfer payment, the maximum expected utility of the Helper-Tx is less than $u_n(\hat{g}_n)$.

In Figure 8, we illustrate the expected utility versus the reported valuation of Helper-Tx$_1$ with different K. It is obtained that Helper-Tx$_1$ gains the maximum expected utility when it reports the true valuation (1.361) with different K. With K increases, Helper-Tx$_1$ gains a higher expected utility. It is because that as K increases, the probability that Helper-Tx$_1$ is being selected as a jammer becomes higher. Furthermore, it is observed that when $K = 3$, the expected utility tends to be fixed as the reported valuation increases.

In Figure 9, we compare the BS's utility under the reverse auction scheme with two cases and the Vickrey auction. It shows that the UBM case outerforms the CP case in terms of the BS's utility. In addition, we can see that for the two cases, the reverse auction scheme outperforms the Vickrey auction scheme. These results show that the reverse auction scheme is valid and has a better performance than the Vickrey auction scheme.

Figure 10 compares the secrecy rate under the reverse auction scheme for UBM case, CP case, and the Vickrey auction scheme. We can see that the reverse auction scheme has a better secrecy performance than the Vickrey auction. It can be explained that our reverse auction takes the secrecy performance of each Helper-Tx into consideration, while the Vickrey auction only considers the price of each Helper-Tx.

In Figure 11, we illustrate the interference cost under CP case and the Vickrey auction scheme. In the UBM case, there is almost no interference cost and can be ignored. It shows that as the transmission power of jammer increases, a higher interference cost is incurred to the BS. In addition, the Vickrey auction scheme causes more interference cost to the BS than the reverse auction scheme. This result shows

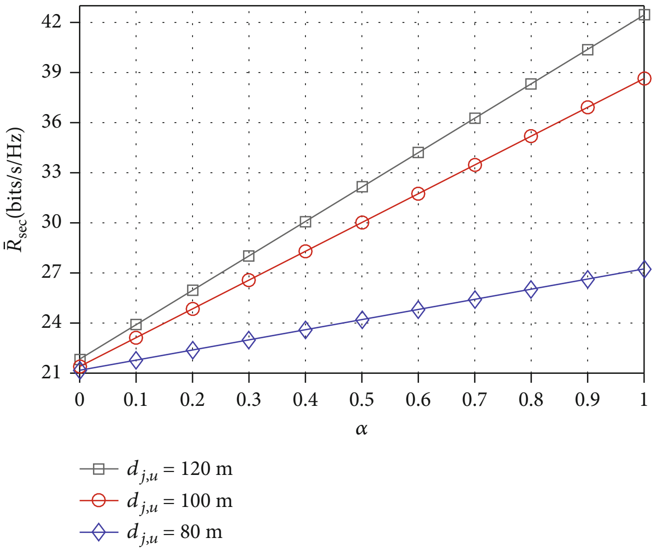


FIGURE 15: The expected secrecy rate versus the trust degree with different $d_{j,u}$.

that the reverse auction scheme has a better performance to degrade the interference to the BS.

6.2. Optimal Beamforming Evaluation in the UBM Case. In this subsection, we focus on the joint beamforming optimization of the BS and jammers. In Figure 12, we illustrate the total secrecy rate versus the transmitted power of the BS with $K = 1, 3, 5$ jammers at the same location ($d_{j_k,p} = 150\,\text{m}$, $d_{j_k,e} = 100\,\text{m}$). It is observed that with the number of jammers increases, the secrecy rate decreases. It means that more jammers can not further improve the secrecy rate. This figure validates the Proposition 1, where the optimal secrecy rate can be achieved by selecting a one best Helper-Tx as jammer, i.e., $K = 1$.

In Figure 13, we compare the secrecy performance of the proposed algorithm ("Joint opt." in the figure) with the jammer-only optimization ("Jammer-only opt.") algorithm. In the proposed algorithm, both the beamforming vector of the BS ($\mathbf{w}_b$) and the beamforming vector of the jammer ($\mathbf{w}_j$) are optimized. In the jammer-only optimization algorithm, the beamforming vector of the BS ($\mathbf{w}_b$) is designed as homogeneous isotropic, and only the beamforming vector of the jammer $\mathbf{w}_j$ is optimized. Figure 13 shows the performance improvement by the proposed joint optimization algorithm compared with the jammer-only optimization algorithm. In this figure, we select $K = 1$ and $K = 2$ jammers at the same location with the jammer-only optimization algorithm. We can obtain that in jammer-only optimization algorithm, more jammers cannot cause more interference to Eve.

In Figure 14, we illustrate the secrecy rate of Helper-Txs at different locations. The location of a Helper-Tx represents its private information (the CSI). It is obvious to see that the secrecy rate would be worse when $d_{j,p}$ decreases or $d_{j,e}$ increases. It can be explained that when $d_{j,p}$ decreases or $d_{j,e}$ increases, the jammer would cause more interference to the data link or less interference to the wiretap link, respectively. This result shows that the location of a Helper-Tx is critical to be selected as a jammer. Thus, a mechanism to make sure each Helper-Tx reports their CSI truthfully is the main task in a jammer selection scheme.

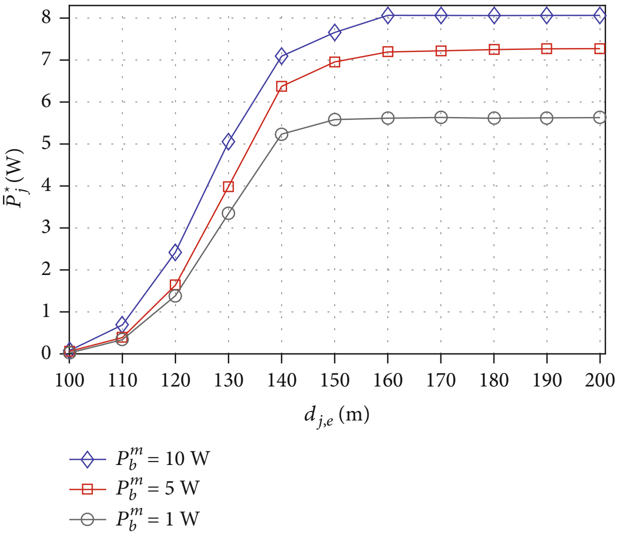


FIGURE 16: The optimal transmitted power of the jammer $\bar{P}_j^\star$ versus $d_{j,e}$.

Figure 15 illustrates the performance comparison with regard to the trust degree for different distances between the jammer and user$_1$. As we can see, the expected secrecy rate increases with a higher trust degree. Thus, we consider a Helper-Tx with a higher trust degree as a more trustworthy friendly jammer. Besides, Figure 15 also leads us to the conclusion that we can get a better expected secrecy rate when the jammer is farther to user$_1$. The reason is that jammer would cause more interference when it is closer to user$_1$, which means the distance is also an important design parameter in the jammer selection scheme.

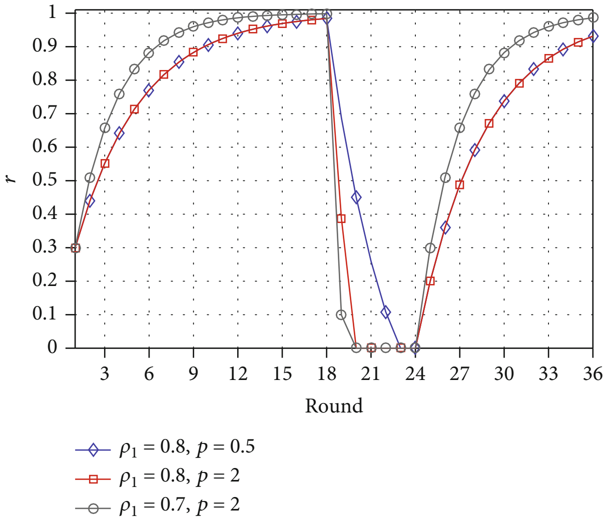


Figure 17: An unstable user: reputation update with different AIMD mechanisms.

In this paper, the jamming distance is defined as the distance between the friendly jammer and Eve, i.e., $d_{j,e}$. It is assumed that Eve is one of legitimate users; thus, we can obtain the jamming distance. In Figure 16, we illustrate the optimal transmit power of the jammer over different maximus power of the BS (P_b^m). Obviously, as P_b^m increases, the jammer should transmit the artificial noise with a higher power. The reason is that the transmited message of a higher power needs more artificial noise to protect. Figure 16 also shows that with the jamming distance increases, a higher transmit power $\bar{P}_j^\star$ of the friendly jammer is required. Then, there is a higher upper bound of the jammer's residual energy. In other words, a jammer farther away from Eve should have more residual energy to guarantee the secrecy performance.

6.3. AIMD Mechanism Evaluation. In Figure 17, taking an unstable user as an example, we illustrate the reputation update process with different kinds of AIMD mechanisms. As we can see in Figure 17, when ρ_1 goes up and ρ_2 goes down, both the rates of increasing and decreasing slow down. In such a situation, the historical reputation plays a more important role while the AIMD mechanism is not sensitive to current reputation. Figure 17 also leads us to the conclusion that when p decreases, the rate of increasing stays the same while the rate of decreasing slows down. As the value of p is the degree of penalty, and it is related to the damage level caused by selfish behavior of a jammer. Thus, a lower value of p means a lower penalty while the reward stays the same.

7. Conclusion

This paper presents a trustworthy friendly jammer selection scheme with truth-telling for WCS. We develop a reverse auction scheme to enforce truth-telling as the dominant strategy for each Helper-Tx. We prove that the BS can achieve the highest secrecy rate by selecting a one best Helper-Tx as the jammer. Furthermore, we introduce trust category and trust degree to evaluate the trustworthiness of each Helper-Tx. We then design a selection scheme based the trust category and trust degree for the EC to select a one best Helper-Tx. Lastly, we present numerical results to demonstrate the performance of our proposed jammer selection scheme. As a part of our future work, we plan to investigate the problem of joint relay and jammer selection in the WCS.

Appendix

Proof of Proposition 1

According to (3), the secrecy rate of the WCS when selecting n Helper-Txs can be expressed as $R_s\{\mathcal{J}_n\} = \log_2(\Psi_n)$. When $n = K$, Ψ_k could be obtained, leading to the largest $R_s\{\mathcal{J}_K\}$. As a result, it is the optimal choice to select K Helper-Txs as jammers in the WCS.

It is assumed that $\mathrm{Tr}(\mathbf{W}_{j_n}\mathbf{H}_{j_n,u}) \gg \delta_u^2$ and $\mathrm{Tr}(\mathbf{W}_{j_n}\mathbf{H}_{j_n,e}) \gg \delta_e^2$. Thus, we can omit δ_u^2 and δ_e^2 in the denominator of $\gamma_{u,n}$ and $\gamma_{e,n}$, respectively. As $q_1 \geq q_2 \cdots \geq q_N$, we could obtain that

$$\begin{aligned}\frac{\gamma_{u,1}}{\gamma_{e,1}} > \frac{\gamma_{u,2}}{\gamma_{e,2}}, &\Rightarrow \frac{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,e}\right)}{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,u}\right)} > \frac{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_2,e}\right)}{\mathrm{Tr}\left(\mathbf{W}_{j_2}\mathbf{H}_{j_2,u}\right)}, \\ &\Rightarrow \mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,e}\right)\mathrm{Tr}\left(\mathbf{W}_{j_2}\mathbf{H}_{j_2,u}\right) \\ &\quad - \mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,u}\right)\mathrm{Tr}\left(\mathbf{W}_{j_2}\mathbf{H}_{j_2,e}\right) > 0.\end{aligned} \tag{A.1}$$

Then, we obtain the result expressed as

$$\begin{aligned}\frac{\gamma_{u,1}}{\gamma_{e,1}} - \frac{\gamma_{u,\{1,2\}}}{\gamma_{e,\{1,2\}}} &= \frac{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,e}\right)}{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,u}\right)} - \frac{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,e}\right) + \mathrm{Tr}\left(\mathbf{W}_{j_2}\mathbf{H}_{j_2,e}\right)}{\mathrm{Tr}\left(\mathbf{W}_{j_1}\mathbf{H}_{j_1,u}\right) + \mathrm{Tr}\left(\mathbf{W}_{j_2}\mathbf{H}_{j_2,u}\right)} > 0, \\ &\Rightarrow \frac{\gamma_{u,1}}{\gamma_{e,1}} - \frac{\gamma_{u,\{1,2\}}}{\gamma_{e,\{1,2\}}} > 0, \Rightarrow \gamma_{u,1}\gamma_{e,\{1,2\}} > \gamma_{e,1}\gamma_{u,\{1,2\}}.\end{aligned} \tag{A.2}$$

It is assumed that $\gamma_{u,1} \gg 1$ and $\gamma_{u,\{1,2\}} \gg 1$. We can compare $\Psi_1 = (1+\gamma_{u,1})/(1+\gamma_{e,1})$ and $\Psi_2 = (1+\gamma_{u,\{1,2\}})/(1+\gamma_{e,\{1,2\}})$ as

$$\begin{aligned}\frac{\Psi_1}{\Psi_2} &= \frac{\left(1+\gamma_{u,1}\right)\left(1+\gamma_{e,\{1,2\}}\right)}{\left(1+\gamma_{e,1}\right)\left(1+\gamma_{u,\{1,2\}}\right)} \approx \frac{\gamma_{u,1}\left(1+\gamma_{e,\{1,2\}}\right)}{\gamma_{u,\{1,2\}}\left(1+\gamma_{e,1}\right)} \\ &= \frac{\left(1/\gamma_{u,\{1,2\}}\right) + \left(\gamma_{e,\{1,2\}}/\gamma_{u,\{1,2\}}\right)}{\left(1/\gamma_{u,1}\right) + \left(\gamma_{e,1}/\gamma_{u,1}\right)} \approx \frac{\gamma_{e,\{1,2\}}/\gamma_{u,\{1,2\}}}{\gamma_{e,1}/\gamma_{u,1}} \\ &= \frac{\gamma_{u,1}\gamma_{e,\{1,2\}}}{\gamma_{e,1}\gamma_{u,\{1,2\}}} > 1 \Rightarrow \Psi_1 > \Psi_2.\end{aligned} \tag{A.3}$$

Thus, $K = 1$ is the optimal choice in the jammer selection scheme, which completes the proof of Proposition 1.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant No. 2019JBZ001, in part by the National Natural Science Foundation of China under Grant No. 61871023 and Grant No. 61931001, and in part by Beijing Natural Science Foundation under Grant 4202054.

References

[1] F. Wang and X. Zhang, "Secure resource allocation for polarizationenabled green cooperative cognitive radio networks with untrusted secondary users," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, Baltimore, MD, USA, 2017.

[2] Y. Wen, T. Jing, Y. Huo, Z. Li, and Q. Gao, "Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 795–799, Maui, HI, USA, March 2018.

[3] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure af relay systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4893–4898, 2015.

[4] S. Cheng, Z. Cai, J. Li, and H. Gao, "Extracting kernel dataset from big sensory data in wireless sensor networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 4, pp. 813–827, 2016.

[5] L. Wang and H. Wu, "Jamming partner selection for maximising the worst D2D secrecy rate based on social trust," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, p. e2992, 2017.

[6] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2016.

[7] X. Zheng, Z. Cai, J. Li, and H. Gao, "A study on applicationaware scheduling in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 7, pp. 1787–1801, 2016.

[8] Z. He, Z. Cai, S. Cheng, and X. Wang, "Approximate aggregation for tracking quantiles and range countings in wireless sensor networks," *Theoretical Computer Science*, vol. 607, pp. 381–390, 2015.

[9] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.

[10] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2016.

[11] Z. Cai, R. Goebel, and G. Lin, "Size-constrained tree partitioning: approximating the multicast k-tree routing problem," *Theoretical Computer Science*, vol. 412, no. 3, pp. 240–245, 2011.

[12] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[13] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[14] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2018.

[15] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2018.

[16] S. Sohaib and M. Uppal, "Full-duplex compress-and-forward relaying under residual self-interference," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2776–2780, 2018.

[17] Z. Chen, P. Fan, and D. O. Wu, "Joint power allocation and strategy selection for half-duplex relay system," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2144–2157, 2017.

[18] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4457–4462, 2017.

[19] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9385–9392, 2018.

[20] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy-efficient beamforming and cooperative jamming in IRS-assisted miso networks," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, Dublin, Ireland, Ireland, June 2020.

[21] Y. Su, X. Lu, Y. Zhao, L. Huang, and X. Du, "Cooperative communications with relay selection based on deep reinforcement learning in wireless sensor networks," *IEEE Sensors Journal*, vol. 19, no. 20, pp. 9561–9569, 2019.

[22] J. Xing, T. Lv, and X. Zhang, "Cooperative relay based on machine learning for enhancing physical layer security," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, Istanbul, Turkey, Turkey, September 2019.

[23] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. S. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[24] Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665–673, 2017.

[25] M. Wen, K. Zhang, J. Lei, X. Liang, R. Deng, and X. Shen, "CIT: a credit-based incentive tariff scheme with fraud-traceability for smart grid," *Security and Communication Networks*, vol. 9, no. 9, pp. 823–832, 2016.

[26] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2789–2800, 2016.

[27] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[28] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, 2012.

[29] Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[30] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Computer Networks*, vol. 102, pp. 157–171, 2016.

[31] J. Deng, R. Zhang, L. Song, Z. Han, and B. Jiao, "Truthful mechanisms for secure communication in wireless cooperative system," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4236–4245, 2013.

[32] Z. Duan, W. Li, X. Zheng, and Z. Cai, "Mutual-preference driven truthful auction mechanism in mobile crowdsensing," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1233–1242, Dallas, TX, USA, USA, July 2019.

[33] M. R. Khandaker, K.-K. Wong, and G. Zheng, "Truth-telling mechanism for two-way relay selection for secrecy communications with energy-harvesting revenue," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3111–3123, 2017.

[34] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *computers & security*, vol. 50, pp. 47–59, 2015.

[35] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2180–2193, 2017.

[36] L. Wang, H. Wu, and G. L. Stuber, "Cooperative jamming-aided secrecy enhancement in p2p communications with social interaction constraints," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1144–1158, 2017.

[37] F. Gao, R. Zhang, Y.-C. Liang, and X. Wang, "Optimal design of learning based mimo cognitive radio systems," in *2009 IEEE International Symposium on Information Theory (ISIT)*, pp. 2537–2541, Seoul, South Korea, July 2009.

[38] B. F. Lo, "A survey of common control channel design in cognitive radio networks," *Physical Communication*, vol. 4, no. 1, pp. 26–39, 2011.

[39] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.

[40] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.

[41] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[42] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[43] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154–1170, 2015.

[44] M. Vojnovic, J. Y. Le Boudec, and C. Boutremans, "Global fairness of additive-increase and multiplicative-decrease with heterogeneous round-trip times," in *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064)*, pp. 1303–1312, Tel Aviv, Israel, 2000.