IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 30, 2020, accepted September 7, 2020, date of publication September 18, 2020, date of current version October 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3025160

A Multi-Domain Anti-Jamming Strategy Using Stackelberg Game in Wireless Relay Networks

YONGCHENG LI[1], SHAOZHUANG BAI[2], (Student Member, IEEE), AND ZHENZHEN GAO[2,3]

[1] State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System (CEMEE), Luoyang 471003, China
[2] School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[3] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

Corresponding author: Zhenzhen Gao (zhenzhengao@xjtu.edu.cn)

This work was supported by the Open Research Found of National Mobile Communications Research Laboratory, Southeast University under Grant 2020D11, the Open Research Found of CEMEE under Grant 2020Z0204B, the National Natural Science Foundation of China under Grant 62071367, the Key Research and Development Program in Shaanxi Province of China under Grant 2020KW-007, and the Fundamental Research Funds for the Central Universities.

ABSTRACT In this paper, we study the influence of a smart jammer on the design of a three-node frequency hopping communication system using an amplify-and-forward relay. The jammer is smart that it senses the frequency and transmit powers used by the legitimate transmitters including the source node and the relay, and optimally adjusts the sensing time and the jamming power allocation to maximize the performance damage of the relay system. We jointly consider the time domain and the power domain to design a multi-domain anti-jamming strategy. To model the interaction between the legitimate transmitters and the jammer, we use Stackelberg game and let the legitimate transmitters act as the leader while the jammer act as the follower. Based on backward induction, a genetic algorithm based on exponential distribution algorithm is proposed to obtain the optimal frequency-hopping speed and the optimal transmit powers of the legitimate transmitters. Simulation results show that the proposed multi-domain strategy outperforms single-domain schemes and the multi-domain random scheme. Moreover, the optimal placement of the relay is also discussed through simulations.

INDEX TERMS Anti-jamming, multi-domain, Stackelberg game, wireless relay network.

I. INTRODUCTION

In 4G and 5G communication networks, wireless relay is an effective solution to extend the coverage and meet the requirement of high data rate. Due to the open characteristic of wireless channels, the information transmissions from the source node and the relay are exposed under the threat of jamming attack, which causes serious damage on the quality of communications [1]. Frequency hopping spread spectrum [2]–[4] is widely used in the wireless communication systems that require anti-jamming protection. The main idea of frequency hopping (FH) is to divide the available bandwidth into many adjacent subchannels and change the carrier frequency according to a pseudo-random code generator.

With the development of cognitive radio technology, a smart jammer, which quickly senses the frequency hopping communication signals, and immediately injects jamming signals on the detected frequency band [5] with the minimum required power, poses a great challenge to the existing defence mechanisms. To deal with the smart jamming in wireless FH systems, an intuitive approach is to increase the frequency hopping rate or increase the transmission power. However, due to the hardware limitations, there exists a frequency switching time as long as the communication system switches the frequency band. During the frequency switching time, the communication system cannot work [6]. If the frequency hopping speed is too fast, the frequency switching time increases and the effective communication time decreases; if the frequency hopping speed is slow, the jammer can detect the signal correctly with higher probability, which results in more precise jamming. Therefore, it is critical to find an optimal frequency hopping speed for FH systems. A similar tradeoff is also found in the power domain. Increasing the transmit power will improve the legal transmission quality, but this will also increase the probability of

The associate editor coordinating the review of this manuscript and approving it for publication was Marco Martalo.

being accurately detected and interfered, which will harm the legal transmission. Therefore, the joint selection of optimal FH speed and transmission power for FH communications is an important issue to be solved.

II. RELATED WORK

Game theory is a powerful mathematical tool to model and analyze the mutual interactions among players. Among the game theoretical models, Stackelberg game, which captures the sequential interactions among players, provides a promising approach of strategic decision-making when dealing with the smart jamming.

So far, the most widely used anti-jamming method is based on power-domain, which refers to using power control method to deal with the jammer with power perception and power adjustment ability. In [7], the problem of anti-jamming is investigated in wireless communication systems using power control method under intelligent interference. The Stacklberg game method is used to establish the model, and the optimal communication strategy is obtained by solving the Nash Equilibrium (NE). In [8], the authors further studied the use of power control methods to resist intelligent interference in cognitive radio networks with observation errors, and derived the Stacklberg Equilibrium (SE) of anti-jamming games. It is proved that the user obtains a higher utility at the SE than that at the NE. Considering the uncertainty of channel state information and transmission cost information, the SE is derived by Bayesian Stackelberg game and the existence and uniqueness of SE are proved in [9]. Considering the rival-type uncertainty, the anti-jamming problem is modeled as two bayesian games, which are incorporated into a unified equilibrium scale to obtain the optimal transmit power in [10]. In [11], the Stackelberg game is used to solve the anti-jamming problem in the UAV communication network where the drones interfere with each other, and derives the optimal transmission power of UAV and smart jammers.

The above works use game theory to model and analyze the dynamic interaction between the smart jammer and the legitimate system, but they take only the power domain into consideration. When FH is used, besides the power domain, the time domain and the frequency domain can also be exploited for anti-jamming design. In [12], the author model the jamming and anti-jamming problems as stochastic game in frequency domain, and obtains smart channel hopping sequences. In [13], the bimatrix game framework is developed for modeling the interaction between the transmitter and the jammer, and the NE of the game are obtained. It has been proved that the multi-domain anti-jamming technology can enhance the anti-jamming ability with greater flexibility [14], [15]. In [14], the shortcomings of the separately application of FH and transmission rate adaptation methods are discussed,, and the idea of joint use of the two technologies is proposed to prevent interference. Power control anti-jamming based on Stackelberg game and channel switching based on multi-armed bandit are used jointly in [15] to effectively resist interference attacks in heterogeneous networks.

As for the anti-jamming issues in wireless relay networks, game theory is also used to design the anti-jamming strategies [16]–[18]. For the interfered relay system, the source and the relay are represented as the legitimate system in [16], and the interaction between the legitimate system and the jammer is modeled as a noncooperative static game. The existence and uniqueness of the NE are proved in [16]. With a total source and relay power constraint, the legitimate system and the jammer optimally allocate power between listening and forwarding phases respectively. For the power control problem in the relay cooperative anti-jamming system, by modeling the interaction between the legitimate system and the jammer as a Stackelberg game, the optimal transmission power of the legitimate system and jammer is analyzed and the SE is derived in [17]. Considers the problem of multi-user power control with incomplete information and observation errors, a bayesian three-layer Stackelberg game approach is constructed in [18] to solve this problem.

Most of the existing anti-jamming schemes in wireless relay networks are designed based power-domain and decode-and-forward protocol. Actually, the AF protocol has been widely used in practical wireless relay systems. In this paper, we try to solve the multi-domain anti-jamming problem by jointly considering optimal FH speed and transmission power for AF relay networks. We model the interaction between legitimate system and a jammer as Stackelberg game. The source and the relay as leader communicate firstly with the optimal hopping speed and transmission power. On the basis of detected hopping speed and transmission power, the jammer as a follower allocates appropriate signal detection time and interference time in time domain, and also allocates interference powers of the two hops in power domain. For the legitimate system, the genetic algorithm is used to obtain the optimal hopping speed and transmission power. For the jammer, the closed-form solution of the optimal parameters is derived under the given legitimate system parameters. Finally, the anti-jamming performance of the proposed method is compared with single-domain schemes and the multi-domain random scheme.

III. SYSTEM MODEL AND PROBLEM FORMULATION

A. SYSTEM MODEL

We consider a three-node two-hop cooperative amplify-and-forward (AF) relay network attacked by a smart jammer shown in Fig. 1, which consists of one source S, one destination D, one trusted relay R and one jammer J. R operates in the Half-Duplex (HD) mode. The channels are assumed to undergo flat fading with CSI perfectly and globally known at all terminals. Inspired by the path-loss model [19] which has been widely used in the communication, the channel gain of the source-relay link and the relay-destination link are denoted as $\alpha_{sr} = K[d_0/d_{sr}]^{\gamma}$ and $\alpha_{rd} = K[d_0/d_{rd}]^{\gamma}$, where K is a coefficient that depends on antenna characteristics and

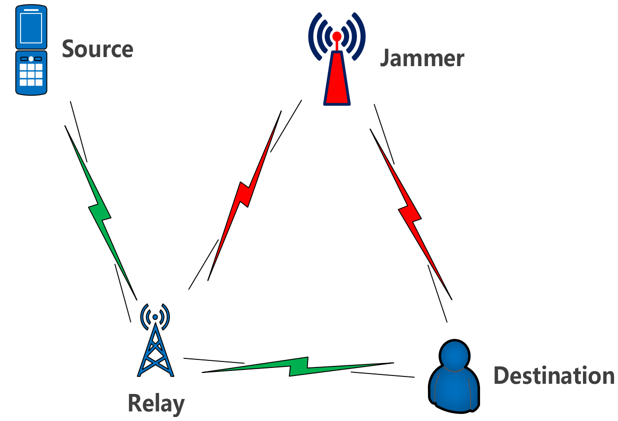

FIGURE 1. Communication attacked by the jammer in Wireless relay networks.

average channel loss, d_0 is the reference distance of antenna far field, γ is the path-loss factor, d_{sr} and d_{rd} denote the distance of the source-relay link and the relay-destination link. Similarly, the channel gain of jammer-relay link and the jammer-destination are denoted as $\alpha_{jr} = K[d_0/d_{jr}]^{\gamma}$ and $\alpha_{jd} = K[d_0/d_{jd}]^{\gamma}$, where d_{jr} and d_{jd} denote the distance of the jammer-relay link and the jammer-destination link respectively. Let $h_{sr}, h_{rd}, h_{jr}, h_{jd}$ denote the complex channel coefficients between S and R, R and D, J and R, and J and D, respectively. The communication takes place in two phases due to the HD mode. In the listening phase, the R receives the signal transmitted by the S, and in the forwarding phase, the R forwards the received signal to D. The jammer interferes in listening and forwarding phases. According to [16], The received signal at D under interference can be express as

$$y = h_{rd}a\left[h_{sr}s + h_{jr}s_{j_1} + n_r\right] + h_{jd}s_{j_2} + n_d, \tag{1}$$

where s, s_{j_1} and s_{j_2} are assumed to be independent zero-mean Gaussian signals with power P_s, P_{j_1} and P_{j_2}, respectively. n_r and n_d are the zero-mean Gaussian noises at R and D with N_r and N_d variance respectively. a is the amplifying weight which can be write as

$$a = \sqrt{\frac{P_r}{\mid h_{sr} \mid^2 P_s + \mid h_{jr} \mid^2 P_{j_1} + N_r}}. \tag{2}$$

It is assumed that the source and the relay have maximum power constraints $P_{s_{\max}}$ and $P_{r_{\max}}$ respectively, the jammer have total power constraints P_J, so $P_s < P_{s_{\max}}$, $P_r < P_{r_{\max}}$ and $P_{j_1} + P_{j_2} = P_J$. Define $\beta = P_{j_1}/P_J$ as the power allocation factor of the jammer. The received Signal-to-Interference-plus-Noise Ratio (SINR) at D $SINR_d$ can be expressed as Equ. (3), as shown at the bottom of the page.

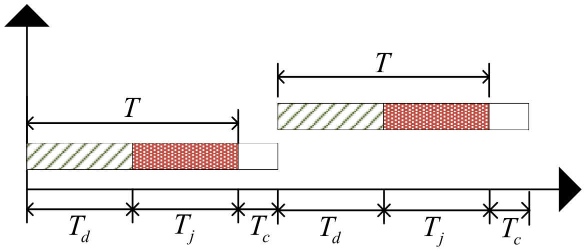

FIGURE 2. The framework of frequency-hopping signal.

The legitimate system uses FH and power control technology for anti-jamming and the jammer optimize their parameters in time domain and power domain. The legitimate system hops based on a pre-specified pseudo-noise sequence in M sub-bands. A schematic diagram of a typical FH signal structure is shown in Fig. 2. The FH period is $T = nT_1$, and $T \in [0, T_{\max}]$, $T_{\max}$ is the maximum FH period, T_1 is the duration of the listening and forwarding time, n is a positive integer. That is, the legitimate system can adaptively adjust the FH period within the range of 0 to $T_{\max}$ according to the parameters of the jammer, and each FH period can only be changed after D receives the information. Due to the limitations of devices, there is inevitably an unstable transient process when the signal frequency is switched. During this process, the FH communication system neither transmits nor receives the signal [6]. Let the duration of the transient process be frequency switching time T_c, which is a fixed value related to the hardware device. In each FH period, the smart jammer performs jamming attack as soon as the legitimate transmission is detected. Therefore, each FH period T can be divided into two parts, signal detection time T_d and jamming time T_j, and $T = T_d + T_j$. For convenience, we set $T_j = mT_1$, m<n that is to say, the jammer will implement jamming after observing m times of complete communication. Because signal detection probability is related to detection time and transmit signal power, the longer the detection time or the greater the detection signal power, the higher the detection probability. Define P_d as the detection probability of FH communication signal. According to the relevant study on the performance of an energy detector [20], P_d can be given as

$$\begin{aligned} P_d &= \sum_{m=0}^{M-1}(-1)^m\binom{M-1}{m}\frac{1}{m+1}\exp\left(\frac{-m}{4(m+1)}\mathrm{SNR}_j T_d\right) \\ &\approx 1-\frac{M-1}{M}\exp\left(-\frac{1}{4}\mathrm{SNR}_j T_d\right), \end{aligned} \tag{4}$$

$$SINR_d = \frac{P_s P_r K[d_0/d_{rd}]^{\gamma} K[d_0/d_{sr}]^{\gamma}}{P_s K\left(\frac{d_0}{d_{rd}}\right)^{\gamma}\left[N_d + (1-\beta)P_J K\left(\frac{d_0}{d_{jd}}\right)^{\gamma}\right] + P_r K\left(\frac{d_0}{d_{rd}}\right)^{\gamma}\left[N_r + \beta P_J K\left(\frac{d_0}{d_{jr}}\right)^{\gamma}\right] + \left[N_r + \beta P_J K\left(\frac{d_0}{d_{jr}}\right)^{\gamma}\right]\left[N_d + (1-\beta)P_J K\left(\frac{d_0}{d_{jd}}\right)^{\gamma}\right]} \tag{3}$$

where $\binom{M-1}{m}$ is the number of all combinations of m elements taken from $M-1$ different elements. SNR_j is the recieve signal-to-noise-ratio (SNR) at J, which can be expressed as

$$SNR_j = \frac{P_sK[d_0/d_{sj}]^\gamma}{N_j} + \frac{P_sP_rK[d_0/d_{rj}]^\gamma K[d_0/d_{sr}]^\gamma}{N_jP_sK[d_0/d_{sr}]^\gamma + N_rP_rK[d_0/d_{rj}]^\gamma + N_rN_j}, \tag{5}$$

where N_j is variance of the zero-mean Gaussian noises at J. Then, the average received SINR of the legitimate system in a FH period can be expressed as:

$$\overline{SINR} = \frac{SNR_d(T_d+(1-P_d)(T-T_d))}{T+T_c} + \frac{SINR_dP_d(T-T_d)}{T+T_c}, \tag{6}$$

where the first term of the righthand expression represents that D is not interfered by J when J is performing detection and J does not detect the existence of the legitimate transmission, SNR_d is the receive SNR at D without interference. The second item represents that J detects the legitimate transmission and perform jamming, $SINR_d$ is the signal-to-interference-plus noise ratio at D which can be found in (3). When no jamming signals, SNR_d can be written as

$$SNR_d = \frac{P_sP_rK[d_0/d_{rd}]^\gamma K[d_0/d_{sr}]^\gamma}{N_dP_sK[d_0/d_{sr}]^\gamma + N_rP_rK[d_0/d_{rd}]^\gamma + N_rN_d} \tag{7}$$

B. PROBLEM FORMULATION

Average SINR is the key indicator of communication reliability, so we give the utility function based on average SINR. Considering the energy-constraint of the capacity-limited battery for practical wireless devices, the transmission should be power-efficient. Therefore, we take the power cost into consideration when formulating the legitimate system's utility function. We define the utility value of the legitimate system in the following:

$$U_c(P_s, P_r, T) = \overline{SINR} - C_sP_s - C_rP_r, \tag{8}$$

where C_s and C_r are unit power costs of the source and the relay respectively. Assume that the jammer is supplied by the power grid so that a worst case to the legitimate communication system is constructed. Compared to the battery-supplied devices, the power cost of the jammer is negligible. We formulate the jammer's utility function as

$$U_j(\beta, T_d) = -\overline{SINR}. \tag{9}$$

According to the utility function given above, the legitimate system and the jammer aim to maximize their own utility value. The problem of multi domain optimization can be solved by the backward induction. According to the detection results of FH signals, the jammer as a follower determines the optimal detection time T_d and the power allocation factor β from the following optimization problem:

$$(\beta^*, T_d^*) = \arg \max_{0\le\beta\le1, 0\le T_d\le T} U_j(\beta, T_d). \tag{10}$$

Similarly, as laeders, the source and the relay determines the optimal transmit power and the FH period from the following optimization problem:

$$(P_s^*, P_r^*, T^*) = \arg \max_{0\le P_s\le P_{smax}, 0\le P_r\le P_{rmax}, 0\le T\le T_{max}} U_c(P_s, P_r, T). \tag{11}$$

Next, we propose an optimization method based on genetic algorithm (GA) to find the optimal solution of the legitimated and the jammer.

IV. THE MULTI-DOMAIN OPTIMIZATION STRATEGY BASED ON STACKELBERG GAME

The expression of the signal to interference plus noise ratio becomes quite complicated due to the AF protocol. Therefore, we can not derive the Stacklberg Equilibrium directly. In this section, we propose a optimization method based on GA to obtain the optimal multi-domain parameters of follower and leaders successively.

A. FOLLOWER SUB-GAME

In the Stackelberg game, the backward induction is an effective method to obtain optimal solution. That is to say, for the jammer, the maximum utility value is achieved by observing the transmission power of the source and the relay and the FH period of the legitimate system. Therefore, we first solve the optimal jammer parameters β^* and T_d^* when the parameters of the legitimate system are determined. The parameter β only affects the $SINR_d$, apparently, the optimization problem (10) is equivalent to the lower form:

$$\beta^* = \arg \min_{0\le\beta\le1} SINR_d(\beta), \tag{12}$$

and

$$T_d^* = \arg \max_{0\le T_d\le T} U_j(\beta^*, T_d). \tag{13}$$

So we make the $SINR_d$ minimum to obtain the optimal β^* first. The jammer's optimal power allocation β^* is given by:

$$\beta^* = [\,\widetilde{\beta}\,]_0^1, \tag{14}$$

where

$$\widetilde{\beta} = \frac{1}{2} + \frac{P_rK^2\left(\frac{d_0^2}{d_{rd}d_{jr}}\right)^\gamma + N_dK\left(\frac{d_0}{d_{jr}}\right)^\gamma - P_sK^2\left(\frac{d_0^2}{d_{jd}d_{sr}}\right)^\gamma - N_rK\left(\frac{d_0}{d_{jd}}\right)^\gamma}{2P_JK[d_0/d_{jd}]^\gamma K[d_0/d_{jr}]^\gamma} \tag{15}$$

and $[x]_0^1 = \min(1, \max(0, x))$. The convex optimization problem how to obtain optimal β^* has been studied in *Lemma* 1 of [16].

Theorem 1: The optimal value T_d^* under discrete constraints can be expressed as

$$T_d^* = \arg \max_{T_d\in\{m^*T_1, (m^*\pm1)T_d\}} U_j(\beta^*, T_d), \tag{16}$$

where

$$m^* = \arg \min_{m \in [0,n]} T_{d_1}^* - mT_1, \tag{17}$$

and T_{d1}^* is shown in Equ. (21).

Proof: After determining β^* to minimize $SINR_d$, we optimize T_d to maximize the utility value of the jammer U_j and Equ. (9) is simplified as follows:

$$U_j = \frac{SNR_d T + (SNR_d - SINR_d)P_d(T - T_d)}{T + T_c}. \tag{18}$$

Because T_d is a discrete variable, the optimal value T_{d1}^* is found without considering its discrete constraints, then the optimal value T_d^* under discrete constraints is found in the discrete feasible region. After the parameters P_s, P_r and T of the legitimate system and β of the jammer are determined, the jammer's utility value U_j only depends on the $P_d(T - T_d)$ from Equ. (18). The $P_d(T - T_d)$ is a concave function about T_d because of:

$$\begin{aligned}\frac{\partial^2 P_d\,(T-T_d)}{\partial T_d^2} &= -\frac{M-1}{16M} SNR_j^2 \exp\left(-\frac{1}{4}SNR_j T_d\right)(T-T_d)\\ &\quad - \frac{M-1}{4M} SNR_j^2 \exp\left(-\frac{1}{4}SNR_j T_d\right)\\ &\quad \times (1 + SNR_j) < 0. \end{aligned} \tag{19}$$

P_d is a strictly increasing function about T_d, and $P_d(0) = 1/M$, $P_d(+\infty) = 1$. However $(T - T_d)$ is monotone decreasing function about T_d. Therefore, there are two cases when different the initial value of $\frac{\partial P_d(T-T_d)}{\partial T_d}$ are considered.

case 1. $\frac{\partial P_d(T-T_d)}{\partial T_d}\big|_{T_d=0} < 0$. $P_d(T - T_d)$ decreases monotonically within $T_d \in [0, T]$, and the utility value takes the maximum value at $T_d = 0$.

case 2. $\frac{\partial P_d(T-T_d)}{\partial T_d}\big|_{T_d=0} > 0$. $P_d(T - T_d)$ increases first and then decreases within $T_d \in [0, T]$. The utility function obtains the maximum value when first derivative of $P_d(T - T_d)$ is equal to 0 as follows:

$$\frac{\partial P_d(T - T_d)}{\partial T_d} = \frac{\partial P_d}{\partial T_d}(T - T_d) - P_d. \tag{20}$$

Therefore, the SNR corresponding to $\frac{\partial P_d(T-T_d)}{\partial T_d}\big|_{T_d=0} = 0$ is the threshold for the jammer to adopt different optimal jamming power strategies. Based on Equ.s (10)-(14) in [21], the approximated jammer's optimal detection time T_{d1}^* can be derived in closed-form as:

$$T_{d1}^* = \begin{cases} 0 \quad SNR_j < \frac{4}{TlnM} \\ \dfrac{-\frac{2M-1}{M} + \sqrt{\left(\frac{2M-1}{M}\right)^2 + \frac{SNR_j}{2}\frac{M-1}{M}T}}{\frac{SNR_j}{4}} \\ \quad SNR_j > \dfrac{4}{TlnM} \end{cases} \tag{21}$$

■

B. LEADER SUB-GAME

The optimal β^* and T_d^* are taken into Equ. (8), and the source and the relay are taken as leaders to optimize P_s, P_r and T. Because of the good performance of GA in solving the optimization problems having discontinuities, constrained parameters and a large number of dimensions, we use GA based on the jammer optimal solution to solve the optimal problem (11). To slove this nonlinear bilevel programming problem, as in [22], we consider a genetic algorithm based on exponential distribution (GAED), which modifies two main steps of the GA, namely, the evaluation and crossover operations. The steps involved in the GAED are delineated as follows.

1) INITIAL POPULATION

First, we create the initial population $pop(0)$, which includes s individuals, and each individual is represented by $\mathbf{S}_i^0 = (\mathbf{S}_{Li}^0, \mathbf{S}_{Ji}^0)$, $(i = 1, 2, \ldots, s)$ with $\mathbf{S}_{Li}^0 = (P_{s_i}^0, P_{r_i}^0, T_i^0)$ and $\mathbf{S}_{J_i}^0 = (\beta_i, T_{d_i})$. For each $\mathbf{S}_{Ji}^0$, the corresponding optimal solution for the jammer $\mathbf{S}_{J_i}^0 = (\beta_i, T_{d_i})$ can be calculated by Equ.s (15) and (16). The parameters of the individuals in the initial population are randomly generated with the bounded and discrete constraints.

2) EVALUATION

For each individual in a certain population $pop(k)$, the fitness values is defined as follows:

$$\begin{aligned} &R(\mathbf{S}_{Li}^k, \mathbf{S}_{Ji}^k)\\ &\quad = U_c + \eta\min(0, P_{s_i}^k, P_{r_i}^k, T_i^k)\\ &\qquad - \eta\max(0, P_{s_i}^k - P_{s_{max}}, P_{r_i}^k - P_{r_{max}}, T_i^k - T_{max}), \end{aligned} \tag{22}$$

where η is a sufficiently large positive number. Let $\mathbf{S}^{*k}$ denote the individual which has the largest fitness value among all the possible values of $R(\mathbf{S}_{Li}^k, \mathbf{S}_{Ji}^k)$, $i = 1, 2 \cdots, s$. Similarity, let $\mathbf{S}'^k$ denote the individual with the largest utility value of the legal system from all the possible individuals inherited from $pop(k - 1)$.

3) CROSSOVER

This algorithm attempts to use the $\mathbf{S}^{*k}$ and $\mathbf{S}'^k$ to improve the search efficiency. The specific method is as follows. Among the s individuals of the kth generation, we select randomly several individuals with probability p_c for crossover. The new individual generated by the crossover of $\mathbf{S}_{Li}^k$ can be write as

$$\bar{\mathbf{S}}_{Li}^k = \mathbf{S}_{Li}^k + \mu(\mathbf{Q}^k - \mathbf{S}_{Li}^k), \tag{23}$$

where $\mathbf{Q}^k$ is to be optimized based on $\mathbf{S}^{*k}$ and $\mathbf{S}'^k$, $\mu \in [0, \tau]$, τ is a limiting factor so that $\mathbf{S}_{Li}^k + \tau(\mathbf{Q}^k - \mathbf{S}_{Li}^k)$ does not exceed the feasible region. It can be seen from Equ. (21) that the crossover operator uses vector $\mathbf{Q}^k$ to provide a crossover direction. Now the problem becomes how to choose $\mathbf{Q}^k$ reasonably. Generally speaking, after a certain iterations, the vector $\mathbf{S}^{*k}$ is a feasible solution, and $\mathbf{S}'^k$ is often not a feasible solution. Among them, the $\mathbf{S}^{*k}$ is the vector with

Algorithm 1 The Proposed GAED Algorithm

```
1: Initial: Generate initial population $pop(0)$, let $k = 0$.
2: Evaluation: Calculate The fitness value of each individual, recorded the $\mathbf{S}^{*k}$ and $\mathbf{S}'^{k}$.
3: Crossover: First, $\mathbf{S}_{Li}^{k}$ is hybridized with a crossover operator to obtain $\bar{\mathbf{S}}_{Li}^{k}$. Then, the corresponding optimal solution of jammer $\bar{\mathbf{S}}_{Ji}^{k}$ is obtained. The set of all crossover offspring $(\bar{\mathbf{S}}_{Li}^{k}, \bar{\mathbf{S}}_{Ji}^{k})$ is denoted as $O_1$;.
4: Mutation: First, $\mathbf{S}_{Li}^{k}$ is mutated with a mutation operator to obtain $\widetilde{\mathbf{S}}_{Li}^{k}$. Then, the corresponding lower optimal solution $\widetilde{\mathbf{S}}_{Ji}^{k}$ is obtained. The set of all mutation offspring $(\widetilde{\mathbf{S}}_{Li}^{k}, \widetilde{\mathbf{S}}_{Ji}^{k})$ is denoted as $O_2$;
5: Selection: Select the best $N_1, N_1 < s$ individuals from the set $pop(k) \cup O_1 \cup O_2$. The remaining $s - N_1$ individuals is randomly selected from the remaining individuals of the this set. These two parts constitute the next generation population $pop(k+1)$ and update $\mathbf{S}^{*k}$ and $\mathbf{S}'^{k}$.
6: Iteration: If the termination condition is true, stop; otherwise, let $k = k + 1$, turn to 2.
```

the largest fitness value that satisfies the constraint, and the $\mathbf{S}'^{k}$ is the vector with the largest utility value of the legal system. From the perspective of fitness value, the $\mathbf{S}^{*k}$ is better than $\mathbf{S}'^{k}$, but the $\mathbf{S}'^{k}$ can provide a possible crossover direction. Therefore, we hope that $\mathbf{Q}^{k}$ can approach $\mathbf{S}^{*k}$ with a higher probability than $\mathbf{S}'^{k}$. The characteristics of the exponential distribution meet this demand. The selection of $\mathbf{Q}^{k}$ is given in the following step-by-step. First, let the random variable D follow an exponential distribution, and its probability density function is:

$$p(d) = \begin{cases} \lambda e^{-\lambda d} & d > 0 \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

Secondly, take sufficiently large number h so that $prob(D \in (h, \infty))$ is sufficiently small. Divide $[0, h]$ into l sub-intervals $\bar{h}_1, \bar{h}_2, \cdots, \bar{h}_l$ of equal length. Divide the difference vector between $\mathbf{S}^{*k}$ and $\mathbf{S}'^{k}$ into corresponding l subintervals $h_1, h_2, \cdots, h_l$. Let $prob(\mathbf{Q}^{k} \in h_i) = prob(d \in \bar{h}_i)$, so

$$prob(\mathbf{Q}^{k} \in h_1) \geq prob(\mathbf{Q}^{k} \in h_2) \geq \cdots \geq prob(\mathbf{Q}^{k} \in h_l). \tag{25}$$

Finally, according to the roulette selection method, an interval h_i is selected and the parameter vector $\mathbf{Q}^{k}$ in h_i is selected randomly, that is, according to the probability $prob(D \in (h, \infty))$ select interval h_i.

4) MUTATION

Mutation individuals were selected randomly from $pop(k)$ with the mutation probability p_m. Gaussian mutation operator is used. That is to say, for the variation of the parent $\mathbf{S}_{Li}^{k}$, the mutation operator can be express as

$$\widetilde{\mathbf{S}}_{Li}^{k} = \mathbf{S}_{Li}^{k} + \varepsilon, \tag{26}$$

where ε is a Gaussian vector, whose elements are i.i.d and distributed as $\mathcal{N}(0, \sigma_p^2)$.

The step of the proposed GAED algorithm is outlined in Algorithm 1.

V. SIMULATION RESULTS AND DISCUSSION

In this section, we first demonstrate the optimal parameters in time-domain and power-domain obtained by the GAED algorithm. Then we compare the proposed multi-domain anti-jamming strategy with single-domain schemes and the multi-domain random scheme. Finally, the influence of different parameters on the utility values of the legitimate system and the jammer are discussed.

In the simulation, we assume the FH period T_1 is 1ms, and the frequency switching time T_c is 0.5ms, the power costs of the source and the relay are set as $C_s = C_r = 0.7$. The transmit power of the jammer is $P_J = 10$W, the maximum power constraints of the source and the relay are set as $P_{s_{max}} = P_{r_{max}} = 1$W. The noise power $N_c = N_r = N_j = N_d = -50$dbm. The number of optional channels M is 32, the initial population number s is 30, the crossover probability p_c and the mutation probability p_m are 0.8 and 0.2 respectively. The simulation adopts outdoor scene, and the location coordinates of the source, the destination and the jammer are set as $[-4\text{km}, 0]$, $[2\text{km}, 0]$ and $[0, 6\text{km}]$. And the default coordinate positions of the relay nodes are $[-1\text{km}, 0]$. The channel parameters are set as $K = 1$, $d_0 = 0.1$km and $\gamma = 3$.

A. THE OPTIMAL POWER-DOMAIN AND TIME-DOMAIN PARAMETERS

The accuracy of the GAED algorithm is illustrated by Fig. 3, Fig. 4 and Fig. 5. Fig. 3 and Fig. 4 show that the GAED algorithm can find the optimal solution (P_s^*, P_r^*, T^*) of the legitimate system, and Fig.5 shows that the proposed GAED algorithm can find the optimal solution (β^*, T_d^*) of the jammer. In the simulations of this part, the unit power cost of the source and the relay are set as $C_s = 0.4$ and $C_r = 1.2$.

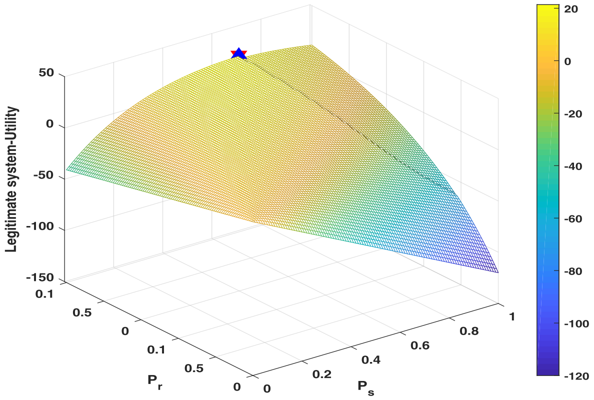

FIGURE 3. Utility value of the legitimate system with different values of P_s and P_r.

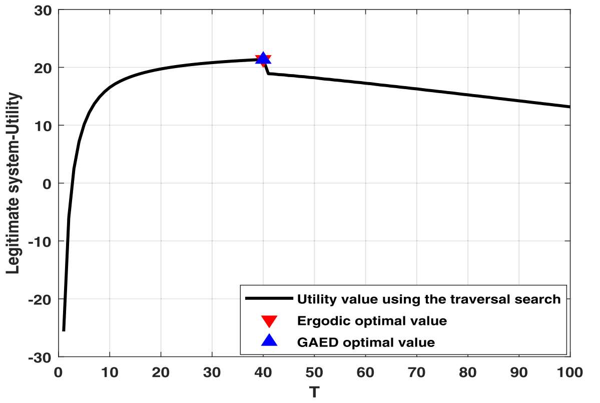

FIGURE 4. Utility value of the legitimate system with different values of T.

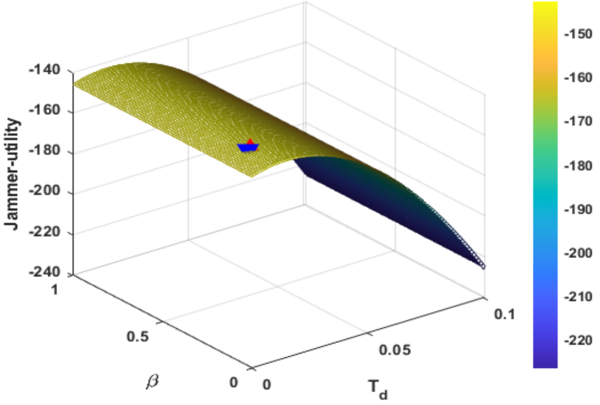

FIGURE 5. Utility value of the jammer with different values of β and T_d.

Fig. 3 shows that in the case of optimal FH period T^*, the legitimate system's utility value corresponding to each value of (P_s, P_r) is calculated by traversing. The blue triangle and the red triangle represents the optimal transmit power of the source and the relay (P_s^*, P_r^*) found by the GAED algorithm and the traversal search. It can be seen that the optimal transmit power (P_s^*, P_r^*) found in the GAED algorithm are consistent with the maximum value found by the traversal search. In the case of fixed optimal powers of the source and the relay, the optimal FH period T found by the GAED algorithm is compared with the optimal value obtained through the traversal search in Fig. 4. We can see that the optimal FH period obtained by the GAED algorithm also coincides with that from the traversal search. Under this parameter setting, we also discuss the complexity of the traversal search algorithm and the proposed algorithm. The complexity of the traversal search is approximately $O(1000)$, and the complexity of the proposed algorithm is approximately $O(Ks) = O(300)$. Therefore the complexity of the proposed algorithm is much lower than that of the traversal search.

From Fig. 5, we can see that the GAED algorithm also finds the optimal (β^*, T_d^*). Moreover, we can also see that the utility value of the jammer is mainly affected by the detection time T_d while the power allocation factor β has little effect. The reason is that from Equ.s (6) and (9), the jammer's utility is dominated by SNR_d, but the parameter β mainly affects $SINR_d$ but not SNR_d.

B. THE UTILITY COMPARISON

The comparisons of the proposed strategy with the single-domain schemes and the multi-domain random scheme are shown in Fig. 6. The multi-domain random scheme selects all parameters $(P_s, P_r, T, \beta, T_d)$ randomly. There are two kinds of single-domain schemes: the power-domain only scheme and the time-domain only scheme. In the power-domain only scheme, the FH period T is selected by blind FH, the optimal power (P_s, P_r) is obtained by traversing, and the optimal detection period T_d and the power allocation β are selected by the derived closed form solution in the GAED algorithm. In the time-domain only scheme, the optimal FH period T is obtained by traversing, the power (P_s, P_r) is selected randomly, and the optimal detection period T_d and power allocation β are selected by the derived closed form solution in the GAED algorithm. The power-domain only scheme optimized the transmit power of the legitimate system and the time-domain only scheme optimized the FH period, while the proposed scheme jointly optimize the parameters both in power domain and time domain. Therefore, the proposed strategy achieves the largest utility value of the legitimate system among four anti-jamming schemes. The legitimate system's utility value of the multi-domain random scheme is the minimum since the parameters of the multi-domain random scheme are selected randomly. Because the legitimate system is the leader and has the first mover advantage, the proposed strategy has the lowest jammer's utility value. The multi-domain random scheme has the largest utility value of the jammer. Through the comparisons, it is found that the proposed strategy has obvious advantages over the single-domain schemes and the multi-domain random scheme.

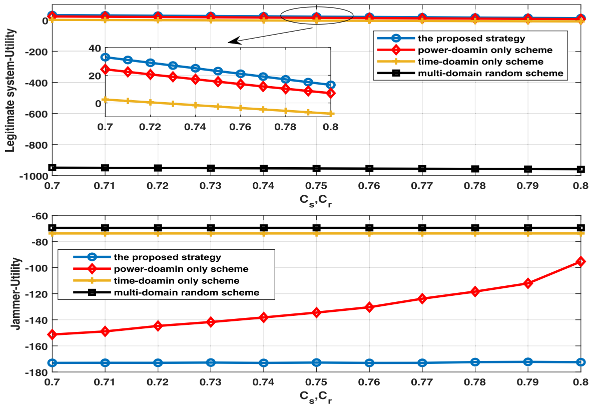

FIGURE 6. Utility value comparisons of the multi-domain anti-jamming scheme with the single-domain schemes and multi-domain random scheme.

C. THE INFLUENCE OF KEY PARAMETERS ON UTILITY

Fig. 7 shows the influence of the jamming power on the proposed strategy. First, it can be seen that under the current parameter settings, the GAED algorithm tends to converge after 15 iterations. It can also be found that the jamming power has little influence on the utility value of the legitimate system. This is because the utility value mainly comes from SNR_d in Equ. (8), which has no interference. Due to the similar reason, the increase of the jamming power has a weak impact on the utility value of the jammer.

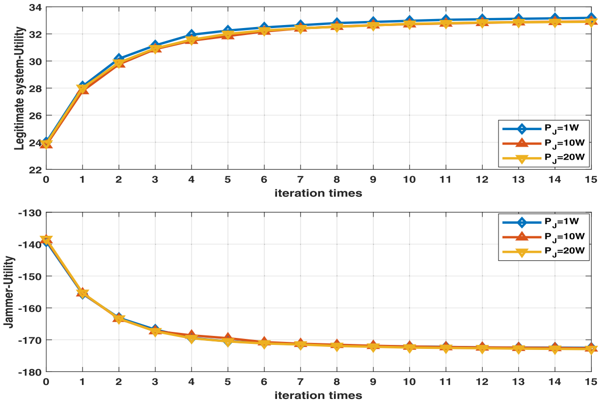

FIGURE 7. Effect of P_J on the utility value of the proposed strategy.

In Fig. 8, the effects of the transmit power constraints of the source and the relay on the proposed multi-domain anti-jamming strategy are investigated. First of all, we can see that with the increase of $P_{s_{max}}$ and $P_{r_{max}}$, the number of iterations required for convergence of the GAED algorithm increases. This is because when $P_{s_{max}}$ and $P_{r_{max}}$ increase, the feasible region is expanded, and the algorithm needs more iterations to find the optimal solution. We can also see that there is a bottleneck effect between the two hops. As long as the maximum power limit of the source or the relay is 1W, the utility value of the legitimate system is relatively low, which is about 33. Only when the maximum power limits of the source and the relay are both 5W, the utility value of the legitimate system of the proposed strategy will increase and the utility value of the jammer of the proposed strategy will decrease.

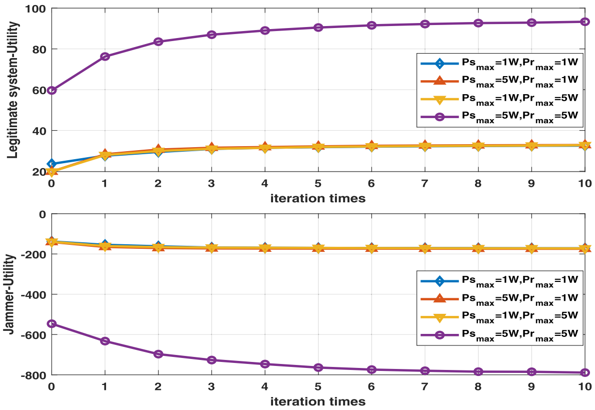

FIGURE 8. Effects of $P_{s_{max}}$ and $P_{r_{max}}$ on the utility value of the proposed strategy.

In Fig. 9, the effects of unit power costs of the source and the relay on the proposed strategy are investigated. As C_s or C_r increases, the utility value of the legitimate system reduces and the utility value of the jammer increases. It can be found that the effects of power costs of the source and the relay on utility value are similar.

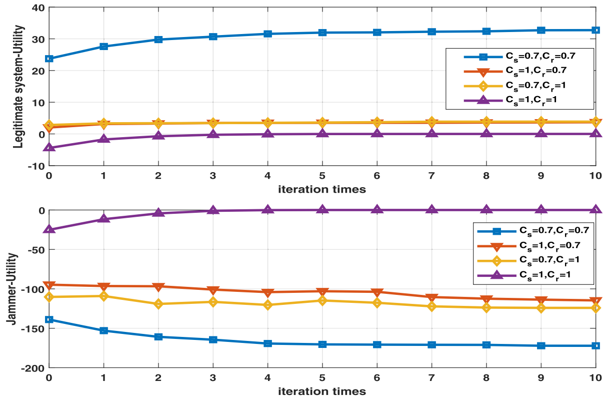

FIGURE 9. Effects of C_s and C_r on the utility value of the proposed strategy.

The effect of the relay location on utility value is shown in Fig. 10. Through the simulations of different jammer locations, we find that the optimal relay location is around the middle point of the source-destination link. This is because the source and the relay can automatically adjust their transmit power, and the utility value is maximum when the relay is in the middle.

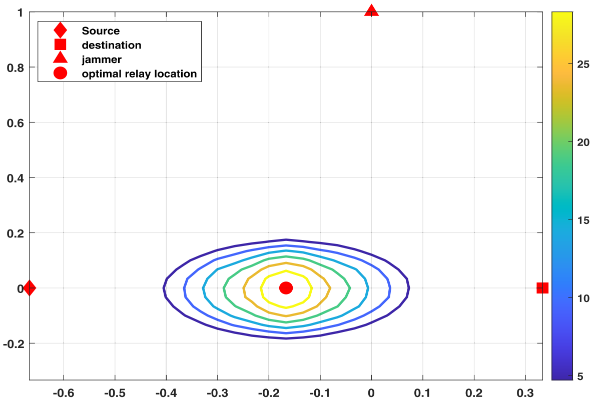

FIGURE 10. Optimal relay location.

VI. CONCLUSION

In this paper, we propose a multi-domain anti-jamming strategy for a wireless AF relay system using FH. We use Stackelberg game to model the interaction between the legitimate transmitter and the jammer in which the legitimate transmitter is the leader and the jammer is the follower. Based on the backward induction method, a GAED algorithm is proposed to find the optimal parameters of the legitimate system and the jammer. The simulation results show that the GAED algorithm can accurately find the optimal solution in time-domain and power-domain. The impacts of jamming power and unit power cost on utility values are analyzed. The bottleneck effect of the power constraints on the relay network performance is analyzed. Numerical simulations show that the optimal relay location under smart jamming is around the middle point of the source-relay link by using the proposed strategy.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] H. Wang, L. Zhang, T. Li, and J. Tugnait, "Spectrally efficient jamming mitigation based on code-controlled frequency hopping," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 728–732, Mar. 2011.

[3] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 16–30, Jan. 2012.

[4] G.-Y. Chang, J.-F. Huang, and Z.-H. Wu, "A frequency hopping algorithm against jamming attacks under asynchronous environments," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 324–329.

[5] F. Q. Yao, *Communication Anti-Jamming Engineering and Practice*. Beijing, China: Publishing House of Electronics Industry, 2012.

[6] Y. F. Q. Zhang and Yao, "The research on impairment of frequency hopping communication systems," *J. Xi'dian Univ.*, vol. 32, no. 6, pp. 472–476, 2005.

[7] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 4038–4047, Aug. 2013.

[8] L. Xiao, T. Chen, J. Liu, and H. Dai, "Anti-jamming transmission stackelberg game with observation errors," *IEEE Commun. Lett.*, vol. 19, no. 6, pp. 949–952, Jun. 2015.

[9] L. Jia, F. Yao, Y. Sun, Y. Niu, and Y. Zhu, "Bayesian stackelberg game for antijamming transmission with incomplete information," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 1991–1994, Oct. 2016.

[10] A. Garnaev, A. P. Petropulu, W. Trappe, and H. Vincent Poor, "A jamming game with rival-type uncertainty," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5359–5372, Aug. 2020.

[11] Y. Xu, G. Ren, J. Chen, L. Jia, and Y. Xu, "Anti-jamming transmission in UAV communication networks: A stackelberg game approach," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–6.

[12] H. Noori and S. Sadeghi Vilni, "Jamming and anti-jamming in interference channels: A stochastic game approach," *IET Commun.*, vol. 14, no. 4, pp. 682–692, Mar. 2020.

[13] Y. Gao, Y. Xiao, M. Wu, M. Xiao, and J. Shao, "Game theory-based anti-jamming strategies for frequency hopping wireless communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5314–5326, Aug. 2018.

[14] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems," in *Proc. 12th Int. Symp. Model. Optim. Mobile, Ad Hoc, Wireless Netw. (WiOpt)*, May 2014, pp. 247–254.

[15] L. Jia, Y. Xu, Y. Sun, S. Feng, L. Yu, and A. Anpalagan, "A multi-domain anti-jamming defense scheme in heterogeneous wireless networks," *IEEE Access*, vol. 6, p. 40 177–40 188, 2018.

[16] G. Zheng, E. A. Jorswieck, and B. Ottersten, "Cooperative communications against jamming with half-duplex and full-duplex relaying," in *Proc. IEEE 77th Veh. Technol. Conf. (VTC Spring)*, Jun. 2013, pp. 1–5.

[17] Y. Li, L. Xiao, J. Liu, and Y. Tang, "Power control stackelberg game in cooperative anti-jamming communications," in *Proc. 5th Int. Conf. Game Theory Netw.*, Nov. 2014, pp. 1–6.

[18] Z. Feng, G. Ren, J. Chen, X. Zhang, Y. Luo, M. Wang, and Y. Xu, "Power control in relay-assisted anti-jamming systems: A Bayesian three-layer Stackelberg game approach," *IEEE Access*, vol. 7, pp. 14623–14636, 2019.

[19] A. Goldsmith, *Wireless Communication*. Cambridge, U.K: Cambridge Univ. Press, 2005.

[20] J. G. Proakis, *Digital Communications*. New York, NY, USA: McGraw-Hill, 2001.

[21] Y. Z. Hu, "Design of optimal hopping speed against follow jamming with detection cost and detection error," *J. Signal Process.*, vol. 34, no. 7, pp. 824–832, 2018.

[22] H. C. Li, *Research on Genetic Algorithm of Nonlinear Bilevel Programming Problems*. Xi'an, China: Xidian University, 2009.

YONGCHENG LI received the master's degree from the University of Science and Technology of China, in 2012.

He joined the State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System. His research interests include cognitive radio networks and comprehensive effect mechanism of electromagnetic environment.

SHAOZHUANG BAI (Student Member, IEEE) received the B.E. degree in opto-electronics information science and engineering from the Xi'an University of Technology, Xi'an, China, in 2017. He is currently pursuing the Ph.D. degree in information and communication engineering with Xi'an Jiaotong University.

His research interests include physical-layer security and index modulation.

ZHENZHEN GAO received the B.S. degree in communication engineering from Lanzhou University, Lanzhou, China, in 2005, and the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China, in 2011.

From August 2009 to September 2011, she was a Visiting Student with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, USA. Since 2012, she has been with the School of Information and Communication Engineering, Xi'an Jiaotong University, where she is currently an Associate Professor. She is also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China. Her current research interests include physical-layer security, index modulation, and green cooperative and cognitive systems.