Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 4870656, 10 pages
https://doi.org/10.1155/2019/4870656

Research Article

Machine Learning Based Antenna Design for Physical Layer Security in Ambient Backscatter Communications

Tao Hong[1], **Cong Liu**[1] and **Michel Kadoch**[2]

[1]*School of Electronics and Information Engineering, Beihang University, China*
[2]*Department of Electrical Engineering, École de Technologie Supérieure, University of Quebec, Canada*

Correspondence should be addressed to Tao Hong; hongtao@buaa.edu.cn

Received 4 October 2018; Accepted 4 December 2018; Published 1 January 2019

Guest Editor: Feng Ye

Ambient backscatter employs existing radio frequency (RF) signals in the environment to support sustainable and independent communications, thereby providing a new set of applications that promote the Internet of Things (IoT). However, nondirectional forms of communication are prone to information leakage. In order to ensure the security of the IoT communication system, in this paper, we propose a machine learning based antenna design scheme, which achieves directional communication from the relay tag to the receiving reader by combining patch antenna with log-periodic dual-dipole antenna (LPDA). A multiobjective genetic algorithm optimizes the antenna side lobe, gain, standing wave ratio, and return loss, with a goal of limiting the number of large side lobes and reduce the side lobe level (SLL). The simulation results demonstrate that our proposed antenna design is well suited for practical applications in physical layer security communication, where signal-to-noise ratio of the wiretap channel is reduced, communication quality of the main channel is ensured, and information leakage is prevented.

1. Introduction

The Internet of Things (IoT) is a vital component of the fifth generation (5G) mobile communications, interconnecting a large number of devices. However, in traditional backscatter communication systems, radio frequency (RF) power is provided by the reader, and the limited power supply limits the widespread use of IoT.

In 2013, the proposed ambient backscatter communication technology solved some of the above shortcomings [1]. Unlike traditional backscatter communication (e.g., for passive sensors and RF identification (RFID) tags), ambient backscatter does not require specific devices to provide energy but instead utilizes RF signals in the environment as both energy resources and signal resources for reflection [2]. As a result, ambient backscatter provides sustainable and independent communications, and the maintenance and implementation costs of the system can be greatly reduced [3, 4]. Because the ambient configuration does not require additional spectrum resources to operate, we chose the 4G, 5G, and Wireless-Fidelity (Wi-Fi) signals with frequencies in the range of 2 GHz - 4 GHz as the ambient resources.

However, several challenges remain. The broadcast characteristics of wireless signals make it easy for some illegal eavesdroppers to obtain information content, and signals of the same frequency are superimposed at the receiver to cause interference, which brings many difficulties to signal detection [5].

Traditional security techniques, which encrypt information with high computationally complex codec algorithms [6], have gradually failed with the rapid increase in the computational power. The fundamental principle behind physical layer security is to exploit the inherent randomness of noise and communication channels to limit the amount of information that can be extracted at the "bit" level by an unauthorized receiver [7]. Therefore, information-theoretic security is considered to be a key technology to ensure the security of wireless communications.

A lot of research has been done on physical layer security. A cooperative relay scheme was investigated in [8]; however it is only applicable to multiantenna and multirelay systems. Artificial noise- (AN-) based methods are also inappropriate because of their higher energy expenditure and increased cochannel interference with any adjacent user [9].

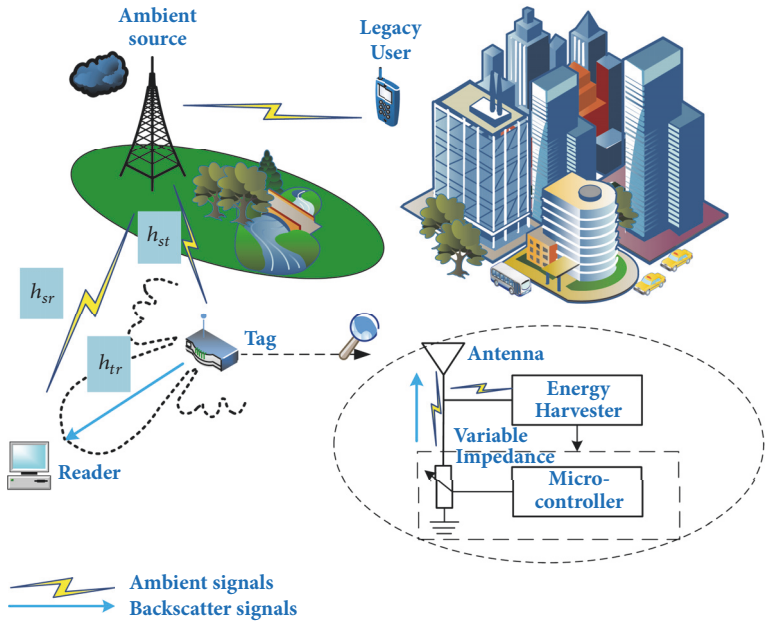

Figure 1: Ambient backscatter system.

Comparisons have shown that the method most suited for IoT sensing applications is beamforming, which allows the signal to propagate in a specified direction [10]. Through beamforming technology, the signal-to-noise ratio (SNR) is increased at the legitimate reader whereas it is reduced at the illegal eavesdropper, thereby enhancing the security performance of the system.

In order to achieve similar beamforming functions in a sensor network, we focused our research on the antenna design of the relay tag. Existing relay antennas have problems such as very large size, poor directivity, and small transmission gain [11]. We designed a dual-antenna system consisting of a patch antenna array and a printed log-periodic dual-dipole antenna (LPDA) with the advantages of orientation and high gain. At the same time, it has a fairly wide operating frequency band, which can effectively utilize various types of signals in the environment. Moreover, the small side lobes reduce the SNR received by eavesdroppers from other directions, ensuring the security of communication. In practical applications, the patch antenna array receives RF signals from all directions and then transmits them through the LPDA in a specified direction.

Traditional antenna designs are mostly based on experience and simulations to continuously modify the relevant parameters, which is time consuming and arduous. As a machine learning algorithm, genetic algorithms have been widely used in antenna design to search for large-scale, nonintuitive solution space and find the optimal parameter value. In [12], a genetic algorithm was used to optimize the structure and length of a wire antenna. In [13], an improved hierarchical Bayesian optimization algorithm was applied to the optimization of the antenna array feed network. However, the single-objective genetic algorithms used in the above-mentioned research may not be suitable for real situations because it over-emphasizes the importance of one metric. To solve this problem, we use a multiobjective genetic algorithm to optimize the antenna by using gain, side lobe, return loss, and voltage standing wave ratio (VSWR) as objective functions.

The remainder of this paper is organized as follows. Section 2 introduces the ambient backscatter communication model and the use of the directional antenna to achieve physical layer security. Section 3 illustrates the structure of the proposed antenna and the optimization process of the multiobjective genetic algorithm. Section 4 presents the simulation and optimization results of the antenna structure, followed by Section 5, which concludes the paper.

2. System Model

Ambient backscatter has become a promising option for self-sustainable communication systems because of its energy-saving features, and has good potential for widespread use in the IoT. A typical ambient backscatter system includes an ambient source, a passive tag, and a reader, as illustrated in Figure 1.

The communication process within the tag is as follows. When an ambient source broadcasts signals to its legacy users, such as mobile phones and laptops, the tag can harvest the RF energy from the signals and use the collected energy to power the entire system. Then the micro-controller in the system tunes the variable impedance based on the signal to indicate bit "1" or "0" by backscattering or absorbing the ambient signals [14, 15]. Finally, the reader decodes the backscattered signals and recovers the two information bits, completing the tag-to-reader communication.

Evaluating the security of the system and selecting an appropriate solution improves the security of the system. A

directional antenna designed for the tag is an effective means to achieve beamforming in the IoT scenario.

2.1. Ambient Backscatter System and Signal Detection. In ambient backscatter systems, the detection of the received signal plays a vital role. Without loss of generality, we denote h_{st}, h_{sr}, and h_{tr} as gains of the channels from the source to the tag, from the source to the reader, and from the tag to the reader, respectively. We assume that $s(n)$ represents the RF source signals with zero mean and unit variance. The power of the ambient source is P_s and is unknown to the receiver. The received signal at the tag is expressed as

$$y_t(n) = \sqrt{P_s} h_{st} s(n) + w_t(n) \tag{1}$$

where $w_t(n)$ is the noise inside the tag which can be ignored because here and the tag is a passive component, i.e., $w_t(n) = 0$ [16].

The signal backscattered by the tag is

$$x_t(n) = \eta x(n) y_t(n) \tag{2}$$

where $x(n) \in \{0, 1\}$ controls the working condition of the tag antenna. The tag reflects the signal when $x(n) = 1$, and the tag does not reflect when $x(n) = 0$. $\eta \in [0, 1]$ is the attenuation factor inside the tag. The signal received at the reader is

$$\begin{aligned} y_r(n) &= h_{sr} s(n) + h_{tr} x_t(n) + w(n) \\ &= \begin{cases} \sqrt{P_s} h_0 s(n) + w(n) & x(n) = 0 \\ \sqrt{P_s} h_1 s(n) + w(n) & x(n) = 1 \end{cases} \end{aligned} \tag{3}$$

where $h_0 \triangleq h_{st}$, $h_1 \triangleq h_{sr} + \eta h_{st} h_{tr}$, and $w(n)$ is the additive white Gaussian noise (AWGN) with zero mean and σ_w^2 variance.

In ambient backscatter systems, the amplitude or phase of the backscattered signals always carries the required information.

According to amplitude or phase modulation, the main task of the backscatter reader is to determine the amplitude or phase variation. In most cases, demodulation from backscattered waves with the binary amplitude modulation requires envelope detection at the receiver. Alternatively, phase demodulation is based on phase detection. Common methods of phase demodulation include the use of a homodyne receiver with an RF in-phase/quadrature demodulation and channel estimation [17]. Subsequently, the demodulator can acquire the information bit modulated on the phase by utilizing the channel estimation value.

The conventional detection scheme of the reflected signals uses preamble packets as thresholds for detection. In recent years, many other detection schemes have been developed. For example, a detector based on differential encoding can finish the detection without the knowledge of the channel state information (CSI) [18]. A joint-energy detection scheme requires only the channel variances without requiring the specific CSI and recently, a maximum-likelihood (ML) detector has been commonly used.

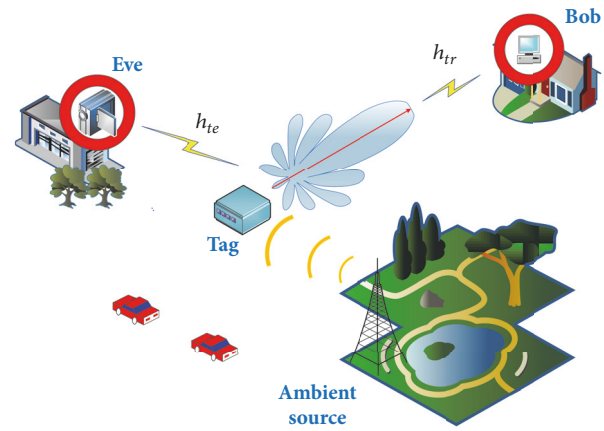

Figure 2: Wiretap channel model.

2.2. Security Assessment. Since the hardware of the tag limits the signal processing capability, the security of communication becomes a challenge for the IoT. Traditional encryption technology that relies on high computational complexity does not meet the requirements of the IoT application scenario. Beamforming, AN, cooperative interference, differential channel estimation, and network coding have become common physical layer security solutions. Among them, beamforming technology is most suitable for IoT security and allows wireless signals to propagate only in specific directions.

As shown in Figure 2, the data in the tag are modulated into the ambient carrier and the information signal is received by the legal receiver Bob over the "main channel," whereas it is received by the eavesdropper Eve over an additional "wiretap channel."

The secrecy capacity is used to measure the security of the system. In the wiretap channel, the secrecy rate is a transmission rate that can be reliably transmitted on the main channel but cannot be transmitted on the eavesdropping channel. In the case of one eavesdropper, the secrecy capacity is

$$R_s = \max\{R_d - R_e\} \tag{4}$$

where R_d is the communication rate of the source-destination link and R_e is the communication rate of the source-eavesdropper link. Usually, it is calculated as the difference between the mutual information in the primary and eavesdropping channels: $I(A; B) - I(A; E)$.

In the case of multiple eavesdroppers, the secrecy capacity is

$$R_s = \max \min_j \left\{R_d - R_e^j\right\} \tag{5}$$

The secrecy outage probability is another important variable in physical layer security communication. It is the likelihood that the instantaneous secrecy rate R_s is below a predefined threshold ε for a particular fading distribution.

$$P_{out} = P\{R_s < \varepsilon\}, \quad \varepsilon > 0 \tag{6}$$

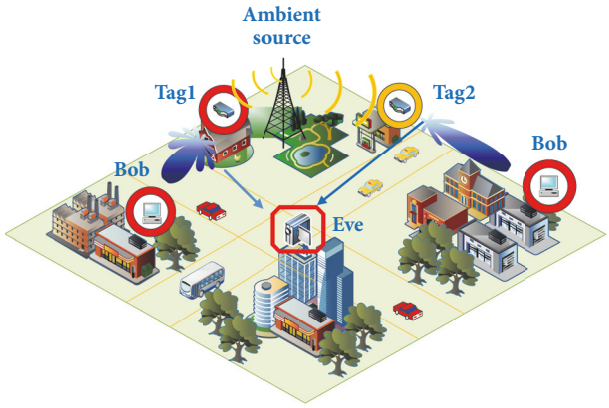

Figure 3: Influence of antenna side lobes on communication.

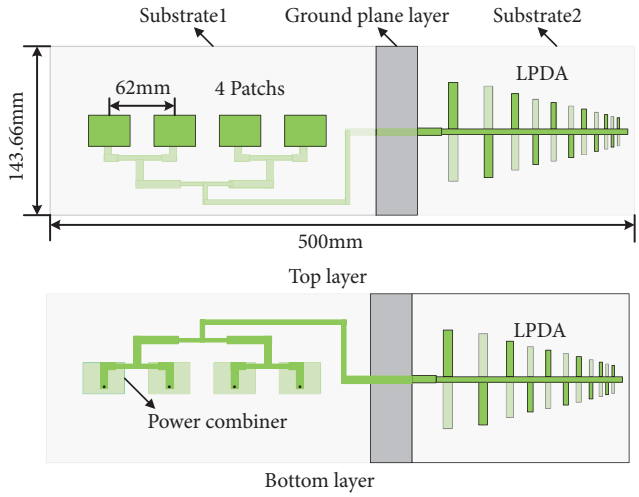

Figure 4: Dual-antenna system structure.

An analysis from the perspective of information theory indicates that the mutual information depends on the SNR of the received signal, which indicates that the secrecy capacity is determined by the SNR of the legal receiver and of the eavesdropper [19].

By using beamforming at the tag, we change the direction of the antenna to increase the gain of the main channel and reduce the signal strength of the wiretap channel by reducing the side lobes. In this way, the security of the system is enhanced and the secrecy capacity is improved, as well.

2.3. Antenna Demand. In the IoT application scenario, in order to achieve beamforming and meet the constraints of limited hardware, we designed a directional antenna with high gain and small side lobes to be used in the tag.

The previous discussion shows that providing different SNRs for eavesdroppers and readers is a key task to improve communication security. The directional antenna increases the peak gain of the antenna, thereby improving spatial reuse and expanding the geographic coverage in a given direction [20]. Moreover, the use of directional antennas improves the wireless network capacity, avoids physical jamming attempts, enhances data availability, and suppresses interference from neighbors. In addition, the antenna is required to have fewer side lobes.

We can observe in Figure 3 that Tag1 has more side lobes than Tag2 and higher side lobe levels. When the side lobes are small, the main lobe has a large transmit power, which maximizes the signal power in the desired direction while suppressing signals in undesired directions. Thus, a goal can be achieved to maximize the ratio of the SNRs received by the reader and the eavesdropper.

In addition, higher frequency signals experience several orders of magnitude of free space path loss and, therefore, communication coverage is small. By using a small sidelobe antenna, we can increase the transmission distance in the specified direction.

In order to achieve these goals, we designed a dual-antenna system consisting of a patch antenna array and a printed LPDA. The patch antenna receives the RF signal from all directions and the LPDA is directed at the reader. In addition, we use a multiobjective genetic algorithm to optimize the antenna side lobes, reduce the peak value of the largest side lobes, and enhance the directionality of the antenna.

The designed antenna does not require additional power, which prevents the disadvantages of traditional physical layer security technology. The specific structure of the antenna is described in detail in Section 3.

3. Antenna Design and Optimization

3.1. Antenna Model. The antenna system structure on the tag is shown in Figure 4 and is located on the XOY plane. The system consists of three components: a four-element patch antenna array, a feeding network, and a printed LPDA. Taking into account the receiving range and antenna gain, the receiving plane uses a simple coaxial probe-fed patch antenna. It is located on the top layer. The feed network consisting of the power combiner and the corresponding substrate is located on the bottom layer and shares the ground plane with the patch antenna array. The patch antennas coaxial probe is connected to the four input ports of the power combiner through two layers of substrate and a ground plane. The printed LPDA acts as a transmit antenna and is connected to the output port of the combiner. The total size of this dual-antenna system is $500 \times 143.66 \times 8.175 mm^3$. It is evident from the reciprocity of the antenna that when the incident wave is irradiated from the +z direction to the four-element patch antenna array, the received electromagnetic wave is transmitted to the printed LPDA through the feed network for reradiation with polarization transition characteristics, thereby changing the incident wave transmission direction and achieving the function of omnidirectional reception and directional transmission.

3.2. Calculation of the Antenna Initial Size

3.2.1. Receiving Antenna. Because high gain is a priority, a rectangular patch antenna fed by a coaxial probe is used as

the receiving antenna for the dual-antenna system. A Rogers TMM4 with a dielectric constant $\varepsilon_r = 4.5$ is chosen as the substrate with a thickness of 5 mm. According to the empirical formula provided in [21], the initial length W and width L of the patch are calculated as

$$L = \frac{c}{2f_0}\frac{1}{\sqrt{1/\varepsilon_e}} - 2\Delta L \tag{7}$$

$$W = \frac{c}{2f_0}\left(\frac{\varepsilon_r + 1}{2}\right)^{1/2} \tag{8}$$

where c is the speed of light, f_0 is the resonant frequency, h is the thickness of the substrate, ε_r is the dielectric constant of the substrate, and ε_e is the effective dielectric constant. ε_e and ΔL are calculated using the following formula:

$$\varepsilon_e = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\left(1 + 12\frac{h}{L}\right)^{1/2} \tag{9}$$

$$\Delta L = 0.412h\frac{\left(\varepsilon_e + 0.3\right)\left(W/h + 0.264\right)}{\left(\varepsilon_e - 0.258\right)\left(W/h + 0.8\right)} \tag{10}$$

The position of the feed point can be calculated by

$$X_f = \frac{L}{2\sqrt{\varepsilon_e}} \tag{11}$$

Considering the mutual coupling effect between the patches, the interval between the adjacent units is $0.5\lambda_g \sim \lambda_g$.

The four-element rectangular patch antenna array is fed in parallel by a 1-4 power combiner. The distances from the input port to every unit are equal to achieve the same phase feed.

3.2.2. Transmitting Antenna. An LPDA is a wideband antenna. In order to make the tag structure more compact, a flat printed structure is used to integrate the transceiver antennas into one plane. The structure of the printed LPDA is shown in Figure 5. The length of the antenna element is denoted by L_n and the extension of the end of each antenna element intersects at a point, called a virtual vertex, with an opening angle of α. The vertical distance from the virtual vertex to each antenna element is represented as R_n, the vibrator width is represented as w_n, and the adjacent two vibrators are separated by d_n.

The geometry of the antenna is determined by the geometric factor τ and the spacing factor σ.

$$\tau = \frac{h_{n+1}}{h_n} = \frac{L_{n+1}}{L_n} = \frac{d_{n+1}}{d_n} \tag{12}$$

$$\sigma = \frac{d_n}{4h_n} \tag{13}$$

The number of antenna elements is obtained by the following formula:

$$N_a = 1 + \frac{lg\left(K_2/K_1\right)}{lg\tau} \tag{14}$$

where K_1 and K_2 are the cutoff coefficients.

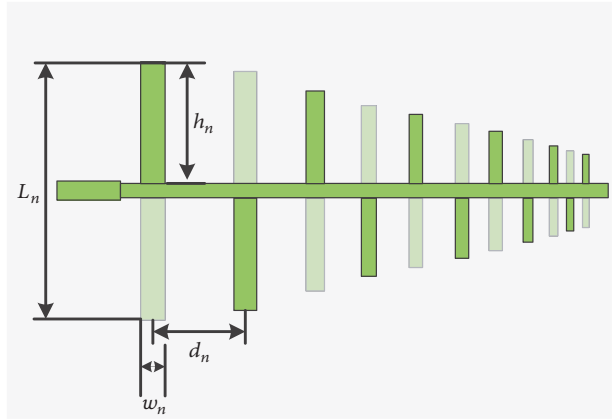

Figure 5: The structure of the printed LPDA.

$$K_1 = 1.01 - 0.519\tau \tag{15}$$

$$K_2 = 7.01\tau^3 - 21.3\tau^2 + 21.98\tau - 7.30 + \sigma\left(21.82 - 66\tau + 62.12\tau^2 - 18.29\tau^3\right) \tag{16}$$

In addition, it is necessary to estimate the width of the elements as follows:

$$Z_a \approx 120\ln\left(\frac{h}{a}\right) - 2.25 \tag{17}$$

where h/a is the half-height-to-radius ratio of the dipole. In the planar printing structure, we use microstrip patches instead of cylindrical dipoles. Considering the equivalent perimeters of the cylindrical and thin rectangular conductors, we used the approximate relationship $w \approx \pi a$, where Z_a represents the average characteristic impedance, which is 50Ω here. w represents the dipole width.

The LPDA is an end-fire antenna and the maximum radiation direction is from the longest oscillator to the shortest oscillator [22]. When the operating frequency changes, the radiation area of the antenna moves around the antenna and maintains similar characteristics; therefore, the pattern of the antenna changes little with the frequency. In general, the larger the value of τ, the higher the number of oscillators in the radiation region, the stronger the directivity of the antenna, and the smaller the half-power angle of the pattern. The lengths of the longest oscillator and the shortest oscillator of the LPDA determine the operating frequency.

The LPDA is a linearly polarized antenna. When the LPDA's oscillator plane is placed horizontally, it radiates or receives horizontally polarized waves; when its oscillator plane is placed vertically, it radiates or receives vertically polarized waves. Circular polarization is easier to achieve with a planar structure.

3.2.3. Optimization Scheme. Since the directional antenna has a larger impact on the physical layer security and the structure of the LPDA is more complex, the transmitting antenna is optimized. We select the lengths, widths, and spacings of the elements as variables for the optimization.

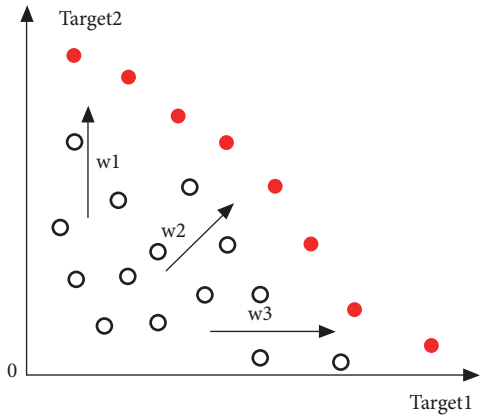

Figure 6: Pareto front.

During the design of the antenna, the gain, bandwidth, side lobes, and standing wave ratio (VSWR) of the antenna are important indicators of the performance of the antenna. Therefore, the function corresponding to the abovementioned four indicators is defined as the objective function.

In the actual design process of the antenna, there are usually multiple targets that need to be optimized. There may be contradictory relationships between the various objectives, and it is impossible to achieve optimality at the same time. Therefore, a multiobjective genetic algorithm (MOGA) was introduced.

In MOGA, there exists a set of Pareto-optimal or nondominated solutions generating a set of Pareto-optimal outcomes/objective vectors, which is called pareto front. Explicitly, the pareto front is generated by the specific set of solutions, for which none of the multiple objectives can be improved without sacrificing the other objectives, as shown in Figure 6.

A traditional multiobjective optimization scheme uses a method of assigning weights to convert multiple goals into a single goal. However, due to the nonconcaveness of multiobjectives, in order to find the Pareto front, a three-dimensional search is required for each weight $\overline{w} = [w_1, w_2, w_3]$, which is very time-consuming. Moreover, as the number of objective functions increases, the complexity of the weighting method is greatly increased. In addition, it is challenging to assign weights to each decision variable. Therefore, a new optimization solution is needed.

In this study, a multiobjective genetic algorithm (MOGA) is introduced as an optimization scheme, namely, the nonsorting genetic algorithm (NSGA)-II. The NSGA-II is considered one of the classic MOGAs. The algorithm obtains a potential uniformly distributed Pareto optimal solution set by fast nondominated sorting, crowded degree calculation, and an elitism strategy. This is very helpful for improving the exploratory capacity of the NSGA.

The specific process is shown in Figure 7.

The NSGA-II first finds nondominated solutions in the population and stratifies the population through nondominated sorting. Subsequently, these points are removed and identified and the nondominated solutions in the remaining population are removed. The algorithm updates the current

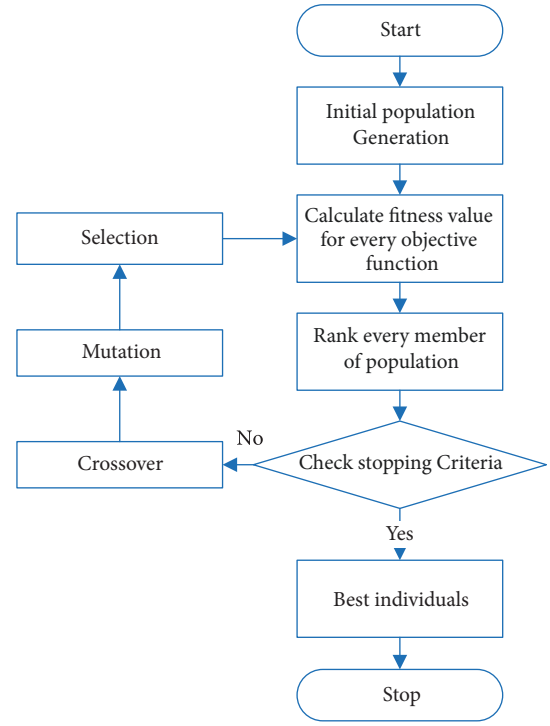

Figure 7: Flowchart of the MOGA.

archive by identifying the old archive and all current nondominated solutions in the aggregate. These layers are used in turn until the maximum archive is reached. The point closest to the target value is obtained by considering the crowding distance operator.

Unlike traditional optimization methods, MOGAs do not convert multiple targets into a single target for optimization using weighting but seek to optimize multiple targets simultaneously. Thereby, an optimal solution set can be found that satisfies multiple goals.

3.2.4. Decision Variables. A multiobjective optimization problem with three decision variables and four objective functions is expressed as

$$Optimal\overline{F}(\overline{x}) = [F_1(\overline{x}), F_2(\overline{x}), F_3(\overline{x}), F_4(\overline{x})] \quad (18)$$

where $\overline{F}(\overline{x})$ is the vector of the objective functions. $F_1(\overline{x}), F_2(\overline{x}), F_3(\overline{x}), F_4(\overline{x})$ represent the objective functions, where $\overline{x} = [L_1, L_2, \ldots, L_n, d_1, d_2, \ldots, d_n, w_1, w_2, \ldots, w_n]$.

Here, X and Z represent the search space and the target space, respectively. Thus, using the mapping $\overline{F} : X \longrightarrow Z$ each vector $\overline{x} \in X$ corresponds to a vector $\overline{z} = \overline{F}(\overline{x}) \in Z$.

We ensure that the height of the high-order oscillator is greater than the length of the low-order oscillator. All are within the appropriate range. According to the physical meaning of the variable, its optimization range is given as $L_i \in [5, 40]$, $d_i \in [1, 15]$, $w_i \in [0.1, 3]$ (unit: mm).

3.3. Objective Function

3.3.1. Bandwidth. The objective function is designed to increase the antenna bandwidth so that the transmit antenna

can operate over a wider frequency range. The target frequency band is determined by a $10dB$ return loss S_{11} and ranges from $2GHz$ to $4GHz$. Therefore, the fitness function is defined as the average of the return loss of less than $-10dB$ in the frequency band.

$$F_1(\overline{x}) = \frac{1}{N}\sum_{i=1}^{N} Q(f_i) \tag{19}$$

$$Q(f_i) = \begin{cases} 10 & S_{11} < -10 \\ |S_{11}(f_i)| & S_{11} \geqslant -10 \end{cases} \tag{20}$$

In the above equation, f_i is the sampling frequency. If the average value of S_{11} at the sampling frequency is less than $-10dB$, it is concluded that the design goal has been achieved.

In the design example, we set the parameters as follows:

The sampling frequency is $N = 5$; $f_1 = 2GHz$, $f_2 = 2.5GHz$, $f_3 = 3GHz$, $f_4 = 3.5GHz$, and $f_5 = 4GHz$. When $F_1(x) \geqslant 10$, the objective function is satisfied.

3.3.2. VSWR. The VSWR is an important indicator to measure the antenna matching state; the VSWR is limited to $[1, 1.8]$

$$VSWR(f_i) = \begin{cases} VSWR & VSWR \leqslant 1.8 \\ 1.8 & VSWR < 1.8 \end{cases} \tag{21}$$

$$F_2(\overline{x}) = \frac{1}{N}\sum_{i=1}^{N} VSWR(f_i) \tag{22}$$

where $N = 5$ is the number of sampling points of $2 \sim 4GHz$. When $F_2(x) \leqslant 1.8$, the objective function is satisfied.

3.3.3. Gain. The antenna gain is a measure of the ability of an antenna to transmit and receive signals in a specific direction. It is an important indicator used for antenna optimization. The average gain in the band is used as the objective function:

$$F_3(\overline{x}) = \frac{1}{N}\sum_{i=1}^{N} Gain(f_i) \tag{23}$$

3.3.4. Side Lobes. Since the antenna has many side lobes, the maximum side lobes tend to have a level that is not much different from the maximum gain of the antenna. In the physical layer security, there is a strict requirement for the orientation of the antenna and it is necessary to reduce the peak value of the highest side lobes as much as possible. This is required because if the eavesdropper is located in the direction of the largest side lobe, information leakage may occur. Therefore, the optimization goal is the minimization of the maximum peak of the side lobes.

The total radiation pattern factor $f(\theta, \phi)$ of the M cells of the LPDA shown in Figure 4 is

$$\begin{aligned} f(\theta,\phi) &= \sin\theta \sum_{p=1}^{M} L_p \\ &\cdot \exp\left[jk\left(X_p \sin\theta\cos\phi + Y_p \sin\theta\sin\phi + Z_p\cos\theta\right)\right] \\ &\cdot \sum_{n=1}^{N} (-1)^n \times \frac{(2n-1)\, L_{np} \cos\left(\pi L_p \cdot \cos\theta\right)}{(2n-1)^2 - \left(2L_p \cdot \cos\theta\right)^2} \end{aligned} \tag{24}$$

The optimization goal is min $F_4(\overline{x})$, subject to

$$F_4(\overline{x}) = \max_{f_i \in [2GHz, 4GHz]} \left(SLL(f_i)\right) \tag{25}$$

3.3.5. Fuzzy Decision Making. Fuzzy set theory is a method to find the optimal compromise solution from the Pareto front. Using linear fuzzy membership function modeling, the objective function value is mapped to the satisfaction function. This defines a linear membership function sf_n

$$sf_n = \begin{cases} 1 & if\ z_n \geqslant z_n^{max} \\ 1 - \dfrac{z_n^{max} - z_n}{z_n^{max} - z_n^{min}} & if\ z_n^{min} < z_n < z_n^{max} \\ 0 & if\ z_n \leqslant z_n^{min} \end{cases} \tag{26}$$

where z_n^{min} and z_n^{max} are the minimum and maximum values of the $n - th$ objective function respectively. The canonical membership function of the $n - th$ nondominated solution of the objective function is expressed as

$$s_j = \frac{\sum_{n=1}^{N_{obj}} sf_n^j}{\sum_{j=1}^{M_{par}} \sum_{n=1}^{N_{obj}} sf_n^j} \tag{27}$$

where N_{obj} represents the number of objective functions and M_{par} is the number of nondominated solutions in the Pareto front. We choose the solution vector with the maximum s_j value as the optimal compromise solution.

4. Numerical Results

The design examples and results are provided in this section and represent the optimal design of the LPDA based on the multiobjective genetic algorithm.

The signals in the domestic environment are mainly composed of four types: WiFi signals, terrestrial digital TV broadcast signals, mobile 4G signals, and upcoming 5G signals which has ultra-high spectrum utilization and ultra-low power consumption and will be widely used in the future. Considering the requirements of the signal coverage in various environments, transmission rate, signal stability, security, signal spectrum, and transmission power, a working frequency band of $2GHz \sim 4GHz$ is used in order to meet the requirements of IoT communications. The antenna design goals are shown in Table 1.

According to the design optimization scheme, 35 variables are selected as the optimization variables, including the length $L_1 \sim L_{12}$, the width $w_1 \sim w_{12}$, and the spacing $d_1 \sim d_{11}$ of the elements. The optimization ranges $L_i \in [5, 40]$, $d_i \in [1, 15]$, and $w_i \in [0.1, 3]$ (unit: mm) are used.

Table 1: Antenna design index.

Index	Value
Working frequency	$2GHz \sim 4GHz$
Maximum VSWR in the band	< 2
Average VSWR	< 1.3
Minimum gain in the band	$> 5dB$
Average gain	$> 6.5dB$
Maximum side lobe level	$< -4dB$
Return loss (S_{11})	$< -10dB$
Antenna size	$< 30cm$

Table 2: Simulation parameter optimization (unit: mm).

L_1	L_2	L_3	L_4	L_5	L_6	L_7
36	32.4	29.16	26.24	23.62	21.26	19.2
L_8	L_9	L_{10}	L_{11}	L_{12}	d_1	d_2
17.22	15.50	13.95	12.55	11.30	13	11.7
d_3	d_4	d_5	d_6	d_7	d_8	d_9
10.53	9.48	8.53	7.68	6.91	6.22	5.60
d_{10}	d_{11}	Gain	SLL			
5.04B	4.53	$7.0dB$	$-5.76dB$			

Based on a large number of simulation calculations, we chose the NSGA-II algorithm to optimize the antenna parameters. We set the population size to 100, the maximum number of iterations to 250, the crossover probability to $p_c = 0.7$, and the mutation probability to $p_m = 1/n_{var}$, where $n_{var} = 35$ is the number of decision variables. The frequency is sampled at intervals of $500MHz$ in the $2GHz$ to $4GHz$ band. After iterative optimization, the antenna parameters were obtained and are shown in Table 2.

The criteria for measuring the quality of an algorithm are time complexity and space complexity. Time efficiency refers to the execution time of the algorithm. Regarding the computational complexity of genetic algorithms, Goldberg et al. proposed the concept of takeover time to discuss the time complexity of the algorithm [23]. In the antenna design of this paper, the time complexity is defined as the calculation time, i.e., the number of iterations it takes to find an optimal solution, which is more practical.

The genetic algorithm can end with convergence or end with the number of iterations [24]. After several iterations, the results began to stabilize. Therefore, this paper selects 250 iterations as the end condition. At this point each target meets the design requirements.

An excitation source is used to stimulate the receiving and transmitting antennas at the same time to simulate the overall gains G_1 and G_2. A pattern of the LPDA antenna at a center frequency of $2.4GHz$ can be obtained, as shown in Figure 7. It can be seen that the planar LPDA has good directivity and can be optimized to achieve gains of $7.0dB$. The reciprocity of the antenna indicates that a certain range of electromagnetic waves received by the patch antenna is radiated through the LPDA and used as a relay antenna on the tag.

In Figure 8, a comparison of patterns before and after optimization is shown. Prior to the optimization, there are

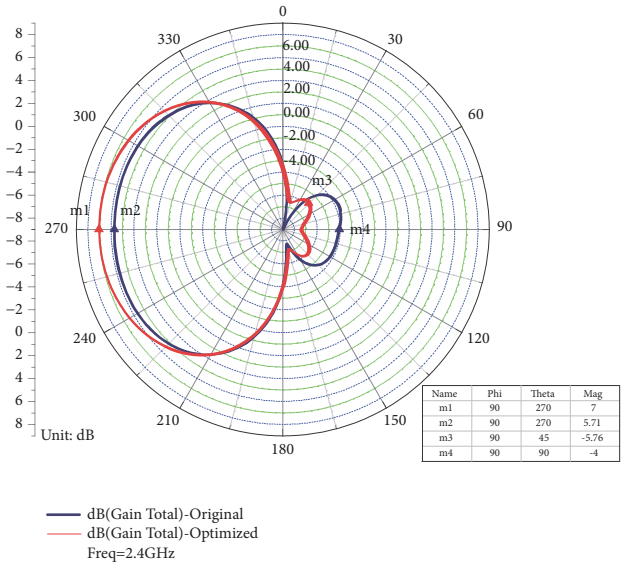

Figure 8: Gain and side lobes before and after optimization.

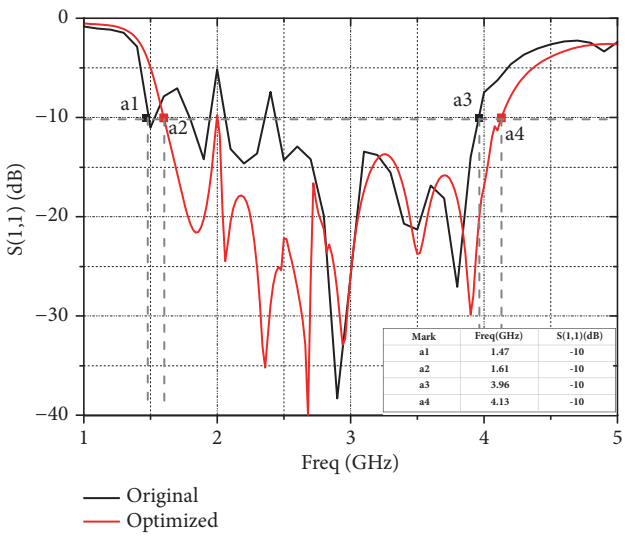

Figure 9: Return loss S_{11}.

1 large side lobes, and the maximum side lobe level is $-4dB$. After optimization, the maximum side lobes are reduced to $-5.76dB$, which effectively enhances the directionality of the antenna.

The curves shown in Figures 9 and 10 show the changes in the return loss S_{11} and the VSWR versus the frequency before and after optimization, respectively. It can be seen that the optimized $10dB$ impedance bandwidth is $2.5GHz$ and the average VSWR in the band is 1.3, reaching the expected target.

In order to prove that the designed antenna can effectively improve the security of the channel, we evaluate the channel secrecy capacity.

Assume that the ambient source power is P_t, the transmission gain is G_t, the distance from the ambient source to the tag is r_1, and the distance from the tag to the reader is r_2.

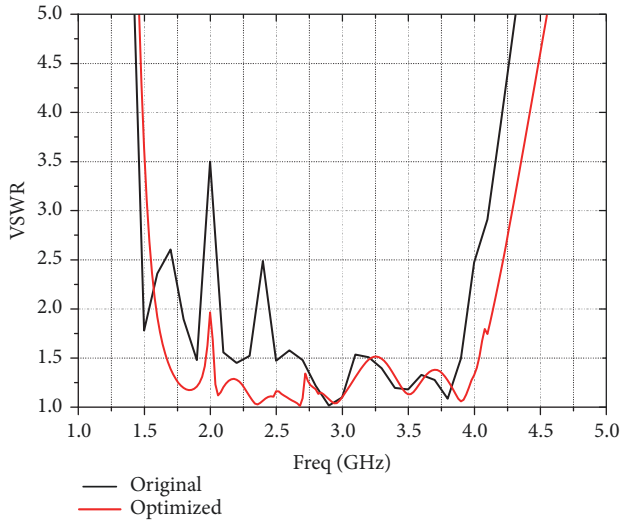

Figure 10: VSWR vs. frequency.

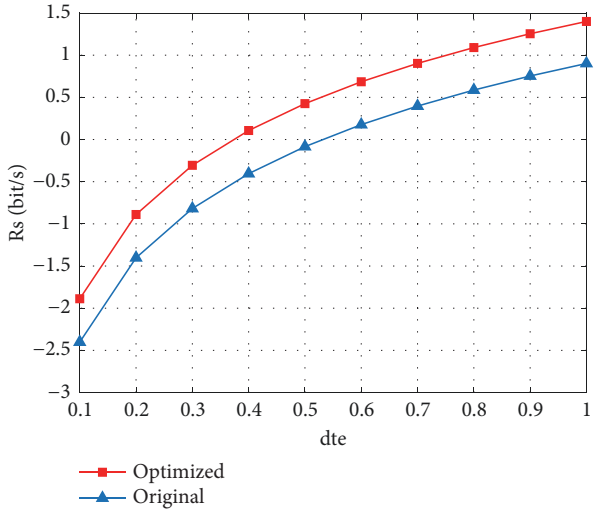

Figure 11: Secrecy capacity assessment.

From the radar equation, the signal power P_r received by the reader can be obtained as

$$P_r = \frac{P_t G_t}{4\pi r_1^2} \cdot \frac{\sigma}{4\pi} \cdot \frac{A_r}{r_2^2} \tag{28}$$

where σ is the radar cross section and $A_r = G_r \lambda_0^2 / 4\pi$ is the effective area of the receiving antenna. G_r is the gain of the reader received signal and λ_0 is the signal wavelength.

Assume that the received power of the legitimate user is P_d, the noise power received by the legitimate user is N_d, the received power of the illegal eavesdropping user is P_e, and the received noise power is N_e. R_d and R_e represent the primary channel and eavesdropping channel capacity, respectively. The secrecy capacity can be calculated as

$$R_s = R_d - R_e = \frac{1}{2} \log\left(1 + \frac{P_d}{N_d}\right) - \frac{1}{2} \log\left(1 + \frac{P_e}{N_e}\right) \tag{29}$$

where P_d and P_e can be obtained from (28). In the same communication system, each node receives the same noise, i.e., $N_d = N_e$. All simulation data were quantified and the results of the evaluation are shown in Figure 11. The abscissa d_{te} indicates the distance between the eavesdropper and the tag, and the ordinate indicates the channel secrecy capacity. After optimization, the channel secrecy capacity is increased by $0.5 bit/s$ overall.

The results indicate that the relay antenna is optimized by the multiobjective genetic algorithm; the gain is 7.0 dB and the maximum side lobe level is reduced to $-5.76 dB$, which enhances the antenna's directionality. This makes it more difficult for the eavesdropper to obtain communication information. The antenna can be safely applied in the ambient backscatter communication of the IoT.

5. Conclusion

In this study, we investigated an important communication form of the IoT, i.e., ambient backscattering, and proposed a machine learning based antenna design scheme for physical layer security. The directional communication from the relay tag to the reader is achieved by combining a patch antenna and an LPDA. In order to reduce antenna side lobes and improve orientation performance, we used a multiobjective genetic algorithm to optimize the antenna size and obtain a set of optimal Pareto fronts. The simulation results justified that our proposed antenna design has a simple structure, saves energy, and can effectively protect the physical layer IoT communications.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," in *Proceedings of the the ACM SIGCOMM 2013 conference*, p. 39, Hong Kong, China, August 2013.

[2] D. T. Hoang, D. Niyato, P. Wang, D. I. Kim, and Z. Han, "Ambient Backscatter: A New Approach to Improve Network Performance for RF-Powered Cognitive Radio Networks," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3659–3674, 2017.

[3] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient Backscatter Assisted Wireless Powered Communications," *IEEE Wireless Communications Magazine*, vol. 25, no. 2, pp. 170–177, 2018.

[4] C. Perez-Penichet, "Ph.D. Forum Abstract: Ambient Backscatter Communication," in *Proceedings of the 15th ACM/IEEE*

International Conference on Information Processing in Sensor Networks, IPSN 2016, Austria, April 2016.

[5] S. Han, S. Xu, W. Meng, and C. Li, "Dense-Device-Enabled Cooperative Networks for Efficient and Secure Transmission," *IEEE Network*, vol. 32, no. 2, pp. 100–106, 2018.

[6] W. Zhang, W. He, X. Chen, Y. Cai, X. Guan, and J. Qu, "Power allocation for improving physical layer security in D2D communication via stackelberg game," in *Proceedings of the 8th International Conference on Wireless Communications and Signal Processing, WCSP 2016*, pp. 1–5, Yangzhou, China, October 2016.

[7] T. Q. Duong, "Keynote talk #1: Trusted communications with physical layer security for 5G and beyond," in *Proceedings of the International Conference on Advanced Technologies for Communications (ATC)*, p. xxxiv, Quy Nhon, Vietnam, 2017.

[8] P. Zhang, Y. Ma, and B. Wang, "Improving physical layer security via multiple-level relay network," in *Proceedings of the 2014 12th IEEE International Conference on Signal Processing, ICSP 2014*, pp. 1851–1854, Hangzhou, China, October 2014.

[9] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[10] Z. Chen, H. Li, G. Cui, and M. Rangaswamy, "Adaptive transmit and receive beamforming for interference mitigation," *IEEE Signal Processing Letters*, vol. 21, no. 2, pp. 235–239, 2014.

[11] Q. Chen, S.-W. Qu, J. Li, L. Wang, Q. Yuan, and K. Sawaya, "Dual-antenna system composed of patch array and planar Yagi-Uda array," in *Proceedings of the 5th European Conference on Antennas and Propagation, EUCAP 2011*, pp. 1023–1026, Rome, Italy, April 2011.

[12] E. E. Altshuler and D. S. Linden, "Wire-antenna designs using genetic algorithms," *IEEE Antennas and Propagation Magazine*, vol. 39, no. 2, pp. 33–43, 1997.

[13] S. Santarelli, T.-L. Yu, D. E. Goldberg et al., "Military antenna design using simple and competent genetic algorithms," *Mathematical and Computer Modelling*, vol. 43, no. 9-10, pp. 990–1022, 2006.

[14] W. Zhao, G. Wang, R. Fan, L. Fan, and S. Atapattu, "Ambient Backscatter Communication Systems: Capacity and Outage Performance Analysis," *IEEE Access*, vol. 6, pp. 22695–22704, 2018.

[15] Y. Liu, G. Wang, Z. Dou, and Z. Zhong, "Coding and Detection Schemes for Ambient Backscatter Communication Systems," *IEEE Access*, vol. 5, pp. 4947–4953, 2017.

[16] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient Backscatter Communication Systems: Detection and Performance Analysis," *IEEE Transactions on Communications*, vol. 64, no. 11, pp. 4836–4846, 2016.

[17] S. J. Thomas and M. S. Reynolds, "A 96 Mbit/sec, 15.5 pJ/bit 16-QAM modulator for UHF backscatter communication," in *Proceedings of the 2012 6th IEEE International Conference on RFID, RFID 2012*, pp. 185–190, Orlando, FL, USA, April 2012.

[18] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High Throughput WiFi Backscatter," in *Proceedings of the 2015 ACM SIGCOMM*, London, UK, 2016.

[19] F. Zhu and M. Yao, "Improving Physical-Layer Security for CRNs Using SINR-Based Cooperative Beamforming," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1835–1841, 2016.

[20] W. X. Liu, Y. Z. Yin, W. L. Xu, and S. Zuo, "Compact open-slot antenna with bandwidth enhancement," *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 850–853, 2011.

[21] K. R. Carver and J. W. Mink, "Microstrip Antenna Technology," *IEEE Transactions on Antennas and Propagation*, vol. 29, no. 1, pp. 2–24, 1981.

[22] R. R. Pantoja, A. R. Sapienza, and F. C. Medeiros Filho, "A Microwave Printed Planar Log-Periodic Dipole Array Antenna," *IEEE Transactions on Antennas and Propagation*, vol. 35, no. 10, pp. 1176–1178, 1987.

[23] S. Han, S. Xu, W. Meng, and C. Li, "An agile confidential transmission strategy combining big data driven cluster and OBF," *IEEE Transactions on Vehicular Technology*, no. 99, article 1, 2017.

[24] S. Qiao, X. Dai, Z. Liu, J. Huang, and G. Zhu, "Improving the optimization performance of NSGA-II algorithm by experiment design methods," in *Proceedings of the 2012 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, CIMSA 2012*, pp. 82–85, Tianjin, China, July 2012.