Security and Safety, Vol. 2, 2023003 (2023)
https://doi.org/10.1051/sands/2023003
sands.edpsciences.org

Research Article

OPEN ACCESS

Information Network

Wireless communications "$N+1$ dimensionality" endogenous anti-jamming: theory and techniques

Fuqiang Yao, Yonggang Zhu*, Yifu Sun, and Wenlong Guo

The Sixty-third Research Institute, National University of Defense Technology, Nanjing 210007, China

Received: 28 December 2022 / Revised: 27 February 2023 / Accepted: 1 April 2023 / Published online: 02 August 2023

Abstract The existing theory and techniques of wireless communication anti-jamming have reached their performance limit recently. With this focus, by leveraging the inherent characteristics of wireless communication and referring to the principle of cyberspace endogenous security, this paper investigates the core issues of endogenous security in the electromagnetic space, namely, endogenous anti-jamming (EAJ), which can defend against unknown electromagnetic attacks effectively. Specifically, the subspace method is first adopted to establish the unified framework for the conventional spread-spectrum, intelligent, and endogenous anti-jamming, in which both the intrinsic development law of each technique and the internal logic between them are revealed. Then, the fundamental concept, key techniques, and development suggestions of wireless communication "$N+1$ dimensionality" endogenous anti-jamming are proposed to seek a disruptive breakthrough.

Keywords Wireless communication, Communication anti-jamming, Endogenous anti-jamming, Electromagnetic space security, Network space security, Command and control

Citation Yao FQ, Zhu YG, Sun YF, and Guo WL. Wireless communications "$N+1$ dimensionality" endogenous anti-jamming: theory and techniques. Security and Safety 2023; **2**: 2023003. https://doi.org/10.1051/sands/2023003

1 Introduction

Wireless communications are the primary or even the only command and control means in war and emergency situations. Thus, enabling infallible anti-jamming communications in the complex electromagnetic countermeasure environment is significantly important for wireless communications. However, the existing theory and techniques of communication anti-jamming have reached their performance limit, especially in dealing with unknown or intelligent jamming attacks. As such, it is necessary to explore new concepts and techniques of communication anti-jamming for breaking the bottleneck of existing ones.

The existing communication anti-jamming techniques can be roughly divided into two broad categories, namely, conventional spread-spectrum anti-jamming (CSSAJ) technique and intelligent anti-jamming (IAJ) technique [1]. The first category adopts Shannon information theory as the foundation, where the essential premise of this technique is to disperse the jamming power by spreading the spectrum of the legitimate signal. Besides, the confrontation between the competitive sides focuses on frequency and power domain, which has two typical techniques, *i.e.*, frequency-hopping (FH) and direct-sequence spread spectrum (DSSS) [1, 2]. However, due to the lack of the spectrum sensing ability, the performance of CSSAJ technique is confined by the limited spread spectrum factor. To elaborate, the communication link will be interrupted when the jamming bandwidth occupies more than 30% of the legitimate one [1]. On the other hand, with the advancement of artificial intelligence technology, the second category

* Corresponding author (email: zhumaka1982@163.com)

focuses on investigating the IAJ technique, in which the principle can be expressed as "change as enemy changed" [1]. In other words, with the assistance of precise jamming recognition, the anti-jammers adapt their communication parameters to the jammers' strategies. Depending on the intelligence level, the IAJ technique can be divided into adaptive one and cognitive. Recently, we proposed an intelligent anti-jamming prototype system to verify the performance of IAJ, in which intelligent recognition, intelligent decision, waveform maneuver, and spectrum maneuver techniques are realized.

However, there are at least two difficulties in the practical implementation of the IAJ technique. First, due to the fast time-varying property of complex electromagnetic environments in the battlefield, it is challenging to recognize and adapt to the unknown electromagnetic environment quickly enough. For example, if the jammers have N jamming patterns (such as single tone, frequency sweep, tracking jamming, *etc.*), they can launch $2^N - 1$ mixed jamming patterns theoretically, which can make the legitimate nodes get suck in the curse of recognition. Second, when the IAJ technique confronts the unknown or time-varying jamming attacks, it may fall into the endless observe-orient-decide-act (OODA) circle, *i.e.*, cognition-decision-adjustment-recognition-redecision-readjustment. Specifically, in the face of intelligent jamming attacks, the confrontation between the competitive sides focuses on the cognitive domain, namely, the side who can recognize the other strategy precisely and execute the confrontation strategy effectively by exploiting the advanced computing resources and intelligent algorithms, will win the competition [3]. However, in vehicular communication, the anti-jammers will not always have more powerful computing resources, advanced intelligent algorithms, and accurate prior knowledge than the jammers.

From the methodological perspective, the IAJ technique is a passive method of defense, *i.e.*, the anti-jammer changes as the jammer changes, whose performance would reach its limit. Motivated by these observations above, this paper proposes a novel methodology of communication anti-jamming to defend against unknown and intelligent jamming attacks, which provides an active mean of defense for anti-jamming communications and cuts off the endless OODA circle.

2 The meaning of endogenous anti-jamming

2.1 The concept of endogenous

In this subsection, we first clarify the concept of endogenous. Wu *et al.* [4] defined the endogenous factors as the interdependent and inseparable elements in a system. Building upon this concept of endogenous, the framework of cyberspace endogenous safety and security (ESS) was proposed in [5], where the executor was dynamically selected from the heterogeneous and redundant executor set such that a more uncertain system structure can be obtained, resulting in the improved security ability against the known or the unknown threats. Besides, by investigating the drawbacks of the existing information security, Hu *et al.* [6] proposed a bionic ESS to address the issue that the security mechanism is separate from the status of the network devices. Moreover, the concept of cyberspace ESS has been adopted for wireless communications. Jin *et al.* developed the concept of wireless endogenous safety and security (WESS) in [7], where the randomness, time-varying, and uniqueness of wireless channels were utilized to construct dynamic, heterogeneous, and redundant (DHR) channels [8].

From the philosophical perspective, the concept of wireless communications endogenous anti-jamming (EAJ) is consistent with that of cyberspace ESS. To elaborate, the passive precise-recognition-based mean of communication anti-jamming is converted into an active immunity-based one. However, EAJ and ESS are different in many aspects, such as the working scenario, attack types, protective objective, defense techniques, and so on. As such, to further elaborate the concept of the proposed EAJ, the subspace method in [9] is adopted to develop the unified framework for CSSAJ, IAJ, and EAJ, where both the intrinsic development law of each technique and the internal logic between them are revealed.

2.2 Existing typical anti-jamming techniques

The block diagram of CSSAJ is shown in Figure 1. It is assumed that the total system bandwidth is W, and the symbol period is T_s. Thus, the degree of freedom (DoF) of the communication signal space is $2T_sW$, namely, all the communication signals can be expressed as the combination of $2T_sW$ normalized

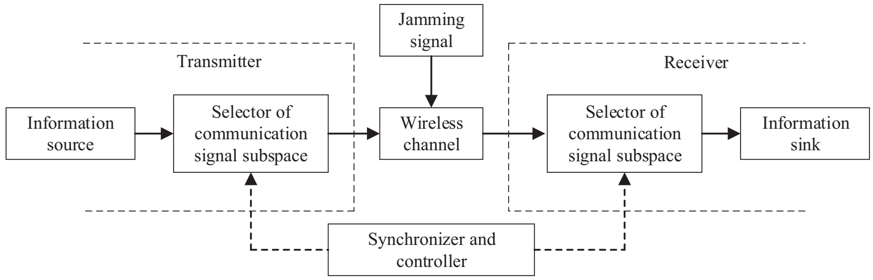

Figure 1. The block diagram of CSSAJ

orthogonal primary functions $\varphi_k\,(k = 0, 1, \ldots, 2T_sW - 1)$ [2]. As such, after dividing the signal space of CSSAJ into K subspaces, the DoF of each subspace is $D = 2T_sW/K$. In each timeslot, the transmitter randomly selects one of the subspaces for communication, *i.e.*,

$$s_k = \sum_{i \in A_k} a_i \varphi_i, \tag{1}$$

where $A_k = \{i : (k-1)\,D \le i < kD\}$, and $\{a_i\}$ is the set of the transmitted symbol. Then, the power of s_k is

$$E_s^t = \sum_{i \in A_k} a_i^2, \tag{2}$$

Besides, the received signal can be expressed as

$$r_k = s_k + J, \tag{3}$$

where J is the jamming signal. Note that the effects induced by the natural channel noise are ignored in the above equation for brevity. In order to launch effective jamming attacks without the knowledge of the communication signal subspace, the jammers should distribute their power in signal spaces as many as possible [2], *i.e.*,

$$J = \sum_{i=0}^{2T_sW-1} J_i \varphi_i + J_0, \tag{4}$$

where $\{J_i\}$ and J_0 are the jamming signals inside and outside the communication signal subspace, respectively. Thus, the power of the jamming signal is

$$E_J^t = \sum_{i=0}^{2T_sW-1} J_i^2 + E_{J_0}, \tag{5}$$

After filtering the received signal r_k by using the set of the primary functions $\{\varphi_{A_k}\}$ synchronously, the output signal is [2]

$$r_k^{\text{out}} = a_i + J_i,\, i \in A_k\,, \tag{6}$$

where the power of the communication signal and the jamming signal are

$$E_s^r = \sum_{i \in A_k} a_i^2, \tag{7}$$

$$E_J^r = \sum_{i \in A_k} J_i^2. \tag{8}$$

Define the spread spectrum processing gain G_p as the ratio of output and input signal-to-jamming energy ratio at receiver [1, 2], namely,

$$G_p = \frac{E_s^r}{E_J^r} \Big/ \frac{E_s^t}{E_J^t}. \tag{9}$$

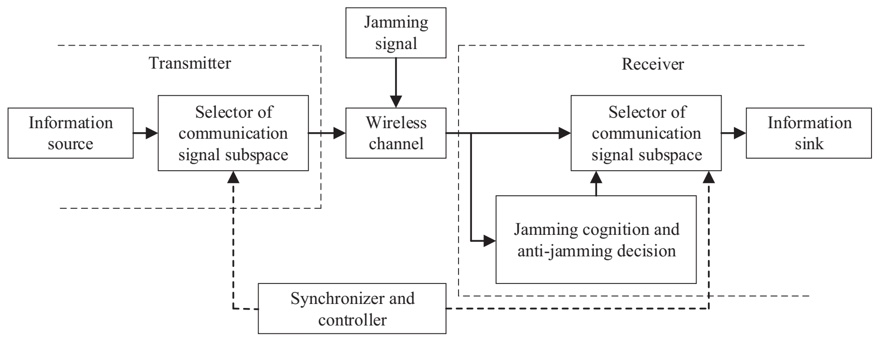

Figure 2. The block diagram of IAJ

Comparing Eq. (2) with (7), it can be observed that the power of the communication signals does not change after spread spectrum processing, *i.e.*, $E_s^t = E_s^r$. Thus, Eq. (9) can be simplified into $G_p = E_J^t / E_J^r$. Assuming that $J_0 = 0$ and jamming power is distributed in the K subspace uniformly, we can obtain $G_p = K$ by comparing Eq. (5) with (8). In other words, the essence of CSSAJ is to disperse the jamming power by expanding the legitimate signal subspace. However, with the significant increase of devices and the advancement of electromagnetic jamming attacks, it is challenging to obtain satisfactory anti-jamming performance by using CSSAJ, which calls for the new capability of anti-jamming communications.

The block diagram of IAJ is shown in Figure 2. Compared with the CSSAJ, the main difference between them is that the jamming recognition and intelligent decision modules are embedded in the receiver of IAJ, such that IAJ can accurately recognize the jamming signal subspace and accordingly adapt its signal subspace for dynamically eliminating the jammer's damage effects. Obviously, the performance of IAJ is directly dominated by the efficiency of the jamming recognition module.

With the advancement of deep learning technology, deep reinforcement learning (DRL) has been adopted to enable IAJ recently, where the jamming recognition and decision-making modules are integrated such that the anti-jammers can obtain their strategy with maximum reward by exploring and exploiting the communication signal space [10–13]. To some extent, DRL-based IAJ has made some progress in defending against unknown jamming attacks.

From the perspective of scientific approaches, IAJ is a passive precise-recognition-based mean, whose performance is significantly dominated by the acquisition and the usage of jamming knowledge. Thus, as the jammer dynamically adapts its strategies, the anti-jammer would easily get suck in the endless OODA circle [14]. Besides, the jammers may launch the attacks on the acquisition process of the jamming knowledge, which constitutes a new threat to anti-jamming communications [15–17].

As observed by these analyses above, although both CSSAJ and IAJ have played an important role in anti-jamming communications, they have reached their performance limit. Figure 3 shows the subspace relationships between CSSAJ, IAJ, and intelligent jamming, where both CSSAJ and IAJ combat the intelligent jamming within the limited signal spaces. Clearly, as the jamming power increases and the jamming pattern becomes more unpredictable, the performance gain of the existing anti-jamming techniques decreases significantly. In other words, when the jamming power can take up all the signal spaces, the abovementioned anti-jamming techniques may be invalid. More specifically, the limited signal space confines their performance. When there exists another signal subspace besides frequency f, time t, and power p, the signal space in Figure 3 becomes a hypersphere.

2.3 Endogenous anti-jamming techniques

A typical system of wireless communication is mainly composed of a transmitter, a wireless channel, and a receiver, which are the irreplaceable endogenous factors of a wireless communication system [18]. Different from the precise-recognition-based IAJ technique which adapts its anti-jamming strategy according to the jammer's strategy, EAJ utilizes the endogenous factors of the wireless communication system to construct a specific channel between the transmitter and the receiver. Thus, the wireless communication system can obtain the innate immunity for defending against various jamming attacks without the precise jamming recognition.

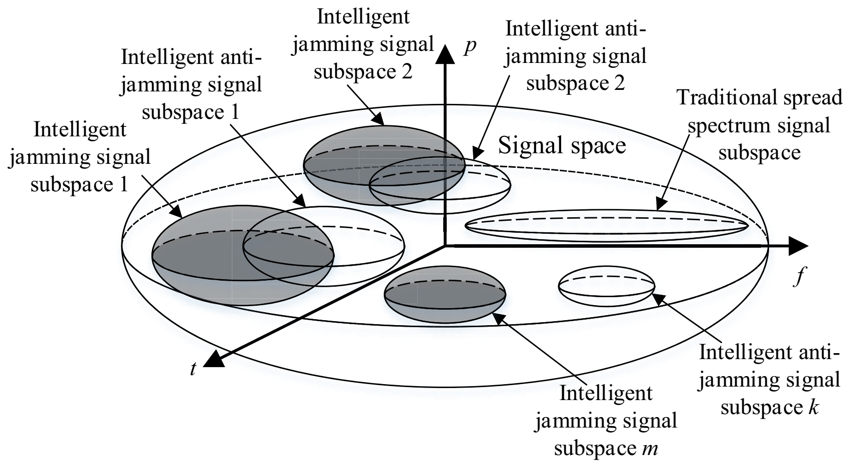

Figure 3. Subspace relationship between CSSAJ, IAJ and intelligent jamming

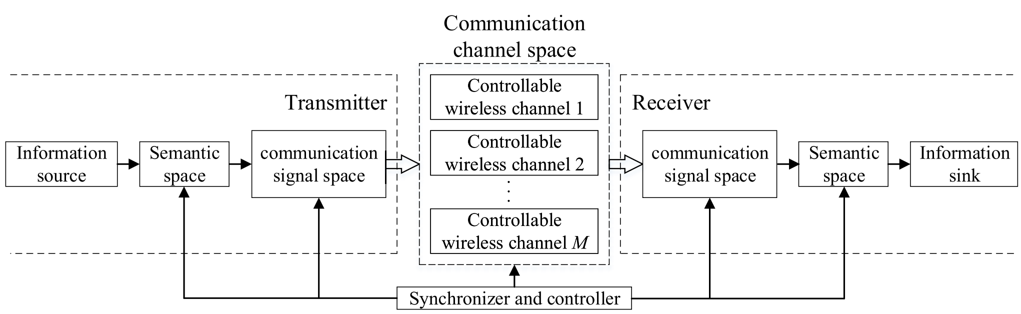

Figure 4. The block diagram of EAJ

In the wireless system, the endogenous factors which can be utilized are mainly the semantic space, communication signal space, and communication channel space. As shown in Figure 4, the above-mentioned spaces constitute a complete anti-jamming space. In particular, the semantic space is the mapping set from the information to the symbols in the different knowledge bases, semantic encoder and decoder. The communication signal space is the mapping set from the symbols to the communication signals with different modulations, encoding, and polarization. Besides, the communication channel space is the channel set between the transmitter and the receiver.

The endogenous properties of semantic space are mainly two folds. First, under the same conditions, the semantic communication would significantly compress the transmitted data such that more resources can be allocated for anti-jamming design [19, 20]. Second, the DHR mapping from the information to the symbols can be generated in the semantic communications, which provides a new scope for defending against intelligent jamming attacks targeting the specific information [10]. In the following, we provide the primary concept of EAJ based on the communication signal and channel space.

Define the DoF of the communication signal space as K, whose normalized orthogonal primary functions is $\varphi_k, k = 1, 2, \ldots, K$. In addition, the communication channel space is composed of M channels, *i.e.*, $h_m, m = 1, 2, \ldots, M$. Note that the M channels are independent of each other, and the amplitude, phase, and polarization of h_m are controllable [21]. Besides, the receiver can accurately distinguish the signals from the different channels h_i, h_j, $i \neq j$. In each timeslot, the anti-jammer randomly selects a primary function φ_k to generate the desired signals and transmit them via a selected channel h_m, which can be expressed as

$$s_k = a_k \varphi_k. \tag{10}$$

Thus, the received signal can be expressed as:

$$r_{k,m} = s_k h_m + J h_J + n_0, \tag{11}$$

where J is the jamming signals, h_J is the channel coefficient between the jammer and the receiver, and n_0 denotes the white noise. For ease of expansion, we denote both the communication signal space and channel space of the anti-jammer as the anti-jamming space, while these of the jammer as the jamming space. Note that when the jammer has no knowledge of anti-jamming space, the jammer would spread the jamming space as wide as possible to obtain satisfactory damage effects. Define the correlation coefficient between the jamming channel h_J and the communication channel h_m as β_m, $0 \le \beta_m \le 1$ [22], then h_J can be decomposed into

$$h_J = \sum_{m=1}^{M} \beta_m h_m + h_0, \tag{12}$$

where h_0 is the component outsides the anti-jamming channel space, and $\sum_{m=1}^{M} \beta_m^2 \le 1$. As such, the received signal can be further expressed as

$$r_{k,m} = s_k h_m + \left(\sum_{k=1}^{K} J_k \varphi_k + J_0 \right) \left(\sum_{m=1}^{M} \beta_m h_m + h_0 \right) + n_0, \tag{13}$$

where $\{J_j\}$ and J_0 are the components of jamming signal inside and outside the anti-jamming signal space, respectively. Since h_i is orthogonal to h_j, $i \ne j$, and the primary functions φ_k is orthogonal to φ_l, $k \ne l$, therefore, after addressing the orthogonal terms in the receive signals, the output signals can be expressed as

$$r_{k,m}^{\text{out}} = a_k + \beta_m J_k + n_k. \tag{14}$$

Comparing (14) with (10), it can be seen that the power of the desired signals does not decrease after receiving processing, whereas the jamming power decreases from $\sum_{k=0}^{K-1} J_k^2$ to $(\beta_m J_k)^2$. Suppose the jamming power is distributed in K communication signal space uniformly. Then, without precise jamming recognition, the transceiver can obtain the anti-jamming processing gain by using the following two means.

First, the transceiver synchronously and dynamically selects an anti-jamming space to transmit the desired signals, whose anti-jamming processing gain can be expressed as

$$G_p = \frac{\sum_{k=0}^{K} J_k^2}{E\left\{ (\beta_m J_k)^2 \right\}} = \frac{K}{E\left\{\beta_m^2\right\}} = \frac{KM}{\sum\limits_{m=0}^{M-1} \beta_m^2}, \tag{15}$$

where $E\{\cdot\}$ is expectation. The last equation in (15) is based on the assumption that all the communication channels are selected uniformly.

Second, by comparing the power of the received signal from a different communication channel, the receiver selects the channel that maximizes the signal-to-jamming ratio to transmit the desired signals. As such, the corresponding anti-jamming processing gain is given by

$$G_p = \frac{K}{\min\limits_{1 \le m \le M} \beta_m^2}. \tag{16}$$

Observing from (15) and (16), the following points can be obtained:

1. Note that the anti-jamming technique corresponding to (15) can be regarded as an extension of the CSSAJ theory, which expands the communication signal space to the whole anti-jamming space. Besides, it can also be viewed as the application of the DHR framework in wireless communication anti-jamming. The key of EAJ is to use the internal factors of the wireless system to construct enough heterogeneous counterparts having the same functions. Thus, different from IAJ which needs to accurately obtain and effectively utilize the knowledge of jamming attacks, EAJ does not depend on the acquisition of jamming information, such that reverses the passive “change as enemy changed” situation and provides a new way to defend against the unknown jamming attacks.

2. Given the communication channel space, (16) provides the maximum anti-jamming processing gain obtained by selecting the desired channels, which is different from the spread-spectrum processing gain.

It should be pointed out that if the channels h_m, $m = 1, \ldots, M$ are reconfigurable or definable, the anti-jamming processing gain in (16) can be further improved. To elaborate, if the channels h_m, $m = 1, \ldots, M$ can be optimized to satisfy the condition that $\min\limits_{1 \le m \le M} \beta_m \to 0$, then, (16) approaches the infinity. It is worth noting that under the worst case that both the space-time coordinate and the selected channels of the jammer are the same as these of the transmitter, and the anti-jamming processing gain of EAJ approaches that of CSSAJ. This phenomenon suggests that EAJ is degraded into CSSAJ under the worst case.

3. The wireless channel contains great potential in EAJ. Specifically, the existing anti-jamming technique exploits the signal space to defend against the jamming attacks at the transceiver, while EAJ can utilize the inherent propagation properties of electromagnetic waves to construct an additional DHR channel space. Obviously, constructing a reconfigurable channel space for exploring the endogenous anti-jamming properties is an application of the dialectical materialism and scientific methodology, *i.e.* understanding, using and transforming nature, as shown in Figure 4.

3 The construction of "$N + 1$ dimensionality" EAJ

The primary issue in this subsection is to enable EAJ under open wireless channels. Arming with the abovementioned subspace description for communication anti-jamming system and the endogenous methodology, we wish to establish a unified framework of "$N + 1$ dimensionality" EAJ. Note that all the following anti-jamming techniques are the engineering implementation of "$N + 1$ dimensionality" EAJ.

3.1 "$N + 1$ dimensionality" EAJ method

Observing from the abovementioned subspace description for anti-jamming communications, the anti-jammer can always find a subspace to enable the signal transmission when the anti-jamming space is not completely taken up by the jamming space, which is the essential premise of "$N + 1$ dimensionality" EAJ. In other words, the jamming attacks can be eliminated when the anti-jamming space has at least one more dimension than the jamming space. Note that the dimensions of both the anti-jamming space and the jamming space can be changed, while the "one more dimension" principle should be constant for realizing "$N + 1$ dimensionality" EAJ.

To accurately depict the concept of "$N + 1$ dimensionality" EAJ, we first provide the definition of domain, DoF, space, and dimension, respectively.

1. Domain is defined as the scope or field of the knowledge and the activities. In wireless communications, the domain is mainly composed of the time domain, frequency domain, spatial domain, modulation domain, coding domain, angle domain, polarization domain, and so on, which corresponds to the range of system changeable parameters [23–27].

2. DoF is the number of controllable independent variables in a system. In the applications of wireless communications, DoF is generally the number of signals that can be transmitted independently on a given channel [28]. In [29], Shannon gave the DoF of the channel with bandwidth W and time T_s as $2T_sW$. Besides, the authors in [30] derived that the DoF of the multi-antenna system with antenna aperture A and the spatial angle $|\Omega|$ was $4T_sWA\,|\Omega|$. Furthermore, [31] and [32] provided the DoF for the reconfigurable intelligent surface (RIS) assisted system and orbital angular momentum aided system, respectively. It should be pointed out that sometimes the definition of DoF is ambiguous with that of domain, where the adjustment capacity in the frequency domain, spatial domain, and modulation domain can be also regarded as the DoF [33–35].

3. Space is a set with a certain structure. Different structures correspond to different spaces, such as vector space, Euclidean space and so on. In this paper, we mainly deal with semantic space [36, 37], signal space, and channel space.

4. Dimension is the elements of the space, such as three-dimensional space and so on. In this paper, we regard wireless communications as the information transmission within the communication space, which is composed of the semantic space, communication signal space, and communication channel space. Besides, the dimension is the controllable factor in the communication space. As such, the dimension of the communication space C can be defined as the product of DoF in the controllable communication

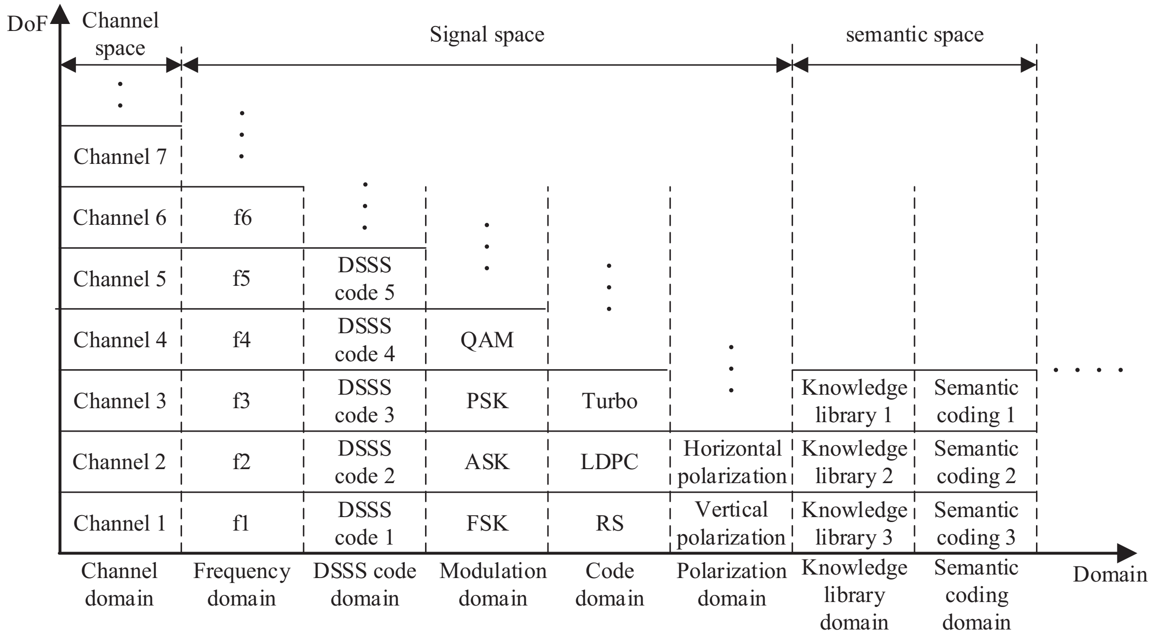

Figure 5. Relationship between parameter domain, DoF and dimension of anti-jamming communication

parameter domain, *i.e.*,

$$C = \prod_i g_i, \tag{17}$$

where g_i denotes the DoF of ith parameter domain.

The relationship between the parameter domain, DoF, and dimension is shown in Figure 5, where the parameter domain can be roughly divided into the semantic domain, communication signal domain, and communication channel domain. As stated before, CSSAJ focuses on the adjustment of signal parameters, while EAJ focuses on the construction and adjustment of the parameters of the whole communication space. Clearly, the adaptable system dimension increases as the increase of parameter domain and the DoF of each domain.

"$N + 1$ dimensionality" EAJ can be summarized as one premise and two capabilities. Specifically, the premise is that the dimension of jamming space is limited and relatively fixed. To elaborate, due to the hardware limitation and the mechanism, the dimension of jamming signal space is limited. For example, although the instantaneous frequency of sweep jamming is changed, its sweep bandwidth is limited. Besides, the patterns of the intelligent jamming attack are various, while its reaction time and the wave patterns are relatively fixed. In fact, the jamming signal always shows sparsity in the high-dimensional space [38]. Moreover, due to the confine of position, the dimension of the jamming channel space is also limited. In particular, the number of the multipath between the jammer and the receiver is limited [39], and their channel coefficients are different when the position of the jammer is not the same as that of the transmitter [13].

On the other hand, the abovementioned two capabilities of EAJ are the characterization capability for jamming space and the construction capability for anti-jamming space, where the first one is to utilize the primary functions of anti-jamming space to characterize the jamming space, and the second one is to construct an anti-jamming space having at least one more dimension than the jamming space. It is worth noting that in contrast to the jamming recognition in IAJ, the jamming-space characterization in EAJ is to detect and recognize the jamming space instead of the jamming signal. Since the jamming space is fixed when the jamming system is determined, the jamming-space characterization is to characterize the invariant in the jamming attacks, where the relationship between the jamming signal and jamming space is shown in Figure 6.

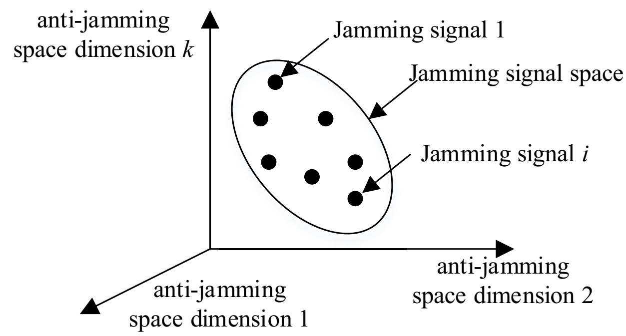

Figure 6. Relationship between jamming signal and jamming space

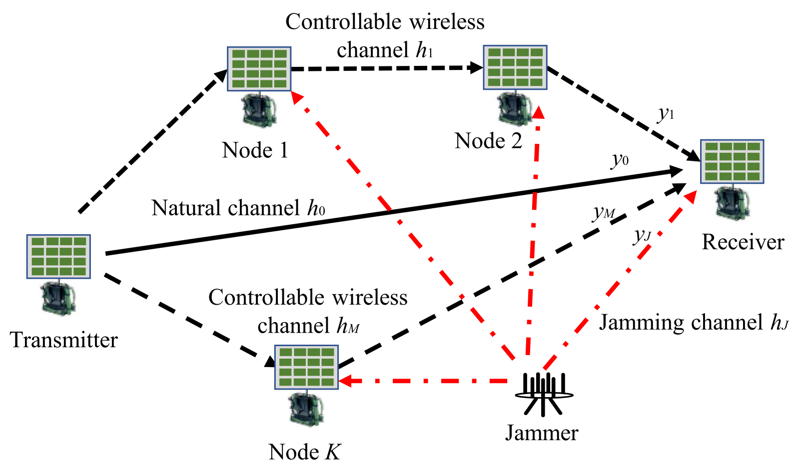

Figure 7. The system model of C-EAJ

3.2 Channel-based EAJ method

Channel-based EAJ (C-EAJ) is to enable EAJ by reconfiguring the wireless channels, which is an engineering implementation of "$N+1$ dimensionality" EAJ. To elaborate, C-EAJ utilizes a new anti-jamming space, *i.e.* communication channel dimension, by constructing the specific channels between the transceiver, which can eliminate the jamming attacks such that only the legitimate signals can be enhanced.

The key to achieving C-EAJ lies in two aspects: channel manipulation and channel identification.

First, channel manipulation is to construct and select the DHR channels for enabling signal transmission. In typical wireless communication, a wireless channel is generally considered to be objective and uncontrollable, and it is adapted by the transceiver. Recently, RIS has been regarded as a promising technique for reconfiguring the wireless channels, which results in the concept of the intelligent wireless environment [40–42]. Specifically, RIS is composed of many low-cost passive components and each component can constructively boost the received signal power or destructively suppress jamming by imposing a phase shift and/or amplitude to the incident signal. In civilian communications, RIS has been widely adopted to increase service coverage, maximize the achievable rate, enable secure communication, and so on [43]. In the application of anti-jamming communication, RIS provides a practical way to realize C-EAJ by controlling the amplitude, phase, frequency, polarization, and propagation direction of the channel. Note that as shown in Figure 7, RIS can be adopted for not only the transceiver design but also the channel manipulation. For simplicity, we denote the natural channel as h_0, the RIS-controllable wireless channel as h_m, $1 \leq m \leq M$, and the jamming channel as h_J. Correspondingly, the received desired signals from h_0 and h_m are y_0 and y_m, respectively, and the received jamming signal is y_J.

Second, channel identification is that the receiver identifies and receives the communication signals from the different channels, which is consistent with the diversity in typical communications. As shown in Figure 7, the receiver identifies and receives y_m from the RIS-controllable wireless channel h_m, $1 \leq m \leq M$.

Building upon the above two key steps, the transceiver can construct the DHR channels, and identify the corresponding received signals y_m, which provides the endogenous anti-jamming capability for wireless communication. Note that C-EAJ can also provide the endogenous anti-jamming capability without the channel identification. As such, the received signals can be expressed as $\sum_{m=1}^{M} y_m + y_0 + y_J$. Then, due to the channel manipulation capability, the received signal-to-jamming-plus-noise-ratio (SJNR) can be still maximized by optimizing each channel h_m, $1 \leq m \leq M$ [44].

4 Key techniques of EAJ

In order to further investigate the theoretical framework and design method of EAJ, we provide the following two key techniques.

4.1 The construction of multi-dimensional anti-jamming space

The essence of "$N+1$ dimensionality" EAJ is to make the anti-jamming space with at least one more dimension than the jamming space. Under the condition that the dimension of jamming space is constrained and relatively fixed, EAJ can be realized by increasing that of anti-jamming space. Hence, any known and unknown jamming attacks can be suppressed effectively without recognizing them.

First, the construction method of multi-dimensional anti-jamming space is briefly described as follows. Suppose $\{\mathbf{h}_n\}$, $n = 1, 2, \ldots N$, is a set of basis vectors of the N-dimensional space S. The anti-jamming space S_C, and jamming space S_J, are the subspace of S, respectively. And the corresponding basis vectors of S_C and S_J are $\left\{\mathbf{h}_n^C\right\}$, $n = 1, 2, \ldots N_C$, and $\left\{\mathbf{h}_n^J\right\}$, $n = 1, 2, \ldots N_J$, respectively. Any jamming attack can be expressed as:

$$\mathbf{s}_J = \sum_{i=1}^{J} \alpha_i \mathbf{h}_i^J, \tag{18}$$

where α_i, $i = 1, 2, \ldots, N_J$, are the components of the jamming attack on each basis vector. The jamming attack $\mathbf{s}_J$ is unknown, which means that α_i, $i = 1, 2, \ldots, N_J$, are unknown.

The aim of EAJ is not to recognize the jamming attack, *i.e.* estimate α_i, $i = 1, 2, \ldots, N_J$, precisely, but to increase the anti-jamming space dimension so that the dimension of anti-jamming space is larger than that of jamming space, *i.e.* $N \geq N_C > N_J$. Then, the jamming space can be considered as a subspace of anti-jamming space,

$$S_C = S_J + \overline{S}_J, \tag{19}$$

where $\overline{S}_J$ is the null-jamming space of dimension $N_C - N_J$. In other words, as long as the dimension of anti-jamming space is larger than that of the jamming space, the anti-jammer can transmit the desired information through the null-jamming space without being attacked by the jammer. Furthermore, any known and unknown jamming attack can be suppressed without recognizing them as long as the anti-jamming space is large enough.

Second, we can increase the dimension of anti-jamming space with the help of some new wireless communication techniques. For example, FH and DSSS obtain the anti-jamming processing gain by exploiting the additional DoF of frequency and code domain, respectively. The multi-antennas technique provides a mean for increasing the DoF in spatial and angle domains [45]. Blind-source separation technique exploits the differences between the desired signals and the jamming signals in the statistical domain [46]. Microwave photonic technique can further expand the system bandwidth such that the DoF in the frequency domain is increased [47]. The Orbital angular momentum (OAM) technique provides a means to utilize the DoF in the OAM domain [32]. To sum up, one of the key aspects of EAJ is that under the DHR framework, the anti-jamming capability is enhanced by increasing the system dimension. Note that all the techniques increasing the system dimension can be exploited in EAJ, and they should be flexibly selected for practical applications.

4.2 RIS-assisted C-EAJ techniques

RIS-assisted C-EAJ techniques can be divided into two aspects, namely, RIS hardware design and RIS-aided channel manipulation, which corresponds to the two parts of RIS hardware architecture, *i.e.*, reconfigurable metasurface and RIS controller, respectively.

(1) RIS Hardware Design in Vehicular Communications

The RIS's manipulation parameters of electromagnetic waves contain frequency, amplitude, phase, polarization, propagation direction, and so on, which provides a promising means to configure the heterogeneous wireless channels [48]. There are a few existing works that have investigated RIS-aided anti-jamming communications, *e.g.*, [49] and [50]. However, there are still some unique challenges in the application of RIS in the vehicular anti-jamming communications, which are detailed in the following.

The first challenge is the miniaturized design of reconfigurable metasurface in a low-frequency range. In general, element size of a reconfigurable metasurface can be seen as a quarter wavelength around the operating frequency since abrupt phase change of a metasurface is mostly introduced by resonances of subwavelength structures [51–53]. In this way, a metasurface will occupy a much larger size at a relatively lower frequency. Recently, most of researches on RIS are carried in the high-frequency range because they are faced with future civil wireless network applications such as 5G-Advanced and 6G. In order to adapt to vehicular communication applications, *i.e.*, shortwave and ultrashort wave communications, miniaturized design of reconfigurable metasurfaces in the low-frequency range are in need.

The second challenge is the issue of RIS's reflection efficiency. Generally, RIS-based wireless communications would suffer from the "double fading" effect, namely, the large-scale fading attenuation first in the transmitter-RIS link and then again in the RIS-receiver link [54]. Thus, the RIS's reflection efficiency is significantly important for RIS-aided wireless communications, especially the vehicular communications which are equipped with omnidirectional antennas. Although increasing the number of RIS units can partially overcome the "double fading" effect, the RIS's area would be significantly increased accordingly, which results in the decrease of RIS's motility, especially in the shortwave and ultrashort wave communications.

The third challenge is the wideband reconfigurable metasurface and reconfigurable metasurface with simultaneous control of multiple parameters of electromagnetic (EM) wave. It's necessary to devise a reconfigurable metasurface to simultaneously modulate the frequency, phase, and amplitude of EM wave since more parameters controlled will enable more complicated functionalities in vehicle communications [55]. Besides, most reported reconfigurable metasurfaces still operate in narrowband even though metasurfaces have been proven to be effective in a spectrum ranging from sound to light [43]. To match anti-jamming signal waveform, such as frequency hopping and spread spectrum, broadband reconfigurable metasurfaces should be explored.

(2) RIS-aided channel manipulation

RIS-aided channel manipulation can be divided into two parts, namely, the acquisition and the transmission of RIS-aided manipulation information.

First, the RIS-aided channel model and its channel estimation method should be investigated. Specifically, RIS converts the uncontrollable channel into the controllable one, such that the statistical channel model adopted in traditional wireless communications is not applicable to the RIS-aided one [54, 56]. To obtain the channel state information (CSI), a few signal processing units can be embedded into RIS, which can assist the channel estimation. Besides, the receiver can estimate the cascade channel instead of each separate channels, *i.e.*, the transmitter-RIS-receiver link, then feedback on the estimated CSI to RIS [57, 58]. Moreover, the acquisition of jammer's CSI can further improve the anti-jamming processing gain [50].

Second, the reliable transmission of the manipulation information of RIS is important for anti-jamming communications. In civilian wireless communications, the deployment position of RIS is generally fixed, and the manipulation information is transmitted over wired channels. However, in the anti-jamming communications, as shown in Figure 7, the deployment position of RIS is varying, and the signals are transmitted over wireless channels, such that the manipulation information of RIS are vulnerable to jamming attacks in vehicular communications. Thus, it is necessary to investigate the reliable and real-time transmission method of manipulating information of RIS.

It should be pointed out that RIS-based EAJ would consume additional resources cost, such as space resources, computing resources, and transmission resources, which is implementation issues that should be comprehensively considered in the system design and technical research of endogenous anti-jamming system.

5 Suggestions for the development of EAJ

We have two suggestions about the development of EAJ, which are given by the following details.

First, the existing principles of anti-jamming development should be changed. Under the framework of "$N+1$ dimensionality" EAJ, we should convert the passive precise-recognition-based principles of anti-jamming communications to an active endogenous one, which can significantly increase the dimension of the anti-jamming space such that the endogenous anti-jamming capacity can be improved.

Second, new supporting techniques for EAJ should be proposed. The advancement of RIS and semantic communication technique provides a possible but not the only way to realize EAJ. Thus, some new supporting techniques should be explored. To elaborate, the nature of EAJ should be explore with the help of wireless communication, artificial intelligence and material technology. At the same time, the potential endogenous anti-jamming factors in the semantic space, signal space, and channel space should be investigated, such that the "$N + 1$ dimensionality" EAJ theory and technology can be improved.

6 Conclusion

The meaning of EAJ is explicated, and the fundamental concept, key techniques, and development suggestions of wireless communication "$N + 1$ dimensionality" EAJ are proposed in this paper. Different from CSSAJ and IAJ, EAJ breaks the performance limitation of the existing anti-jamming techniques by expanding the anti-jamming space, which is composed of semantic space, signal space and channel space, and so on. In this way, the electromagnetic wave and the information can be controlled with the same framework. "$N + 1$ dimensionality" EAJ can be utilized to realize the new communication paradigm, i.e, the low-power communication, which can break through the performance limitations of existing techniques and provide support against unknown and intelligent jamming.

Note that neither the jammers nor the anti-jammers can achieve absolute dominance in the communication countermeasure domain [1]. In the long term, this conclusion holds true. However, it is still possible for the anti-jammers to break the performance limitation by seeking a new dimension of anti-jamming space, which will provide additional anti-jamming performance gains for a wireless communication system. Then, the anti-jammers may obtain absolution dominance for a certain period of time, which is the ultimate goal that the researchers pursue.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Fuqiang Yao proposed the core idea of this paper, namely, wireless communication "$N + 1$ dimensionality" endogenous anti-jamming. Fuqiang Yao and Yonggang Zhu contribute to the main part of this paper. They surveyed the existing anti-jamming techniques and proposed the fundamental concept, key techniques, and development suggestions for wireless communication "$N + 1$ dimensionality" endogenous anti-jamming. In addition, they designed and drafted the whole frame and the details of the paper. Yifu Sun provided the writing guidance for drafting the whole paper, improved the readability of the paper by grammatical modification and polishing, and also typeset the whole paper. Wenlong Guo provided the writing guidance for Section 4 and modified this section for the readability of the paper.

Acknowledgements

The authors would like to thank Jiangxing Wu, Tiejun Cui, and Liang Jin for their helpful discussions and supports.

Funding

No funding are associated with this article.

References

[1] Yao FQ. Communication Anti-jamming Engineering and Practice (in Chinese). Beijing: Publishing House of Electronics Industry, 2012.
[2] Simon MK, Omura JK and Scholtz RA et al. Spread Spectrum Communications. New York: McGraw-Hill, Inc, 1985.
[3] Wang SF, Bao YF and Li Y. The architecture and technology of cognitive electronic warfare (in Chinese). Sci Sin Inf 2018; **48**: 1603–13.
[4] Wu JX. Development paradigms of cyberspace endogenous safety and security (in Chinese). Sci Sin Inform 2022; **52**: 189–204.
[5] Wu JX. Principles of Cyberspace mimic Defense: General Robust Control and Endogenous Safety & Security (in Chinese). Beijing: Science Press, 2018.
[6] Hu AQ, Fang LT and Li T. Research on bionic mechanism based endogenous security defense system (in Chinese). Chin J Network Inf Secur 2021; **7**: 11–9.
[7] Jin L, Hu XY and Lou YM et al. Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions. China Communications, 2021; **18**: 88–99.
[8] Jin L, Lou YM, Sun XL, et al. Concept and vision of 6G wireless endogenous safety and security (in Chinese). Sci Sin Inform, 2023; **53**: 344–364.
[9] Zhang XD. Matrix Analysis and Applications (in Chinese). Beijing: Tsinghua University Press, 2004.
[10] Erpek T, Sagduyu YE and Shi Y. Deep learning for launching and mitigating wireless jamming attacks. IEEE Trans Cognit Commun Networks 2019; **5**: 2–14.
[11] Liu X, Xu YH and Jia LL et al. Anti-jamming communications using spectrum waterfall: a deep reinforcement learning approach. IEEE Commun Lett 2018; **22**: 998–1001.
[12] Li YY, Xu YH and Xu YT et al. Dynamic spectrum anti-jamming in broadband communications: a hierarchical deep reinforcement learning approach. IEEE Wireless Commun Lett 2020; **9** 1616–19.
[13] Xiao L, Jiang DH and Xu DJ et al. Two-dimensional antijamming mobile communication based on reinforcement learning. IEEE Trans Vehicular Technol 2018; **67**: 9499–512.
[14] Pirayesh H and Zeng HC. Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey. IEEE Commun Surv Tutorials 2022; **24**: 767–809.
[15] Peng QH, Cosman PC and Milstein LB. Spoofing or Jamming Performance Analysis of a Tactical Cognitive Radio Adversary. IEEE J Sel. Areas Commun. 2011; **29**: 903–11.
[16] Sadeghi M and Larsson EG. Adversarial attacks on deep-learning based radio signal classification. IEEE Wireless Commun Lett 2019; **8**: 213–16.
[17] Sagduyu YE, Shi Y and Erpek T. Adversarial deep learning for over-the-air spectrum poisioning attacks. IEEE Trans Mobile Comput 2021; **20**: 306–19.
[18] Shannon CE. A mathematical theory of communication. Bell Syst Techn J 1948; **27**: 379–423.
[19] Luo XW, Chen HH and Guo Q. Semantic communication: overview, open issues, and future research directions. IEEE Wireless Commun 2022; **29**: 210–19.
[20] Zhang YC, Zhang P and Wei JB et al. Semantic communication for intelligent devices: architectures and a paradigm (in Chinese). Sci Sin Inf 2022; **53**: 907–21.
[21] Do TN, Kaddoum G and Nguyen TL et al. Multi-RIS-Aided wireless systems: statistical characterization and performance analysis. IEEE Trans Commun 2021; **69**: 8641–58.
[22] Molisch AF. Wireless Communications, second edition. UK: John Wiley & Sons Ltd, 2011.
[23] Venugopal A and Leib H. A tensor based framework for multi-domain communication systems. IEEE Open J Commun Soc 2020; **1**: 606–35.
[24] Jia LL, Xu YH and Sun YM et al. A multi-domain anti-jamming defense scheme in heterogeneous wireless networks. IEEE Access 2018; **6**: 40177–188.
[25] Li YC, Bai SZ and Gao ZZ. A multi-domain anti-jamming strategy using stackelberg game in wireless relay networks. IEEE Access 2020; **8**: 173609–3617.
[26] Xiao J, Yang CG and Anpalagan A et al. Joint interference management in ultra-dense small-cell networks a multi-domain coordination perspective. IEEE Trans Commun 2018; **66**: 5470–81.
[27] Yucek T and Arslan H. A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Commun Surv Tutorials 2009; **11**: 116–30.
[28] Somaraju R and Trumpf J. Degrees of freedom of a communication channel: using DOF singular values. IEEE Trans Inf Theory 2010; **56**: 1560–73.
[29] Shannon CE. Communication in the presence of noise. Proc I.R.E 1949; **37**: 10–21.
[30] Poon AS, Brodersen RW and Tse DN. Degrees of freedom in multiple-antenna channels: a signal space approach. IEEE Trans Inf Theory 2005; **51**: 523–36.
[31] Seddik KG. On the degrees of freedom of IRS-assisted non-coherent MIMO communications. IEEE Commun Lett 2022; **26**: 1175–79.
[32] Xu J. Degrees of freedom of OAM-based line-of-sight radio systems. IEEE Trans Antennas Propag 2017; **65**: 1996–2008.
[33] Lu L, Li GY and Maaref A et al. Opportunistic transmission exploiting frequency- and spatial-domain degrees of freedom. IEEE Wireless Commun 2014; **21**: 91–7.
[34] Bogucka H and Conti A. Degrees of freedom for energy savings in practical adaptive wireless systems. IEEE Commun Mag 2011; **49**: 38–45.
[35] Chung ST and Goldsmith AJ. Degrees of freedom in adaptive modulation: a unified view. IEEE Trans Commun 2001; **49**: 1561–71.
[36] Wang XH, Dong JS and Chi CY et al. Semantic space: an infrastructure for smart spaces. IEEE Pervasive Comput 2004; **3**: 32–9.

[37] Zhang SY, Yang ZL and Yang JS et al. Linguistic steganography: from symbolic space to semantic space. IEEE Signal Process Lett 2021; **28** 11–5.
[38] Chen YD and Chi YJ. Harnessing structures in big data via guaranteed low-rank matrix estimation. IEEE Signal Process Mag 2018; **35**: 14–31.
[39] Friedlander B. Communications through time-varying subspace channels. IEEE J Sel Areas Commun 2008; **26**: 338–47.
[40] Renzo MD, Debbah M and Phan-Huy D et al. Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come. EURASIP J Wireless Commun Networks 2019; **129**: 1–20.
[41] Wu QQ and Zhang R. Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network. IEEE Commun Mag 2020; **58**: 106–112.
[42] Gacanin H and Renzo MD. Wireless 2.0 toward an intelligent radio environment empowered by reconfigurable meta-surfaces and artificial intelligence. IEEE Vehicular Technol Mag 2020; **15**: 74–82.
[43] Cui TJ, Jin S and Zhang JY et al. Research Report on Reconfigurable Intelligent Surface (RIS) (in Chinese). IMT-2030 (6G) Promotion Group, 2021.
[44] Sun YF, An K and Zhu YG et al. Intelligent reflecting surface assisted anti-jamming approach for wireless communications (in Chinese). Chin J Radio Sci 2021; **36**: 877–86.
[45] Yuan SA, He Z and Chen XM et al. Electromagnetic effective degree of freedom of an MIMO system in free space. IEEE Antennas Wireless Propag Lett 2022; **21**: 446–50.
[46] Luo ZQ, Li CJ and Zhu LD. A comprehensive survey on blind source separation for wireless adaptive processing: principles, perspectives, challenges and new research directions. IEEE Access 2018; **6**: 66685–708.
[47] Yan XL, Zou XH and Li PX et al. Covert wireless communication using massive optical comb channels for deep denoising. Photonics Res 2021; **9**: 1124–33.
[48] Zhang L, Chen MZ and Tang WK et al. A wireless communication scheme based on space- and frequency-division multiplexing using digital metasurfaces. Nat Electron 2021; **4**: 218–27.
[49] Sun YF, An K and Zhu YG et al. Intelligent reflecting surface enhanced secure transmission against both jamming and eavesdropping attacks. IEEE Trans Vehicular Technol 2021; **70**: 11017–022.
[50] Sun YF, An K and Zhu YG et al. RIS-assisted robust hybrid beamforming against simultaneous jamming and eavesdropping attacks. IEEE Trans Wireless Commun 2022; **21**: 9212–231.
[51] Glybovski SB, Tretyakovb SA and Belov PA et al. Metasurfaces: from microwaves to visible. Phys Rep 2016; **634**: 1–72.
[52] Dai JY, Tang WK and Chen MZ et al. Wireless communication based on information metasurfaces. IEEE Trans Microwave Theory Tech 2021; **69**: 1493–510.
[53] Yu NF, Genevet P and Kats MA et al. Light propagation with phase discontinuities generalized laws of reflection and refraction. Science 2011; **334**: 333–7.
[54] Ozdogan O, Bjornson E and Larsson EG. Intelligent reflecting surfaces: physics, propagation, and pathloss modeling. IEEE Wireless Commun Lett 2020; **9**: 581–85.
[55] Cui TJ, Wu HT and Liu S. Research progress of information metamaterials (in Chinese). Acta Phys Sin 2020; **69**: 158101.
[56] Tang WK, Chen MZ and Chen X et al. Wireless communications with reconfigurable intelligent surface path loss modeling and experimental measurement. IEEE Trans Wireless Commun 2021; **20**: 421–39.
[57] Zheng BX, You CS and Mei WD et al. A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications. IEEE Commun Surv Tutorials 2020; **24**: 1035–71.
[58] Basar E and Yildirim I. Reconfigurable intelligent surfaces for future wireless networks: a channel modeling perspective. IEEE Wireless Commun 2021; **28**: 108–14.

Fuqiang Yao received his M.S. and Ph.D. degrees in communication and electronic system from Xidian University, Xi'an, China, in 1990 and 1993, respectively. He is currently a science researcher fellow with the Six-third Research Institute, National University of Defense Technology (NUDT), Nanjing, China. He is also an academician of the Chinese Academy of Engineering (CAE). His current research interest is in anti-jamming communications.

Yonggang Zhu received his B.S. degree in electronical engineering and a Ph.D. degree in science of military equipment from PLA University of Science and Technology, Nanjing, China, in 2004, and 2009, respectively. Currently, he is an associate researcher fellow with the Six-third Research Institute, National University of Defense Technology (NUDT), Nanjing, China. His research interests include anti-jamming communications, statistical signal processing, and reconfigurable intelligent surface.

Yifu Sun received his B.Eng. in communications engineering from the National University of Defense Technology (NUDT), Changsha, China, in 2019, where he is currently pursuing a Ph.D. degree in information and communications engineering with the Six-third Research Institute. His current research interests are in anti-jamming communications, reconfigurable intelligent surface, physical layer security, cooperative and cognitive communications, and signal processing for wireless communications.

Wenlong Guo received his B.S. degree in radar engineering and a Ph.D. degree in electromagnetic field and microwave technology from Air Force Engineering University, Xi'an, China, in 2014 and 2020, respectively. From Apr. 2018 to Jan. 2020, he was a Visiting Student with the Department of Electronic Science and Engineering, Nanjing University, at Nanjing, China. He is currently a Postdoctoral fellow with the Six-third Research Institute, National University of Defense Technology (NUDT), Nanjing, China. He has authored or co-authored over 30 journal articles or referred international conference papers. His research interests include the electromagnetic metasurface and its application to wireless communications in a low frequency band, and novel microwave functional materials.