Wireless Communications \( N + 1 \) dimensionality: Endogenous Anti-Jamming: Theory and Techniques

Fuqiang Yao\(^1\), Yonggang Zhu\(^*\), Yifu Sun\(^1\), and Wenlong Guo\(^1\)

\(^1\) The 63th Research Institution, National University of Defense Technology, Nanjing, 210007, China

Abstract  The existing theory and techniques of wireless communication anti-jamming has reached its 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 the 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 F. Yao, Y. Zhu, Y. Sun, and W. Guo. Wireless Communications \( N + 1 \) dimensionality Endogenous Anti-Jamming: Theory and Techniques. Security and Safety 2022; x: xxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

Wireless communications are the primary or even the only command and control means in the war and emergency situations. Thus, enabling the 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 the unknown or intelligent jamming attacks. As such, it is necessary to explore the 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 focuses on investigating the IAJ technique, in which the principle can be expressed as "change as enemy changed".

* Corresponding author (email: zhumaka1982@163.com)
In other words, with the assistance of the precise jamming recognition, the anti-jammers adapt their communication parameters as the jammers strategies. Depending on the intelligence level, IAJ technique can be divided into adaptive one and cognitive one. 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 IAJ technique. First, due to the fast time-varying property of complex electromagnetic environment 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 and tracking jamming, etc.), they can launch \( 2^N - 1 \) mixed jamming patterns theoretically, which can make the legitimate nodes get stuck in the curse of recognition. Second, when IAJ technique confronts with 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 cognitive domain, namely, the side who can recognize the others strategy precisely and execute the confrontation strategy effectively by exploiting the advanced computing resources and intelligent algorithms, will win the competition [3]. However, in the 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, IAJ technique is a passive mean 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 the unknown and the 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. in [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 were dynamically selected from the heterogeneous and redundant executor set such that 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. in [6] proposed a bionic ESS to address the issue that the security mechanism is separate with the status of the network devices. Moreover, the concept of cyberspace ESS has been adopted to the 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 (E AJ) 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, E AJ and ESS are different from 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 E AJ, the subspace method in [9] is adopted to develop the unified framework for CSSAJ, IAJ, and E AJ, 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 Fig.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 orthogonal primary functions \( \varphi_k (k = 0, 1, \cdots, 2T_sW - 1) \) [2]. As such, after dividing the signal space of
CSSAJ into subspaces, the DoF of each subspace is \( D = 2T_s W/K \). In each timeslot, the transmitter randomly selects one of the subspaces for communication, i.e.,

\[
s_k = \sum_{i \in A_k} a_i \varphi_i,
\]

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

\[
E_s^t = \sum_{i \in A_k} a_i^2,
\]

Besides, the received signal can be expressed as

\[
r_k = s_k + J,
\]

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.

\[
J = \sum_{i=0}^{2T_s W-1} J_i \varphi_i + J_0,
\]

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

\[
E_J^t = \sum_{i=0}^{2T_s W-1} J_i^2 + E_{J_0},
\]

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

\[
r_{\text{out}}^t = a_i + J_i, \ i \in A_k
\]

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

\[
E_s^r = \sum_{i \in A_k} a_i^2,
\]

\[
E_J^r = \sum_{i \in A_k} J_i^2.
\]

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,

\[
G_p = \frac{E_s^r / E_J^r}{E_s^t / E_J^t}.
\]
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., $E_{ts} = E_{rs}$. Thus, Eq. (9) can be simplified into $G_p = E_{tJ} / E_{rJ}$. Assuming $J_0 = 0$ 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, that calls for the new capability of anti-jamming communications.

The block diagram of IAJ is shown in Fig. 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 jammers 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 in the communication signal space [10–13]. To some extent, DRL-based IAJ has made some progress for defending against the 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 the jamming knowledge. Thus, as the jammer dynamically adapts their 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].

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 respectively. Fig. 3 shows the subspace relationships between CSSAJ, IAJ, and intelligent jamming, where both CSSAJ and IAJ combat with 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 the 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 Fig. 3 becomes a hypersphere.

### 2.3 Endogenous Anti-Jamming Techniques

A typical system of wireless communication is mainly composed of transmitter, wireless channel, and receiver, which are the irreplaceable endogenous factors of wireless communication system [18]. Different from the precise-recognition-based IAJ technique which adapts its anti-jamming strategy according to the jammers 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.
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 Fig. 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 base, and 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, at the same conditions, the semantic communication would significantly compress the transmit 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 the intelligent jamming attacks targeting at 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 $\varphi_k, k = 1, 2, \cdots, K$. In addition, the communication channel space is composed of $M$ channels, i.e., $h_m, m = 1, 2, \cdots, M$. Note that the $M$ channels are independent from 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 $\varphi_k$ to generate the desired signals and transmit them via a selected channel $h_m$, which can be expressed as

$$s_k = a_k \varphi_k.$$  

(10)
Thus, the received signal can be expressed as:

\[ r_{k,m} = s_k h_m + J h_J + n_0, \]  

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 the ease of expansion, we denote both the communication signal space and channel space of anti-jammer as the anti-jamming space, while these of the jammer as 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 \( \beta_m \), \( 0 \leq \beta_m \leq 1 \), then \( h_J \) can be decomposed into

\[ h_J = \sum_{m=1}^{M} \beta_m h_m + h_0, \]  

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

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

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 \( h_j \), \( i \neq j \), and the primary functions \( \varphi_k \) is orthogonal to \( \varphi_l \), \( k \neq l \), therefore, after addressing the orthogonal terms in the receive signals, the output signals can be expressed as

\[ r_{m,k}^{\text{out}} = a_k + \beta_m J_k + n_k. \]  

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 the 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

\[ G_p = \frac{\sum_{k=0}^{K} J_k^2}{E \{ (\beta_m J_k)^2 \}} = \frac{K}{E \{ \beta_m^2 \}} = \frac{K M}{\sum_{m=0}^{M-1} \beta_m^2}, \]  

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

\[ G_p = \frac{K}{\min_{1 \leq m \leq M} \beta_m^2}. \]  

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 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 \( h_m, m = 1, \cdots, M \) are reconfigurable or definable, the anti-jamming processing gain in (16) can be further improved. To elaborate, if the channels \( h_m, m = 1, \cdots, M \) can be optimized to satisfy the condition that \( \beta_m \to 0 \), then, (16) approaches the infinity. It is worth to note that under the worst case that both the space-time coordinate and the selected channels of the jammer are the same as those of the transmitter, 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 Fig.4.

3 The Construction of “\( N + 1 \) dimensionality” EAJ

The primary issue in this subsection is to enable EAJ under the 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 technique 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, domain is mainly composed of 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 the 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 given the DoF of the channel with bandwidth \( W \) and time \( T_s \) as \( 2T_s W \). Besides, the authors in [30] derived that the DoF of the multi-antenna system with antenna aperture \( A \) and the spatial angle \( |\Omega| \) was \( 4T_s W A |\Omega| \). 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 point 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 the vector space, Euclidean space and so on. In this paper, we mainly deal with the 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 the 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 parameter domain, i.e.,

$$C = \prod_i g_i,$$

where $g_i$ denotes the DoF of $i$-th parameter domain.

The relationship between parameter domain, DoF, and dimension is shown in Fig. 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 whole communication space. Clearly, the adaptable system dimension increases as the increasing of the 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 the 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 jammer is not the same as that of 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 jamming space. It is worth to note 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 Fig. 6.
Figure 6. Relationship between jamming signal and jamming space

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 the typical wireless communication, 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 the civilian communications, RIS has been widely adopted to increase the service coverage, maximize the achievable rate, enable the 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, propagation direction of channel. Note that as shown in Fig.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 the typical communications. As shown in Fig.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 the 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. And then, 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 \( \{h_n\}, n = 1, 2, \ldots, N \), 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 \( \{h^C_n\}, n = 1, 2, \ldots, N_C \), and \( \{h^J_n\}, n = 1, 2, \ldots, N_J \), respectively. Any jamming attack can be expressed as:

\[
s_J = \sum_{i=1}^{J} \alpha_i h^J_i,
\]

where \( \alpha_i, i = 1, 2, \ldots, N_J \), are the components of the jamming attack on each basis vector. The jamming attack \( s_J \) is unknown mainly refer to \( \alpha_i, i = 1, 2, \ldots, N_J \), are unknown.

The aim of EAJ is not to recognize jamming attack, i.e. estimate \( \alpha_i, i = 1, 2, \ldots, N_J \), 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,

\[
S_C = S_J + S_J,
\]

where \( S_J \) 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 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 frequency domain is increased [47]. Orbital angular momentum (OAM) technique provides a means to utilize the DoF in OAM domain [32]. To sum up, one of the key aspects in 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 RISs manipulation parameters of electromagnetic wave contain frequency, amplitude, phase, polarization, propagation direction, and so on, which provides a promising mean to configure the heterogeneous wireless channels [48]. There are a few existing works have investigated the 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 details in the following.

The first challenge is miniaturized design of reconfigurable metasurface in 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. Till now most researches on RIS are carried in high frequency range because they are faced to 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 low frequency range is in need.

The second challenge is the issue of RISs reflection efficiency. Generally, RIS-based wireless communications may 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 RISs reflection efficiency is significantly important for the 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 RISs area would be significantly increased accordingly, which results in the decrease of RISs motility especially in the shortwave and ultrashort wave communications.

The third challenge is wideband reconfigurable metasurface and reconfigurable metasurface with simultaneous control of multiple parameters of electromagnetic (EM) wave. It’s necessary to devise reconfigurable metasurface to simultaneously module 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 proved to be effective in 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 the 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 the 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 the estimated CSI to RIS [57, 58]. Moreover, the acquisition of jammers CSI can further improve the anti-jamming processing gain [50].

Second, the reliable transmission of the manipulation information of RIS is important for the anti-jamming communications. In the 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 Fig.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 the 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.

First, the existing principles of anti-jamming development would 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 anti-jamming space such that the endogenous anti-jamming capacity can be improved.

Second, the new supporting technique for EAJ would 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 break 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 limit 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 new dimension of anti-jamming space, which will provide additional anti-jamming performance gains for wireless communication system. Then, the anti-jammers may obtain the 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 the main part of this paper. They surveyed the existing anti-jamming techniques, and proposed the fundamental concept, key techniques, and development suggestions of wireless communication “N + 1 dimensionality” endogenous anti-jamming. In addition, they designed and drafted 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 Academician Jiangxing Wu, Academician Tiejun Cui, and Prof. Liang Jin for their helpful discussions and supports.
F. Yao et al.: Wireless Communications “N + 1 dimensionality” Endogenous Anti-Jamming

Funding
No Funding are associated with this article.

References

F. Yao et al.: Wireless Communications “N + 1 dimensionality” Endogenous Anti-Jamming


[40] Fuqiang Yao received the 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 Sixth 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 the B.S. degree in electronic engineering and 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 Sixth 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 the B.Eng. in communications engineering from National University of Defense Technology (NUDT), Changsha, China, in 2019, where he is currently pursuing the Ph.D. degree in information and communications engineering with the Sixth 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 the B.S. degree in radar engineering and the 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, Nanjing, China. He is currently a Postdoctoral fellow with the Sixth Research Institute, National University of Defense Technology (NUDT), Nanjing, China. He has authored or coauthored over 30 journal articles or referred international conference papers. His research interests include the electromagnetic metasurface and application to wireless communications in low frequency band, and novel microwave functional materials.