Introduction to Wireless Endogenous Security and Safety: Problems, Attributes, Structures and Functions

SUBMISSION DATE / POSTED DATE

26-02-2021 / 07-03-2021

CITATION

Hu, Xiaoyan; Jin, Liang; Lou, Yangming; Zhong, Zhou; Sun, Xiaoli (2021): Introduction to Wireless Endogenous Security and Safety: Problems, Attributes, Structures and Functions. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.14125346.v1

DOI

10.36227/techrxiv.14125346.v1

CHINA COMMUNICATIONS

Introduction to Wireless Endogenous Security and Safety: Problems, Attributes, Structures and Functions

Xiaoyan Hu,Liang Jin*,Yangming Lou, Zhou Zhong, Xiaoli Sun

[1] PLA Strategic Support Force Information Engineering University, Zhengzhou 450002, China
[*] The corresponding author, email: liangjin@263.net

Abstract: The information security and functional safety of wireless communication systems have become the focus of current research. The endogenous security principle based on Dynamic Heterogeneous Redundancy provides a direction for the development of wireless communication security and safety technology. This paper introduces the concept of wireless endogenous security from the following four aspects. First, we sorts out the endogenous security problems faced by the current wireless communication system, and then analyzes the endogenous security and safety attributes of the wireless channel. After that, the endogenous security and safety structure of the wireless communication system is given, and finally the applications of the existing wireless communication endogenous security and safety functions are listed.
Keywords: wireless communication; endogenous security; information security; functional safety; DHR

I. INTRODUCTION

Wireless signals use electromagnetic waves as the carrier to transmit information freely and openly at the speed of light in space, which greatly facilitates people's lives and promotes the progress and development of society. At the same time, information security issues faced by wireless communications have also received widespread attention[1]. The free propagation of wireless signals also exposes the endogenous "gene" defects of electromagnetic waves, that is, anyone within the signal coverage area can eavesdrop or attack at the physical layer. However, the existing security mechanisms mainly follow the encryption mechanism in traditional wired communication and are designed at the high level, which can not implement precise measures against security issues caused by the openness of wireless channels. With the improvement of computing power, encryption algorithms will inevitably have the risk of being breached in the future[2]. For example, the A51 and A52 encryption algorithms in 2G have been breached long ago, and the KASUMI encryption algorithm in 3G was also conditionally cracked due to loopholes in 2014 [3]. Faced with such problems, the existing security mechanisms always adopt the remedy/patching method to solve the past security problems, e.g., 4G uses technologies such as Snow3G/AES/Zuc-based hierarchical keys to solve security attacks such as SS7 signaling hijacking in 3G, which makes it difficult to deal with the unknown risks and vulnerabilities/ loopholes in the current system. Furthermore, as future wireless devices become more diverse and wireless networks become more open and integrated, communication links are facing severe security threats and the bucket effect brought by the security shortcomings of the air interface will be more obvious [2]. Therefore, it is urgent to study new security mechanisms from the essential attributes of wireless communication security to deal with known and unknown security threats in wireless communication systems.

The endogenous security theory proposed by Wu[4–10] an ideal way to solve the above problems. Endogenous safety and security (ESS or endogenous secu-

Received:
Revised:
Editor:

rity) theory is to use the endogenous security structure with dynamic, heterogeneous, and redundant (DHR) attributes to realize the endogenous security function. Its main feature is to dynamically select the executor set from the heterogeneous and redundant executors, which can achieve the expected function of the system and make its structure more uncertain. Under this mechanism, it not only ensures the reliability of the system, but also makes the attacker have cognitive dilemma about the system structure and operation mechanism, which makes it difficult to carry out effective attacks. Therefore, endogenous security theory can not only be used to resist known security threats, more importantly, it can also resist the unknown security threat and the unknown attack against unknown security threats. In recent years, the theory has made important achievements in principle exploration, technical advancement, system development [6].

Inspired by the endogenous security, the research on wireless endogenous security is gradually developing. Different from the classical endogenous security, wireless channel naturally has endogenous security attributes with dynamic, heterogeneous and redundant. Based on this, we can design a unique endogenous security structure of wireless communication system to ensure the security and reliability of information transmission from transmitter to receiver. In order to introduce the concept of wireless endogenous security proposed in this paper, we start from the four aspects of wireless communication endogenous security problems, attributes, structure, and functions. This paper first introduces the endogenous security problems caused by the endogenous defects in electromagnetic wave, then explores the endogenous security attributes in the wireless communication system or operation mechanism, and then constructs the endogenous security structure based on these attributes, finally introduces several existing key technologies of wireless endogenous security.

II. THE ENDOGENOUS SAFETY AND SECURITY PROBLEM

2.1 Basic Concept

Wireless communication network is one of the important components of cyberspace[11]. To discuss the wireless endogenous safety and security (WESS) problem, we should first clarify what is the endogenous safety and security (ESS) problem in cyberspace. In essence, the endogenous security problem and the cyberspace are interrelated and interdependent. This is because in addition to the expected function (EF), any natural or artificial system also has the associated visible sub-effect function (VSEF) or invisible dark function (IDF). As shown in Figure 1, the VSEF and IDF are represented by white dots and gray circles, respectively, and they are widely distributed around the expected function. The current solution is to design security patches once these VSEFs are discovered. But this is only a small part of the undiscovered functions. Moreover, the introduction of additional security patches may also bring new security issues. This shows that when various software and hardware perform their expected functions, the VSEF and IDF generated by loopholes and backdoors cannot be eradicated [7]. If the VSEF and IDF have an

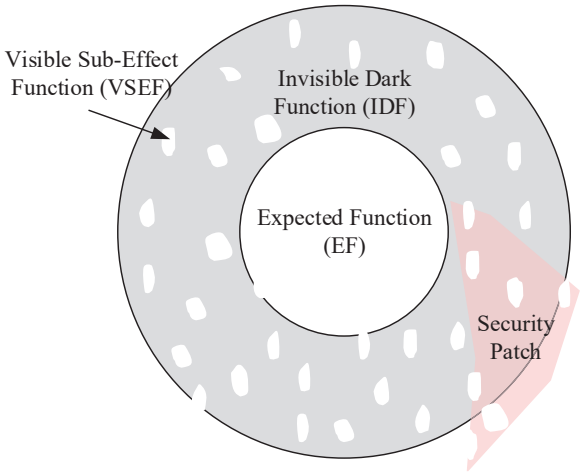

Figure 1. *The relationship among EF, VSEF and IDF.*

adverse effect on the system, they become the endogenous safety and security problems. The ESS problems include not only functional safety problems that affect the robustness and reliability, but also information security problems that affect the privacy and credibility. Once endogenous security problems are caused by artificial or natural disturbances (for example, active attacks or natural interference), undesired security events will be triggered. This type of disturbance is called general uncertain disturbance [9]. Many cybersecurity incidents have shown that ESS problems in cyberspace are usually caused by the general uncertain

disturbance, VSEF and IDF [10]. Such endogenous security issues cannot be fundamentally solved by the traditional patching or plug-in security mechanisms.

2.2 The WESS Problem

Different from cyberspace, the wireless communication network is faced with unique endogenous security problems caused by the inherent defects of electromagnetic propagation. For wireless communication systems, the desired function is to transmit information safely and reliably on the reachable path between the transmitter and receiver. However, due to the multipath propagation characteristics of electromagnetic waves and the uncertainty and uncontrollability of the electromagnetic environment, random fading and noise (i.e., VSEF) are inevitable at the receiver. At the same time, the broadcast characteristics of electromagnetic waves will also cause unpredictable dark functions, that is, passive eavesdropping can be implemented in any unknown place within the broadcast range, and unknown wireless access attacks can be launched.

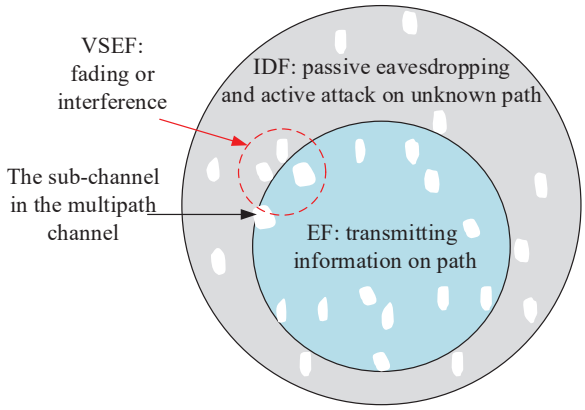

Figure 2. *Causes of WESS problems.*

Figure 3 shows the causes of WESS problems of wireless communication. Due to the multipath effect of electromagnetic waves, after the signal is sent from the transmitter, it will go through many different paths to reach different locations. We expect the signal to pass through some reachable paths and converge at the legal receiver with greater energy. However, the phases of signals that experience different reachable paths are different, and fading may occur after superposition (i.e., VSEF). Fading occurs on the reachable path of the desired function, so this kind of sub-effect can also be called the on-path VSEF. At the same time, attackers may also receive signals from the unknown path (i.e., off-path) to eavesdrop or launch attacks, which is the off-path IDF of wireless communication. It can be seen from Section 2.1 that once the above VSEF and IDF are triggered, there will be endogenous security problems. Wireless endogenous security problems can also be divided into two categories. Safety problem mainly refers to random fading, natural and man-made interference; security problem mainly refers to man-made eavesdropping and access attacks. The relationship between them is shown in the figure below. Among them, the general uncertainty disturbance in wireless communication represents the safety problem caused by natural and man-made interference, and the security problem caused by man-made attack.

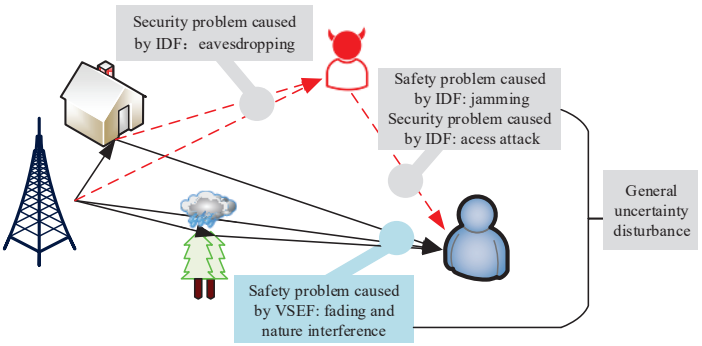

Figure 3. *The WESS problem of wireless communication system.*

III. ENDOGENOUS SECURITY ATTRIBUTES AND STRUCTURE

3.1 Classic DHR Structure

In the face of endogenous security problems, the traditional network security methods mostly use precise defense based on threat perception, such as patching the system and checking poison. These methods can only implement effective defense on the premise of acquiring prior knowledge of attack sources, characteristics, approaches, behaviors and mechanisms. However, they can neither eradicate the uncertain threats caused by VSEF or IDF, nor predict or resolve the attacks against unknown threats. In order to deal with

this network security problem, the idea of reference [4, 5, 8] is that since the endogenous security problem comes from the structure itself, we should follow the endogenous security mechanism of "structure determines function", and design the information system structure with the attribute of endogenous security. The classic cyberspace endogenous security structure

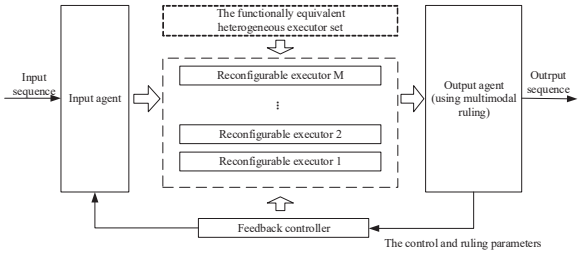

Figure 4. *Classic cyberspace endogenous security structure.*

is shown in Figure 4, which mainly includes input agent, heterogeneous executor and output agent. The region of the three is called mimicry bound, which is the region protected by endogenous security mechanism. The advantages of the structure are mainly reflected in the following two aspects: first, the "relatively correct"axiom can transform an unknown problem scene in a single space into a perceptible scenario under the consensus mechanism in a functionally equivalent multi-dimensional heterogeneous redundant space. In other words, unless multiple unknown problems produce wrong results at the same time, the safety and security of the system will not be affected. The other is dynamic multimode consensus mechanism, which can make the system form "uncertainty" effect. Therefore, even if the attacker knows a certain dark function, his "trial and error tactics" will fail because he does not know which heterogeneous executors the system has selected. It can be seen that the endogenous security mechanism can deal with unknown security threats and uncertain random disturbances without relying on prior knowledge about vulnerabilities, backers or attackers.

3.2 Wireless Endogenous Security Attributes

The key to solve the problem of endogenous security is to explore the attributes of endogenous security, construct the structure of endogenous security and realize the function of endogenous security. Inspired by this idea, this section first discusses the endogenous security attributes of wireless communication. Different from wired network system, wireless communication system itself has endogenous security attributes. This is caused by the propagation characteristics of electromagnetic wave and electromagnetic environment. The propagation mode of electromagnetic wave can be expressed by Maxwell equation as follows

$$\begin{aligned} &\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0} \\ &\nabla \cdot \mathbf{B} = \mathbf{0} \\ &\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \\ &\nabla \times \mathbf{B} = \mu_0(\mathbf{J} + \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t}) \\ &subject\ to\ \Delta\zeta \end{aligned} \tag{1}$$

where E is the electric field intensity, B is the magnetic induction intensity, ρ is the charge density, and $\mathbf{J}$ is the current density; ε_0 and μ_0 are the permittivity and permeability in vacuum, respectively, ∇, $\nabla\cdot$ and $\nabla\times$ are the vector differential operator, divergence and curl, respectively; $\Delta\zeta$ is a set of boundary conditions, which is a set of equations that determine the relationship between the electromagnetic field on both sides of the interface. According to the completeness of Maxwell's equations, when the initial conditions and boundary conditions are determined, the equations set has a unique solution. The boundary conditions are determined by the various medium in the propagation of electromagnetic waves, i.e., electromagnetic environment. Generally speaking, the medium experienced by the electromagnetic wave received at each point in space is different. This means that the boundary conditions at different locations are different, resulting in different solutions to equation (1). Moreover, the complexity of the electromagnetic environment makes it difficult for us to determine the boundary conditions and predict electromagnetic waves at different locations. Therefore, the unpredictability of the electromagnetic environment is the endogenous security attribute of wireless communication. One of the usual concrete manifestations of the electromagnetic environment is the wireless channel. In the following, we introduce the DHR characteristics in the endogenous security properties of the wireless channel in detail.

3.2.1 Heterogeneity

The heterogeneity stems from the unique propagation mode and complicated propagation environment of electromagnetic wave. The refraction, scattering, diffraction, and reflection effects of electromagnetic wave propagation reach the receiver in different paths and at different times, which leads to random multipath fading after the signals of each path are superimposed on each other according to their phases [12]. From the above analysis, it can be seen that the boundary conditions of the two points with large differences in space are different, so the fading of the wireless channels are also different. Unless the attacker and the legitimate user are exactly the same in the time, frequency, and space domains, there must be a difference between the legitimate and illegitimate channels [13]. The diversity and complexity of the wireless channel makes it difficult to predict the boundary conditions. Therefore, the wireless channel between legitimate communication nodes has non-replicable and non-measurable heterogeneity to third parties at different locations.

3.2.2 Redundancy

Compared with traditional wired communication, the broadcasting characteristic of electromagnetic waves obscures the limitations of communication boundaries to a certain extent, which enables the signals from the transmitter to be received at multiple points in space. When considering the multi-antenna system, each antenna within the array can acquire signals and decode information. In addition, the channels of the antennas at different locations are also different, which enables the multi-antenna system to use redundant space resources to achieve diversity or multiplexing gain. Therefore, the wireless channel has redundancy in the spatial domain[14].

3.2.3 Dynamic

The dynamic nature of the wireless channel comes from its natural time-varying nature. Time-varying is caused by the movement of transceivers, scatterers, and changes of the propagation medium in the electromagnetic environment. The real-time changing electromagnetic environment leads to different channels at different times for the same location, which makes the channel dynamic. Although the dynamics of wireless channels are often regarded as a factor that is detrimental to reliability in wireless communication systems, we can use natural or man-made dynamics to construct endogenous security mechanisms inspired by the concept of endogenous security. Specifically, the wireless channel can be used as a heterogeneous executor with dynamic and redundant characteristics to construct the DHR structure shown in section 3.1, which makes the protected system obtain the ”unpredictable” attribute and increase the difficulty of successful attack.

3.3 Wireless Endogenous Security Structure

Utilizing the inherent security attributes of wireless channel in Section 3.2, we can construct a wireless endogenous security structure to inherit the security effects of classic DHR structure and cope with unknown security threats. As shown in Figure 5, the heterogeneous executor corresponding to the classic DHR structure is the wireless channel, the input agent is the transmitter, and the output agent is the receiver. The area covered by the above three is called the mimicry bound, which is the range that our wireless endogenous security mechanism needs to protect. In addition, the diversity technology performed by the output agent (such as maximum ratio combining, etc.) can reduce the impact of random noise (VSEF), similar to the ruling mechanism output agent in Figure 4. The beamforming technology after the transmitter estimates the channel can be compared with the policy scheduling and feedback control of DHR structure. If we compare

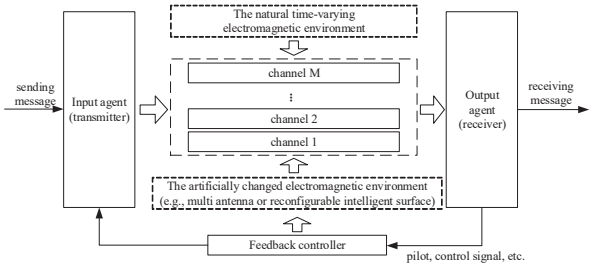

Figure 5. *The WESS structure.*

the wireless endogenous security with the classical wireless communication, we can find that the essence of wireless endogenous security is based on using endogenous security attribute of the channel to solve the natural and man-made general uncertain disturbance.

Nevertheless, the essence of classical wireless communication is to fight against the disturbance caused by the uncertainty of natural channel. The difference between the two lies in the design concept. The wireless endogenous safety based on the fine cognition, optimizing customization and fine control of the electromagnetic environment, while the classic wireless communication is passively adapted to the electromagnetic environment. What they have in common is that they both make use of the endogenous security properties of the channel. A symbiotic relationship that is different from the traditional binding and splicing security mechanism exists between wireless endogenous security and classic wireless communication. They are both endogenous integration and can symbiotic development. For example, the Channel State Information (CSI) estimation technology can not only better combat the random channel fading, but also make better use of CSI to scramble the signal and enhance the endogenous security algorithm. Similarly, as for the channel coding technology, a good coding method can not only improve the robustness of the communication system, but also help to realize the physical layer secure transmission (a kind of wireless endogenous information security) technology.

IV. ESS FUNCTION AND TECHNOLOGY

4.1 Wireless Endogenous Information Security Technology

The purpose of wireless endogenous information security technology is to protect the confidentiality, reliability and integrity of information. As shown in Figure 6, we use the wireless channel as the executor to realize the secure transmission technology based on random signal scrambling [15–17], and can also realize the physical layer key generation technology based on "one time pad" [11, 18, 19]. Among them, the essence of the physical layer security transmission technology is to design a signal transmission and processing mechanism that is strongly associated with the wireless channel, so that only users on the legal channel can correctly demodulate the signal, while the signals on the channels in other locations are scrambled and unrecoverable. The essence of the physical layer key generation technology is to directly use the CSI to generate keys. The key can be seen as a simplified

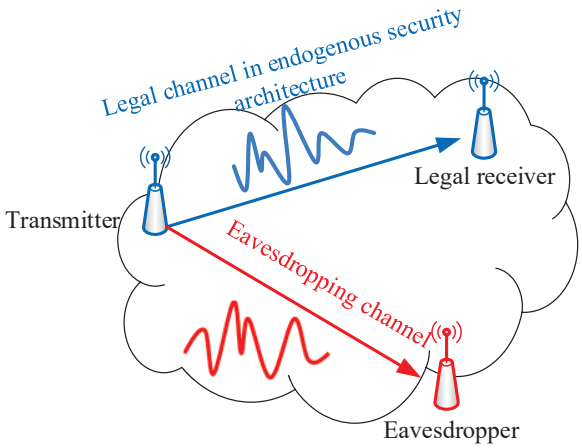

Figure 6. *Wireless endogenous information security technology based on wireless channel.*

representation of the executor. After the key is used for authentication or encryption, the information can be bound to the executor, thereby preventing attacks or eavesdropping from other unknown locations. The realization of the above two wireless endogenous security functions does not rely on any prior knowledge and behavior characteristics of the attacker, so it can deal with unknown security threats.

Moreover, reference [11] points that physical layer key generation technology can be used to realize "one time pad". Because the amount of information of the electromagnetic environment itself is large enough, and the communication process of transmitting the source naturally contains the same amount of electromagnetic environment information, which can provide enough keys. Therefore, as long as we can realize the precise and meticulous cognition and shaping of the environment, no matter how high the communication rate is, we can obtain the matching key rate from the endogenous electromagnetic environment. And the extracting procession does not dissipate additional energy or occupy additional resources. The reference [11] also shows that we can improve the randomness and dynamics of channel fingerprints by some enabling techniques. As shown in Figure 7, the Reconfigurable Intelligent surface (RIS) of metamaterial has the characteristics enabling to control electromagnetic waves effectively, fast and flexibly, which can enrich and amplify the DHR characteristics of electromagnetic environment to improve security and safety [20]. Reference [21] also gives a method to improve the key generation rate in static environment by fully

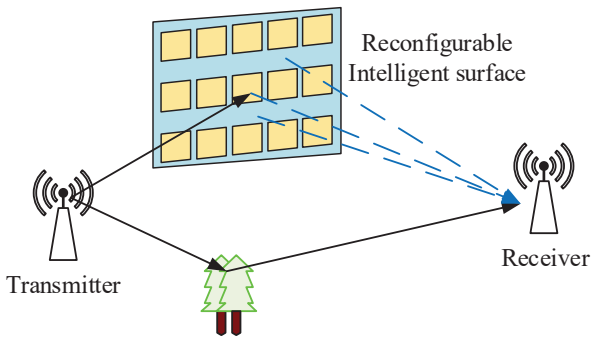

Figure 7. *The reconfigurable intelligent surface aided wireless communication.*

exploring the electromagnetic environment and signal entropy. These enabling technologies are helpful to realize the "one time pad" endogenous security function based on the endogenous security attributing of electromagnetic environment.

4.2 Wireless Endogenous Functional Safety

Wireless endogenous security can not only provide information security, but also provide reliability and availability of functional safety. Many traditional wireless communication technologies are designed to ensure the functional safety of communication, such as spread spectrum communication [22], multi-antenna diversity technology and so on. They are mainly against generalized uncertain disturbances which includes uncertain disturbances of natural channels and anthropogenic disturbances. These technologies generally use some DHR characteristics and belong to endogenous security technology based on atypical DHR structure . Take wireless communication anti-interference technology as an example. Anti-jamming the technique can generally be divided into time domain [23], spatial domain and frequency domain [24] anti-interference. Taking classical time-hopping, frequency-hopping and space-hopping communication as examples, they use time-domain, frequency-domain or spatial domain redundancy to randomly select different time, frequency points or actuators (i.e., wireless channels) on the antenna to communicate according to the hopping image. Therefore, wireless communication anti-jamming technology introduces dynamic and random elements, which makes the defense mechanism have uncertainty effect and can effectively increase the interference difficulty of the attacking party. However, most of the existing arrays use isomorphic elements, which have the problems of heterogeneity and limited degree of freedom. [25] presents an array of space-time heterogeneous antennas, in which each heterogeneous antenna can scan quickly and distinguish multipath to realize fine sensing and manipulation of electromagnetic environment. Based on metamaterials, the DHR antenna array is constructed by spatial heterogeneity, which makes the array elements in different positions have heterogeneous and uncorrelated patterns. The array can make the spatial resources get rid of the limitation of the spatial spectrum wall and improve the efficiency under the condition of antenna aperture limitation. As shown in Figure 8, theoretically N array elements and K heterogeneous degrees of freedom can achieve the actual degrees of freedom of NK, and the receiving capacity increases linearly with the degree of isomerism (including time domain isomerism and spatial heterogeneity)[25]. As a result, DHR antennas are not only achieve array gain but also obtain the gain of array elements, thus amplifying the dynamic and heterogeneous nature of wireless endogenous security structure, further improving signal-to-noise ratio and anti-interference ability, and obtaining better wireless endogenous function security effect.

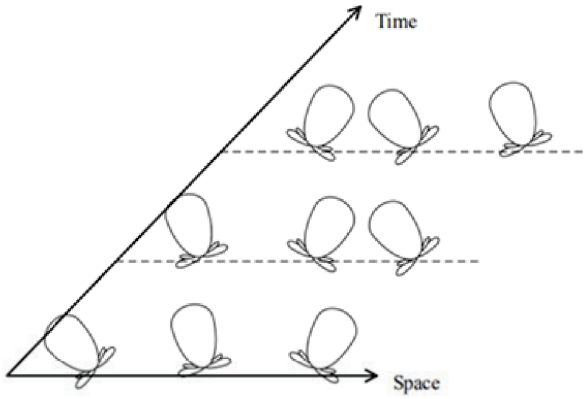

Figure 8. *The DHR antenna array.*

V. CONCLUSION

From the perspective of the principle of endogenous security, this paper combs the endogenous security

problems of wireless communication, analyzes the attributes of wireless endogenous security and the characteristics of DHR. Then, the structure of wireless endogenous security is given. Finally, the application of wireless endogenous information security and functional security is introduced. It can be predicted that in the future development of wireless communication, the theory of endogenous security in cyberspace will play an important guiding role as described in this paper. Moreover, the DHR structure of wireless communication system will become an important supplement to the theory of endogenous security in cyberspace. Taking the massive machine communication scenarios that will exist in the future as an example, communication nodes have the characteristics of dense distribution, high concurrent communication, low communication delay, and dynamic migration. The artificial introduction of DHR features will inevitably increase the overhead. Fortunately, wireless channels naturally have endogenous security attributes. The endogenous security structure based on wireless channels can reduce the cost of introducing heterogeneous redundancy and relax the requirements on software, hardware or algorithms, which has important engineering significance. It can be seen that the integration and mutual penetration of ESS theory and WESS theory can not only provide guidance for the development of new wireless communication reliability and security methods, but also provide ideas for the further development of ESS.

ACKNOWLEDGEMENT

This work was supported by National Natural Science Foundation of China (No. 61941114).

References

[1] AHMAD I, KUMAR T, LIYANAGE M, et al. Overview of 5g security challenges and solutions [J]. IEEE Communications Standards Magazine, 2018, 2(1):36-43.

[2] JI X, HUANG K, JIN L, et al. Overview of 5g security technology[J]. Science China Information Sciences, 2018, 61(8):081301.

[3] HWANG T, YANG C, WU G, et al. Wireless communications-ofdm and its wireless applications: A survey[J]. IEEE Transactions on Vehicular Technology, 2009, 58(4):1673.

[4] HU H, WANG Z, CHENG G, et al. Mnos: A mimic network operating system for software defined networks[J]. IET Information Security, 2017, 11(6):345-355.

[5] Ren Q, Wu J, He L. Performance modeling based on gspn for cyberspace mimic dns[J]. Chinese Journal of Electronics, 2020, 29(4):738-749.

[6] GUO W, WU Z, ZHANG F, et al. Scheduling sequence control method based on sliding window in cyberspace mimic defense[J]. IEEE Access, 2019, PP(99):1-1.

[7] Li H, Hu J, Ma H, et al. The architecture of distributed storage system under mimic defense theory[C]//2017 IEEE International Conference on Big Data (Big Data). [S.l.: s.n.], 2017: 2658-2663.

[8] HU H, WANG Z, CHENG G, et al. Mnos: a mimic network operating system for software defined networks[J]. IET Information Security, 2017, 11(6):345-355.

[9] HU H, WU J, WANG Z, et al. Mimic defense: a designed-in cybersecurity defense framework[J]. Iet Information Security, 2018, 12(3):226-237.

[10] WU J. Cyberspace mimic defense[M]. [S.l.]: Springer, 2020.

[11] Jin L, Wang X, Lou Y, et al. Achieving one-time pad via endogenous secret keys in wireless communication[C]//2020 IEEE/CIC International Conference on Communications in China (ICCC). [S.l.: s.n.], 2020: 1092-1097.

[12] CHEN C, JENSEN M A. Secret key establishment using temporally and spatially correlated wireless channel coefficients[J]. IEEE Transactions on Mobile Computing, 2010, 10(2):205-215.

[13] WANG X, JIN L, HUANG K, et al. Physical layer secret key capacity using correlated wireless channel samples[C]//2016 IEEE Global Communications Conference (GLOBECOM). [S.l.]: IEEE, 2016: 1-6.

[14] QIN D, DING Z. Exploiting multi-antenna non-reciprocal channels for shared secret key generation[J]. IEEE Transactions on information forensics and security, 2016, 11(12):2693-2705.

[15] Sun X, Yang W, Cai Y, et al. Secure transmissions in wireless information and power transfer

millimeter-wave ultra-dense networks[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(7):1817-1829.
[16] Sun X, Yang W, Cai Y, et al. Secure transmissions in millimeter wave swipt uav-based relay networks[J]. IEEE Wireless Communications Letters, 2019, 8(3):785-788.
[17] Goel S, Negi R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6):2180-2189.
[18] Maurer U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39 (3):733-742.
[19] HU X, JIN L, HUANG K, et al. A secure communication scheme based on equivalent interference channel assisted by physical layer secret keys[J]. Secur. Commun. Netw., 2020:1-15.
[20] HU X, JIN L, HUANG K, et al. Secret key generation assisted by intelligent reflecting surface with discrete phase shift in static environment [M]. [S.l.]: TechRxiv, 2020.
[21] Jin L, Zhang S, Lou Y, et al. Secret key generation with cross multiplication of two-way random signals[J]. IEEE Access, 2019, 7:113065-113080.
[22] Poor H V, Xiaodong Wang. Code-aided interference suppression for ds/cdma communications. i. interference suppression capability[J]. IEEE Transactions on Communications, 1997, 45(9): 1101-1111.
[23] Adem N, Hamdaoui B, Yavuz A. Pseudorandom time-hopping anti-jamming technique for mobile cognitive users[C]//2015 IEEE Globecom Workshops (GC Wkshps). [S.l.: s.n.], 2015: 1-6.
[24] Hanawal M K, Abdel-Rahman M J, Krunz M. Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems [J]. IEEE Transactions on Mobile Computing, 2016, 15(9):2247-2259.
[25] Jin L, Lou Y, Xu X, et al. Separating multistream signals based on space-time isomerism [C]//2020 International Conference on Wireless Communications and Signal Processing (WCSP). [S.l.: s.n.], 2020: 418-423.