Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Cyberspace Security—Article

Cyberspace Endogenous Safety and Security

Jiangxing Wu *

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

ARTICLE INFO

Article history:
Received 14 April 2020
Revised 26 August 2020
Accepted 16 May 2021
Available online 6 August 2022

Keywords:
Cyberspace endogenous security problem
Uncertain threat
Cyberspace endogenous safety and security
Relative right axiom
Dynamic heterogeneous redundant architecture

ABSTRACT

Uncertain security threats caused by vulnerabilities and backdoors are the most serious and difficult problem in cyberspace. This paper analyzes the philosophical and technical causes of the existence of so-called "dark functions" such as system vulnerabilities and backdoors, and points out that endogenous security problems cannot be completely eliminated at the theoretical and engineering levels; rather, it is necessary to develop or utilize the endogenous security functions of the system architecture itself. In addition, this paper gives a definition for and lists the main technical characteristics of endogenous safety and security in cyberspace, introduces endogenous safety and security mechanisms and characteristics based on dynamic heterogeneous redundancy (DHR) architecture, and describes the theoretical implications of a coding channel based on DHR.

1. Introduction

A large number of cyber security events have demonstrated that most security threats are caused by interaction between external causes (i.e., human-made attacks) and internal causes (i.e., the so-called "endogenous security problems") [1–4] through the vulnerabilities in the target object itself. Unfortunately, thus far, traditional ways of thinking and technical network security routes rarely leave the inertial thinking of "do your best to get rid of the problem." Thus, network security routes typically involve digging holes, patching, sealing doors, checking poisons, and killing Trojan horses; they may also involve setting honeypots and sandboxes and cascading additional protective measures, including the built-in hierarchical detection method (which draws on the idea of biological endosymbiosis). However, the introduction of traditional security functions inevitably introduces new endogenous security risks. Solving the problem of diminishing the uncertain threat impact stemming from endogenous security problems requires major theoretical and technological innovation.

Based on the philosophy of "everything inherently contains contradiction and has both advantages and disadvantages," this paper analyzes the inevitability of the existence of endogenous security problems in information systems. It also describes the concept and characteristics of endogenous security problems in cyberspace and points out that the endogenous security problem—which is inherently contradictory—cannot be completely eliminated, whether in theory or engineering. Avoiding or resolving the security risks caused by self contradiction can only be effectively done by developing or using the endogenous safety and security effects of the system meta-structure (i.e., the algorithm) or by forming a so-called "endogenous safety and security system mechanism." This article provides a definition for and lists the technical characteristics of the proposed endogenous safety and security mechanism. Inspired by the reliability theory and method, we have created a dynamic heterogeneous redundancy (DHR) architecture and propose the principle that DHR architecture can deal with traditional reliability problems and nontraditional network security problems in a normalized way.

2. The cyberspace endogenous security problem

2.1. Definition and implications of the endogenous security problem

The German philosopher G.W.F. Hegel stated, "contradiction is the root of all movements and vitality; things move only because they have contradictions." In this sense, cyberspace shares the same philosophical nature as the real world. The existence and development of everything is based on contradiction, making contradiction a condition for development. The conflicting nature of contradiction prompts the elimination of the two sides of a contradiction; this results in an imbalance in the development of the

* Corresponding author.
E-mail address: ndscwjx@126.com.

https://doi.org/10.1016/j.eng.2021.05.015
2095-8099/© 2021 THE AUTHOR. Published by Elsevier LTD on behalf of Chinese Academy of Engineering and Higher Education Press Limited Company.

strength of the two sides. For example, in information technology (IT), big data technology can be used to discover unknown rules or characteristics based on algorithms and data samples; however, the deliberate pollution of data samples and malicious exploitation of algorithm vulnerabilities can also yield incorrect or skewed results that can misdirect the system or people using the data. Moreover, blockchain technology is providing a new era of decentralized bookkeeping, while the 51% consensus mechanism fails to avoid the exploitation of vulnerabilities in commercial-off-the-shelf-level software and hardware products with a market share greater than 51%.

To summarize, although the development of contemporary computing technology has enabled humans to step into the brilliant age of information, the internal security flaws of computing technology also bring risks and uncertain threats. Therefore, an endogenous security problem and an endogenous security service system structure are different forms or performances of the same system structure or the same algorithms under different scenarios with different application targets and under different technological conditions, based on the essential contradictions that are inherent to any system. Cyberspace is no exception to this rule: Any software/hardware configurations or algorithms are inevitably associated with side effects or with an invisible "dark side" apart from their fundamental functions. Once triggered, such side effects or "dark functions" may have negative impacts on the correct expression of the intrinsic functions; in cyberspace, such side effects and dark functions are known as "endogenous security problems."

Endogenous security problems can be further abstracted into two types. *Narrow endogenous security issues* refer to the phenomenon by which any software or hardware entities have visible or invisible unexpected functions such as side effects, vulnerabilities, or natural failure, aside from their designed functions. *General endogenous security issues* in addition to having the same problems as narrow endogenous security issues, also involve design functions that are subjectively and intentionally invisible to end users, and include all hidden functions of hardware and software that have not been explicitly declared or disclosed to users, such as deliberately designed front doors, backdoors, and traps.

2.2. The characteristics of endogenous security problems

The characteristics of endogenous security problems [4] can be concluded from the definition and implications of endogenous security problems.

2.2.1. The necessity of existence

For years, vulnerabilities and backdoors have continued to be a problem in cybersecurity. According to statistical laws, there is a certain proportional relationship between the number of vulnerabilities and the number of codes in a cyber system [5]. Vulnerabilities also increase with the rising complexity of the system and the number of codes. At the same time, due to the development of the globalized economy and the specialization and refinement of the industrial division of labor, integrated innovation or manufacturing has become a universal production organization model. Supply chains such as design chains, tool chains, production chains, support chains, and service chains for various products are becoming longer. In addition, the scope and the number of links involved are increasing, providing many opportunities for backdoors to be embedded. The emergence of software and hardware code loopholes (i.e., trapdoors) introduced by these non-subjective factors or of artificially embedded backdoors that enter the information system is inevitable—whether from the perspective of technological development or from the perspective of the game of interest—and is fundamentally difficult to avoid.

2.2.2. Contingency

Although vulnerabilities are found from time to time, when and how each vulnerability is discovered differ, making vulnerabilities an irregular phenomenon. From the perspective of epistemology, the philosophical study of knowledge, things can always be known; thus, the existence and discovery of vulnerabilities are inevitable events, even though the specific time, target system, and manner in which they are presented are accidental. Events that unearth vulnerabilities include the technical stages or era limitations, as well as the theoretical methods and technical capabilities for the completeness checking of complex codes.

2.2.3. Spatiotemporal characteristics of cognition

Based on the cognition of "vulnerabilities exist objectively, but finding vulnerabilities is spatiotemporal, and vulnerabilities need to be accumulated to a certain degree," a system that is considered safe today may not be safe tomorrow; a system that one person thinks is safe may not be safe in the eyes of another; and a system that is safe in Environment A may not be safe in Environment B [3]. This is the spatiotemporal difference between vulnerabilities based on cognition.

2.2.4. The uncertainty of the threat

In economics, Frank Hyneman Knight distinguished the relationship between risk and uncertainty as follows: *Risk* is an uncertainty whose probability distribution can be known and whose future possibility can be inferred; in contrast, *uncertainty* means that it is simply not possible to predict the future events. It is not difficult to see that an endogenous security problem may cause two types of security threats. One threat is that the security problem significantly affects the reliability, credibility, and availability of the target object's intrinsic or service functions. The other threat is that the problem results in someone illegally obtaining or violating the privacy information and data resources of others. Due to the nature of an endogenous security problem, the occurrence of the above two types of security threats is unpredictable, so they are unknown and uncertain threats.

In a more general sense, due to the staged characteristics of human technological development and cognition levels, vulnerabilities in software and hardware design cannot be completely avoided or thoroughly investigated. In addition, due to globalization, the industrial ecology environment is open and technologies are collaborative. Such an inseparable industry chain makes it impossible to completely eliminate hardware and software backdoors. Thus far, the defense against uncertain threats based on endogenous security problems scarcely includes quantitative design and verifiable measurement-based defense solutions, apart from the additional use of security technology, as security technicians try their best to block the impact of disturbances from the attack surface.

3. Considering a solution to the cyberspace endogenous security problem

3.1. Changing problem-solving ideas

Based on the concept that the external causes of most security threats in cyberspace are human-conducted attacks, whereas the internal causes of security threats are backdoors and vulnerabilities in target systems (i.e., the endogenous security problem), an intuitive corollary is that in order to completely eliminate cyberspace security threats, endogenous security problems must be completely ruled out, because external factors can only operate through internal factors. However, according to both theory and practice, endogenous security problems cannot be completely eliminated. First of all, following globalization, open and collaborative innovation chains and industrial chains are becoming the basic model for the development of modern industry. It is almost impossible to achieve complete independence and control at the supply-chain level with the power of one country alone. Second, there are currently no effective theoretical and technical solutions to eliminate the vulnerabilities caused by software and hardware design defects. Attempting to fundamentally eliminate such problems is also contrary to the objectiveness of human cognition and the current stage of technological development law. This means that, theoretically, technically, and economically, it is impossible to completely guarantee that cyberspace is an environment without endogenous security problems; that is, the vision of a "non-toxic and sterile" cyberspace is almost impossible to achieve.

A trivial inference from the analysis above is that it may be necessary to alter the current problem-solving ideas, given the presence of so-called "bacteria" carrying "toxins" in cyberspace, and alleviate the threat challenges of the "known unknowns" and "unknown unknowns." It is necessary to break away from the traditional mindset of "making up for the dead" and enable the safety of information equipment to no longer depend excessively on the degree of independence and controllability of the software, hardware design, production, operation and management of components, devices, components, or individual forms. Security and credibility can be obtained by giving the basic structure of the information system an endogenous security function or an endogenous safety and security mechanism. Under certain conditions or constraints, this function or mechanism can tolerate the endogenous security problems of software and hardware components, so that the intrinsic function has combined stability robustness and quality stability, regardless of random failures or network attacks.

3.2. Inspiration from bio-immunology

From biology, we know that the innate nonspecific immunity obtained by humans through genetic characteristics can respond with the nonspecific elimination of most invading pathogenic microorganisms, in what is a kind of surface-level defense. Scientific research has shown that pathogenic microorganisms are constantly mutating in nature. But what factors ensure that nonspecific immunity depends only on biological genetic information, so that the body is capable of the nonspecific selective removal of various invading pathogenic microorganisms that change in the real world? Under what circumstances and by what means can specific immune mechanisms be activated? Genetic information is relatively stable and needs to be updated throughout the life cycle of the organism. But when and how should such information be updated? In addition, specific immunity is a type of point defense, but how can the memory of immunity affect the genetic information of nonspecific immunity?

Based on these thoughts, inspiration can strike: Can we design a combined defense capability similar to the vertebrate immune mechanism in order to generate endogenous security problem of target system based no specific selective clearance function to unknown attack activities, and trigger point defense functions such as specific immune mechanisms in a timely fashion? It is the belief of this author that such a defensive function, derived from the target's own construction mechanism, is possible and best described as endogenous security.

3.3. Cyberspace endogenous safety and security

Endogenous safety and security refers to structures or algorithms and their institutional mechanisms that have endogenous effects or endogenous safety or security effects [4]. *Endogeneity* is literally an endogenous effect that a system produces by itself rather than obtaining it by means of external factors. Thus, *endogenous safety and security* refers to the safety or security functions or properties obtained by using internal factors such as the system architecture, algorithms, mechanisms, or scenarios. For example, the nonspecific and specific immune learning mechanisms of vertebrates are an endogenous security function. The institutional mechanisms and technical characteristics of endogenous safety and security are as follows.

3.3.1. Expected endogenous safety and security systems

An endogenous safety and security system should

(1) Be based on an open organizational architecture and cover all endogenous security issues in its architectures, modules, and components;

(2) Be an integrated and convergent structure that can simultaneously provide highly reliable, highly trustable, and highly available functions;

(3) Be able to use the defensive elements of diversity, randomness, and dynamics;

(4) Have heterogeneity, redundancy, dynamics, adjudication, and feedback control, in addition to structural elements;

(5) Be able to cooperate with traditional solutions to security protections or other technologies in order to obtain exponential defense gains;

(6) Be universally applicable.

3.3.2. Expected endogenous safety and security mechanisms

(1) The relationship between endogenous safety and security mechanisms and generalized uncertainty disturbances can be categorized into human–computer, computer–computer, and computer–human games.

(2) An endogenous safety and security mechanism should be able to conditionally control or suppress generalized uncertainties without attempting to eliminate their effects.

(3) The effectiveness of endogenous safety and security mechanisms should not rely on any prior knowledge about the attacker, additional built-in internal symbiosis, other security measures, or other technical means.

(4) Endogenous safety and security mechanisms should be able to provide integrated, highly reliable, highly trustable, and highly available performance for the target system in a converged manner.

(5) Generalized security led by endogenous safety and security mechanisms should have stable and high-quality robustness with a quantitative design and verifiable metrics.

(6) The effectiveness of endogenous safety and security mechanisms should only be weakly associated or unassociated with the technical capabilities and experience of the operator or maintenance managers.

3.3.3. Expected technical characteristics

(1) Endogenous safety and security is part of the target object's built-in safety function; it has a defense mechanism that combines both generality and focus, similar to a vertebrate's nonspecific and specific immune mechanism. Endogenous safety and security is structurally indivisible from the target's intrinsic function.

(2) Endogenous safety and security methods should not depend on any prior knowledge or on the attackers' behavioral characteristics. Endogenous security has a natural suppressive effect against differential-mode attacks formed by independent attack resources, attack technologies, and attack methods. In other words, any network attacks based on zero-day vulnerabilities, backdoors, viruses, or trojans are ineffective in principle against target objects with endogenous security characteristics.

(3) In addition to social engineering methods, the only way to break through endogenous security defense and achieve common-mode escape is through precise and coordinated attacks with spatiotemporal consistency. First, the attacker should overcome the uncertainty effect that stems from the inconsistency of space and time. Next, constructing a common-mode escape situation requires breaking through the iterative feedback scheduling mechanism of heterogeneous and redundant targets, based on the policy decision. Finally, the attacker must face the problem of maintaining the stability of the common-mode escape.

(4) Endogenous security functions should be able to solve traditional reliability problems and target-based network threat problems in a normalized manner.

(5) In theory, differential-mode escape cannot occur, and common-mode escape has an extremely low probability; even if the latter succeeds, it may only occur once. In the endogenous security environment, both the attack action and the attack result do not have stability robustness and quality robustness

4. Endogenous safety and security mechanisms based on DHR architecture

4.1. Implications of reliability issues

Through long-term research and exploration, I have found that although the reliability problem and the cybersecurity problem are two different fields with different disturbance factors (the former is mainly manifested by random disturbances, while the latter is completely dominated by attackers' behavior), there are many similar or even identical theoretical and technical problems in these two areas. Thus, it should be possible in one area to learn from the related theoretical methods and institutional mechanisms of the other.

It is well known that the most challenging problem in the field of reliability is how to deal with the uncertain breakdown or failure of the system. Two basic issues are involved: ① how to deal with physical errors or the failure of passive and active components; and ② how to avoid uncertain failures caused by undetected software or hardware design defects. Although the mechanisms and impacts of such failures differ, they share a common characteristic: The time, location, nature, and result of the failure are all uncertain. In other words, reliability technologies need to overcome uncertain errors and failures caused by endogenous security issues.

4.2. The rediscovery of the relatively correct axiom

The relatively correct axiom (also known as the consensus mechanism) refers to the fact that although everyone has their own shortcomings, it is rare for many people to make the same mistake when carrying out the same task independently. A successful application of the relatively correct axiom in engineering is the dissimilar redundant structure (DRS) [1], which was first proposed in the 1970s in the field of flight controllers (Fig. 1). Given certain prerequisites and under certain constraints, even the randomness effect caused by unknown design defects in software and hardware components may fail, or the statistical uncertainty effect may become invalid due to unknown design defects; such circumstances can all be converted into differential-mode or common-mode events and expressed as a probability through the multi-modal voting mechanism. In this way, it is possible to significantly improve the system reliability by improving not only the quality of its components, but also the level of innovation in the technology used to construct it.

In terms of uncertain threats to the endogenous security in the target objects, the DRS structure has the same or a similar effect as the "enemy" and "friend" identification, in a sense. Although the heterogeneous redundant functional equivalent effect of the uncertain attacks cannot be expressed using probability, the reflection of such attack events at the group level is usually presented as a differential mode. In a small-scale space, DRS-based target objects can suppress generalized uncertainties (including unknown human-made attacks) with designable and measurable high-quality robustness.

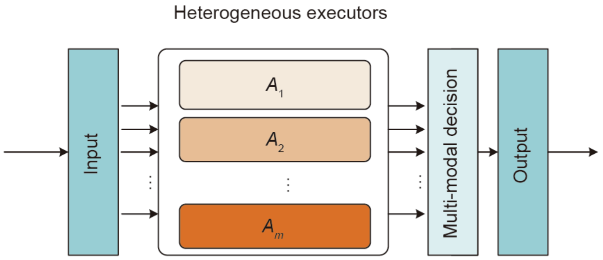

Fig. 1. An abstract model of DRS architecture. A_i (i = 1, 2, ..., m): the ith heterogeneous executor; m: the number of heterogeneous executors.

4.3. Dynamic heterogeneous redundant architecture

It is not difficult to determine that, although a target object whose construction is based on a DRS can suppress general uncertain disturbances including unknown human-made attacks, the available conditions of the various executors' environment and related vulnerable backdoors are statically determined in the DRS architecture. The parallel deployment of the executors does not usually change the reachability of the attack surface. Therefore, a successful attack experience against a DRS is inheritable, and the attack method is reproducible. The attacker can sustainably make use of the previous attack knowledge. In other words, a DRS architecture still has defects at the genetic nontraditional security level of nontraditional security in terms of statics, similarity, and determinacy; thus, it does not have the characteristics of stable and high-quality robust control.

From the perspective of information entropy, it can be found that attack and defense behaviors can be thought of as a game concentrating on the increase or decrease of the initial information entropy of the defending side. The invasion tolerance of a DRS structure lacks time stability. With an increase of trial-and-error attacks, there is no self-sustaining invasion-resistance mechanism. Hence, without a self-sustaining mechanism, the initial information entropy can only cause entropy reduction until the initial information entropy is low enough so that the attack chain can reliably play the expected role, and the intrinsic structure function or the defense effect is completely lost.

It is not difficult to infer that if the initial information entropy maintenance (or entropy balance) mechanism can be introduced into the DRS architecture, it can enable the architecture's tolerance with a certain degree of robustness. For example, adding some traditional defense elements (i.e., dynamicity, randomness, diversity, reconstruction, encryption authentication, intrusion detection, intrusion prevention, etc.) or robust control mechanisms (i.e., policy ruling, feedback control, iterative convergence, etc.) should make it possible to change the static nature of the DRS operating environment. Such "genetic engineering" reconstruction has the property of not reducing the initial information entropy, so the quantifiable design and verifiable measurement of this control structure and the operating mechanism should have stable and high-quality robustness in terms of intrusion tolerance and fault tolerance.

I call this innovative technology "DHR." The abstract model of DHR is shown in Fig. 2.

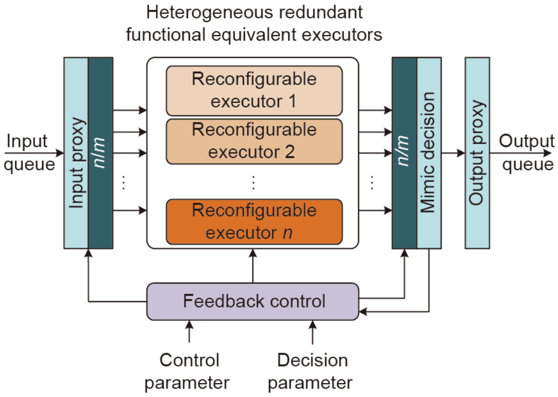
Heterogeneous redundant functional equivalent executors
Input queue
Input proxy
n/m
Reconfigurable executor 1
Reconfigurable executor 2
Reconfigurable executor n
n/m
Mimic decision
Output proxy
Output queue
Feedback control
Control parameter
Decision parameter

Fig. 2. Abstract model of DHR architecture. n: the number of reconfigurable executors.

Here is the core idea of the DHR architecture: Based on the well-known axiom "construction determines security," under the condition that the intrinsic service set functions are ensured, DHR combines the multi-modal decision-based scheduling mechanism and the multi-dimensional dynamic reconstruction robust-control mechanism; endows the operating environment with dynamicity, reconfigurability, software definability, and an algorithm-reconfigurable functionality; establishes the uncertainty effects from the attackers' perspective; and adds dynamicity, randomness, and diversity to the target operating scene when suppressing generalized uncertain disturbances.

At the same time, it is vital to strictly control the collaborative approach and eliminate synchronization among the executors as much as possible. The avoidance and destroying effect of the DHR, non-cooperative mode, and multi-mode decision should be maximally utilized in order to significantly improve the tolerance of the software and hardware's differential fault or random failure. In other words, it is expected that the multi-functional integration endogenous security obtained through the DHR architecture can not only effectively suppress the object-based uncoordinated or differential-mode attack disturbance, but also ensure that the model perturbation range can be controlled within the given threshold, even if a coordinated attack escape occurs. The DHR architecture can not only significantly increase the uncertainty of the attack chain, but also fully enhance the performance of the generalized robust-control service or application, including the integration of high levels of reliability, availability, and trustability. It is expected that the severe heterogeneous design requirements can be significantly weakened so that the DHR structure can become a new enabling technology with broad application prospects. Relevant discussions on DHR's basic principles, typical and atypical structures, technical objectives, and typical efficacy can be found in Refs. [1–4].

4.4. Endogenous security features of the DHR architecture

DHR architecture has all the elements needed for an endogenous safety and security system in terms of organizational structure, operating mode, and institutional arrangements. The process of using DHR is the process of establishing an endogenous safety and security system for the target object, which is specifically manifested in the following aspects.

(1) DHR is a completely open organizational structure, allowing software and hardware components to contain any endogenous security issues; that is, it can reliably function well in any contaminated or vulnerable scenarios.

(2) DHR is an integrated fusion structure that can simultaneously provide the functions of high levels of reliability, availability, and trustability. It can not only solve traditional functional security problems, but also manage nontraditional security issues.

(3) DHR architecture can corporately take defense elements such as diversity, randomness, and dynamicity in order to obtain endogenous uncertainty effects and form an unobservable defense fog.

(4) DHR architecture is composed of five significant supporting segments: heterogeneity, redundancy, dynamicity, ruling, and feedback control. It can maximize the synergy of the three defense elements of dynamicity, diversity, and randomness.

(5) When combined with traditional security protection technologies or other technologies, the DHR architecture can obtain exponential defense gains.

(6) DHR architecture has universal application significance for all software and hardware systems.

In addition, the collaborative relationship based on DHR architecture, functions, and related policies has created an endogenous safety and security mechanism with unique advantages, which are specifically manifested in the following aspects.

(1) The unmeasurable defense fog formed by the DHR security mechanism is precisely designed to control or suppress the generalized uncertain disturbance of the endogenous security problem. It can be categorized as a typical human–computer game relationship. If artificial intelligence and big data technology are employed to run in the background, the defender can gain more advantages in human–computer, computer–computer, and computer–human games.

(2) The DHR security mechanism can conditionally control or suppress generalized uncertain disturbances to the target object, but it is impossible to prevent the common-mode escape phenomenon completely.

(3) The effectiveness of the DHR security mechanism does not rely on any prior knowledge or on other additional built-in endogenous security measures; however, these related technical means can be used in conjunction with DHR to obtain exponential security gain.

(4) The DHR security mechanism can provide a highly reliable, highly available, and highly trustable performance for the target objects in an integral manner;

(5) The white-box injection test can verify the security effects of the DHR, which has both stable and high-quality robustness, with a quantifiable design and verifiable measurement.

(6) The efficiency of the DHR is weakly associated with or even unassociated with the technical ability and experience of the administrator, which has a substantial cost-effective advantage throughout the life cycle.

It must be specifically stated that DHR is just one type of cyberspace endogenous safety and security mechanism and does not describe all possible types.

4.5. The coding channel model of DHR architecture

In 1949, Shannon and Weaver [6] proposed the famous channel coding theorem, which laid the theoretical foundation for modern communication—especially error-correction coding. The purpose of Shannon's second theorem (the noisy channel coding theorem) is to reconstruct a properly designed redundancy in the transmitted message in the case of random noise introduced by a memoryless channel, and then use the redundancy to reconstruct the original message at the receiver and finally complete the normal delivery of the message. Although the theorem only provides a proof of existence, its guiding significance to communication is very obvious. It points out new directions and new ways for reliable communication. Error-correction coding was developed under the guidance of this theorem. The endogenous safety and security mechanism constructed by DHR can also be described as a way to correctly process and transmit information on a reconfigurable memory channel with non-random noise. The author believes that the information-processing and transmission errors, reliability errors, and communication noise errors caused by network attacks can be similar in nature and can be solved using error-correction coding ideas. But, unlike the assumption of memoryless channels in the classic Shannon communication model, DHR can be abstracted as a reconfigurable memory channel with processing capabilities. Unlike the random noise assumed by Shannon, network attacks have obvious non-randomness and can be abstracted as non-random noise. Here, random communication noise, random physical failure, and human-made attack noise are collectively referred to as "generalized uncertain disturbances." The equivalent transmission channel model of DHR architecture and the Shannon transmission channel model are shown in Figs. 3 and 4 below.

From the perspective of Shannon's redundant coding theory, the DHR structure can be expanded in time and space into a set of coding structures [4] based on DHR. The purpose is to combat similar channel noise that is random or non-random "structural disturbance noise (SDN)." However, the analysis object of Shannon's channel coding theory is a random memoryless channel, while DHR's heterogeneous redundant iterative defense scenario is equivalent to a random or non-random memory channel. Therefore, Shannon's theory and methods cannot be used directly to quantify the security or generalized robustness of the DHR structure. According to the coding channel theory (CCT) [4], a CCT needs to be developed to enable quantitative analysis of the performance of the coding structure mechanism of the DHR in suppressing SDN. To determine whether the CCT is true, the key is to prove the existence theorem. It is necessary to theoretically clarify the problem of how to construct a suitable channel and coding in order to provide the correct service for a specific discrete memory channel under the condition of generalized disturbance. The so-called "correct" concept is to use the appropriate encoding and decoding steps so that within the system architecture with endogenous security attributes, the error of information transmission and processing is sufficiently small when there is random or artificial additive interference. In short, the CCT is composed of a secure construction endogenous mathematical model, two existence theorems, and their related definitions, lemmas, and mathematical proofs. It covers and should cover the content of Shannon's second theorem.

4.6. A coding channel mathematical model of the DHR architecture

Assume that the attack arrives at a rate λ ($\lambda > 0$). It is assumed that there are three types of single-executor attack success probabilities $P_s(t)$ and a mathematical expression of time t.

$$P_s(t) = \begin{cases} p = 1 - \dfrac{1 - e^{(t-T_s)}}{1 - e^{-T_s}}, t \le T_s \\ 1, t > T_s \end{cases} \tag{1}$$

$$P_s(t) = \begin{cases} p = 1 - \dfrac{1 - e^{(-t+T_s)}}{1 - e^{T_s}}, t \le T_s \\ 1, t > T_s \end{cases} \tag{2}$$

$$P_s(t) = \begin{cases} p = \dfrac{t}{T_s}, t \le T_s \\ 1, t > T_s \end{cases} \tag{3}$$

where T_s refers to the time when the interference arrives and p is the probability of deploying a differential mode channel.

There is no harm in deploying the differential mode element channel with probability p for the first time.

It can be proved [4] that the DHR and feedback-elimination memory-channel construction scheme causes the coding channel structure and the meta-channel memory to have uncertainty, thereby ensuring the randomness of system failure.

4.7. The existence theorem of the coding channel

Sub-channels with the same function and performance in the coding channel are called meta-channels, and the noise of the meta-channels arrives randomly (represented by unknown backdoors in endogenous security problems). For any random noise, the probability of channel output error P_e is $P_e < 1$. In addition to the channel being memoryless, for random noise at any time t, the probability of channel output error is $P_e(t) < 1$. Therefore, under the condition of random noise and no memory channel, the channel structure of n' memoryless meta-channels in the coding channel satisfies the constraint of Shannon's second theorem: The channel noise is random and the channel is expanded n' times without a memory condition [6].

The sample space for input X is $x = \{0,1\}$, and the sample space for output response Y is $y = \{0,1\}$.

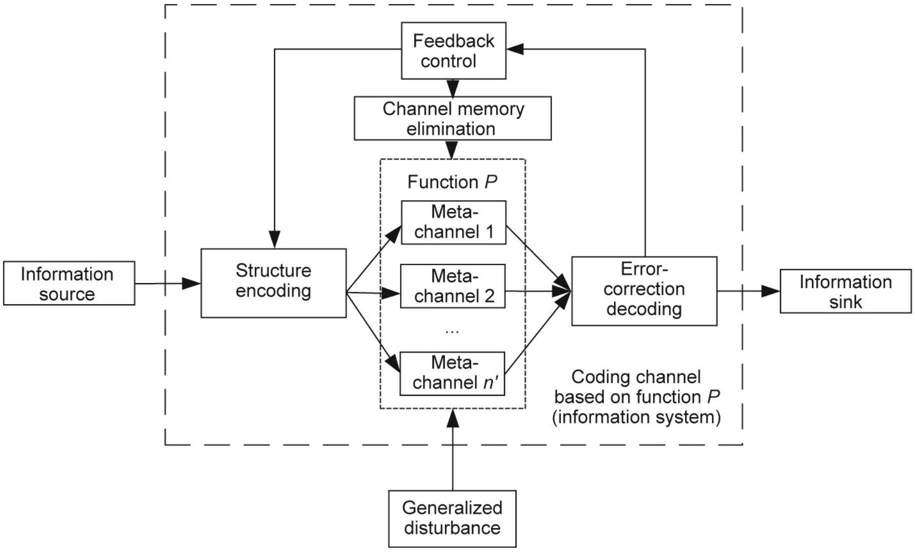

Fig. 3. The equivalent transmission channel model of DHR architecture. P: a function of a channel; n': the number of meta-channels, a similar meaning with n in Fig. 2.

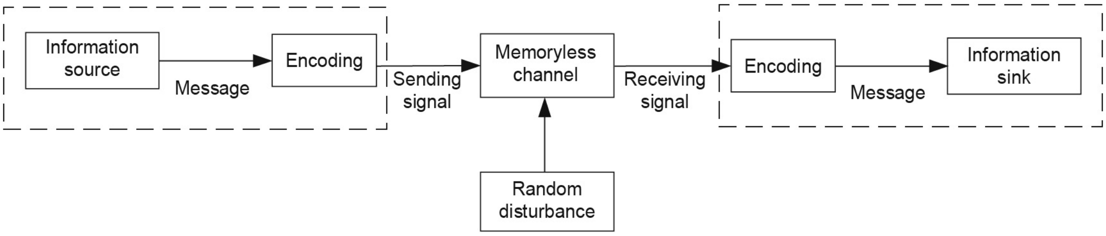

Fig. 4. The Shannon transmission channel model.

4.7.1. The first existence theorem of coding channel

Noise arrives randomly. If the coded information transmission rate R is less than C, where C is the channel capacity of discrete memoryless channel, and if the n' memoryless meta-channels in the coding channels are large enough, then $M = 2^{n'R}$ codewords can be found in the input set to form a code set (code length n'), where M is the total number of heterogeneous meta-channel combinations, the similar meaning with m in Fig. 1. The certain decoding rules can cause the channel output error probability to be $P_e \leq \varepsilon$, where ε is any small positive number.

Under the conditions of random noise and memoryless channels, the coding channel noise is random, and the constructed meta-channels are all memoryless channels. Shannon's second theorem requires the channel to perform memoryless expansion n' times. The noise of each extended channel is random, and all are memoryless channels. Therefore, the first existence theorem of the coding channel under the conditions of random noise memoryless channels and Shannon's second theorem satisfies the same conditions [4,5].

4.7.2. The second existence theorem of the coding channel

Noise (disturbance) arrives randomly, and the channel capacity of the discrete memory coded channel is C after the construction of DHR and feedback-elimination memory, $\forall t > 0, C(t) \in [C_s, C_0]$, where C_s is the channel capacity in steady state and C_0 is the channel capacity in initial state. If, at time t, the encoded information transmission rate $R(t) < C(t)$, then as long as the code length and the number of coded meta-channels n' are large enough, $M = 2^{n'R}$ codewords can always be found in the input set to form a code set, and ε is an arbitrary small positive number. Under certain decoding rules, the channel output error probability can be $P_e(t) \leq \varepsilon$.

5. Conclusions

Attack and defense theory and methods based on endogenous security issues are one of the most important and widespread cyberspace threats. Although endogenous security problems are unavoidable, such security threats can be avoided or defused through endogenous safety and security mechanisms (e.g., the cyber mimic defense is a successful application of this mechanism). An endogenous safety and security mechanism involves not only a change in the current ways of thinking about and concepts regarding cyberspace security defense, but also a leap forward in the development of security theories in IT, information communication technology (ICT), cyber-physical system (CPS), industrial control system (ICS), and other fields. The concept of an endogenous safety and security mechanism also expands new research directions in many disciplines.

This paper analyzes ideas and methods for solving endogenous security problems in cyberspace, proposes the concept and technical characteristics of endogenous security, and introduces the core ideas and generation process of DHR architecture. We believe that endogenous security in cyberspace will become an enabling technology for a new generation of software and hardware products, which will make it possible to manage the cyberspace security issues at the source of software and hardware products.

Acknowledgments

This work was supported by the National Natural Science Foundation Innovation Group Project (61521003).

References

[1] Wu J. [Introduction to cyberspace mimic defense]. Beijing: Science Press; 2017. Chinese.
[2] Wu J. [Principle of cyberspace mimic defense: endogenous safety–security & generalized robust control]. Beijing: Science Press; 2018. Chinese.
[3] Wu J. Cyberspace mimic defense: generalized robust control and endogenous safety–security. Berlin: Springer International Publishing; 2019.
[4] Wu J. [Endogenous safety and security in cyberspace: mimic defense and generalized robust control]. Beijing: Science Press; 2020. Chinese.
[5] Nie C, Zhao X, Chen K, Han Z. An Software vulnerability number prediction model based on micro-parameters. Comput Res Dev 2011;48(7):1279–87. Chinese.
[6] Shannon CE, Weaver W. The mathematical theory of communication. Urbana: University of Illinois Press; 1949.