Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9982351, 14 pages
https://doi.org/10.1155/2021/9982351

Research Article

Cognitive Covert Traffic Synthesis Method Based on Generative Adversarial Network

Zhangguo Tang,[1,2] **Junfeng Wang**,[1] **Huanzhou Li**,[2] **Jian Zhang**,[2] **and Junhao Wang**[2]

[1]*College of Cybersecurity, Sichuan University, Chengdu 610065, China*
[2]*School of Physics and Electronic Engineering, Sichuan Normal University, Chengdu 610101, China*

Correspondence should be addressed to Junfeng Wang; wangjf@scu.edu.cn

Received 21 March 2021; Accepted 27 May 2021; Published 10 June 2021

Academic Editor: Di Zhang

In the intelligent era of human-computer symbiosis, the use of machine learning method for covert communication confrontation has become a hot topic of network security. The existing covert communication technology focuses on the statistical abnormality of traffic behavior and does not consider the sensory abnormality of security censors, so it faces the core problem of lack of cognitive ability. In order to further improve the concealment of communication, a game method of "cognitive deception" is proposed, which is aimed at eliminating the anomaly of traffic in both behavioral and cognitive dimensions. Accordingly, a Wasserstein Generative Adversarial Network of Covert Channel (WCCGAN) model is established. The model uses the constraint sampling of cognitive priors to construct the constraint mechanism of "functional equivalence" and "cognitive equivalence" and is trained by a dynamic strategy updating learning algorithm. Among them, the generative module adopts joint expression learning which integrates network protocol knowledge to improve the expressiveness and discriminability of traffic cognitive features. The equivalent module guides the discriminant module to learn the pragmatic relevance features through the activity loss function of traffic and the application loss function of protocol for end-to-end training. The experimental results show that WCCGAN can directly synthesize traffic with comprehensive concealment ability, and its behavior concealment and cognitive deception are as high as 86.2% and 96.7%, respectively. Moreover, the model has good convergence and generalization ability and does not depend on specific assumptions and specific covert algorithms, which realizes a new paradigm of cognitive game in covert communication.

1. Introduction

In recent years, the use of traffic camouflage, channel invisibility, and other means of covert communication has become a hot spot of network countermeasures. Network covert communication refers to the violation of communication restriction rules in the network environment [1, 2], which makes some network resources in the network protocol that are not used for communication have the ability to transfer information [3], so as to avoid review and supervision. The existing network covert communication is based on the prisoner's dilemma model in narrow sense, and the related research can be divided into three aspects, namely, symbol design [4, 5], channel coding [6–8], and channel optimization [9]. These researches focus on the behavior concealment at the traffic level. In principle, it is the abnormal use of communication protocol; that is, the protocol behavior (semantic plane) does not match the application content (pragmatic plane). As a result, the covert channel not only has statistical abnormalities in the traffic behavior but also causes cognitive abnormalities in the sense of security censors. Therefore, it is difficult to resist the content-based protocol restoration review. With human being as an element added to the security detection model of human-computer symbiosis, the existing network covert communication shows the following disadvantages:

(1) At the model level, the traditional covert communication only focuses on the machine detection rules, without the cognitive modeling of human sensory abnormalities, which is difficult to resist the cognitive review of "human in the system." This is a blank in the model of covert communication

(2) At the algorithm level, the information carrying of traditional covert communication is the explicit intervention and modulation of symbols, so it is necessary to write a fixed covert algorithm, which leads to poor diversity of covert channel and weak antianalysis ability

(3) At the application level, traditional covert communication destroys the normal use of protocol, resulting in abnormal protocol resolution at the legitimate receiver. The anomaly is a principle anomaly, which is difficult to eliminate

In recent years, machine learning has made great progress, especially in the Generative Adversarial Network (GAN), which shows strong ability in image synthesis, traffic processing, content reconstruction, cross modal generation, and other fields [10–13]. By combining GAN with covert communication, it is possible to automatically generate new covert traffic and eliminate both behavioral and cognitive anomalies. Based on this, this paper focuses on the new paradigm of cognitive game in the context of human-computer symbiosis, brings cognitive elements into the traditional prisoner model, and proposes a new covert traffic generation model, which can automatically synthesize traffic with covert functional equivalence and protocol cognitive equivalence. The contributions of this paper are outlined as the following:

(1) The paper proposes a "cognitive deception" method, improves the narrow-sense prisoner model, establishes a cognitive game framework of covert confrontation, and realizes a new paradigm of covert communication game

(2) In this paper, a Wasserstein Generative Adversarial Network of Covert Channel (WCCGAN) model is proposed. By defining the activity loss function of traffic and the application loss function of protocol, the cognitive equivalent mechanism is established to effectively constrain the prediction space of the model, and the adaptive generation of covert traffic is realized

(3) This paper proposes a dynamic strategy updating learning algorithm. Dynamic batch size (DBS) and dynamic parameter update (DPU) are used to improve the utilization rate of traffic samples and the convergence performance of the model

(4) Through experiments, the paper verifies the existence and effectiveness of cognitive deception traffic. It provides a new way to explore the new concept of covert communication

The rest of this paper is organized as follows: Section 2 introduces the related work. In Section 3, the detailed principle and technical path of this method are introduced. Experimental evaluation is discussed in Section 4. Finally, Section 5 presents some conclusions and discusses future work.

2. Related Work

2.1. Covert Communication and Its Game Method. Covert communication can be divided into storage type and time type, which are usually based on first-order morphological parameters and second-order statistical characteristics [14–17]. The covert storage channel [18, 19] takes the object of the protocol as a symbol to transmit covert information, such as unused or reserved elements in data packets, data frames, and data segments. The covert timing channel [20] abstracts the time-domain statistical characteristics into symbols to transmit covert information, such as the interval time of protocol data units or protocol instructions [21] or the sequential coding of data packets [22]. Traditional covert communication mainly includes symbol design and channel mode design. The existing channel modes of covert communication mainly include technologies such as Microprotocol, Dynamic routing, Multiprotocol transmission, Statistical coding, Link frequency hopping, and other technologies [23]. Network symbol is not only the basic signal unit to carry the covert information but also the metapoint against the game between the two sides. Traditional covert symbols include network resource carriers, carrier features, and feature patterns. For the first-order parameter symbols based on physical form, there are mainly seven patterns, such as Size Modulation Pattern, Sequence Pattern, Add Redundancy Pattern, PDU Corruption/Loss Pattern, Random Value Pattern, Value Modulation Pattern, and Reserved/Unused Pattern [24, 25]. For the second-order statistical probability distribution symbols based on attribute regularity, there are mainly four patterns: Interarrival Time Pattern, Rate Pattern, PDU Order Pattern, and Retransmission Pattern [26].

The traditional game method of covert communication is machine-oriented rule deception or pattern deception [23], which is limited to the narrow-sense prisoner model. Constrained by the data space, the traditional covert communication algorithm is reduced to the conditional distribution of some kind or several kinds of data, so its symbol is first-order or second-order in mathematical sense. As shown in Table 1, different symbol vectors have different paradigms and abilities to express information. From the perspective of information theory, the degree of freedom of covert symbol vector to express information has multiscale, hierarchical, and structured attributes in cognitive space. Covert communication can carry out feature game, statistical game, pattern game, and even cognitive game in the three dimensions of grammar, semantics, and pragmatics. Traditional covert communication only focuses on the concealment of machine rules and only plays games on the grammatical and semantic levels. Due to the lack of consideration of the pragmatic information of traffic, there are cognitive defects. It is just like the physical disguise of a man disguised as a woman. There is no conversion in physiology, so there is a loophole in principle.

Table 1: Symbol vector and information modulation from the perspective of information hierarchy.

Information type	Covert carrier	Symbol vector	Information modulation mode
Syntax (feature class)	Packet	Specific protocol domain	Morphological parameters
Semantic (statistical)	Conversation group	Packet interval, packet sequence	Statistical rules
Pragmatic (pattern)	Data flow	Flow behavior, application	Pattern classification

Therefore, in essence, the traditional covert communication methods are the invasion, parasitization, and multiplexing of existing protocols and public channels. From the behavior point of view, the information expression is the explicit intervention and modulation of the code element. The code element has changed in essence, and there is a statistical offset, so it is inevitable to be accompanied by statistical traces. In terms of content, the protocol session has lost its normal application, which is manifested in that it cannot be opened by normal application (such as browser), or it cannot be decoded and restored by normal protocol analysis software, or the restored content cannot be read manually. For the machine, the symbol vector which can represent the problem space is used for training and reasoning, so the symbol feature space contains cognition. For human beings, whether the symbol is data, language, or application, its essence is cognition. Therefore, covert communication needs to expand from machine-oriented rule deception to human-computer symbiotic cognitive deception. High dimensional game based on cognitive symbol can eliminate the cognitive mismatch between semantic plane and pragmatic plane in principle, which is the key to improve concealment fundamentally.

2.2. GAN and Its Application in Traffic Processing. In recent years, Generative Adversarial Network (GAN) has shown strong ability in many application fields [27–30] and has also made a lot of achievements in the field of traffic transformation and traffic synthesis. GAN is a kind of generative model [31], which learns data distribution and synthesizes sample data from distribution. GAN maps the generative modeling to a game between two networks, namely, generator and discriminator. The generator is used to generate synthetic data of given noise variables, and the function of discriminator is to distinguish whether the sample data is real data. Generally, both generator and discriminator adopt feedforward neural network. Through game learning and closed-loop feedback regulation mechanism, the model itself is continuously optimized in the training process until they reach Nash equilibrium.

In the field of traffic transformation, Oh et al. [32] used GAN to transform traffic characteristics, which significantly improved the anonymity of traffic. McPherson [33] transformed one kind of traffic into another, embedded in the deep coupling of streaming media, and built an encryption tunnel to transfer sensitive information. Xu [34] used popular encrypted online services to transmit censored content and used YouTube live streaming to build covert channels. On this basis, Hu [35] further confused encrypted traffic by changing the statistical characteristics of traffic. Rigaki [10] focuses on white box malware and uses GAN to transform malicious traffic into normal traffic before communication, which leading the covert channel to adaptive malware and adaptive IPS. In 2019, Ring [13] proposed a new flow-GAN technology, whose core idea is to automatically extract the characteristics of the target network flow and then convert the source stream (or review flow) into the target flow (or allowed flow). It makes the generated flow indistinguishable from the target flow, so as to achieve the purpose of privacy protection and review avoidance. In addition, GAN is developing to a more dynamic adaptive flow camouflage direction by combining with other supervised learning methods [36–39].

In the field of traffic synthesis, it has been successful to generate adversarial traffic samples automatically by using known data patterns. Lin [11] used GAN to automatically build a variety of malicious attack traffic samples to enhance the robustness of security software. Chen [40] used GAN to generate malicious domain name data automatically. Yan et al. [12] used GAN to synthesize DoS attack automatically and disguised DoS network traffic as normal network traffic to defeat the existing NIDS system. In 2019, Pan et al. [41] proposed a new model based on the GAN, which realized the generation of adversary traffic samples directly using malicious network flows as the original samples. The generated adversary samples can not only effectively cheat black box IDS based on deep learning but also retain the activity and aggressiveness of malicious network traffic. Cheng et al. [42] proposed PAC-GAN, which is able to generate traffic that can be successfully transmitted through the internet to elicit desired responses from the network. Shahid et al. [43] combined auto-encoder with GAN to generate packet size sequence corresponding to bidirectional flow. The synthetic two-way flow is close enough to the real two-way flow to cheat the anomaly detector and mark it as legitimate.

The above research has solved the expression of the nonlinear complex relationship between channel traffic input and output, which has a certain reference significance for the synthesis of cognitive covert traffic. However, the existing research is to use GAN to modify malicious traffic features into normal traffic features. Although to a certain extent, it has achieved the concealment against machine statistical detection rules, there are some defects in the application level. That is, in terms of cognition, it is still the abnormal use of communication protocol, which leads to the mismatch between protocol behavior and application content. For example, the browser cannot open HTTP covert stream, the mail client cannot open SMTP or POP3 covert stream, and so on. This can trigger the security common sense alarm of the reviewers, which can not effectively resist the application-based cognitive review. Therefore, in the context of human-computer symbiosis, it is urgent to model the safety common sense and cognition of censors, so as to improve the nonlinear expression ability of GAN on cognitive characteristics.

3. Our Method

3.1. Cognitive Game Model of Covert Communication. Traditional covert communication in different computing environments is limited to the narrow-sense prisoner model [44–47]. By introducing cognitive elements in the context of human-computer symbiosis, this paper extends the narrow-sense prisoner model and establishes a generalized prisoner model of covert communication game. As shown in Figure 1, Alice and Bob communicate with each other using two networked computers. In order to confront Wendy's monitoring, limiting, and restoring of traffic, Alice and Bob embed covert channel in the overt channel which looks normal, and encode, decode, decrypt, or authenticate the covert information by sharing secret information. Covert communication depends not only on traffic behavior and statistical information but also on cognitive reasoning of high-level common sense knowledge. In order to enhance the intensity of concealment, "Wendy" is promoted to an agent with Turing significance, which has both data driven machine rules and common sense driven cognitive review. Therefore, concealment can be defined as a kind of information and its transmission mechanism with both rule deception and cognitive deception in a certain space-time range. The significance of cognitive game model based on generalized prisoner's dilemma lies in two aspects. One is that cognition is calculation. The cognitive level of human to the security world determines the way and intensity of covert confrontation. On the other hand, the symbol vector in cognitive space has high-order dynamic generalization, and the covert state space can not be closed due to dimension disaster, which makes the detection model of human-machine symbiosis, Wendy, decay or fail. The above two aspects fundamentally establish the paradigm and underlying logic of high-order game of covert communication.

3.2. WCCGAN Model. In order to generate cognitive covert traffic, this paper proposes a Wasserstein Generative Adversarial Network of Covert Channel (WCCGAN). The core of the model is to establish a cognitive equivalent mechanism. The cognitive loss function is defined from two dimensions of traffic behavior and protocol application to simulate human's common sense cognition of covert communication. Through the union expression learning of machine rules and covert cognition, the prediction space of the model is constrained, and the traffic with cognitive covert ability is generated automatically.

As shown in Figure 2, the WCCGAN model is divided into three modules: generation module, equivalent module, and discrimination module. The generation module trains a high-quality cognitive covert traffic generator, which takes the legitimate application traffic as prior knowledge to improve the expressiveness and discriminability of features. The equivalent module establishes constraint sampling from two dimensions of "functional equivalence" and "cognitive equivalence." Among them, the functional equivalent is a support vector machine (SVM) classifier for detecting covert channels, and the cognitive equivalent is a support vector machine (SVM) classifier for judging the validity of protocol application. The two equivalent devices extract the covert and cognitive features of traffic and give the discrimination results and label the extracted features and then guide the model to learn the pragmatics association features. Synthetic labels are used to train discriminator to approach the detection ability of equivalent module, that is, to identify whether the generated confrontational traffic samples have the ability of both behavior concealment and cognitive deception at the same time. In order to enhance the convergence and generalization ability of the model, the three modules are trained end-to-end through a dynamic strategy updating learning algorithm. WCCGAN can automatically generate new covert traffic which can meet both functional equivalence and cognitive equivalence without relying on specific assumptions and specific concealment algorithms.

3.2.1. Generation Module Integrating Prior Knowledge. The generation model takes the legitimate application traffic as prior knowledge, which is composed of the generator and its input vector set. According to the learned covert features and cognitive features, the model dynamically changes the ongoing conversation flow to generate confrontational covert traffic. In order to improve the ability to express cognitive features of legitimate applications, the model is no longer only based on random noise. Instead, the normal application traffic of the normal protocol is taken as a part of the input elements to guide the generation model to obtain more cognitive prior distribution during training, so as to improve the convergence speed of the model. Therefore, the loss function of the generation model is improved, and the normal flow is introduced to optimize the parameters of the generation model. The algorithm process of generating model is as follows:

Firstly, the normal traffic samples are extracted, converted, and normalized, and the expression of normal traffic and protocol application is vectorized.

Secondly, constrained sampling is performed based on reverse derivation. The mapping relationship between the driver noise and the category information of the generator is established. By defining a loss evaluation standard and updating strategy, the cost loss of feature information extraction is minimized by means of reverse derivation. The loss function is defined as shown in equation (1):

$$G\_\mathrm{Loss} = E_{M\sim(\mathrm{NF}),N} D(G(M, N)), \tag{1}$$

where NF is the normal flow of the input generator, N is the noise, D is the discriminator, and G is the generator. The normal flow NF and noise N are superimposed, and the adversary flow $G(M, N)$ is generated by the generator. $G(M, N)$ enters the discriminator for discriminating operation $D(G(M, N))$, and finally, the generator loss value G_Loss is obtained to optimize the generator parameters.

Then, the traffic with normal application information is taken as the constraint condition, and the constraint

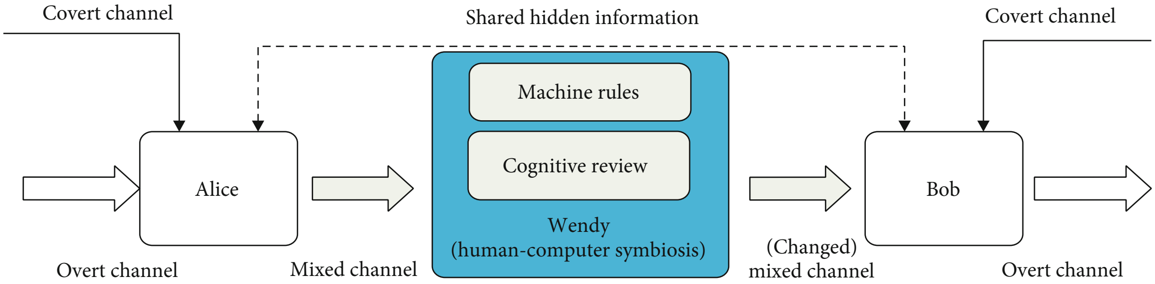

Figure 1: Cognitive game model of covert communication in the context of human-computer symbiosis.

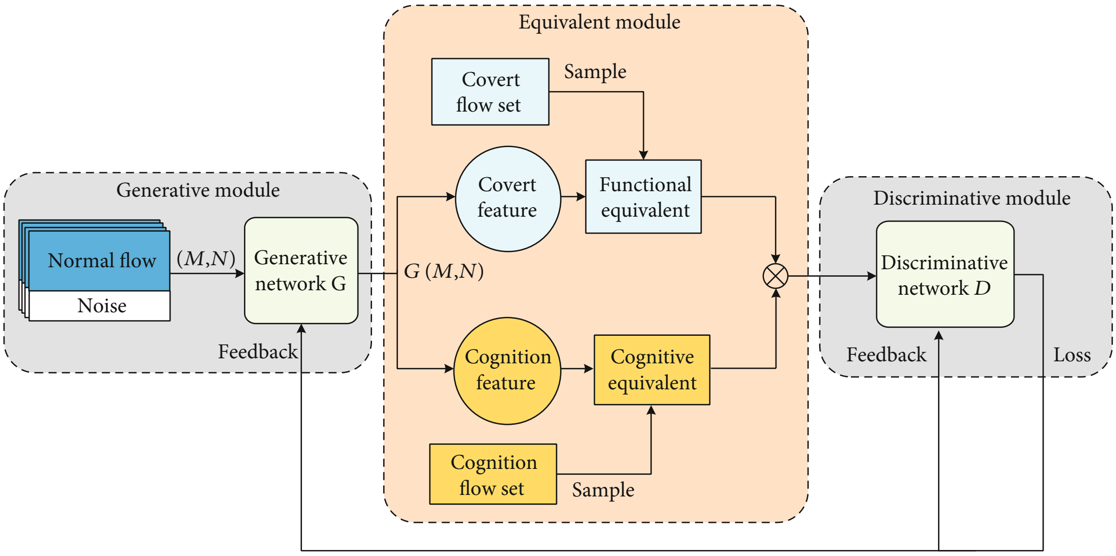

Figure 2: Framework of WCCGAN.

sampling is carried out by the training generator. The process of generating traffic not only realizes traffic activity but also realizes the embedding of cognitive prior information.

3.2.2. Equivalent Mechanism for Human Machine Symbiosis. In order to learn the covert ability of the channel and the cognitive ability of the legitimate application of the protocol at the same time, WCCGAN model constructs a specific equivalent mechanism. In the GAN game learning model, classifying and marking the output of the generator helps to improve the directional convergence ability of the model [48, 49]. Inspired by this, the equivalent model performs joint expression learning through the activity loss function of the flow and the application loss function of the protocol. Based on the covert and cognitive features of the generated traffic, the equivalent module is trained and two-classified labeled by two equivalent devices. Different from the traditional model, the goal of WCCGAN training is not to avoid the detection of equivalent. On the contrary, the detection rate of the two equivalents is used to judge the ability and effect of the generator to generate adversary covert traffic. The functional equivalent and cognitive equivalent are, respectively, composed of two classifiers based on support vector machine SVM. The working principle is shown in Figure 3.

The input of the functional equivalent is the covert channel data set, which is trained based on the covert feature vector to judge whether the generated traffic samples have covert ability. The cognitive equivalent works on the legitimate application traffic data set and is trained based on the cognitive feature vector to detect whether the generated traffic samples have the cognitive ability of legitimate application of normal protocol. The equivalent module plays the role of conditional constraint in the process of model training, and its Bayesian reasoning process based on conditional probability is shown in formula (2).

$$P(S \mid \mathrm{FE\&CE}) = P(S) \times \frac{P(\mathrm{FE\&CE} \mid S)}{P(\mathrm{FE\&CE})}. \tag{2}$$

In the formula, $\mathrm{P}(S \mid \mathrm{FE\&CE})$ represents the probability that the characteristics of generated traffic samples are the same as those of covert traffic and normal application traffic when both the covert characteristics of traffic and cognitive characteristics of protocol are satisfied. FE&CE is the characteristics of the original covert traffic and the normal application traffic, respectively, and $S$is the characteristics of the generated traffic samples. $P(S)$ is the prior probability, which depends on the initial weight of the equivalent module.

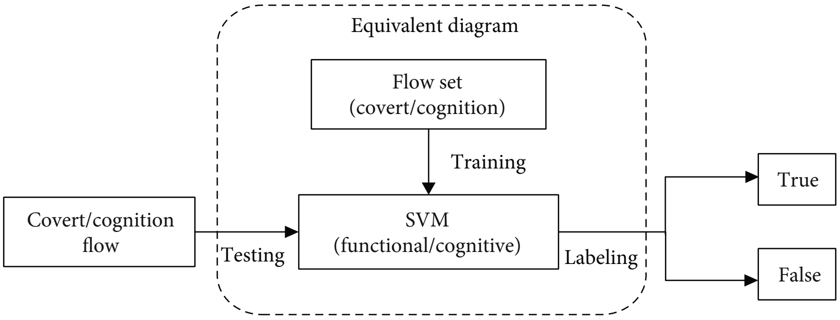

Figure 3: Working principle diagram of equivalent.

$P(\mathrm{FE\&CE} \mid S)$ is the probability of generating traffic samples with covert characteristics and normal application characteristics. By comparing $P(S \mid \mathrm{FE\&CE})$ with the threshold, the equivalent module network can label the generated traffic with a classification label and pass it to the discriminant module. The discriminant module optimizes its own parameters to learn and approach the classification ability of the equivalent module.

3.2.3. Discriminant Logic Coupling. Two equivalences provide knowledge for the training of discrimination module. The discriminant module is composed of discriminant network, which function is to discriminate the generated adversary traffic samples, covert traffic, and normal application traffic labeled by the equivalent module and calculate the loss value to feed back to the generator, so that the traffic generated by the generator can meet the classification requirements of functional equivalence and cognitive equivalence at the same time. The traditional WGAN model only calculates the Wasserstein distance between the real samples and the generated samples. In order to quantitatively express the constraint capability of WCCGAN equivalent module, an improved discriminator loss function is proposed, as shown in formula (3).

$$\begin{aligned} D\_\mathrm{loss} = \lambda E_{\overset{\Lambda}{x} \sim p \overset{\Lambda}{x}}\left[\left(\left\| \nabla \overset{\Lambda}{x} D\left(\overset{\Lambda}{x}\right)\right\| - 1\right)^{2}\right] \\ + E_{x\sim(\mathrm{FE\&CE})} D(x) - E_{x\sim(\mathrm{CF})} D(x), \end{aligned} \tag{3}$$

where CF is the sample of covert traffic data set. FE&CE is the generated traffic that satisfies both cognitive equivalence and functional equivalence, which is labeled as "True" by two equivalents. The discriminating module logically couples the labels given by the two equivalents and outputs the category information for the traffic of different label combinations. According to the classification result of the discriminator and the labeling result of the equivalent module, the deviation value of the generator is calculated. Furthermore, the gradient penalty (the first part of formula (3)) is used to update the generator parameters to improve the convergence rate and stability of the model.

3.3. Dynamic Strategy Updating Learning Algorithm. WGAN has a gradient penalty mechanism [49]. In order to improve the sparse problem of experimental samples and enhance the convergence and generalization of the model, this paper proposes a dynamic strategy updating learning algorithm. The algorithm combines dynamic batch size (DBS) and dynamic parameter update (DPU) to improve the model performance.

3.3.1. Improved DBS Method. There is a problem of sparse samples in the research of covert communication. One feasible way is to improve the availability and utilization of existing data samples. In traditional GAN training, every time the generator generates a sample, the discriminator discriminates it and obtains a corresponding loss value according to the loss function [50]. WCCGAN model is no longer fixed batch size value but uses an improved DBS method for model training, as shown in formulas (4) and (5).

$$\mathrm{WD} = D\_\mathrm{Real\_loss} - D\_\mathrm{Fake\_loss}, \tag{4}$$

$$D_{\mathrm{WD}} = \frac{|\mathrm{WD}_N - \mathrm{WD}_P|}{|\mathrm{WD}_P|}. \tag{5}$$

In the formula, WD_P and WD_N are the Wasserstein distance of the last training and the Wasserstein distance of the current training, respectively. D_Re al_loss and D_Fake_loss are the loss value of the discriminator. D_{WD} is the Wasserstein distance change rate, and λ is the update threshold set by DBS. When $D_{\mathrm{WD}} < \lambda$, try to increase the batch size value to 2^{n+1} in the next training. After increasing the batch size to 2^{n+1}, if $D_{\mathrm{WD}} > \lambda$ at the end of training, the batch size value will be retained. If $D_{\mathrm{WD}} < \lambda$ at the end of training, the batch size value will be reduced to 2^{n-1} or increased to 2^{n+2}. At this time, the larger value of D_{WD} is selected, and the corresponding batch size value is retained for the next training.

3.3.2. Improved DPU Method. Equivalent mechanism brings delay and technical complexity to model training. The traditional training method adopts the updating strategy with fixed parameters, which will affect the convergence of the model [51]. For example, the generator parameter update is performed every five discriminator parameter updates. In order to solve the influence of adding equivalent mechanism on the convergence performance of the model, WCCGAN adopts an improved DPU method to train, as shown in formulas (6)–(9).

$$C_g = \log^{L_g^N} - \log^{L_g^P}, \tag{6}$$

```
• parameters: learning rate ($\alpha$) =0.01; alpha($\gamma$) =0.99; batch size ($m$); change threshold($\lambda$) =1.5;
• require: generator parameters ($\theta_g$); discriminator parameters ($\theta_d$); generator loss change rate ($C_g$); discriminator loss change rate($C_d$); Wasserstein Distance change rate($D_{WD}$); Wasserstein Distance($WD$); Functional Equivalent(FE); Cognitive Equivalent(CE);
while $\theta_g$ has not converged do
For I = 1,…,m Do
Covert traffic data $x \sim CF$
Noise sample $z \sim U(z)$ ; Interpolation sampling of samples $x \longleftarrow G(\theta_g(z+x))$
$L = E_{\tilde{x}\sim(FE\&CE)}D(x) - E_{x\sim(CF)}D(x) + E_{\hat{x}\sim p(\hat{x})}[(\|\nabla x D(x)\| - 1)]^2$
$WD = D(\theta_d(\tilde{x})) - D(\theta_d(x))$
If $C_g > C_d$ Then // dynamic parameter update strategies
    $\theta_d = \alpha \cdot$ RMSProp $(\gamma, \Delta\theta_d)$
Else
    $\theta_g = \alpha \cdot$ RMSProp $(\gamma, \Delta\theta_g)$
end
If $D_{WD} < \lambda$
    $m_1 = m \cdot 2$
Else if $D_{WD1} < \lambda$ Then
    $m_2 = m \cdot 2^{-1}$
Else if $D_{WD2} < \lambda$ Then
    Flag $= D_{WD2} - D_{WD1}$
End for
If Flag $\geq 0$
    $m = m_2$
Else $m = m_1$
End while
```

Algorithm 1: WCCGAN, our proposed algorithm.

Table 2: Feature vector table of covert DOH data set.

Parameter	Feature	Parameter	Feature
F1	Number of flow bytes sent	F15	Mode packet time
F2	Rate of flow bytes sent	F16	Variance of packet time
F3	Number of flow bytes received	F17	Standard deviation of packet time
F4	Rate of flow bytes received	F18	Coefficient of variation of packet time
F5	Mean packet length	F19	Skew from median packet time
F6	Median packet length	F20	Skew from mode packet time
F7	Mode packet length	F21	Mean request/response time difference
F8	Variance of packet length	F22	Median request/response time difference
F9	Standard deviation of packet length	F23	Mode request/response time difference
F10	Coefficient of variation of packet length	F24	Variance of request/response time difference
F11	Skew from median packet length	F25	Standard deviation of request/response time difference
F12	Skew from mode packet length	F26	Coefficient of variation of request/response time difference
F13	Mean packet time	F27	Skew from median request/response time difference
F14	Median packet time	F28	Skew from mode request/response time difference

$$C_d = \log^{L_d^N} - \log^{L_d^P}, \tag{7}$$

$$\theta_g^N = \theta_g^P + \alpha \cdot RMSProp(\triangle\theta_g), \tag{8}$$

$$\theta_d^N = \theta_d^P + \alpha \cdot RMSProp(\triangle\theta_d). \tag{9}$$

In the formula, C_g and C_d represent the loss change rate of generator and discriminator, respectively. L_g^P and L_d^P represent the generator loss and discriminator loss of the previous iteration, respectively. L_g^N and L_d^N represent the generator loss and discriminator loss of the current iteration, respectively. θ_g^N and θ_d^N represent the generator network parameters and discriminator network parameters of the current iteration, respectively. $\Delta\theta_d$ and $\Delta\theta_g$ represent the variable discriminator parameters and the variable generator parameters, respectively. And, α is the learning rate. When $C_d > C_g$, the change rate of the loss value of the discriminator function is bigger; the RMSProp optimizer should be used to update the parameters of the generator, while the parameters of the discriminator network remain unchanged; when $C_d < C_g$,

Table 3: Feature vector table of cognitive feature data set.

Parameter	Feature	Parameter	Feature	Parameter	Feature
F1	protocol_type	F13	num_file_creations	F25	diff_srv_rate
F2	Service	F14	num_access_files	F26	srv_diff_host_rate
F3	Flag	F15	num_outbound_cmds	F27	idst_host_count
F4	Land	F16	is_hot_login	F28	dst_host_srv_count
F5	wrong_fragment	F17	is_guest_login	F29	dst_host_same_srv_rate
F6	Urgent	F18	Count	F30	dst_host_diff_srv_rate
F7	Hot	F19	srv_count	F31	dst_host_same_src_port_rate
F8	num_failed_logins	F20	serror_rate	F32	dst_host_srv_diff_host_rate
F9	logged_in	F21	srv_serror_rate	F33	dst_host_serror_rate
F10	num_compromised	F22	rerror_rate	F34	dst_host_srv_serror_rate
F11	root_shell	F23	srv_rerror_rate	F35	dst_host_rerror_rate
F12	dst_host_rerror_rate	F24	same_srv_rate	F36	dst_host_srv_rerror_rate

that is, the change rate of the loss value of the generator g function is bigger, the parameters of the discriminator should be updated, while the parameters of the generator network remain unchanged.

WCCGAN integrates the improved DBS method and DPU method and proposes a dynamic strategy updating learning algorithm as follows.

4. Experimental Evaluation

This section first briefly introduces the two databases in the field of network traffic and the method of merging the two databases. Then, the metrics used in the paper are defined. Based on these measures, the experimental results are given, and the performance of cognitive equivalence mechanism and WCCGAN model under different parameters is evaluated and compared with the related methods.

4.1. Experimental Data Set and Computer Environment. In order to solve the problem of sparse sample of covert traffic data set and the difference distribution between the covert features of traffic and protocol cognitive features, this paper integrates covert traffic data set and intrusion detection data set. The data set CIRA-CIC-DoHBrw-2020 comes from the Canadian Cyber Security Institute (CIC) project funded by the Canadian Internet Registration Authority (CIRA). The data set uses two methods: DOH protocol browser and DNS tunnel tool to capture DOH traffic and non-DOH traffic [52]. The data set gives rich time series characteristics and related statistical characteristics of network traffic, which can be used to simulate and test covert traffic, normal application traffic, and other attack traffic.

In the aspect of covert channel functional equivalence, CIRA-CIC-DoHBrw-2020 DOH data set and kdd-cup99 data set are used as the experimental samples of covert ability equivalence. The two types of data sets provide time interval characteristics, stream byte rate characteristics, retransmission mode characteristics, and regular statistical characteristics, as shown in Table 2.

In the cognitive equivalent level of legitimate protocol application, the non-DOH data set in CIRA-CIC-DoHBrw-2020 is used as the experimental sample of normal protocol cognitive ability. The data set contains a variety of protocol applications and supports the analysis of legitimate protocol application from the aspects of protocol usage characteristics, channel traffic characteristics, payload capacity characteristics, and protocol application characteristics, as shown in Table 3.

In the experimental scheme, 20000 malicious DOH data samples and 20000 non-DOH data samples are used to reduce the impact of imbalanced data sets on training. The training set consists of 10000 malicious DOH data samples and 10000 non-DOH data samples, and the test set consists of 10000 malicious DOH data samples and 10000 non-DOH data samples. The above improvements are used to verify the generalization ability of the model training and the multidimensional comparative evaluation experiments of other performance parameters.

WCCGAN model and code are written based on Pytorch, version 1.2.0. Pytorch provides a deep neural network for tensor calculation and automatic derivation system with powerful GPU acceleration capability. The related experiments are carried out on Windows 10 system, which is configured with 4-core 2.50 GHz CPU and 16 G memory.

4.2. Evaluation Metrics. Based on the widely used measurement methods, this paper evaluates the quality of WCCGAN generated traffic and the performance of the model itself and compares the quantitative performance of different methods.

In order to evaluate the effectiveness of the equivalent mechanism, the definition of detection rate is given, as shown in formula (10) and formula (11).

$$\mathrm{FDR} = \left(\frac{\mathrm{NDFT}}{\mathrm{NIT}}\right) \times 100\%, \tag{10}$$

$$\mathrm{CDR} = \left(\frac{\mathrm{NDCT}}{\mathrm{NIT}}\right) \times 100\%. \tag{11}$$

In the formula, NIT refers to the total number of input traffic; NDFT and NDCT, respectively, indicate the number of traffic with concealment ability and cognitive ability detected in the input traffic. The function equivalent detection rate (FDR) is used to evaluate whether the generated traffic has the function of covert communication. The higher the value is, the better the covert attribute is. Cognitive equivalent detection rate (CDR) is used to evaluate whether the generated traffic has cognitive characteristics. The higher the value is, the better the validity of the corresponding protocol is.

Furthermore, in order to evaluate the indistinguishability between WCCGAN generated flow and real flow from the flow level, in addition to Clustering Visualization on the distribution of feature space, two quantitative indicators, true positive rate (TPR) and false positive rate (FPR), are also used. TPR is the ratio of all samples that are actually normal flow, which is correctly judged as normal flow, as shown in formula (12). FPR represents the ratio of all actual counter flow samples that are wrongly judged as normal flow, as shown in formula (13).

$$\mathrm{TPR} = \frac{\mathrm{TP}}{(\mathrm{TP}+\mathrm{FN})}, \tag{12}$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{(\mathrm{FP}+\mathrm{TN})}. \tag{13}$$

In order to evaluate the influence of dynamic parameter updating algorithm and equivalent mechanism on the convergence rate of WCCGAN model, the cross entropy between generated traffic and dataset traffic samples is defined, and its value reflects the quality and degree of model convergence, as shown in equation (14).

$$H(p, q) = -\sum p(x) \ln q(x). \tag{14}$$

4.3. Quality Evaluation of Generated Traffic

4.3.1. Distribution of Generated Traffic in Feature Space. In order to intuitively display the distribution of various types of traffic in the covert feature space and cognitive feature space, t-SNE (t-Distributed stochastic Neighbor Embedding) algorithm is used for visualization. The covert DOH traffic and normal traffic in CIRA-CIC-DoHBrw-2020 and kddcup99 data sets are visualized in two dimensions, and its t-SNE distribution is shown in Figure 4. Among them, yellow and orange represent the functional and cognitive distribution of normal traffic, respectively, while purple and blue represent the functional and cognitive distribution of covert DOH traffic, respectively. It can be seen that the two types of traffic are far away in the distribution area of functional equivalence and cognitive equivalence, and the degree of aggregation is low, so they are easy to be separated and classified.

Furthermore, the adversary traffic generated by WCCGAN, normal traffic, and covert DOH traffic are visualized by t-SNE in the same coordinate system, as shown in Figure 5. Among them, yellow and pink represent the functional and cognitive characteristics of normal flow, respectively. Purple and blue represent the functional and cognitive characteristics of hidden DOH traffic, respectively.

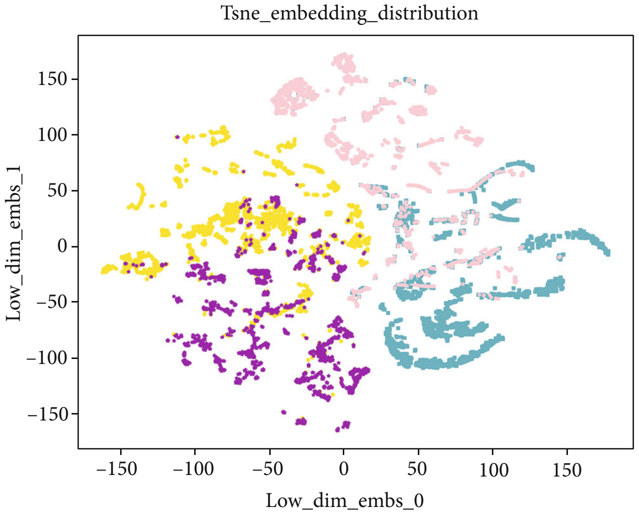

FIGURE 4: Characteristic distribution of traffic samples in original experimental data set.

Red and green refer to the functional characteristics and cognitive characteristics of generating confrontation samples, respectively. It can be seen from Figure 5 that in terms of functional equivalent feature distribution, the distribution of generated adversary traffic samples and covert DOH traffic are almost in the same area, with a high degree of coincidence, but far away from the distribution of normal traffic; in terms of cognitive equivalent feature distribution, the distribution of generated adversary traffic samples and normal traffic is almost in the same area, with a good degree of coincidence, but more distant from the distribution of covert DOH traffic.

As can be seen from Figures 4 and 5, WCCGAN model can indeed generate a new type of traffic with both concealment ability and cognitive deception ability. It shows that Gaussian mixture prior can help the model learn the implicit variable space more clearly, and the fuzzy regions shared by different types of samples are less. It should be noted that the generated adversary traffic is not based on the simple transformation of the traditional covert traffic in the behavior level nor is it the functional transformation of the traditional covert traffic, but a new covert traffic with cognitive deception function is synthesized from scratch.

4.4. Influence of Equivalent Mechanism on the Function of Generated Traffic. In order to evaluate the effects of functional equivalence and cognitive equivalence and their effects on the model, the validity of the equivalence mechanism was observed by dynamically adjusting the two equivalents. With or without the functional equivalent and cognitive equivalent, four groups of adversary traffic samples were obtained, and the covert ability and cognitive deception ability of the four groups of adversary traffic samples were tested.

As shown in Table 4, in the columns of "functional equivalent" and "cognitive equivalent," "×" indicates that the corresponding module has not been started in this line of test, and "√" indicates that the corresponding module has been started. It can be seen that the covert and cognitive detection

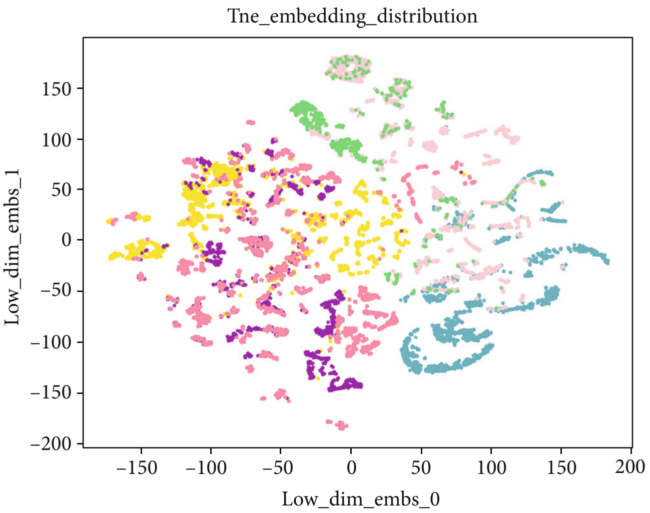

Figure 5: Characteristic distribution of generative adversary traffic samples.

Table 4: Effectiveness test of equivalent mechanism.

Functional equivalence	Cognitive equivalence	Performance	Detection rate (%)
×	×	FDR	70.5
		CDR	13.4
√	×	FDR	87.0
		CDR	15.4
×	√	FDR	22.3
		CDR	97.2
√	√	FDR	86.2
		CDR	96.7

rates of generated adversary traffic are low without adding functional equivalent and cognitive equivalent, which indicates that the covert ability and cognitive deception ability are poor. After adding functional equivalent and cognitive equivalent, respectively, the detection rate of corresponding ability was improved. By using two equivalent modules at the same time, the generated adversary traffic samples maintain both high covert detection rate and cognitive detection rate.

These four groups of comparative experiments show that there is a high correlation between the ability of concealment and cognitive ability of generating adversary traffic. By introducing the equivalent mechanism, WCCGAN implements an effective supervised learning, which enables the generation of adversary traffic to have the ability of concealment and cognitive deception at the same time, thus verifying the effectiveness of the new paradigm of covert traffic synthesis.

4.4.1. Indistinguishability Test of Generated Traffic. According to the ratio of 1 : 1, the generated flow and normal flow are mixed into a group of flow, and the generated flow and hidden DOH flow are mixed into another group of flow. In the experiment, the mixed traffic is detected and classified, and the classification results are used as the calculation data of receiver operating characteristic (ROC) model. ROC curve is a two-dimensional coordinate drawn by TPR and FPR. Area under the curve (AUC) is defined as the area surrounded by the lower part of the ROC curve, and its value is between 0 and 1, indicating the differentiation of flow. For the “random guess” classifier, the AUC value should be close to 0.5.

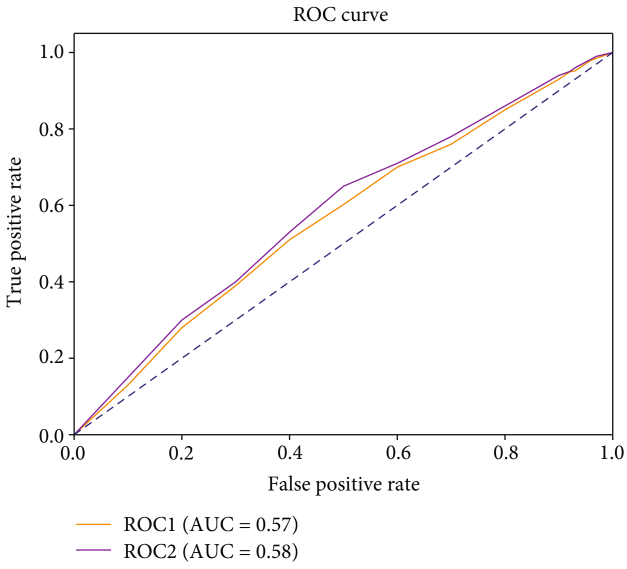

Figure 6: Indistinguishability of generated traffic.

The curve ROC1 and ROC2 are obtained through the experiment of two groups of mixed flow, respectively, and the results are shown in Figure 6. AUC of ROC1 is 0.57, which indicates that WCCGAN model can generate traffic which is difficult to distinguish from normal traffic in cognitive ability. AUC of ROC2 is 0.58, which indicates that WCCGAN model can generate traffic which is difficult to distinguish from covert DoH traffic. Therefore, this experiment further shows that the traffic generated by WCCGAN is indistinguishable from the target traffic, which effectively eliminates the behavioral and cognitive abnormalities of

Table 5: Effect of various batch sizes on model performance.

BS\EM	64		128		256		DBS ($\lambda = 1.0$)		DBS ($\lambda = 1.5$)		DBS ($\lambda = 2.0$)	
Epochs	WD	MMD	WD	MMD	WD	MMD	WD	MMD	WD	MMD	WD	MMD
50	68.8	0.432	48.1	0.124	47.9	0.113	76.8	0.445	48.5	0.123	70.3	0.543
100	69.2	0.437	50.4	0.137	46.6	0.132	65.3	0.512	43.2	0.142	78.5	0.452
150	76.7	0.446	57.2	0.147	52.9	0.149	63.2	0.456	42.5	0.119	73.2	0.342
200	78.4	0.449	53.2	0.136	54.7	0.158	59.6	0.467	42.7	0.245	71.3	0.326

Table 6: Performance comparison of models with different update strategies.

Time	50		100		150		200	
Module	FID	NRDS	FID	NRDS	FID	NRDS	FID	NRDS
WGAN ($n_d = 3n_g = 1$)	156.274	0.20	126.257	0.21	90.257	0.21	78.997	0.21
WGAN ($n_d = 5n_g = 1$)	134.765	0.23	105.725	0.21	80.789	0.22	65.645	0.21
WGAN ($n_d = 10n_g = 1$)	170.832	0.22	157.987	0.24	134.413	0.25	115.879	0.22
WCCGAN (DPU)	81.924	0.35	67.567	0.34	57.876	0.32	44.112	0.36

covert traffic and achieves the purpose of privacy protection and review evasion.

4.5. Performance of WCCGAN Model

4.5.1. DBS Performance Evaluation. In order to test the effect of dynamic batch size (DBS) on the performance of WCCGAN model, four experiments with different batch size values and different λvalues were carried out with training times of 50, 100, 150, and 200. Wasserstein Distance (WD) and Maximum Mean Diversity (MMD) were used to evaluate the performance. The smaller the values of WD and MMD, the better the performance of the model. The experimental results are shown in Table 5.

In Table 5, when the batch size increases gradually, the values of WD and MMD generally show a downward trend. When the batch size value is 256 and the number of training is 150, the MMD value becomes larger. When the batch size value is 256 and the number of training is 200, the WD and MMD values become larger. Thus, it can be seen that the value of batch size does not mean that the larger the model is, the better the effect will be. An optimal batch size for model training is not fixed. In addition, different λvalues have different effects on DBS. In the test, when the value of λ is 1.5, the convergence effect of WCCGAN model is the best. Therefore, the improved DBS method in this paper shows better convergence than the fixed batch size method.

4.5.2. DPU Performance Evaluation. In order to evaluate the impact of Dynamic Parameter Update (DPU) on the WCCGAN model, a comparison was made with the traditional WGAN on the premise of keeping the network structure and initial parameters consistent. It is very important to set the number of updates between the discriminator and the generator. If the number of updates is too large or too small, it will directly affect the gradient and then affect the convergence of the model. In order to reduce the randomness of parameter setting in the comparative experiment, four groups of control experiments were designed according to the general experience. In addition, the dynamic parameter update strategy used by WCCGAN is evaluated in two different ways: FID (French awareness distance) and NRDS (normalized relative differential score). The total number of training is 200, and the experimental results are shown in Table 6.

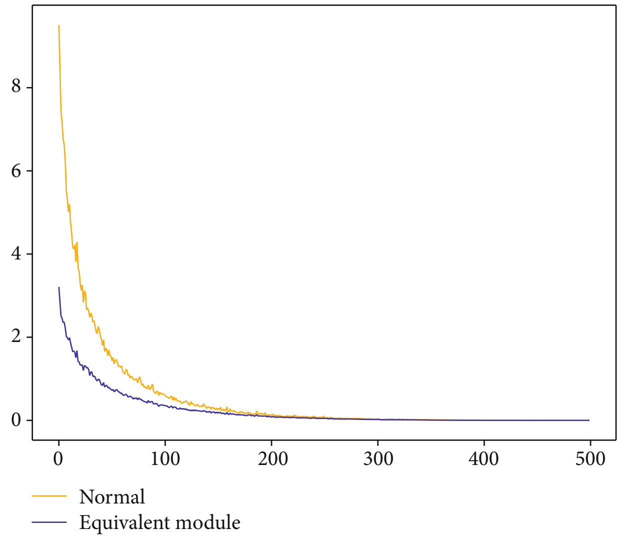

Figure 7: Comparison of the convergence ability with the related models.

n_d and n_g represent the fixed number of update steps of discriminator and generator, respectively. The smaller the value of FID, the better the performance of the model, while the opposite is true for NRDS. As can be seen from Table 6, compared with the first three WGAN using fixed update strategy, WCCGAN using DPU strategy has smaller FID value and larger NRDS value after the same number of training. It shows that DPU dynamically adjusts the parameter update step value in the process of training, so that the model training can achieve better results.

4.5.3. Convergence Ability. In order to verify the influence of the equivalent module on the convergence rate of WCCGAN model, the equivalent module is removed and retained, respectively, for experiments with other structures and parameters unchanged, and the difference of training time required to achieve the same sample quality is compared. The quality and degree of convergence of the model are evaluated by calculating the cross entropy between the counter flow samples and the data set samples. The training times are taken as the abscissa and the cross entropy as the ordinate. The results are shown in Figure 7.

In the figure, the equivalent module curve is the network model with equivalent module, and the normal curve is the network model without equivalent module. Compared with the two curves, it can be seen that after adding the equivalent module, the number of training times required to achieve the same training effect is reduced, and the convergence ability of the model is stronger. In addition, after adding the equivalent module, the cross entropy of the same data sample size is reduced compared with that without the equivalent module, which shows that the utilization rate of experimental samples is improved, and the sparse problem of experimental samples is improved. The possible reason is that WCCGAN model introduces normal traffic as cognitive prior knowledge and establishes an equivalent constraint mechanism, which plays an effective role in dimensionality reduction and model training.

5. Conclusions and Future Work

In this paper, cognitive deception is introduced into the game research of covert communication, and a new framework of covert communication, WCCGAN model, is proposed, and the effectiveness of related technologies is verified. Relevant experiments show that the equivalent mechanism and dynamic strategy updating algorithm can effectively constrain the training of the model, and the generated traffic can satisfy both behavioral concealment and cognitive concealment, which improves the concealment of communication traffic in principle. The next work will further improve the performance of the model, optimize the equivalent mechanism, and apply it to the adaptive synthesis of more types of traffic.

Data Availability

The data set CIRA-CIC-DoHBrw-2020 comes from the Canadian Cyber Security Institute (CIC) project funded by the Canadian Internet Registration Authority (CIRA).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

The first author, Zhangguo Tang, and the corresponding author, Junfeng Wang, were responsible for the overall work, proposed the idea and experiments of the method in the paper, and the paper was written mainly by the two authors. The third author, Huanzhou Li, performed part of the experiments and contributed to many effective discussions in both the ideas and paper writing. The fourth author, Jian Zhang, provided many positive suggestions and comments for the paper. The fifth author, Junhao Wang, performed part of the experiments and gave many good suggestions.

Acknowledgments

This work was supported by the National Key Research and Development Program (2018YFB0804503, 2019QY1400), the National Natural Science Foundation of China (U20A20161, U1836103), the Basic Research Program of China (2019-JCJQ-ZD-113), and the key research and development task of Sichuan science and technology planning project (2020YFS0364).

References

[1] P. Nowakowski, P. Zórawski, K. Cabaj, and W. Mazurczyk, "Network covert channels detection using data mining and hierarchical organisation of frequent sets: an initial study," in *Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event Ireland*, pp. 1–10, Ireland, 2020.

[2] P. Sarosh, S. A. Parah, and G. M. Bhat, "Utilization of secret sharing technology for secure communication: a state-of-the-art review," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 517–541, 2021.

[3] F. Iglesias, R. Annessi, and T. Zseby, "DAT detectors: uncovering TCP/IP covert channels by descriptive analytics," *Security and Communication Networks*, vol. 9, no. 15, 3029 pages, 2016.

[4] J. Keller and S. Wendzel, "Reversible and plausibly deniable covert channels in one-time passwords based on hash chains," *Applied Sciences*, vol. 11, no. 2, p. 731, 2021.

[5] Q. Zhang, H. Gong, X. Zhang, C. Liang, and Y. A. Tan, "A sensitive network jitter measurement for covert timing channels over interactive traffic," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3493–3509, 2019.

[6] E. R. L. Castro, R. G. Cardenas, and M. C. Euan, "Design of a steganographic system for hiding information in TCP/IP packets[J]," *International Advanced Research Journal in Science, Engineering and Technology. 2018. ISO 3297:2007 Certified*, vol. 5, no. 6, 2018.

[7] V. Sabeti and M. Shoaei, "New high secure network steganography method based on packet length[J]," *ISeCure*, vol. 12, no. 1, 2020.

[8] R. Zhang, N. Ye, S. Mao, L. Peng, and B. Zhang, *Channel Coding Information Hiding Technology Based on Spacecraft Application[M]//Signal and Information Processing*, Networking and Computers, Springer, Singapore, 2021.

[9] F. Iglesias, V. Bernhardt, R. Annessi, and T. Zseby, "Decision tree rule induction for detecting covert timing channels in TCP/IP traffic," in *International Cross-Domain Conference for Machine Learning and Knowledge Extraction*, pp. 105–122, Springer, Cham, 2017.

[10] M. Rigaki and S. Garcia, "Bringing a GAN to a knife-fight: adapting malware communication to avoid detection," in *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 70–75, San Francisco, CA, USA, 2018.

[11] Z. Lin, Y. Shi, and Z. Xue, "Idsgan: generative adversarial networks for attack generation against intrusion detection[J]," 2018, arXiv preprint arXiv: 1809.02077.

[12] Q. Yan, M. Wang, W. Huang, X. Luo, and F. R. Yu, "Automatically synthesizing DoS attack traces using generative adversarial networks," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 12, pp. 3387–3396, 2019.

[13] M. Ring, D. Schlör, D. Landes, and A. Hotho, "Flow-based network traffic generation using Generative Adversarial Networks," *Computers & Security*, vol. 82, pp. 156–172, 2019.

[14] J. Tian, G. Xiong, Z. Li, and G. Gou, "A survey of key technologies for constructing network covert channel," *Security and Communication Networks*, vol. 2020, Article ID 8892896, 20 pages, 2020.

[15] G. Asharov, G. Segev, and I. Shahaf, *Tight Tradeoffs in Searchable Symmetric Encryption[C]//Annual International Cryptology Conference*, Springer, Cham, 2018.

[16] M. Nasseralfoghara and H. Hamidi, "Web covert timing channels detection based on entropy," in *2019 5th International Conference on Web Research (ICWR)*, pp. 12–15, Tehran, Iran, 2019.

[17] A. Ameri and D. Johnson, "Covert channel over network time protocol," in *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy - ICCSP '17*, pp. 62–65, Wuhan, China, 2017.

[18] D. M. Dakhane and V. E. Narawade, "Reference model storage covert channel for secure communications[M]," in *Advanced Computing Technologies and Applications*, pp. 489–496, Springer, Singapore, 2020.

[19] L. Zhang, Z. Zhang, W. Wang et al., "A covert communication method using special bitcoin addresses generated by Vanitygen," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 597–616, 2020.

[20] S. Lu, Z. Chen, G. Fu, and Q. Li, "A novel timing-based network covert channel detection method," *Journal of Physics: Conference Series*, vol. 1325, no. 1, p. 12050, 2019.

[21] F. Shang, X. Li, D. Zhai, and Y. Qian, "On the distributed jamming system of covert timing channels in 5G networks," in *Jun 2020 in 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, pp. 1107–1111, Dalian, China, 2020.

[22] J. W. Ho, K. R. Won, and J. S. Kim, "POSTER," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery*, pp. 2499–2501, New York, NY, United States, 2017.

[23] Y. Sun, L. Zhang, and C. Zhao, "A study of network covert channel detection based on deep learning," in *2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC)*, pp. 637–641, Xi'an, China, 2018.

[24] A. Swinnen, R. Strackx, P. Philippaerts, and F. Piessens, "ProtoLeaks: A Reliable and Protocol-Independent Network Covert Channel," in *International Conference on Information Systems Security*, pp. 119–133, Springer, Berlin, Heidelberg, 2012.

[25] L. Zhang, T. Huang, X. Hu et al., "A distributed covert channel of the packet ordering enhancement model based on data compression," *Computers, Materials & Continua*, vol. 64, no. 3, pp. 2013–2030, 2020.

[26] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-based survey and categorization of network covert channel techniques," *ACM Computing Surveys*, vol. 47, no. 3, pp. 1–26, 2015.

[27] J. Li, H. Li, G. Cul, Y. Kang, Y. Hu, and Y. Zhou, "GACNet: a generative adversarial capsule network for regional epitaxial traffic flow prediction," *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 64, no. 2, pp. 925–940, 2020.

[28] F. Zhang, H. Zhao, W. Ying, Q. Liu, A. Noel Joseph Raj, and B. Fu, "Human face sketch to RGB image with edge optimization and generative adversarial networks," *Intelligent Automation and Soft Computing*, vol. 26, no. 4, pp. 1391–1401, 2020.

[29] Y. Wang, Y. Cao, L. Zhang et al., "YATA: yet another proposal for traffic analysis and anomaly detection," *Computers, Materials & Continua*, vol. 60, no. 3, pp. 1171–1187, 2019.

[30] M. Zhao, X. Liu, X. Yao, and K. He, "Better visual image super-resolution with Laplacian pyramid of generative adversarial networks," *Computers, Materials & Continua*, vol. 64, no. 3, pp. 1601–1614, 2020.

[31] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza et al., "Generative adversarial networks," 2014, arXiv preprint arXiv: 1406.2661.

[32] S. E. Oh, S. Sunkam, and N. Hopper, "Traffic analysis with deep learning," 2017, arXiv preprint arXiv: 1711.03656.

[33] R. McPherson, A. Houmansadr, and V. Shmatikov, "Covertcast: using live streaming to evade internet Censorship," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 3, pp. 212–225, 2016.

[34] W. Xu, Y. Qi, and D. Evans, "Automatically evading classifiers," *Proceedings of the 2016 network and distributed systems symposium*, vol. 10, 2016.

[35] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on GAN," 2017, arXiv preprint arXiv:1702.05983.

[36] P. Wang, X. Chen, and F. Ye, "A survey of techniques for mobile service encrypted traffic classification using deep learning," *IEEE Access*, vol. 7, pp. 54024–54033, 2019.

[37] S. Fathi-Kazerooni and R. Rojas-Cessa, "GAN tunnel: network traffic steganography by using GANs to counter internet traffic classifiers," *IEEE Access*, vol. 8, pp. 125345–125359, 2020.

[38] V. Rimmer, D. Preuveneers, M. Juarez, T. Van Goethem, and W. Joosen, "Automated website fingerprinting through deep learning," 2017, arXiv preprint arXiv:1708.06376.

[39] R. Overdorf, M. Juarez, G. Acar, R. Greenstadt, and C. Diaz, "How unique is your .onion?," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2021–2036, Dallas Texas USA, 2017.

[40] Y. Chen, Q. Liping, and Z. H. Z. Ting, "Generation of malicious domain training data based on generative adversarial net-work[J]," *Application Research of Computers*, vol. 36, no. 5, pp. 1540–1568, 2019.

[41] Y. M. Pan and J. Lin, "Generation and verification of malicious network flow based on generative adversarial networks[J]," *Journal of East China University of Science and Technology*, vol. 45, no. 2, pp. 344–350, 2019.

[42] A. Cheng, "PAC-GAN: packet generation of network traffic using generative adversarial networks," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0728–0734, Vancouver, BC, Canada, 2019.

[43] M. R. Shahid, G. Blanc, H. Jmila, Z. Zhang, and H. Debar, "Generative deep learning for Internet of Things network traffic generation," in *2020 IEEE 25th Pacific Rim International*

Symposium on Dependable Computing (PRDC), pp. 70–79, Perth, WA, Australia, 2020.

[44] Y. Zou, G. Zhang, and L. Liu, “Research on image steganography analysis based on deep learning,” *Journal of Visual Communication and Image Representation*, vol. 60, pp. 266–275, 2019.

[45] A. Nikoo, A. R. Kahoo, H. Hassanpour, and H. Saadatnia, “Using a time-frequency distribution to identify buried channels in reflection seismic data,” *Digital Signal Processing*, vol. 54, pp. 54–63, 2016.

[46] Z. Yang, Y. Hu, Y. Huang, and Y. Zhang, “Behavioral Security in Covert Communication Systems,” in *International Workshop on Digital Watermarking*, pp. 377–392, Springer, Cham, 2019.

[47] Y. Shen, “Research on network protocol covert channel detection and new construction scheme [Ph.D. Thesis],” China University of Science and Technology, Hefei, 2017, (in Chinese with English abstract).

[48] M. Mirza and S. Osindero, “Conditional generative adversarial nets[J],” 2014, arXiv preprint arXiv:1411.1784.

[49] I. Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin, and A. Courville, “Improved training of Wasserstein GANs[J],” 2017, arXiv preprint arXiv:1704.00028.

[50] G. Peyré and M. Cuturi, “Computational optimal transport: with applications to data science,” *Machine Learning*, vol. 11, no. 5-6, pp. 355–607, 2019.

[51] X. Ouyang, Y. Chen, and G. Agam, “Accelerated WGAN update strategy with loss change rate balancing[C],” in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pp. 2546–2555, Waikoloa, United States, 2021.

[52] M. Montazeri Shatoori, L. Davidson, G. Kaur, and A. H. Lashkari, “Detection of DoH tunnels using time-series classification of encrypted traffic [C],” in *2020 IEEE Intl Conf on dependable, autonomic and secure computing, Intl Conf on pervasive intelligence and computing, Intl Conf on cloud and big data computing, Intl Conf on cyber science and technology congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 63–70, 2020.