Network dynamic defense system based on holographic transformation

Jinglei Tan¹,², Cheng Lei¹,², Hongqi Zhang¹,², Hao Hu¹,² and Hengwei Zhang¹,²

Abstract
Aimed at the problem of the boundary defense easily being out of availability caused by the static network structure, a novel dynamic enterprise network defense system based on holographic transformation is designed and implemented. To increase the uncertainty of network structure and the position of target nodes, the network view is dynamically changed by constantly transforming endpoint information. Virtual endpoint mutation and hopping period selection are achieved by the hopping address generation module. It takes the advantages of anti-collision and good randomicity of the Chinese national SM3 hash algorithm. The full-cycle hopping period is managed and controlled by the hopping period management mechanism based on the ciphertext policy attribute-based broadcast holographic transformation. Experiments show that the system achieves expected security goals and has good interactivity and high stability.

Keywords
Defense without detection, whole network endpoint transformation, Chinese national SM3 hash algorithm, attribute-based access control, moving target defense, enterprise network security

Date received: 5 October 2019; accepted: 20 March 2020

Handling Editor: Mohammad Abdur Razzaque

Introduction
With the continuous development of network technology, enterprise network has become an increasingly important strategic infrastructure. Network applications are continuing to influence people’s lifestyles. The asymmetric security situation of cyberspace, “easy to attack but difficult to defend,” has become a severe challenge for network security defense.¹⁻⁴ The root cause of the asymmetry network security situation is the deterministic, static, and homogeneity compositions in the network.⁵ Aimed at the asymmetry of attackers and defenders caused by the certain network structure and the static defense mechanism, network dynamic defense (NDD) proposes a new defense concept.⁶ By actively changing the presentation mode of the protected nodes and the exposed attack surface, NDD increases the difficulty for the attacker.⁷,⁸ Therefore, network defense without detection is achieved by increasing the uncertainty of the network structure and the protected nodes. However, the difficulty of distributed network management in the traditional network architecture is a key bottleneck restricting the development of NDD. Software-defined network (SDN)⁹ provides a new idea for enterprise network security defense management.¹⁰ Since the control layer can abstract the distributed state of network devices into the global view, the customized application can configure the whole network node uniformly. Thus, centralized management and global view can effectively manage the transformation of the whole network nodes.

¹PLA SSF Information Engineering University, Zhengzhou, China
²The State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China

Corresponding author:
Hengwei Zhang, The State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
Email: wlby_zzmy_henan@163.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
Consequently, NDD based on SDN can dynamically modify hopping elements, hopping periods, and hopping rules, which can effectively improve the manageability of enterprise network transformation.11–13

The overall design of the NDD system

Existing SDN-based NDD methods14,15 mainly concentrate on the study of network address transformation method. However, in practical applications, the failure generation of hopping endpoint information often occurs caused by the conflict of hopping endpoint address generation and high implementation consumption of transformation update. Therefore, aimed at the problem of collision and inefficient distribution of address transformation, a novel NDD system based on holographic transformation is designed. It can solve the problems of active scanning, passive monitoring, and internal overstepping and abuse caused by defense invalidation. The system is based on the Chinese national hash algorithm called SM3 to achieve the random generation of endpoint hopping information. The attribute-based holographic transformation access control mechanism is used to implement full-cycle control of network hopping. Therefore, a dynamically transformed network view is constructed to achieve defense without detection by continuous transforming endpoint information of the entire network. The main functions of the system are as follows:

1. The system takes the defense without detection theory as the core, complexity, and cost of scanning attack are dramatically increased by virtual network holographic transformation.
2. Based on the attribute-based holographic transformation access control, the system achieves full-cycle hopping management and control, where the strength and effectiveness of the access behavior control of the hopping endpoint are enhanced.
3. Taking the SM3 hash algorithm as the core, the holographic transformation-based hopping information selection method ensures anti-collision and unpredictability features of generated hopping information.

Table 1 provides the notation used in our article.

Overall design of system architecture

The composition of the proposed system is shown in Figure 1. It consists of hopping endpoint address generation module based on the SM3 algorithm, holographic transformation-based hopping full-cycle management module, and integrated management and display platform. In terms of the collision problem in the process of hopping endpoint address selection, the SM3-based hopping endpoint address generation module implements an anti-collision random selection of hopping
endpoint address using the SM3 hash algorithm. Therefore, the unpredictability of endpoint hopping information is maximized while ensuring reliability. Aimed at the problem of information leakage and high-performance overhead in hopping parameter transmission, holographic transformation–based hopping full-cycle control module implements ciphertext access control by attribute-based holographic transformation algorithm. The integrated management and display platform provide a system management portal for administrators by means of visualization.

The NDD system deployment architecture is shown in Figure 2. It is a layered architecture based on SDN. The system consists of a hopping control center and SDN switches. As the core of the dynamic defense system, the hopping control center obtains the SDN switches and endpoint information through the SDN controller, thereby generating a global view of the network. At the same time, relying on the centralized control feature of SDN, the hopping control center generates hopping endpoint information by hopping endpoint address generation module and manages hopping endpoint address in full life cycle through hopping full-cycle management module. SDN switches interact with the hopping control center to collect and report the status of endpoints and networks. Besides, SDN switches implement network endpoint information hopping.

**Workflow of the hopping control center and defense system**

Since the hopping control center is the header of the proposed dynamic defense system, it plays a critical role in dynamic defense. The workflow of the hopping control center in the NDD system is shown in Figure 3. Furthermore, the workflow of the proposed dynamic defense system is shown in Figure 4. It implements dynamic defense based on the SDN architecture.

When a user attempts to access the network, the hopping full-cycle control module performs identity authentication according to the attribute information reported by the user. If the user is a malicious adversary, it is not registered, and the hopping full-cycle management module rejects the illegal access. However, if the malicious adversary uses an active scanning method to scan the whole network view, the protected SDN network deploys dynamic transformation using the SM3 hash algorithm–based hopping endpoint address generation module. Virtual network holographic transformation is implemented by a holographic transformation–based hopping full-cycle
management module. What’s more, in order to prevent transient problems during hopping, flow table consistency update policy is adopted. Since all endpoints of the target network are continuous, dynamically, and randomly transformed, it is difficult for the malicious adversary to successfully scan the real network structure. Besides, since the attribute-based holographic transformation algorithm is adopted to protect the confidentiality of hopping endpoint information pool and hopping period range during the transition, the
malicious adversary is unable to crack the information within the effective time. Consequently, the proposed defense system not only ensures the security of the hopping process but also improves the security of the protected network system.

### Key techniques in the proposed defensive system

#### Hopping endpoint address generation technique based on SM3 hash algorithm

Aimed at the collision problem in the process of hopping endpoint information generation, hopping endpoint address generation technique based on the SM3 hash algorithm\(^\text{17}\) is designed. SM3 is designed based on the SHA-256 cryptographic hash algorithm. It meets the security requirements of multiple cryptographic applications. SM3 is a kind of hash algorithm based on the group iterative structure. The algorithm adopts a kind of information process called a two-character combination method, which uses a mixture of different group operations so as to achieve fast diffusion and chaos in a local scope. It effectively prevents the security threats caused by bit tracking and other known cryptographic analysis methods. SM3 is used to generate random numbers in this module, and it has the following characteristics:

| Hopping control center | SDN switch | User endpoint | Targeted network server | Authentication server |
|------------------------|------------|---------------|-------------------------|-----------------------|
| Report user attribute information through `packet_in` | Parse the packet and verify that the user node is a registered user | Discharge flow table | The switch discards user session data according to the priority `P1` flow table. | The user accesses the target service node for the first time |
| Parse the packet and extract the user ID | The switch discards user session data according to the priority `P1` flow table. | Parse the data packet and extract the user ID | Legal user registration, attribute information is stored in the authentication server |

![Figure 4. Encrypted network dynamic defense system workflow chart.](image-url)
Property 1 (Unidirectional). Given hash value $h$ of message $m$, it is not feasible to calculate message $m$ according to $hash(m) = h$.

Property 2 (Anti-collision). Given hash algorithm $hash()$, it is infeasible in computation to find two different messages $m_1 \neq m_2$ making the hash value $hash(m_1) = hash(m_2)$.

Property 3 (Fixed-length output). Since there is no limit to the length of the input message, the length of the output string is fixed.

Since the properties of SM3 guarantee the availability in hopping endpoint information selection, hopping endpoint information generation algorithm based on SM3 avoids network address collision in the process of endpoint information generation under the premise of ensuring the unpredictability of the hopping endpoint information. Based on hopping endpoint information generation algorithm, hopping endpoint address generation module is designed. The attribute information of hopping endpoint is used to determine the hopping period ($THP$) and hopping information range ($AddrBlck$). And SM3 is used to generate hopping endpoint address ($vIP$) and endpoint hopping period ($THP$). Specifically, Algorithm 1 is shown as follows:

**Algorithm 1.** Hopping endpoint address generation algorithm based on SM3

**Input:** $AddrBlck$, $THPrange$, $Attri$, $Key_{SM3}$

**Output:** $vIP$, $THP$

1. Initialize parameter;
2. Obtain Attribute Information of endpoint;
3. Get identity symbol ID and security level $S_level$;
4. Get private key index $k$;
5. ($subAddrBlck$, $THP$) = $f(Attri, AddrBlck, THPrange)$;
6. If (Low-security level)
   7. Choose hopping period from low-level hopping period in $THPrange$;
   8. Else
   9. Choose hopping period from high-level hopping period in $THPrange$;
10. End If
11. Get hopping endpoint address sub-block $subAddrBlck$;
12. $h = hash_{SM3}(Attri, t)$;
13. If (Low-security level)
14. $addr_0 = addri \oplus h$;
15. $vIP = Prefix : addri$
16. Else
17. If ($h$ is odd)
18. $Prefix' = Prefix_i$;
19. $addr_0 = addri \oplus h$;
20. Else
21. $Prefix' = Prefix_{i+1}$;
22. $addr_0 = addri \oplus h$;
23. $vIP = Prefix : addri'$;
24. End If
25. If ($vIP = vIP'$)
26. Redo;
27. Else
28. Return ($vIP$, $THP$);
29. End If

**Hopping full-cycle control technique based on ciphertext policy attribute-based broadcast holographic transformation**

Aimed at the problems of forgery and replay attacks during the identity authentication process, hopping a full-cycle control technique guarantees the uniqueness of endpoint attribute information by the identity identifier. What's more, the timeliness of the attribute information is guaranteed by timestamp. Consequently, the ciphertext policy attribute-based broadcast holographic transformation (CP-ABE)-based hopping full-cycle control technique is proposed.

As shown in Figure 5, attribute holographic transformation is a kind of ciphertext access control mechanism, in which access control structure is embedded into ciphertext. Attribute holographic transformation can judge which users are able to decrypt the encrypted message without using a trusted server. Currently, there are two typical attribute holographic transformation methods: CP-ABE and key policy attribute-based broadcast holographic transformation (KP-ABE). The proposed defense system adopts CP-ABE, since it is a widely used attribute holographic transformation method. By adopting CP-ABE, the message owner encrypts and sends the message to a group of recipients. Among all recipients, whose attribute conforms to the access structure is the authorized user. On the one hand, authorized recipients can decrypt the corresponding ciphertext into plaintext by its private key. On the other hand, whose attribute does not conform to the access structure is the unauthorized user. The above decryption operation cannot be successfully performed by its private key.

For the problem that the number of hopping endpoint address increases with the increase of the hopping frequency, CP-ABE is adopted to deliver the hopping address block of service server in a unified way. As a result, it greatly reduces the increase in performance overhead of the hopping control center caused by the hopping endpoint address delivery. Besides, in order to cope with the leakage of hopping endpoint address caused by plaintext transmission of hopping address block, holographic transformation is performed using CP-ABE. At the same time, because the attribute information of different users is different, the hopping endpoint address range that can be decrypted by different users should be different. Thereby, CP-ABE can effectively prevent the leakage of hopping endpoint address range of different service servers. The hopping full-cycle control mechanism based on CP-ABE is shown in Figure 6. The workflow is as follows:
1. The user generates the authentication information \( \text{hash}_{SM3}(Attri, t) \) using its attribute information.

2. The hopping control center authenticates the user’s identity by comparing the received \( \text{hash}_{SM3}(Attri, t) \) with the calculated \( \text{hash}_{SM3}(Attri, t') \).

3. After the authentication succeeds, the hopping control center runs the Setup algorithm of the CP-ABE to generate the public parameter \( PK \) and the master key \( MSK \) of the protected network system. \( PK \) is sent to each registered endpoint.

4. When the user accesses the targeted network, the attribute information is sent to the hopping control center by packet_in message.

5. The hopping control center parses the attribute information in a packet_in message to judge whether the user is registered.

Figure 5. Attribute-based holographic transformation algorithm.

Figure 6. Ciphertext access control mechanism based on CP-ABE.
(5.1) If it is a registered user, the hopping control center runs the KeyGen algorithm in the CP-ABE according to the attribute information of endpoint so as to generate the private key $SK_{(i, w)}$ of the endpoint.

(5.2) Otherwise, the packet is dropped.

6. The hopping control center uses attribute information of endpoint to select hopping address range and hopping period.

7. The hopping control center uses SM3 to generate the current hopping endpoint address.

8. When the user needs to get access to network service, it sends an access request.

9. The SDN switch sends the request information to the hopping control center by packet_in message.

10. The hopping control center parses the access request and encrypts the symmetric key $K$ using the Encrypt algorithm of CP-ABE. Based on it, it encrypts the accessible network resource list by the symmetric key and sends the message as a reply.

11. The user obtains an encrypted list of the accessible network resource and an attribute key $SK_{(i, w)}$.

12. The user decrypts the reply message using the Decrypt algorithm to obtain symmetric key $K$.

What’s more, it decrypts the accessible network resource list.

(12.1) If the security level of the service resource is higher than the user’s security level, the symmetric key $K$ cannot decrypt the network resource list successfully using the private key $SK_{(i, w)}$.

(12.2) Otherwise, the symmetric key is decrypted successfully using the private key $SK_{(i, w)}$, and the user can obtain the list of access network resources.

System test and results analysis

Testing environment and system configuration

The test network topology is shown in Figure 7. The hardware equipment is a portable computer, whose conditions are as follows: CPU 2.6 GHz, 500G hard disk capacity, 8 GB memory, Windows 10 64-bit OS. The software conditions are as follows: Java 1.8.0_144 and VirtualBox 5.1.22 virtual machines are installed. The Linux operating system Ubuntu14.04 is installed in the virtual machine. The hopping control center is developed based on the Ryu controller.18

Functional test results and analysis

The NDD system based on holographic transformation has two main modules: hopping endpoint address
generation module and global view management module. The interface of hopping endpoint address generation module is shown in Figure 8. It contains management and query of endpoint address allocation, hopping address generation, and hopping period. The interface of a global view management module is shown in Figure 9. It provides administrators with visual management of the network global view and real-time update display of the whole network view.

Test of hopping endpoint address generation module based on SM3. The hopping endpoint address generation experiments for legitimate users mainly test the module function by simulating the generation of hopping endpoint address of the legal user by its attribute information. The hopping endpoint addresses of dynamic defense against attack are mainly aimed at the distributed denial-of-service (DDoS) attacks. During the DDoS attacks, malicious adversaries usually use active
scanning and passive monitoring for information collection at the first step. Based on this, the DDoS attacks are launched to the target.

1. Test of hopping endpoint address generation for the legitimate user. This experiment mainly tests the module function by simulating the generation of hopping endpoint addresses of the legal users by its attribute information. As shown in Figure 10, the hopping control center generates endpoint address blocks and hopping periods of high-level and low-level endpoints separately based on endpoint’s attribute information. The hopping control center adopts SM3 to generate the hash value of each endpoint attribute and timestamp as shown in Figures 11 and 12. The results of the test show that the SM3-based hopping endpoint address generation technique can effectively prevent the collision during endpoint address hopping generation.

2. Test of hopping endpoint address generation for the malicious adversary. When DDoS attack is implemented by the malicious adversary to the targeted network without dynamic defense mechanism, Figure 13 shows the comparison between the time delay of the legitimate user accessing the network service server and that of the user accessing the normal network service server. Figure 14 shows the result of a malicious adversary implementing DDoS when the dynamic defense is operated in the targeted network. The result shows that the hopping endpoint address generation module based on SM3 can confuse adversary and hide real endpoint address information of both session parties by endpoint information hopping. A malicious adversary cannot accurately locate the target endpoint while implementing the DDoS attacks. At the same time, the net-flow capacity of the DDoS attacks is dispersed because of endpoint address hopping. Thereby, the effectiveness of DDoS can be effectively resisted and weakened.

The test result of hopping endpoint address generation function based on the SM3 shows that the proposed module achieves random and anti-collision
Figure 12. Generate hash values for high-level user.

Figure 13. Results of DDoS attack when the dynamic defense system is closed.
hopping endpoint address selection and hopping period generation. At the same time, the hopping control center can synchronize the integrated management and display platform, users, and Open vSwitch in real time so as to make sure all endpoints in the targeted network communicate synchronously using the latest hopping endpoint address.

Test of hopping full-cycle control module based on CP-ABE. The function test of hopping full-cycle control based on CP-ABE is mainly the hopping endpoint identity authentication and access control. Each part of the test is divided into functional tests for legitimate users and security defense to malicious adversaries. By comparing the defense system feedback in the process of identity authentication and access control to registered users and malicious adversaries, the security and usability of this module are tested.

1. Test of attribute-based identity authentication. This test is mainly about the identity authentication operation of different kinds of users accessing the network. The type of users tested is divided into registered users and malicious adversaries. As shown in Figure 15, user1 is registered on the integrated management and display platform, and the status of user1 can be checked. This step is primarily to test the usability of the user registration function. Based on this, as shown in Figure 16, after the legitimate user opens the client to select the authentication option and enters the identity for identity authentication, the hopping control center compares its endpoint attribute hash value with that in the authentication server so as to authenticate the user’s identity.

The experimental results are shown in Figure 17. It shows that the malicious adversary cannot pass the identity authentication by forging the attribute information of other legitimate users. What’s more, the

```
Nmap scan report for 10.0.4.173
Host is up (0.28s latency).
MAC Address: 00:00:00:00:13 (Xerox)
Nmap scan report for 10.0.4.177
Host is up (0.30s latency).
MAC Address: 00:00:00:00:00:12 (Xerox)
Nmap scan report for 10.0.4.224
Host is up (1.0s latency).
MAC Address: 00:00:00:00:00:0E (Xerox)
Nmap scan report for 10.0.4.226
Host is up (0.38s latency).
MAC Address: 00:00:00:00:00:12 (Xerox)
Nmap scan report for 10.0.0.3
Host is up.
Nmap done: 2048 IP addresses (21 hosts up) scanned in 97.14 seconds
root@lei:/home/lei/mininet/custom# python dos.py
please input ip of the target you want to attack:
10.0.4.177
PING 10.0.4.177 (10.0.4.177) 56(84) bytes of data,
From 10.0.0.3 icmp_seq=1 Destination Host Unreachable
From 10.0.0.3 icmp_seq=2 Destination Host Unreachable
From 10.0.0.3 icmp_seq=3 Destination Host Unreachable
From 10.0.0.3 icmp_seq=4 Destination Host Unreachable
From 10.0.0.3 icmp_seq=5 Destination Host Unreachable
From 10.0.0.3 icmp_seq=6 Destination Host Unreachable
From 10.0.0.3 icmp_seq=7 Destination Host Unreachable
From 10.0.0.3 icmp_seq=8 Destination Host Unreachable
From 10.0.0.3 icmp_seq=9 Destination Host Unreachable
From 10.0.0.3 icmp_seq=10 Destination Host Unreachable
From 10.0.0.3 icmp_seq=11 Destination Host Unreachable
From 10.0.0.3 icmp_seq=12 Destination Host Unreachable
From 10.0.0.3 icmp_seq=13 Destination Host Unreachable
From 10.0.0.3 icmp_seq=14 Destination Host Unreachable
From 10.0.0.3 icmp_seq=15 Destination Host Unreachable
```

Figure 14. Results of DDoS attack when the dynamic defense system is opened.
result indicates that the designed module can prevent the attribute information forgery attack according to the unique endpoint identity and timestamp of the registered user.

2. Test of CP-ABE-based access control. The test is mainly about the list of network service resources being accessed by different users with different attributes. In this test, the security level of endpoints is divided into
three categories: low-security level users, high-security level users, and network servers.

As shown in Figure 18, since the proposed module adopts CP-ABE to make access control, users, using the private key, with low-security level cannot decrypt network service resource list with high-security level successfully. Besides, the user with the high-security level can successfully decrypt the network service resource list with the high-security level using its private key, as shown in Figure 19. As shown in Figure 20, the server can successfully decrypt the high-security level network service resource list using its private key.

The functional test results show that the hopping endpoint address generation module can achieve hopping endpoint address generation and hopping period selection, which has good unpredictability and usability. Based on this, the dynamic defense system can effectively cope with attacks such as active scanning, passive monitoring, and DDoS, thus effectively ensuring the security of the protected network and endpoints. However, according to the test of hopping full-cycle control module, CP-ABE-based identity authentication and access control can successfully implement hopping full-cycle control of hopping endpoints. It can prevent attribute information forgery attack and replay attack by the unique endpoint identity and timestamp of registered users. Besides, the proposed defense system can not only generate encrypted network service resource list according to the access control policy but also perform access control to users’ session requests on network service resource according to the security level of the registered user. Consequently, it prevents internal users from violating unauthorized access.

We have added a comparison of this method to other similar methods. Compared with existing moving target defense (MTD) mechanisms, such as Dynamic Network Address Translation (DYNAT), Network Address Space Randomization (NASR), OpenFlow Random Host Mutation (OF-RHM), and Spatial and Temporal Random Host Mutation (ST-RHM), our proposed method first proposes the concept of holographic transformation and realizes transparent transition of end node information through virtual address transformation. Compared with traditional defense mechanisms, such as shutting down unnecessary services, setting up security groups and private networks, and filtering traffic, we have increased the association between the security level and the access path in strong access control, which can effectively save defense costs, resist multiple types of attacks, and improve defense effectiveness.

The time-consuming test of SM3 hash algorithm address hopping. As shown in Table 2, the longest time to generate 25,000 virtual addresses is 29 s, and the average time is 27.6 s. Therefore, theoretically, when the hopping period is 30 s, the dynamic defense system can achieve 25,000 end node hopping at the same time, while a class C address can access 254 end nodes and a class B address can access 65,535 end nodes, which is far less than 25,000. Therefore, the hopping address generation algorithm based on the SM3 hash algorithm can realize the efficient generation of hopping addresses.

The analysis of system performance. The performance overhead of static networks and NDD systems based
on holographic transformation is shown in Table 3. It mainly includes the algorithm complexity, average delay, and flow table length of the hopping algorithm.

**For algorithm complexity:** When the number of sessions in a subnet is \( n_{vIP} \) and the node space that can be transitioned is \( S_{vIP} \), because the static network does not have transitions, the algorithm complexity can be made to be \( O(1) \). Since the dynamic defense system based on holographic transformation uses random spatial hopping, its algorithm complexity is \( O(S_{vIP}) \).

**For average delay:** The network delay is mainly composed of the processing delay of the node and the transmission delay. Because the dynamic defense system based on holographic transformation uses random spatial hopping, the forwarding delay will increase due to the end information hopping. However, the network hopping does not affect the data transmission, so the transmission delay is the same as the static network.

**For the flow table length:** In a static network, the flow table length is \( jS_{vIP} \). For the dynamic defense system based on holographic transformation, because each hopping is randomly selected from all available node spaces, the flow table length is \( 1 + n_{vIP} \).

### Analysis of attack complexity.
Suppose there are \( n \) target nodes in the network, the node space is \( m \), the scanning width is \( w \), the scanning frequency is \( 1/T_{SCN} \), the hopping frequency is \( 1/T_{HP} \), the number of scanned addresses is \( n_s = w \cdot t/T_{SCN} \), the scanning frequency, and the hopping frequency ratio is \( r = T_{HP}/T_{SCN} \). Since the majority of active scans collect active end node information through non-repeated uniform scans, for a static network, \( T_{HP} = \infty \), the probability that a malicious adversary successfully scans \( x \) addresses obeys the hypergeometric distribution, and the probability that a malicious adversary successfully scans is \( p_{static}(x>0) = 1 - C_{n_s}^{m-n_s}/C_m^n \). In the dynamic defense system based on holographic transformation, because of the address of the end node changes, the probability that a malicious adversary successfully scans \( x \) target nodes after a change follows the Bernoulli distribution, which can be expressed as \( p_{moving}(x>0) = 1 - [1 - rwn_l/(mn_l + mr_w)]^n \). Therefore, the success rate of scanning strategies implemented by malicious adversaries is \( p_{moving}(x>0) = 1 - [1 - wnl/(mn_l + mr_w)]^n \). In particular, when \( r = 1 \), the frequency of the malicious scan is the same as the hopping frequency, and the probability that the malicious adversary successfully performs the scan can be reduced to \( p_{moving}(x>0) = 1 - C_{m-n_s}^{m-n_s}/C_m^n \) and \( p_{moving}(x>0) = 1 - [1 - wnl/(mn_l + mr_w)]^n \). It can be known that the dynamic defense system based on holographic transformation is more effective.

### Table 2. The time-consuming test results of SM3 hash algorithm address hopping.

| The number of generated addresses | 1000 | 5000 | 10,000 | 20,000 | 25,000 | 30,000 |
|----------------------------------|------|------|--------|--------|--------|--------|
| Statistics                       | 50   | 50   | 50     | 50     | 50     | 50     |
| Average time (s)                 | 1    | 5    | 11.5   | 22     | 27.6   | 33.4   |
| Longest time (s)                 | 1    | 5    | 12     | 23     | 29     | 36     |

### Table 3. The system performance overhead.

| Hopping mode                  | Algorithm complexity | Average delay | Flow table length |
|-------------------------------|----------------------|---------------|-------------------|
| Static network                | \( O(1) \)           | \( t_{ran} \) | \( n_{vIP} \)     |
| Dynamic defense network       | \( O(S_{vIP}) \)     | \( t_{ran} + t_{proc} \) | \( 1 + n_{vIP} \) |

Figure 20. The server decrypts the high-security level service resource list with the private key.
transformation can effectively reduce the probability of successful scanning by malicious adversaries compared to static networks.

**Conclusion**

Aimed at the problem of ineffective endpoint hopping implementation in enterprise network due to hopping endpoint address failure and high-performance consumption caused by hopping endpoint address update, a novel of NDD system based on holographic transformation is designed and implemented. It is adopted to solve the external reconnaissance attack and internal users' abuse problems. The core inspiration of the designed system takes example by the theory of non-detection defense. On the one hand, in order to achieve the security goal, the virtual hopping endpoint address generation based on SM3 is to prevent external scanning attacks, while the hopping full-cycle control based on CP-ABE is to prevent replay attacks, forgery attacks, and internal abuse. On the other hand, in order to achieve effective availability and low-performance overhead, the SM3 hash algorithm is embedded into the generation hopping endpoint address generation algorithm so as to cope with the collision problem in the process of endpoint address hopping. Furthermore, in order to decrease the update frequency of hopping endpoint addresses during the defense process, CP-ABE is adopted in identity authentication and access control management module. Experiments show that the proposed defense system has features of high unpredictability, effective defense, good stability, easy operation, and real-time interaction.

**Acknowledgements**

The authors thank all the reviewers for their valuable comments.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the National Key Research and Development Program of China (Grant No. 2016YFF0204003) and the National Natural Science Foundation of China (Grant Nos. 61471344 and 61902427).

**ORCID iDs**

Jinglei Tan https://orcid.org/0000-0002-3231-6793
Hao Hu https://orcid.org/0000-0003-4888-6368

**References**

1. Liu Y, Peng W and Su J. A study of IP prefix hijacking in cloud computing networks. *Secur Commun Netw* 2014; 7(11): 2201–2221.
2. ZDNet C and Zack W. PRISM: here’s how the NSA wiretapped the Internet, 2013, http://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/ (accessed on 21 February 2014).
3. Hu H, Zhang HQ, Liu YL, et al. Security metric methods for network multistep attacks using AMC and big data correlation analysis. *Secur Commun Netw* 2018; 2018: 5787012.
4. Hu H, Liu YL, Zhang HQ, et al. Optimal network defense strategy selection based on incomplete information evolutionary game. *IEEE Access* 2018; 6: 29806–29821.
5. Zhang HQ, Lei C, Chang DX, et al. Network moving target defense technique based on collaborative mutation. *Comput Secur* 2017; 70: 51–71.
6. MacFarland DC and Shue CA. The SDN shuffle: creating a moving-target defense using host-based software-defined networking. In: *Proceedings of the second ACM workshop on moving target defense*, Denver, CO, 12 October 2015, pp.37–41. New York: ACM.
7. Syversen J, Syversen J, Syversen J, et al. Automated effectiveness evaluation of moving target defenses: metrics for missions and attacks. In: *ACM workshop on moving target defense*, Vienna, 24 October 2016, pp.129–134. New York: ACM.
8. Luo YB, Wang BS and Cai GL. Analysis of port hopping for proactive cyber defense. *Int J Secur Appl* 2015; 9(2): 123–134.
9. Kirkpatrick K. Software-defined networking. *Commun ACM* 2013; 56(9): 16–19.
10. Aamir M and Zaidi MA. DDoS attack and defense: review of some traditional and current techniques, 2014, https://arxiv.org/abs/1401.6317
11. Sun K and Jajodia S. Protecting enterprise networks through attack surface expansion. In: *Proceedings of the 2014 workshop on cyber security analytics, intelligence and automation*, Scottsdale, AZ, 3 November 2014, pp.29–32. New York: ACM.
12. Narain S and Chee D. Moving-target defense with configuration-space randomization. US20160323313 Patient, 2016.
13. Lei J. Cyber situational awareness and mission-centric resilient cyber defense. In: *International conference on computer science and network technology*, Harbin, China, 19–20 December 2015, pp.1218–1225. New York: IEEE.
14. Morrell C, Ranstbottom JS, Marchany R, et al. Scaling IPv6 address bindings in support of a moving target defense. In: *Internet technology and secured transactions*, London, 8–10 December 2014, pp.440–445. New York: IEEE.
15. Chung CJ, Xing T, Huang D, et al. SeReNe: on establishing secure and resilient networking services for an SDN-based multi-tenant datacenter environment. In: *2015 IEEE international conference on dependable systems and networks workshops (DSN-W)*, Rio de Janeiro, Brazil, 22–25 June 2015, pp.4–11. New York: IEEE.
16. Lei C, Zhang H, Ma D, et al. Network moving target defense technique based on self-adaptive end-point hopping. *Arab J Sci Eng* 2017; 42(8): 3249–3262.
17. Yang J, Han Q and Li HY. The Design and Implementation of 2D-DCT algorithm based on FPGA. *Appl Mech Mater* 2015; 738–739: 409–412.
18. Gorasia N, Srikanth RR and Doshi N. Multi authority ciphertext policy attribute based holographic transformation schemes with constant ciphertext length: a survey. *Netw Commun Eng* 2014; 7(1): 16–28.
19. Sun J, Hu Y and Zhang L. A key-policy attribute-based broadcast holographic transformation. *Int Arab J Inf Technol* 2013; 10(5): 444–452.
20. Kewley D, Fink R, Lowry J, et al. Dynamic approaches to thwart adversary intelligence gathering. In: *Proceedings DARPA information survivability conference & exposition II*. Anaheim, CA, 12–14 June 2001, pp.176–185. New York: IEEE.
21. Antonatos S, Akritidis P, Markatos EP, et al. Defending against hitlist worms using network address space randomization. *Comput Netw* 2007; 51(12): 3471–3490.
22. Jafarian JH, Al-Shaer E and Duan Q. Openflow random host mutation: transparent moving target defense using software defined networking. In: *Proceedings of the first workshop on Hot topics in software defined networks*, Helsinki, 13 August 2012, pp.127–132. New York: ACM.
23. Jafarian JH, Al-Shaer E and Duan Q. An effective address mutation approach for disrupting reconnaissance attacks. *IEEE T Inf Foren Sec* 2015; 10(12): 2562–2577.