Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 14, no. 3, March 2018, pp. 512-520
DOI: 10.23940/ijpe.18.03.p12.512520

DDoS Attacks Defense Mechanism based on Secure Routing Alliance

Xiaohui Yang* and Yue Yu

School of Cyberspace Security and Computer, Hebei University, Baoding, 071002, China

Abstract

Distributed Denial of Service (DDoS) attacks on the cloud computing platform has become one of the key issues affecting cloud security. According to the sources of security threat of cloud computing platform, construct secure routing alliance, filter and resist DDoS from the route of cloud user to cloud computing center, design data forwarding mechanism and fault nodes replacement mechanism. The strategy of secure overlay services is combined with the structural characteristics of the ubiquitous routing platform to defend against DDoS attacks. The Chord ring is improved, the nodes are divided according to the distance in the physical network, and the Chord algorithm is avoided repeatedly ignoring the forwarding of physical paths. Since the original Chord algorithm is applied to the P2P network, in order to make it more suitable for the hierarchical physical topology, only the first three jumps of the Chord algorithm's query steps are taken. Fault nodes replacement mechanism uses virtual machine technology to convert nodes in the network into a large number of virtual nodes and serve as backup nodes in the security structure in time to replace the attacked nodes with backup nodes to minimize the impact of attacks on the nodes. The simulation results show that with the increase of the number of nodes, the data passing rate of the secure routing alliance can exceed 90% and the pass rate can be guaranteed to be over 35% when the number of attack nodes is large, which ensures data security and the availability of the transmission paths.

Keywords: cloud security; DDoS attacks; secure routing alliance; algorithm improvement

(Submitted on December 25, 2017; Revised on January 16, 2018; Accepted on February 20, 2018)

1. Introduction

Cloud computing introduces a utility model to remotely supply extensible and measurable resources [4], so users store many resources on it, which also led to the greed of many illegal users outside the cloud who want to use illegal means to obtain resources in the cloud for profit. Cloud security has become the focus of attention.

Distributed Denial of Service (DDoS) attacks are one of the major security threats to large-scale networks and one of the security threats to cloud computing platforms. DDoS attacks can paralyze the cloud computing platform, resulting in users cannot use their services, and even reveal or lose users information, the damage caused is unpredictable. In 2010, the Cloud Security Alliance viewed DDoS attacks as an important security issue facing cloud computing [2]. Therefore, the study of DDoS attacks on cloud environment is very necessary. In this paper, DDoS attacks are defended and resisted by establishing a secure routing alliance.

2. Related Work

In order to ensure that the cloud computing center can work normally, Zhijie Han proposed to reduce the defense mechanism of DDoS attacks by increasing the number of servers [6]. Wei Han proposed using the heartbeat mechanism of the cloud computing center server. The attacked server will be withdrawn from the cloud computing center until after the attack; then, it will join the cluster [5]. Yogesh et al proposed using intrusion detection system on routers to detect the passing of traffic according to predetermined rules. Once an attack is found, virtualization of cloud computing is utilized to transfer the attacked virtual server to a data center in another location [1]. S. Zhao puts forward some resources reserved on the server. When a DDoS attack is detected, the victims are migrated to these reserved resources and restored when the

* Corresponding author.
E-mail address: yxh@hbu.edu.cn

attack is stopped. However, cost considerations will be high if the attack lasted longer or repeated [20]. Y. Wang proposed to reduce the cost of victim migration through a virtual machine. However, migration caused by DDoS attacks may cause overall damage to users' resources during the migration process [16].

R. Sahay proposed an SDN based solution in which ISP level traffic monitoring and malicious traffic routing are performed on specially designed security switches [10,13]. The victim needs to ask the ISP for DDoS detection. The ISP imports the traffic abstraction view through the application traffic tag of the OpenFlow switch. Suspicious traffic will be redirected to the secure middle box and the suspicious traffic will be detected by accessing the traffic policy; the part that has been detected and the DDoS attacks are mitigated remains on the client side. X. Wang proposed a prototype implementation of the SDN based detection mechanism [11,14]. The main idea of this approach is strict access control policies, and strict authentication of incoming traffic. SDN plays a very effective role in alleviating large-scale and low-rate DDoS attacks due to its reconfigurable and fast network view and monitoring features. However, studies such as Q. Yan et al show that even the SDN infrastructure itself can be a victim of DDoS attacks [19].

Most of the above methods passively respond to attacks within the cloud computing center. In a large-scale network, the research on DDoS defense in the access path from users to cloud computing centers mainly includes the following points. Angelos D. Keromytis et al proposed Secure Overlay Services (SOS) to prevent DDoS attacks through filtering and secure tunneling. In order to prevent the access points from being scanned and attacked by attackers, Angelos D. Keromytis proposed the use of Chord protocol to solve [8]. After that, A. Stavrou also assumed that attackers could focus attacks on access nodes in the SOS method and proposed to improve the access mode of the clients so that users can access the SOS structure randomly through multiple access nodes, thereby avoiding the attackers traced [12]. Xun Wang et al proposed a new mode of attack combined with intrusion attacks and congestion attacks on the structure of the original secure overlay services and analyzed the service performance of the secure overlay services by changing parameters such as the number of structural layers, the degree of mapping, and the number of nodes [15,18]. The above methods all propose a new mode of attack for the existing structure, but ignore the possibility that the SOS nodes may also be attacked and how to deal with it after being attacked. Chi Hyung In et al proposed a burst attack and a gradual attack on the original secure overlay services' vulnerabilities to improve the attacks efficiency, and proposed using network clustering method to detect traffic anomalies [17]. However, this strategy needs to be changed by all the nodes in the secure overlay services, so it is complicated to implement and needs to deal with a large amount of data traffic and establish a corresponding rule base. This is not a small burden on nodes in the secure overlay services.

According to the analysis of the above methods, based on the SOS and the structural characteristics of the ubiquitous routing platform, the secure routing alliance is established, which solves the problems existing in the above strategies.

3. System structure

Cloud computing transmits a large amount of data from users to the cloud computing center through the ubiquitous routing platform [9], which plays an important role as a data carrier in the cloud computing. The ubiquitous routing platform has the hierarchical characteristics. There is an access layer, area center and core layer of the three-tier architecture. User requests are sent to the access layer routers first, and then through the area core routers and core layer routers to the cloud computing center.

The purpose of the SOS is to construct a large overlay network between the users and the servers. The SOS consists of the access nodes (SOAP), Beacon and Secret Servlet [8]. By authenticating users at the edge of the network and filtering large amounts of attack traffic by the network high-rate core routers, while introducing a random, anonymous transmission structure, the attacks dispersed to each node, making it harder for an attacker to reach a goal protected by the secure overlay services through one path.

Secure Overlay Services Disadvantages:

The route forwarding algorithm used in the SOS is an algorithm that ignores the physical topology and may cause the detour problem. How to deal with it after the nodes are attacked in the SOS.

In order to solve the above problems and implement the SOS to the cloud computing routing platform, combine the SOS with the ubiquitous routing platform to make it structured and hierarchical; the secure routing alliance is established.

Secure routing alliance is a cloud computing routing platform that combines the application layer routing method, which using the consistent hash algorithm Chord, with the hierarchical structure of the ubiquitous routing platform. The

routing nodes are divided into different hierarchical structures so that they can complete the corresponding forwarding functions, make the routing method more suitable for the hierarchical physical topology and filter out DDoS attacks.

Firstly, the Chord ring is improved; the nodes are divided according to the distance of each other in the physical network to avoid the Chord algorithm repeatedly ignoring the forwarding of the physical paths. This makes the Chord algorithm more suitable for the layered physical topology; only the first three jumps of the query steps are taken. The nodes replacement mechanism is taken, virtualized nodes with virtualization technology and replaces the attacked nodes with backup nodes to ensure the availability of the secure routing alliance. Figure 1 shows the structure of a secure routing alliance.

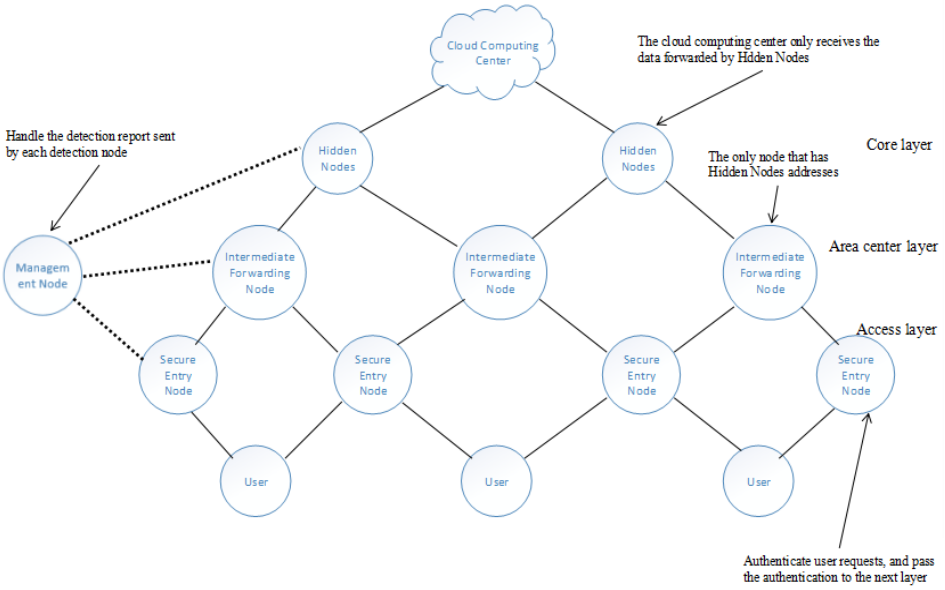

Figure 1. Secure routing alliance structure

3.1. Data Forwarding Mechanism

Data forwarding mechanism sets some nodes in the access layer, the area center layer and the core layer as secure entry nodes, intermediate forwarding nodes and hidden nodes in the secure routing alliance respectively in the three-layer architecture of the ubiquitous routing platform; the final forwarding target is cloud computing center.

If the cloud user sends a request to access the cloud center, the request is sent to the secure entry nodes. With the function of the SOS, the user request is authenticated. The authentication can be performed using IPSec or TLS. After the authentication is passed, in the same way, the intermediate forwarding nodes forward the data packets to the hidden nodes in the core layer, according to the Chord algorithm. After receiving the data packets, the hidden nodes do not need to forward, according to the Chord algorithm. Instead, it is directly forwarded to the cloud computing center.

Since the address of the hidden nodes are stored only by a few nodes, that is, only the intermediate forwarding nodes know their address, the data forwarded by the hidden nodes are safe and reliable, Therefore, the filter between the cloud computing center and the secure routing alliance only allows for the data packets, which forwards from the hidden nodes into the cloud center.

The data forwarding paths formed by the secure entry nodes, the intermediate forwarding nodes, and the hidden nodes are called the secure paths. Legitimate users who have been authenticated by the secure entry nodes use the Chord route search algorithm during transmission. Legitimate users can complete the data transfer through the application layer routing; based on the network layer routing protocol, the attacker can only complete the data transfer.

If the rules that discard data forwarded by unsecured path nodes are set in the intermediate forwarding nodes and the hidden nodes, the attack traffic will be difficult to reach the cloud computing center through the secure path nodes. This will prevent an attacker from using puppet machines to send a large number of packets to attack the target nodes, achieving the purpose of distinguishing legitimate users from illegal users. The data forwarding process is shown in Figure 2.

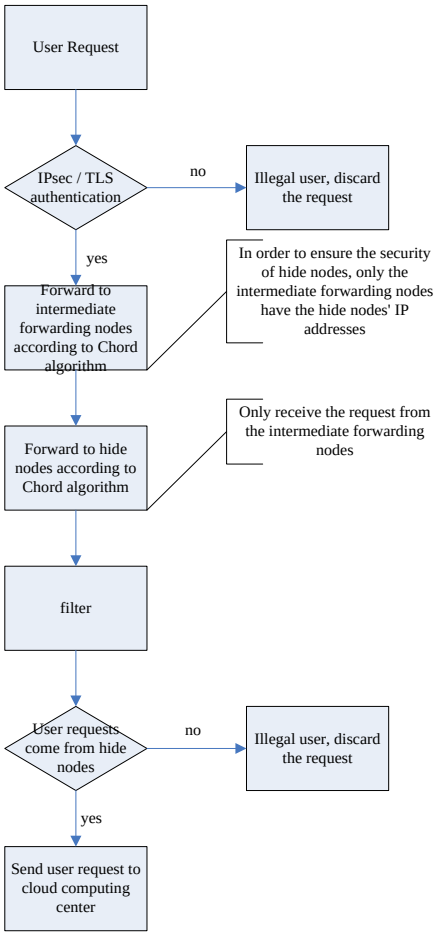

Figure 2. Data forwarding process

The data forwarding mechanism is based on the Chord network model that is representative of the structured P2P overlay network model.

Chord Algorithm Problems and Improvements:

In order to filter illegal attack traffic in the secure routing alliance, Chord routing algorithm is used to guide legitimate traffic to the secure nodes. The illegal attack traffic can only be forwarded through normal routing way and cannot reach the secure nodes. However, The Chord algorithm used in this method is a routing algorithm that ignores the physical topology. If a legitimate traffic needs to reach the correct secure nodes, it will ignore the forwarding of the physical path repeatedly, which is very time-consuming.

Dividing the nodes that are close to each other in the physical network into one group, we can obtain multiple node groups. Selecting some nodes with good performance in the network as the main nodes for resource positioning. Each main node manages a node group. All main nodes are distributed on one Chord ring, which is the main node group. In this way, the entire network is a Chord ring made up of multiple Chord-type node groups. The network model is shown in Figure 3.

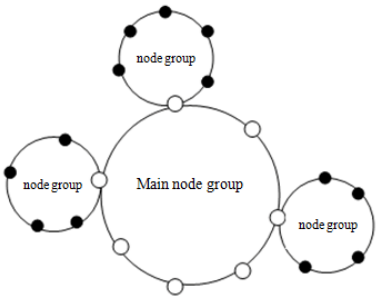

Figure 3. Improved Chord network model

(1) Nodes grouping

- In the spatial level of division

Dividing the nodes with the same network address and sub-net address into the same Chord type node group.

- In the time level of division

Use a random function to select some distributed arrangement of the reference nodes in the Chord ring. Record the round-trip time of each node to the reference nodes and sort them. Each node will measure a sorted sequence. The nodes with the same sequence may be deployed in the same node group. If the sequence is similar, the nodes placed in the neighboring node groups.

(2) Improved Chord algorithm query steps

- Step 1. Hash operation

In order to complete the Chord ring three jumps, hash operate the address of the nodes and the target server, get the mapping values and all mapped in the Chord ring.

- Step 2. Divided area

Chord ring is divided into three areas, namely access area, the middle area and the core area.

The access area is located in the clockwise direction of the backward node of the target map value. According to the required number of nodes, the size of the access area can be adjusted in the condition of no more than 1/2 Chord ring. The main nodes that in the area and located in the ubiquitous routing platform access layer can be used as secure entry nodes and the nodes in the corresponding node group are also secure entry nodes.

The middle area is located on the opposite side from the access area, which is similar to the secure entry nodes selection in the access area. The nodes are in the middle area and is located in the area center of the ubiquitous routing platform, which can be selected as the intermediate forwarding nodes.

Similarly, a node is located in the core area and the ubiquitous routing platform's core layer may be selected as the hidden nodes; the address of the target nodes is stored in the hidden nodes. Therefore, the hidden nodes can send the data packets to the target directly; it does not need to be forwarded, according to the Chord ring, after receiving the data packets.

- Step 3. Area judgment

If the next hop node of the secure entry node is not in the middle area or fails to work due to a fault, according to the Chord algorithm before the improvement, the secure entry nodes in the pointer table directly treat the hidden nodes in the core area as the forwarding object. In this case, if the secure routing alliance is attacked, as a result of the absence or failure of the intermediate forwarding nodes, the data packets are forwarded directly to the hidden nodes and then directly forwarded to the target server. Therefore, a judgment function needs to be added at the secure entry nodes. If the backward node of the query target goes beyond the range of the intermediate area, the largest identifier in the middle area is selected, so that the data packets can be forwarded normally in the divided area.

3.2 Fault Nodes Replacement Mechanism

Although the improved Chord algorithm can mitigate the damage of DDoS attacks to the cloud computing center, it cannot effectively solve the problem of nodes being attacked in the secure routing alliance. If an attacker attacks all nodes in the secure routing alliance, its nodes exit SOS after being attacked according to the description of the SOS [7,8].

If each attack is targeted at some nodes, and an attacker finds out that the nodes are not in the secure routing alliance through technology such as network sniffing, the target will be targeted at the next attack. In addition, the Chord ring has a self-repair function; that is, a node in the ring will query its own neighbor nodes, and delete the node that is faulty or a failure to prevent the fault node from affecting the network. However, this will result in nodes in the secure routing alliance

being consumed continuously.

From the probability of the above problems are analyzed:

The number of nodes in each layer of the secure routing alliance is N_i. The number of nodes located in the secure access path is u_i; in each round of attack, the total number of each layer's nodes attacked is R.

In the first round of attacks, if the number of nodes attacked in the secure routing alliance is 0, then in the second round of attacks, the probability P of attacks on nodes at all layer of the secure routing alliance is:

$$P_i = u_i / N_i - (P \times N_i) / \sum_{i=1}^{3} N_i$$

Where i represents the number of layers in the secure routing alliance.

Through the above analysis, it can be known that the attacks consume more nodes and increase the probability that the nodes in the secure routing alliance are being attacked, thereby increasing the packet loss rate during transmission. The self-repair function of the secure routing alliance causes the nodes to exit the Chord ring. As the number of nodes decreases, the communication quality may be affected, and the restarting cannot solve the problem well. According to the above analysis, SOS is vulnerable to attack by cyclically changing targets.

When the attacked secure nodes are exiting the Chord ring, in order to prevent no new nodes to replace their work, virtualization technology [3,7] can be used to virtualize a large number of network nodes by building virtual machines on the computer as the backup nodes of secure nodes. The network nodes after virtualization are easy to reconfigure and the repair time is shortened. Once the secure nodes are attacked, according to the self-repair function of Chord ring, the nodes in the ring will query their own neighboring nodes, delete the node if it is found faulty or invalid, and the backup node as a new node to join Chord ring to continue working. Then, the repair work is done, the impact of attacks on the network are minimal and smooth progress of network communications is ensured.

4. Experiments

First, the OMNeT++ software [21] is used to simulate a network model and analyze the total number of nodes (N) and attack nodes (A) respectively to get the change of the data passing rate in the secure routing alliance. The main purpose is to simulate the process that legitimate cloud users' packets reach the destination through the secure routing alliance.

In the three-layer routing platform's nodes of the network simulation model, which uses the improved Chord ring forwarding strategy, some nodes are selected from the nodes of the routing platform as the attacked nodes. At the same time part of the attacked nodes are selected to repair, the nodes after attack will lose response and be unable to work, and the repaired nodes can continue to work or simply exit the network. In addition, the target nodes need to be counted and statistics on all the packets that arrive at the target need to be calculated. From the related work mentioned above, there is no research on how to deal with the SOS network nodes after being attacked. Therefore, this paper compares and analyzes the methods described in the article with SOS by setting different parameters.

(1) Model simulation of the relationship between the number of network nodes and the network successful transmission packets ratio.

Experimental parameters: Select 50 attack nodes, attack period 1s, repair period is 1s (the repair cycle refers to the period during which the Chord ring in the secure routing alliance removes the attacked nodes and adds the replacement nodes ready to work to the secure routing alliance). The number of nodes in each area in the secure routing alliance is 20, 10, and 5, respectively.

Using Matlab simulation data analysis, as shown in Figure 4. The two curves in the figure indicate the relationship between the number of different nodes and the data rate of successful transmission in the network. The overall trend of these two curves is that as the number of nodes increases, the data successful transmission rate also increases. This is because when the number of nodes in the network increases, the probability that the attacker can attack the nodes in the secure routing alliance decreases, so the probability of data loss also becomes smaller. When using the virtual nodes mentioned in this article can guarantee the data transmission rate to be over 50% even when N is small, and the data passing rate can exceed 90% with the increase of the number of nodes, which is much better than the SOS method.

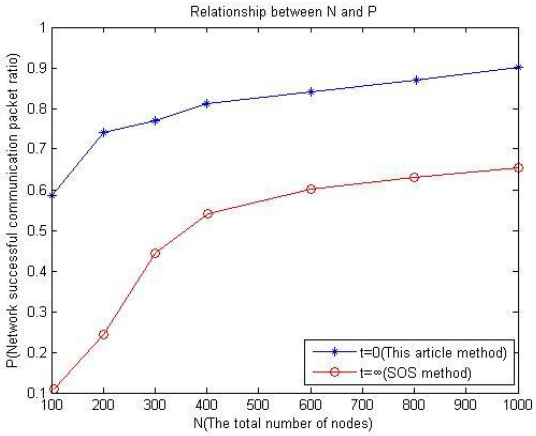

Figure 4. Relationship between N and P

(2) Model simulation of the relationship between the number of network attack nodes and the network successful transmission packets ratio.

The number of network nodes N is set to 1000, and the number of nodes in each area in the secure routing alliance is 200, 100 and 50 respectively.

Simulation results shown in Figure 5:

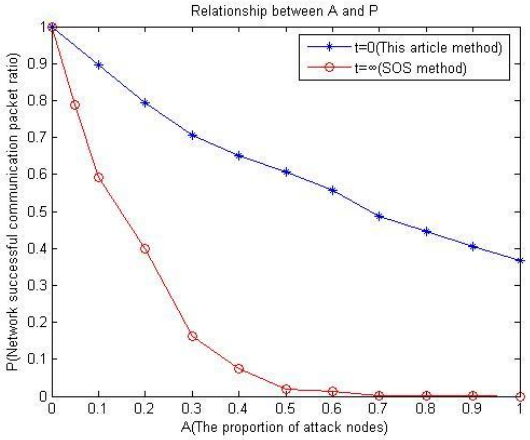

Figure 5. Relationship between A and P

The overall trend of the two curves in the graph is that as the number of attack nodes increases, the data packet passing rate decreases. At first, when there is no attack, the passing rate of the two methods are all 100%. However, with the increase of the number of attack nodes, the data passing rate of SOS method dropped obviously. Because the method of nodes replacement is not adopted, the final passing rate is 0, the method of this article can guarantee the passing rate to be over 35% when there are many attack nodes.

Through the above two sets of experimental results, we can draw a conclusion: the secure routing alliance strategy can deal with DDoS attacks well.

(3) Model simulation of the relationship between the attack and repair cycle ratio and the network successful transmission packets ratio.

Experimental parameters: the number of network nodes N is set to 1000, the number of attack nodes Na is 500,remain the repair interval 1s unchanged, the attack interval varies from 0.1s to 10s on the horizontal axis, and the number of nodes in the secure paths of each layer in the secure routing alliance respectively 200,100,50. Figure 6 horizontal axis W represents the attack cycle and repair cycle ratio. Cycle ratio range from 1/10 to 10. The vertical axis P represents the data passing rate of the network in a certain period of time.

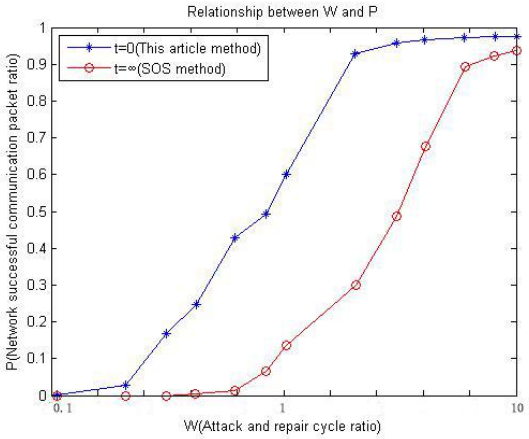

Figure 6. Relationship between W and P

The experimental result shows that as the ratio of attack and repair cycle gradually increases, the overall network transmission success rate increases significantly. When the ratio of attack cycle to repair cycle is small, the attack is frequent; an attacker can find and attack nodes in the secure paths within a relatively short time, whereas network repair is slow. Because the execution cycle of the whole network repair process is longer than the attack cycle, the backup nodes cannot join the secure paths in time. Although the nodes replacement mechanism is adopted, the data passing rate in the network is still low. When the attack period is close to 1/10 of the repair cycle, the data passing rate is close to 0.

With the gradual increase of the attack cycle, the gap between attack and repair cycle gradually narrowed, and the data passing rate in the network begin to rise rapidly. When the ratio of attack cycle to repair cycle is 1, the data passing rate of the nodes replacement mechanism reaches more than 60%, while the data passing rate of the SOS is only 15%. Therefore, the nodes replacement mechanism to achieve better communication than the original SOS strategy.

5. Conclusions

In this paper, a secure routing alliance, combined with the SOS strategy and the hierarchical structure of the ubiquitous routing platform, is established. The improved Chord algorithm effectively solves the detour problem during the query jumps, reduces the delay in the transmission process, and effectively filters the attack traffic by layering Chord. The experimental results show that with the increase of the number of nodes, the data passing rate of the secure routing alliance can reach 90%, and the pass rate can be guaranteed to be over 35% when the number of attack nodes is large, which is better than the SOS method. The nodes replacement mechanism in the secure routing alliance can deal with the attacked nodes in a timely and efficient manner. From the experimental results, it can be seen that when the ratio of attack cycle to repair cycle is 1, amd the data passing rate of the nodes replacement mechanism reaches over 60%. At this time, the data passing rate of the SOS method is only 15%. Therefore, the secure routing alliance can effectively defend against DDoS and ensure the availability of transmission paths.

In the future work, there is a need for improvement in:

- Aim at the problem that the secure routing alliance nodes may be attacked. An early-warning mechanism can be added to the secure routing alliance to make each node take the task of detecting DDoS attacks and try to use the traffic entropy recognition algorithm to identify the attack traffic and respond in advance.

- Secure routing alliance does not address DDoS attacks from the root cause. The single packet tracing method can be used to trace the attack source, solving the threat of DDoS attacks to the cloud environment.

Acknowledgements

This work is supported by the National Key R&D Program of China under Grant 2017YFB0802300.

References

1. A. Bakshi and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," *Communication Software and Networks*, pp. 260-264, 2010.
2. Cloud Security Alliance, "Top Threats to Cloud Computing," *https://cloudsecurityalliance.org/group/top-threat*, August 2015.
3. X. Chen, H. Cheng, and Z. J. Zheng, "Cloud Computing Virtualization Technology Development and Trends", *Electronic Technology and Software Engineering*, no. 21, 2017.
4. T. Erl, Z. Mahmood, and R. Puttini, "Cloud Computing Concepts, Technology and Architecture," *Mechanical Industry Press*, Beijing, China, pp. 14-76, 2014.
5. W. Han, "Research on DDoS Attacks Defense based on Hadoop Cloud Computing Platform," *Taiyuan University of Science and Technology*, Taiyuan, China, 2011.
6. Z. J. Han, "Defence of Denial of Service Attack based on Cloud Computing Platform," *Institute of Information Technology*, vol. 37, no. 3, pp. 67-69, 2011.
7. C. H. In, C. S. Hong, and J. Wei, "An Enhanced SOS Architecture for DDoS Attacks Defense Using Active Network Technology," *Proceedings of Advanced Industrial Conference on Telecommunications/ Service Assurance with Partial and Intermittent Resources Conference/ Learning on Telecommunications Workshop*, Lisbon, Portugal, pp. 90-95, 2005.
8. A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: An Architecture for Mitigating DDoS Attacks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 1, pp. 176-187, 2004.
9. G. Q. Lu, "Ubiquitous Routing Platform of Cloud Computing," *Journal of Information Security and Technology*, pp. 106-108, August 2010.
10. R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "Towards Autonomic DDoS Mitigation Using Software Defined Networking," *NDSS Workshop on Security of Emerging Networking Technologies, Internet Society*, 2015.
11. G. Somani, M. S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, and R. Buyya, "Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions," *IEEE Cloud Computing*, 2017.
12. A. Stavrou and A. D. Keromytis, "Countering DoS Attacks with Stateless Multipath Overlays," *Proceedings of the 12th ACM Conference on Computer and Communications Security CCS'05*, pp. 249-259, Virginia, USA, 2005.
13. S. C. Tsai, I. H. Liu, C. Lu, C. H. Chang, and J. S. Li, "Defending Cloud Computing Environment against the Challenge of DDoS Attacks based on Software Defined Network," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceeding of the Twelfth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, vol. 1, pp. 21–292, 2017.
14. X. Wang, M. Chen, and C. Xing, "SDSNM: A Software Defined Security Networking Mechanism to Defend Against DDoS Attacks," in *Frontier of Computer Science and Technology (FCST), 2015 Ninth International Conference on, IEEE*, pp. 115–121, 2015.
15. X. Wang, S. Chellappan, and P. Boyer, "On the Effectiveness of Secure Overlay Forwarding Systems under Intelligent Distributed DoS Attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 7, pp. 619-632, 2006.
16. Y. Wang, J. Ma, D. Lu, X. Lu, and L. Zhang, "From High-Availability to Collapse: Quantitative Analysis of 'Cloud Droplet Freezing' Attack Threats to Virtual Machine Migration in Cloud Computing," *Cluster Computing*. vol. 17, no. 4, pp. 1369–1381, 2014.
17. Z. J. Wu, Y. Cui, and M. Yue, "Defensive DDoS Attack Method based on Virtual Hash Secure Access Path VHSAP for Cloud Computing Routing Platforms," *Journal of Communication*, vol. 36, no. 1, pp. 34-41, 2015.
18. D. Xuan, S. Chellappan, and X. Wang, "Analyzing the Secure Overlay Services Architecture under Intelligent DDoS Attacks," *Proceedings of the 24th International Conference on Distributed Computing Systems*, pp. 408-417, Tokyo, Japan,2004.
19. Q. Yan and F. Yu, "Distributed Denial of Service Attacks in Software Defined Networking with Cloud Computing," *Commun. Mag. IEEE*, vol.53, no. 4, pp. 52-59, 2015.
20. G. Yossi, H. Amir, S. Michael, and G. Michael, "CDN on Demand: An Affordable DDoS Defense via Untrusted Clouds," *Network and Distributed System Security Symposium (NDSS)*, 2016.
21. Y. L. Zhao and J. Zhang, "OMNeT++ and Network Simulation," *People's Posts and Telecommunications Press*, pp. 22-102, Beijing, China, 2012.