An Active Defense Model in Edge Computing Based on Network Topology Mimetic Correlation

Shuo Wang[1], Qianmu Li[1,2(✉)], Shunmei Meng[1], Bo Zhang[1], and Cangqi Zhou[1]

[1] School of Computer Science and Engineering, Nanjing University of Science and Technology, P.O. Box 210094, Nanjing, People's Republic of China
qianmu@njust.edu.cn

[2] Intelligent Manufacturing Department, Wuyi University, P.O. Box 529020, Jiangmen, People's Republic of China

Abstract. A large amount of real-time data, including user privacy information, control commands, and other sensitive data, are transmitted in edge computing networks. Aiming at the high-speed and reliable transmission requirements of data in the uncontrollable environment of edge computing networks, and maximizing the defense revenue, this paper proposes an active defense method for data interaction attacks in edge computing networks based on network topology mimic correlation, by pseudo-randomly constructing a moving communication path alliance and combining the network security state with a reliable prediction of transmission. A network topology mimetic association diagram and a communication path alliance mimetic transformation method based on dynamic threshold are proposed to ensure the data transmission service quality of the active defense technology of edge computing networks. The active defense model of the edge data network interaction process against the new attack and with the optimal defense cost is constructed, which provides a powerful guarantee for the active defense before the attack. The experimental results show that our method outperforms the popular methods in terms of transmission efficiency, reliability, and anti-attack performance.

Keywords: Network attack · Active defense · Edge computing

1 Introduction

One of the primary latent risks in a network is a cyber-attack on the network data interaction layer in the form of edge computing. This is due to the large amount of real-time state acquisition data, user privacy information and control command data present in an edge computing network. These data play a decisive role in user privacy protection and system decision control [3]. Alternatively, an edge computing network can

This paper supported by The Fundamental Research Funds for the Central Universities (No. 30918012204), Jiangsu province key research and development program (BE2017739), 2018 Jiangsu Province Major Technical Research Project "Information Security Simulation System".

Y. Yin et al. (Eds.): MobiCASE 2019, LNICST 290, pp. 198–212, 2019.
https://doi.org/10.1007/978-3-030-28468-8_15

perform real-time monitoring and control services on the edge of the critical infrastructure, with strict requirements on the performance of real-time data transmission [14, 15]. Considering data security interactions in an edge computing network, it is important to suppress attacks and execute evasive responses before a network attack causes damage [2, 3]. Therefore, edge computing networks urgently require active defense during data transmission.

However, the current network attack methods (CNAMs) such as the advanced persistent threat (APT) are concealed, and the attack principle is complex. Attack monitoring and passive blocking technologies based on traditional misuse detection have been unable to cope with such attacks. For this reason, active defense faces challenges. Fortunately, the self-organizing nature of edge computing networks provides a foundation for active defense of data interaction [21, 22]. However, previous technologies do not consider a moving adjustment in the case of reduced network connectivity and link quality caused by an attack [4]. Thus, the defense strategy of a moving adjustment algorithm requires further optimization and improvement.

Therefore, this paper proposes an active defense model for data interaction processes in edge computing based on a network topology mimetic correlation, achieved by pseudo-randomly constructing a moving communication path alliance under the premise of ensuring service quality. Then, this method integrates the network security state and transmission reliability prediction to adaptively mimic change and actively evade network attacks. The model includes an edge-aware node, an edge computing terminal node, and a primary station system and uses a negotiated moving multipath communication alliance to secure data communication. Figure 1 shows the framework of our research.

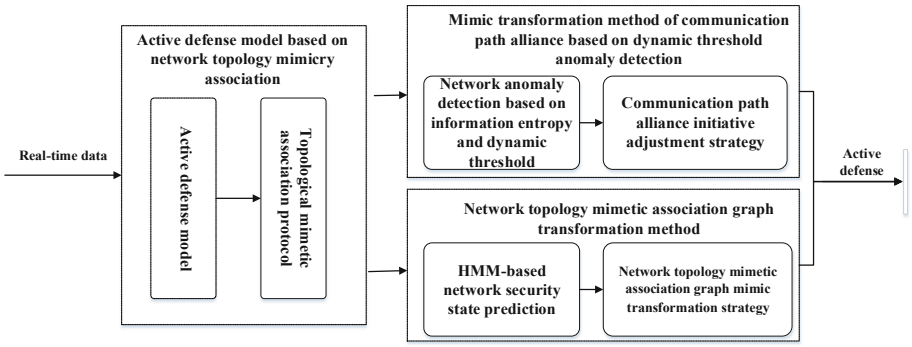

Fig. 1. Framework of active attack defense technology for edge computing network data interactions

The rest of this paper is organized as follows: Sect. 2 discusses relevant studies on moving network technology in mimicry defense. Section 3 gives the overall model framework and design for network topology mimetic association protocols. In Sect. 4, it describes a mimetic transformation method of communication path and a mimetic transformation method utilizing a mimetic topology correlation graph. In Sect. 5, the security of the model and verify the performance through experiments is analyzed. Section 6 summarizes the contents of this paper.

2 Related Works

In recent years, the moving target defense (MTD) proposed by the US Science and Technology Commission has attracted much attention as a new cybersecurity mimicry defense technology [1]. Moving network technology, as one of the most critical technologies for MTD at the network layer, has a promising application prospect in active defense.

A suitable communication path transformation strategy is crucial for implementation in moving networks. The communication path transformation strategy is used to generate a network management configuration of nodes that are used during the subsequent adjustment period. The randomness of the configuration increases the difficulty for the attacker in predicting the network management configuration. Recently, the pseudorandom approach has been extended to address the transformation strategy of moving networks. Atighetchi et al. [5] proposed a virtual port address association scheme for the client association proxy and a network address translation gateway to fill fake random addresses and ports into the corresponding fields of the data packet. Then, the data stream is redirected to defend against the attack. Once an "expired" node network management configuration is used, the possibility of detection will increase. Antonatos et al. [6] established a method for randomizing the network address space based on a transparent address association, which performs a header address translation of data stream packets. This approach maintains the novelty of the address translation table and prevents connection requests outside the service period. Badishi et al. [7] developed a random port association mechanism termed random port hopping (RPH). In this paper, the author designed a robust communication protocol to spread the impact of attackers. This protocol calculates the next association based on the number of successfully transmitted data packets and a shared private key. The port information is synchronized by sending an Acknowledgement (ACK) confirmation message. In 2012, Jafarian et al. proposed an OpenFlow random host mutation (35) [9] based on OpenFlow. The authors used OpenFlow to transparently change the IP address of the host to ensure the consistency of the host configuration. Aimed at the problems of limited hopping space in IPv4 and fixed hopping period, Dunlop et al. [16, 17] proposed moving target defense mechanism based IPv6 (MT6D). In order to enlarge the hopping space, IPv6 address space is adopted. Besides, MT6D uses pseudo-random number to set hopping period so as to improve the randomness. In 2014, Jafarian et al. [8] associated a host IP address with an address block with a short lifetime. The authors proposed a random association method based on the time and space domains to block, spoof and detect attackers. In 2015, MacFarland et al. [18] hide the link, IP, and port numbers of endpoint by setting up DNS hopping controller so as to prevent the leakage of MAC address. In 2016, Skowyra et al. [19] proposed network identity elimination mechanism called PHARE. It prevents MAC address leakage by randomly transforming header when packets flow out of the endpoint. Moreover, Sun et al. [20] proposed Decoy-Enhanced Seamless IP Randomization (DESIR) to increase the unpredictability. When unauthenticated nodes access the platform, DESIR uses honeypots to observe its behavior. When the user is judged as the attacker, DESIR prevents attack by changing endpoint information of node providing service and

increasing the number of honeypots deployed. In order to prevent service interruption, DESIR separates the network identifier and transmission identifier of endpoint when it migrates services, thus ensuring the continuity of service provision by reserving the transmission identifier. Pseudorandom functions are exposed to higher security; however, it is possible that the node network management configuration will collide, in which case, scalability is not desirable.

In general, the implementation of the current moving network technology is simple, but there are several shortcomings: (1) The moving network adjustment strategy needs to compress or amplify the state space of the available node network management configuration. However, current methods with a pseudorandom function have a single control factor, and the generated space of the node network management configuration is difficult to accurately control. Thus, the scalability of the algorithm is weak. (2) In the existing literature, moving network adjustment strategies primarily focus on static and fixed methods. These approaches cannot be adaptively adjusted in combination with the current network security status.

Therefore, this paper proposed a moving network active defense technology based on network topology mimicry correlation, with the consideration of high security and real-time requirements of data interaction in an edge computing network.

3 Secure Transmission Model Based on Network Topology Mimic Association

3.1 Framework

The proposed model deploys the network topology mimicking association agent in the primary station system and the sensor node. The structure of the model is shown in Fig. 2.

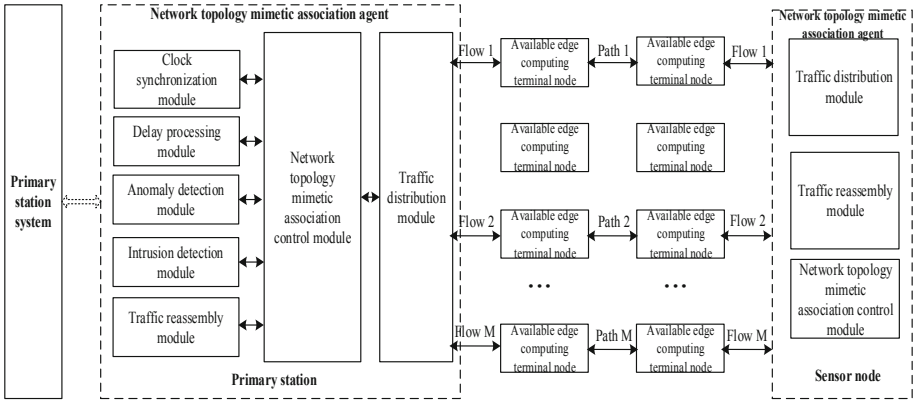

Fig. 2. Model of active defense for edge computing network data interaction

- The network topology mimicking association agent module is essential. This module controls other modules and available associated communication nodes, coordinating the communication path between the sensor node and the primary station service node server. This module generates a moving communication path alliance, and after the sensor node and the primary station server node negotiate the network topology mimetic map, the time synchronization module is used to calibrate the local clock and to enter the network topology mimetic association communication mode.
- The traffic distribution module allocates traffic according to the established communication path. The data legally sent by sensor nodes are transmitted to the proxy control module through the currently active communication path. Then, the data are sent to the primary station service node by the traffic reorganization module. The server is also returned to the client by passing the traffic distribution module and the active path node.
- The delay processing and anomaly detection modules sample the network data stream to evaluate network anomalies and delays. The associated agent control module dynamically changes the mimetic mapping configuration of the network topology and the moving communication path alliance according to the evaluation results by using a self-tuning strategy.
- The intrusion detection module detects intrusion based on the redundancy voting mechanism of the mimicry defense model for the edge computing terminal. By comparing the execution results of the heterogeneous redundant execution body, result deviations and network intrusion behavior can be identified.

The moving communication path alliance and the network topology mimetic association graph in the network topology mimetic association model change by using an adaptive strategy. This action increases the diversity and randomness of transmission throughout the entire edge computing network and increases the defense strength. In addition, only the available edge computing terminal nodes in the active period can be activated at any time. Each available edge computing terminal node is allocated a node association configuration for the communication path, which will further reduce the possibility that the system communication process will suffer from a network attack.

3.2 Process of Network Topology Mimetic Secure Transmission

This section designs the network topology mimetic association protocol flow. In this step, the server and the client determine the network topology weighted directed graph by negotiation and generate the corresponding network topology mimetic association graph. Then, the client pseudo-randomly selects the communication path alliance. The communication parties are allowed to establish independent transport layer connections on multiple dynamic communication paths. In this manner, they can communicate safely according to the established communication path. This process is shown in Fig. 3.

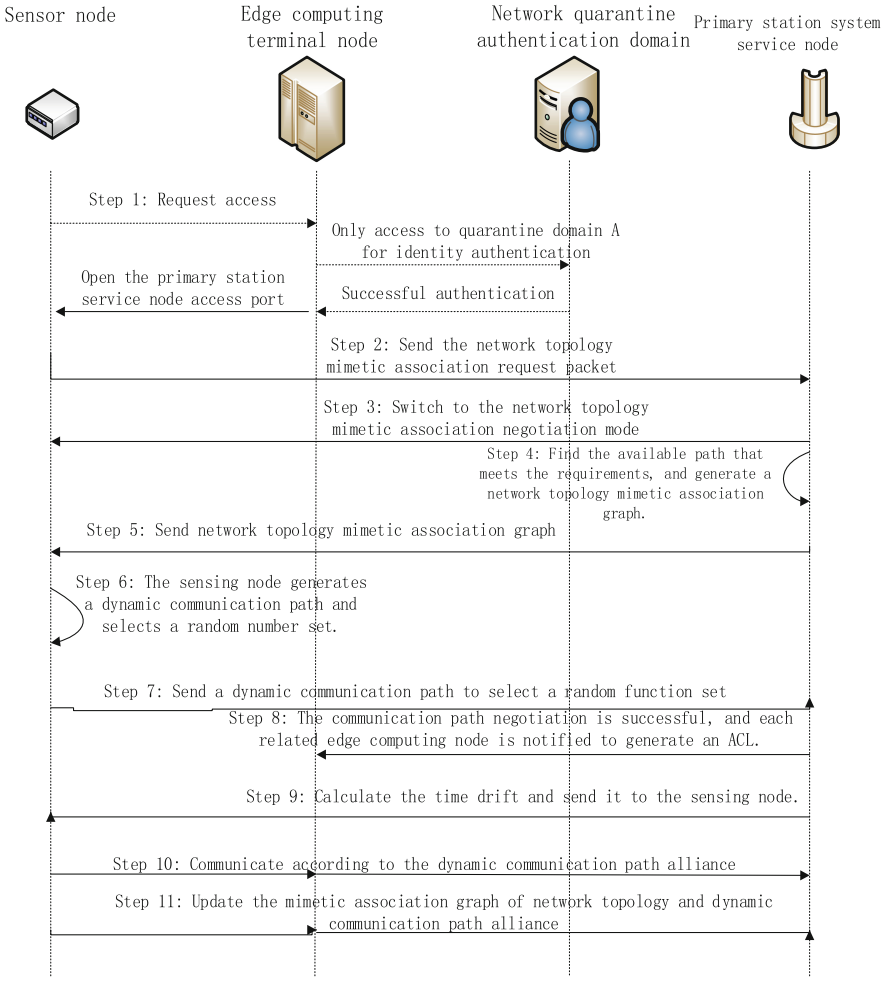

Fig. 3. Network topology mimetic association protocol

Step 1: When a sensor node supporting the network topology mimicking association accesses the edge access network for the first time and prepares to communicate with the primary station system, direct access will be denied. Because the edge computing terminal node does not control the related network access for data transmission, the sensor node can access only quarantine authentication domain A for identity authentication and trust evaluation. However, once the node authentication and trust evaluation are successful, the edge computing terminal node will open the network access port of the primary station service node.

Step 2: The sensor node sends the regular request message Req$\{ID_c, Ip_c, ReqID, p_{lower}, mark, T_1\}$ to the primary station node. ID_c is the identity of the sensor node, Ip_c is the IP address of the sensor node, and $ReqID$ is the

corresponding unique ID of each Req message. p_{lower} is the minimum reliability requirement, *mark* is the support flag of the network topology mimetic association, and T_1 is the time.

Step 3: The primary station service node records the time T_2 at which the message *Req* is received. If the server does not support the network topology mimetic association, the message can be ignored. If the association is supported, the primary station service node switches to the network topology mimetic association negotiation mode.

Step 4: The primary station service node initiates a deep search algorithm to find an available path that satisfies p_{lower} between the sensor nodes. Then, a network topology weighted directed graph is generated. Let us use $p_{i,j}$ to denote the path reliability between the connecting nodes i and j. $p_{s,t}^k$ denotes the path reliability of the kth path between the primary station serving node s and the sensor node t at time t. In this case, $p_{s,t}^k = \prod_{(i,j)\in k} p_{i,j}$, and $p_{s,t}^k$ should be greater than p_{lower}.

Step 5: The primary station service node generates a corresponding network topology mimetic association graph $S_i = \{s_k | 1 \le k \le m\}$ based on the network topology weighted directed graph. Next, a response message $\mathrm{Rsp}\{ID_s, S_i, T_3\}$ is sent to the sensor node, including the server identity ID_s, the network topology mimicking association graph S_i, and the response packet sending timestamp T_3.

Step 6: The sensor node records the time T_4 at which the message $\mathrm{Rsp}\{ID_s, S_i, T_3\}$ is received. At the same time, the sensor node generates $\Phi_{i1}, \Phi_{i2}, \Phi_{GS}$ by a random function to determine the network topology mimicking dynamic communication path alliance $GS_i(t)$ and the communication path node association network configuration space $\Omega_i(t)$.

Step 7: The sensor node sends a response message $\mathrm{Rsp}\{ID_\mathrm{c}, \Phi_{i1}, \Phi_{i2}, \Phi_{GS}, T_5\}$ to the primary station serving node.

Step 8: The primary station serving node receives the packet $\mathrm{Rsp}\{ID_\mathrm{c}, \Phi_{i1}, \Phi_{i2}, \Phi_{GS}, T_5\}$ and records the time at which the packet is received as T_6. Then, a corresponding ACL is sent to notify all edge computing terminal nodes on the communication path with Ip_c and $\Omega_i(t)$ together.

Step 9: The primary station service node calculates the time drift $\theta = (T_2 - T_1 + T_3 - T_4 + T_6 - T_5)/2$ according to the timestamps T_1 , T_2 , T_3 , T_4 , T_5 , T_6 and sends θ to the sensor node.

Step 10: The primary station service node adjusts the local time according to the time drift θ by synchronization correction. The sensor node and primary station node implement secure communication according to the established dynamic communication path alliance.

Step 11: When any life cycle of the network topology mimicry, T_S^i or T_{GS}^i, ends normally or abnormally at the end of the network attack, the network topology mimetic association is re-updated.

4 Mimetic Transformation Method

4.1 Communication Path Alliance Mimetic Transformation Method

Cyber-attacks necessitate a process of scanning, lifting, destroying, and so on. Before some of the preliminary steps are completed, the attack does not pose a real threat to the entire system, but it does cause network anomalies to a certain degree [12, 13]. Therefore, in this section, the communication path is adjusted based on a network anomaly metric. When the network anomaly metric exceeds a certain threshold, the moving communication path will be adjusted automatically.

The dynamic adjustment of the life cycle of the moving communication path alliance must meet the principle of "increase slowly and decrease rapidly". That is, when no network abnormality is detected and the probability a network attack is small, the survival time of the moving communication path alliance of the next association cycle slowly increases. Moreover, as the duration of the non-attack state increases, the growth rate of the current moving communication path alliance should also increase to improve the quality of the communication service. When a network abnormality is detected and the probability of a network attack is substantial, the survival time slot of the active communication path alliance in the next period is rapidly reduced. As the abnormal state duration increases, the reduction range of the survival time slot of the active communication path alliance in the next cycle should also increase to ensure communication security [23, 24].

Here, let us assume that $\sigma'_{t,f}$ is the standard deviation at time t and δ' is the threshold for a network outlier. Based on expert experience, this method chooses a function that meets the principle of "increase slowly and decrease rapidly", i.e.,

$$g(\sigma'_{t,f}) = \begin{cases} g_1(\sigma'_{t,f}), & 0 < \sigma'_{t,f} \le \delta' \\ g_2(\sigma'_{t,f}), & \sigma'_{t,f} > \delta' \end{cases} \tag{1}$$

with $g_1(\delta') = g_2(\delta')$, $g'_1\left(\sigma'_{t,f}\right) < 0$, $g'_2\left(\sigma'_{t,f}\right) > 0$, $g'_1\left(2\delta' - \sigma'_{t,f}\right) + g'_2\left(\sigma'_{t,f}\right) > 0$. The active adjustment strategy is

$$T_{GS}^{i+1} = \begin{cases} (1 + g_1(\sigma'_{t,f})) * T_{GS}^{i}, & 0 < \sigma'_{t,f} \le \delta' \\ (1 - g_2(\sigma'_{t,f})) * T_{GS}^{i}, & \sigma'_{t,f} > \delta' \end{cases} \tag{2}$$

4.2 Transformation Method for the Network Topology Mimetic Association Graph

When there is a given sequence of observed symbols, the hidden Markov model is suitable to predict the probability of occurrence of a new observed symbol sequence. The hidden Markov model is a stochastic process of the relationship between the observable variable O and the hidden variable S. It is very similar to the abnormal metric (hidden state) and the security state (observable state) of the security situation system [25, 26]. Therefore, using the hidden Markov model can well analyze the network security situation.

Here, this section proposes a hidden Markov based reliability prediction model of network security to realize a network security reliability prediction based on network security anomaly metric data. Based on the security reliability prediction results, the proposed method expands or compresses the network topology mimetic association graph and set a reasonable survival time slot T_S^i for the network topology mimetic association graph.

Network Security State Prediction Based on the HMM

The HMM can be described by a quintuple $\lambda = (N, M, \pi, A, B)$. In this quintuple, N indicates the number of possible hidden state values in the HMM, which can be recorded as $IS = \{IS_i | 1 \le i \le N\}$. Each hidden state value IS_i corresponds to M observable states O, which is recorded as $O = \{O_i | 1 \le i \le M\}$. Here, π is a $1 \times$ N-order initial probability distribution matrix, indicating the initial probability distribution of the hidden state q_1 for each possible hidden state value for the observable sequence O at time t = 1, $\pi_i = P(q_1 = IS_i), 1 \le i \le N$

$A = (a_{ij})_{N \times N}$ is a hidden state probability transfer matrix for Markov chains. For a first-order HMM,

$$a_{ij} = P(q_{t+1} = IS_j | q_t = IS_i), \sum_{j=1}^{N} a_{ij} = 1, 1 \le i \le N, 1 \le j \le N \tag{3}$$

$B = (b_{im})_{N \times M}$ is a probability matrix of the observed indicators, and the observed probability is $b_{im} = P(O_t = v_m | q_t = IS_i), 1 \le i \le N, 1 \le m \le M$.

To predict the security reliability of all accessible paths in the network topology mimetic map, the network security reliability hidden state levels are classified into five categories: safe, mild, general, moderate, and high-risk, expressed as $IS_1, IS_2, IS_3, IS_4, IS_5$ and assigned to 1, 2, 3, 4, and 5, respectively. Then, the reliability of each accessible path is transferred at a given probability in these five states. At the same time, the network security reliability of each path is defined by two observable indicators, the network transmission efficiency TE and network threat TH. The reliability is expressed as a random variable $x_i (1 \le i \le 2)$. The current security reliability of the entire network is measured from two different dimensions. Then, after time t, the observation sequence $O = \{o_1, o_2, \cdots, o_t\}$ is obtained from observation x_i.

Mimetic Transformation Strategy for the Network Topology Mimetic Association Graph

In the network topology mimetic correlation graph, it is assumed that there are n available nonintersecting paths at time t being assessed as medium-risk or high-risk paths at time $(t+1)$ in forming the network topology mimetic map $S_n^-(t+1)$. At the same time, there are m non-usable and nonintersecting paths at time t being assessed as safe, mild or general risk at time $(t+1)$ for the network topology mimetic association graph $S_m^+(t+1)$. Thus, the next network topology mimic map is $S_i(t+1) = S_i(t) - S_n^-(t+1) + S_m^+(t+1)$.

At time $(t+1)$, the new path $S_m^+(t+1)$ will be added; if this path is selected as the communication path, only the primary station serving node needs to notify the edge computing terminal node on the path with the relevant ACL and other information,

according to the network topology mimetic association negotiation algorithm. However, for the communication path $S_n^-(t+1)$ at time t, the primary station service node needs to notify the relevant parties to revoke the ACL and other information.

After the network topology mimetic map is adjusted at the completion time $(t+1)$, there will be a new map $S_i(t+1) = \{s_k(t+1) | 1 \le k \le m\}$. Then, the overall reliability prediction value corresponding to $S_i(t+1)$ can be obtained as $SA_{S_i(t+1)} = \sum_{i=1}^{m} Sp_{t+1}^i$. The function is then updated, satisfying the principle of "increase slowly and decrease rapidly".

$$h(SA_{S_i(t+1)}) = \begin{cases} h_1(SA_{S_i(t+1)}), & SA_{S_i(t+1)} = 1 \\ h_2(SA_{S_i(t+1)}), & SA_{S_i(t+1)} \in (2,3) \end{cases} \tag{4}$$

The self-adjusting strategy is as follows:

$$T_S^{i+1} = \begin{cases} (1 + h_1(SA_{S_i(t+1)})) * T_S^i, & SA_{S_i(t+1)} = 1 \\ (1 - h_2(SA_{S_i(t+1)})) * T_S^i, & SA_{S_i(t+1)} \in (2,3) \end{cases} \tag{5}$$

5 Experiments

The experiment performs a system simulation of the network topology mimetic association algorithm based on the NS2 network simulation environment. This model uses C++ to write the synchronization module, association module, communication module, attack module, delay processing module, sampling module, anomaly detection module, and deception processing module, and implements the network topology simulation by writing an OTcl script. The number of available IPv4 addresses in the network is 28, and the number of available ports is 1000. The initial correlation period is 120 s. We suppose that $g_1(x) = -ln(20x + 0.5)$, $g_2(x) = 16x^2 - 0.8x + 0.01$, $h_1(z) = -ln(20x + 0.6)$, $h_2(z) = 16z^2 - 0.64z + 0.064$. To mention that the simulation experiments are conducted in different scenarios with the same resources. The simulation results are shown in Figs. 6 and 7.

5.1 Security Analysis

Security is an important indicator for evaluating the advantages and disadvantages of a defense method. This section analyzes the anti-attack capability of the proposed active defense technology for an edge defense network attack based on network topology mimetic correlation. The active defense principle for edge computing network attacks based on the network topology mimetic association algorithm is shown in Figs. 4 and 5.

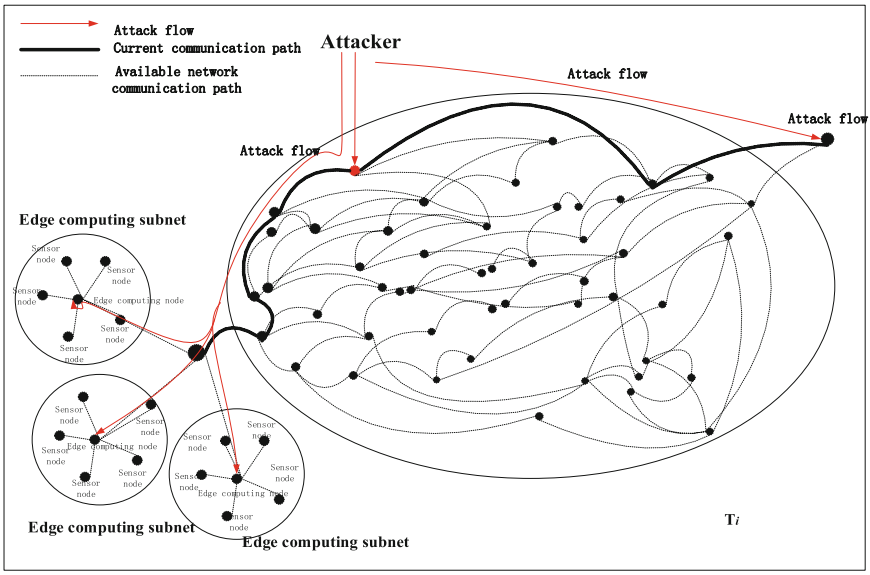

Fig. 4. Defense before network topology mimetic correlation

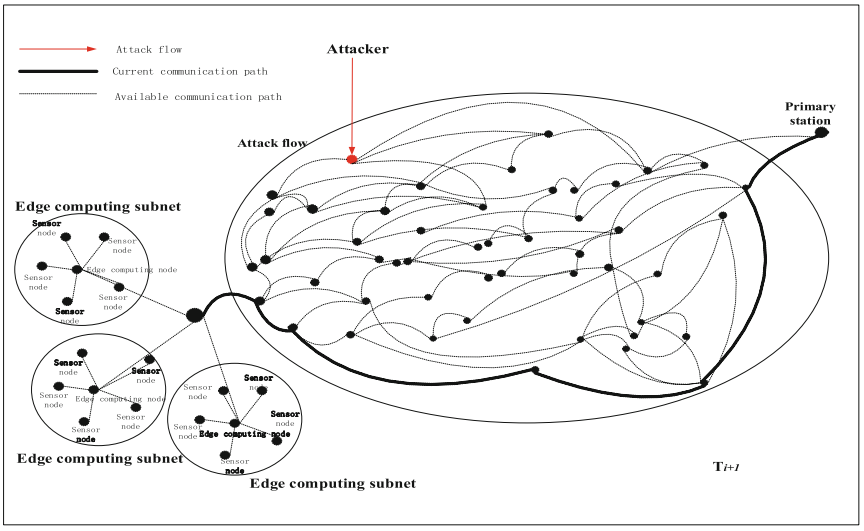

Fig. 5. Defense after network topology mimetic correlation

- DDos attacks

After the network topology mimetic association defense strategy is implemented, the IP address and port of the communication host and the protocol used by the communication parties will be associated after each corresponding time slot. For an attacker who performs a DoS attack, it is necessary to continuously send a large

number of service requests to the target host and consume the target host resources. However, the node network configuration of the target host is continuously associated; thus, a DoS attack cannot be initiated [27].

- Anti-semi-blind attacks

A blind attack occurs when an attacker cannot locate the current active node network configuration and attacks all available nodes of the node network configuration state space that are detected. The attack strength is evenly distributed across all available nodes. The network topology mimetic association algorithm further increases the difficulty for an attacker to detect and locate the current active node network configuration of the associated system, and thus, the ability to resist and anti-semi-blind attacks is improved [28].

5.2 Experiment Against DDoS Attacks

In this section, the SYN-Flood mode is used to guide a DoS attack. Experiments test the average service response time of the network topology mimetic association system under different SYN-Flood attack rates to reflect the service availability performance. Figure 6 shows results for the non-topology-association algorithm (No NTAA), the simple topology association algorithm (Simple NTAA), the end-hopping-based topology association algorithm (EH NTAA) proposed in [10, 11], and the network topology mimetic association (PA NTAA) proposed in this paper. The results show that the network topology mimetic association strategy proposed in this paper can better resist DoS attacks. This result occurs because the mimetic correlation technology of the network topology dynamically measures network anomalies according to the strength of cyber attacks. Then, the network topology mimetic maps and communication paths are automatically adjusted. Adjustments increase the difficulty of hitting a path for DDoS attacks. However, the difference between the results for the association strategy in EH NTAA and PA NTAA is not significant. Moreover, when the mimetic map space of the network topology is compressed to almost zero, the DDoS attack enters an unsupervised blind attack state, that is, an average attack on all nodes in the accessible path detected by the attacker.

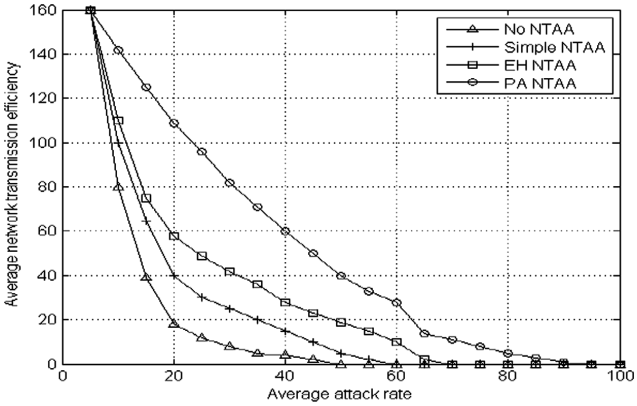

Fig. 6. Results for DDoS attack defense test

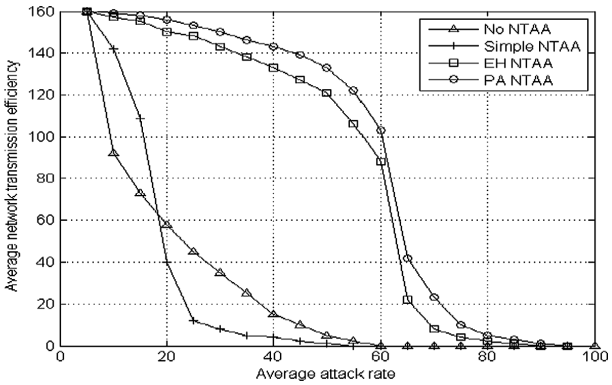

Fig. 7. Results for semi-blind attack defense

5.3 Experiment Against a Semi-blind Attack

Here, it uses a perceptual node edge access system with 20 communication paths for experiments. It can be seen from Fig. 7 that when the edge of the access node is connected to the network, the network transmission delay increases rapidly as the proportion of the received attack path reaches 50%. When the proportion exceeds 60%, the network transmission delay tends to infinity. The average response time of the EH topology association strategy is better than that of the No NTAA but is not as good as that of the Simple NTAA, which is consistent with the analysis presented in [10]. The average response time of the PA NTAA is better than that of the Simple NTAA.

6 Conclusion

Based on a thorough study of the mobile self-organizing characteristics of edge computing networks, this paper combines a moving network transmission with path mimicry adjustment techniques to propose a strict, formal description and definition. An active defense framework for data transmission in an edge computing network based on a link layer and application layer network topology mimetic correlation is designed to ensure scalability of the algorithm. To solve the problem of attacks and to improve defense and transmission quality with a moving periodic adjustment of the network, this research proposes a moving communication path alliance and a mimetic map dislocation transformation method for network topology. Starting from the temporal and spatial dimensions, the model combines moving threshold network anomaly detection and reliability prediction of network security based on the HMM. In this way, the experiment can perform a reasonable transformation of the network, minimize the mimetic adjustment overhead and resolve active defense problems in a DDoS attack and semi-blind attack. Experimental results show that the transmission efficiency of the network topology mimetic association algorithm proposed in this paper is higher than that of other popular methods and the reliability and anti-attack performance are significantly improved.

References

1. Dunlop, M., Groat, S., Urbanski, W., Marchany, R., Tront, J.: MT6D: a moving target IPv6 defense. In: Military Communications Conference, 2011 – Milcom, pp. 1321–1326. IEEE (2012)
2. Bunz, M., Meikle, G.: The internet of things. Sci. Am. **4**(1), 20–25 (2018)
3. Roman, R., Lopez, J., Mambo, M.: Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges. Future Gener. Comput. Syst. **78**(2), 680–698 (2018). S0167739X16305635
4. Wang, F., Xu, J., Wang, X., Cui, S.G.: Joint offloading and computing optimization in wireless powered mobile-edge computing systems. IEEE Trans. Wirel. Commun. **17**(3), 1784–1797 (2017)
5. Atighetchi, M., Pal, P., Webber, F., Jones, C.: Adaptive use of network-centric mechanisms in cyber-defense. In: IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, pp. 183–192. IEEE (2003)
6. Antonatos, S., Akritidis, P., Markatos, E.P., Anagnostakis, K.G.: Defending against hitlist worms using network address space randomization. In: ACM Workshop on Rapid Malcode, pp. 30–40. ACM (2005)
7. Badishi, G., Herzberg, A., Keidar, I.: Keeping denial-of-service attackers in the dark. IEEE Trans. Dependable Secure Comput. **4**(3), 191–204 (2007)
8. Jafarian, J.H.H., Al-Shaer, E., Duan, Q.: Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers. In: ACM Workshop, pp. 69–78. ACM (2014)
9. Jafarian, J.H., Al-Shaer, E., Duan, Q.: Openflow random host mutation: transparent moving target defense using software defined networking. In: The Workshop on Hot Topics in Software Defined Networks, pp. 127–132. ACM (2012)
10. Zhao, C.: Research on adaptive strategy of end information hopping system. Nankai University (2012)
11. Zhang, X., Niu, W., Yang, G., Zhuo, Z., Lv, F.: APT attack prediction method based on tree structure. J. Univ. Electron. Sci. Technol. China **45**(4), 582–588 (2016)
12. Haggerty, J., Shi, Q., Merabti, M.: Beyond the perimeter: the need for early detection of denial of service attacks. In: Computer Security Applications Conference 2002 Proceedings, pp. 413–422. IEEE (2002)
13. Zhang, J., Gunter, C.A.: Application-aware secure multicast for power grid communications. In: IEEE International Conference on Smart Grid Communications, pp. 339–344. IEEE (2010)
14. Li, H., Ota, K., Dong, M.: Learning IoT in edge: deep learning for the internet of things with edge computing. IEEE Netw. **32**(1), 96–101 (2018)
15. Ai, Y., Peng, M., Zhang, K.: Edge computing technologies for internet of things: a primer. Digital Commun. Netw. **4**(2), 77–86 (2018)
16. Dunlop, M., Groat, S., Urbanski, W., Marchany, R., Tront, J.: MT6D: a moving target IPv6 defense. In: Proceedings of the Military Communications Conference (MILCOM 2011), pp. 1321–1326. IEEE, Baltimore, November 2011
17. Dunlop, M., Groat, S., Urbanski, W., Marchany, R., Tront, J.: The blind Man's bluff approach to security using IPv6. IEEE Secur. Priv. **10**(4), 35–43 (2012)
18. MacFarland, D.C., Shue, C.A.: The SDN shuffle: creating a moving-target defense using host-based software-defined networking. In: Proceedings of the 2nd ACM Workshop on Moving Target Defense, MTD 2015, USA, pp. 37–41 (2015)

19. Skowyra, R., Bauer, K., Dedhia, V., Okhravi, H.: Have No PHEAR: networks without identifiers. In: Proceedings of the 2016 ACM Workshop on Moving Target Defense, MTD 2016, Austria, pp. 3–14 (2016)
20. Sun, J., Sun, K.: DESIR: decoy-enhanced seamless IP randomization. In: Proceedings of the 35th Annual IEEE International Conference on Computer Communications, pp. 1–9. IEEE INFOCOM, April 2016
21. Chen, J., Su, C., Yeh, K.-H., Yung, M.: Special issue on advanced persistent threat. Future Gener. Comput. Syst. **79**(Part 1), 243–246 (2018)
22. Yang, L.-X., Li, P., Yang, X., Tang, Y.Y., et al.: A risk management approach to defending against the advanced persistent threat. IEEE Trans. Dependable Secure Comput. **2018**, 1 (2018)
23. Wan, J., Chen, B., Imran, M., et al.: Toward dynamic resources management for IoT-based manufacturing. IEEE Commun. Mag. **56**(2), 52–59 (2018)
24. Wang, J., Cao, J., Ji, S., et al.: Energy-efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks. J. Supercomput. **73**, 3277–3290 (2017)
25. Liang, W., Long, J., Chen, Z., et al.: A security situation prediction algorithm based on HMM in mobile network. Wirel. Commun. Mob. Comput. **2018**, 241–257 (2018)
26. Wan, M., Yao, J., Jing, Y., Jin, X.: Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. Comput. Mater. Contin. **55**(3), 447–463 (2018)
27. Yan, Q., Huang, W., Luo, X., et al.: A multi-level DDoS mitigation framework for the industrial internet of things. IEEE Commun. Mag. **56**(2), 30–36 (2018)
28. Vaidya, P., Chandra Mouli, P.V.S.S.R.: A robust semi-blind watermarking for color images based on multiple decompositions. Multimedia Tools Appl. **76**, 25623–25656 (2017)