OpenHIP Random Host Hopping in Network Layer

Li Kechao [a], Xiong Xinli [b]

Graduate School,Army Engineering University of PLA,Nanjing, China

[a]kechaoli@yeah.net,[b]xxlyx25@hotmail.com

Keywords: moving target defense (MTD), OpenHIP, end-hopping, network security

Abstract. Reconnaissance of IP address and communication port is prerequisite to network attacks. Static configurations furnish great advantage for the intruder in discovering network targets and launching attacks. In this paper, we present a novel approach that turns end-hosts into unpredictable moving targets by transparently transform their IP addresses or ports intelligently and randomly without sacrificing network performance. OpenHIP is used to develop an MTD architecture that mutates real IP addresses of the host with a high rate or replaces a real port value in the packet with a dynamically changing virtual port. The presented technique is called Random Host Hopping (RHH). Our implementation and evaluation show that RHH can effectively defend against scanning-based attack and performed well in a practical network setup for moving target defense.

INTRODUCTION

Moving target defense confuses an attacker by implementing dynamic and untraceable changes to increase its attack cost and complexity and reduce the success rate of attack. The research on the theory and technology of moving target defense has made significant progress. MTD technology in the network layer is an essential content of moving target defense. The IP address and communication port is the fundamental property of communication between end-hosts, which is often easily hacking by attackers through information scanning and collection, so they are the most commonly used moving target defense objects. However, when hosts move (changes its IP address or communication port), the communication parties will not be able to send or receive data on the original communication link, resulting in communication interruption.

HIP protocol proposed by Robert Moskowitz [1] solves the problems of host mobility, multi-hosting, and security. A new encrypted namespace, Host Identifier (HI), is introduced. There are three Host identifiers: Host Identifier (HI), Host Identifier Tag (HIT) and Local Scope Identifier (LSI), which can uniquely identify every host connected to the Internet globally. HIP protocol adds a host identity layer in the transport layer and network layer to separate the transport layer from the network layer. The host identity layer completes the host identifier and IP address conversion in the packet. The network layer is shielded from the transport layer, and any changes in the network layer (for example, changes IP address during communication) do not affect the transport layer link.

In this paper, we propose a novel proactive moving target defense, called *Random Host Hopping (*RHH*),* which carries out network layer moving target defense in end-hosts, which is compatible with the traditional network and does not need to transform existing network intermediate equipment. For end-hosts, the HIP protocol is implemented in OpenHIP project, in which protocol stack is expansion virtually and is easy to deploy with not change the kernel. We transform the host identity layer to the MTD controller layer by modifying OpenHIP, so IP hopping and port hopping is added.

The rest of the paper is organized as follows. Section II describes the related works. In Section III the RHH architecture is described. Section IV describes security analysis. Section V presents implementation and evaluation, and Section VI concludes the paper.

  DOI: 10.25236/icemit.2019.048

RELATED WORK

Given the asymmetry of network attack and defense, the U.S. network and information technology research and development plan proposed the idea of moving target defense [2]-[4]. Inspired by military frequency hopping, Shi Leyi et al. proposed an end-hopping model [5]. In terms of network address hopping technology, research results such as APOD [6], NASR [7], DyNAT [8] and RHM [9] have appeared. Ehab ai-shaer et al. proposed the OF-RHM model on the basis of RHM [10].

At present, MTD technology based on OpenFlow/SDN [11] in the network layer is most representative. Reference [9] uses virtual IP as the network address and dynamically changes virtual IP to realize the hiding of communication information. On the basis of [9], reference [10] realized IP hopping combined with low and high frequency, and reduced the burden of IP hopping on OpenFlow switch. By deploying moving target defense components, reference [11] provides all-around protection for intra-domain communication of the internal network and cross-domain data transmitted over the Internet.

In general, current theories and technologies are still in the research stage, lacking mature products and technical solutions. By integrating the host mobility idea of HIP protocol for reference, a novel solution for random host hopping is proposed. Different from OpenFlow-based end-hopping on the path of data transmission, RHH does not need to modify the internodes, and the change is implemented in the terminal, which can disperse the pressure of network traffic and effectively reduce network congestion. The protocol stack changes as shown in Fig.1. Applying the security policy of information encryption and access control, adopting the technology of end-hopping and authentication, transforming service mode dynamically, changing from the traditional static target defense to the multi-dimensional space target defense, RHH could build a secure and reliable network environment and form the risk control system for moving target defense.

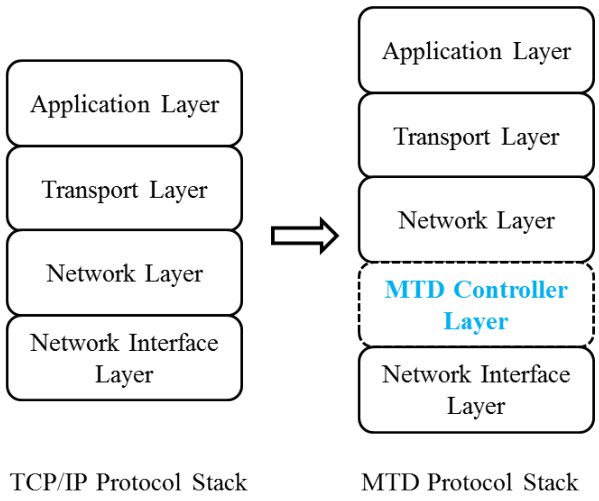

Figure 1 MTD protocol stack

RHH ARCHITECTURE

A. *Architecture*

The RHH consists of four modules: Server, Client, HDNS and Management platform.

- Server consists of three functional modules: end-hopping, service provision, and identity authentication. It maintains a trusted client list for identity authentication and provides the client with regular service and end-hopping service. The server type includes a Web server, database server and so on.
- Client is composed of three functional modules: end-host information processing, communication, and identity authentication. After two-way identity authentication, Client communicates with the Server.

- HDNS provides addressing for Client initially connecting Server, including three functional modules: server registration, server address update, and service provision.
- Management platform is the control system, which realizes the man-machine interaction of RHH, and consists of two functional modules: situation presentation and state control. The management platform controls the hopping strategy of Server by the instruction according to the network situation presentation.

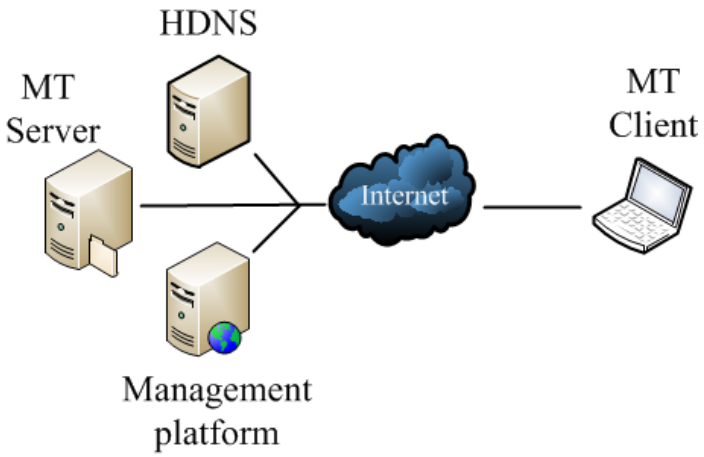

Figure 2 The Architecture of RHH

As shown in Fig.2, RHH is deployed in the WAN environment, which constitutes a virtual Intranet, and the communication parties deploy defensive agent plug-ins to form the communication channel of the Intranet. End-hopping and identity authentication technology achieve protection for Server. Server first registers with the HDNS to record the domain name, IP address, and ports for Client to inquire. When Client accesses Server, it first initiates IP address query to HDNS, and then conducts two-way authentication with Server, establishes a connection with the server and makes service request. The server verifies the identity of the other party according to the white list of Client. Management platform communicates with Server to achieve the purpose of data collection and configuration management. According to the policy rules of Management platform, Server dynamically changes the IP address and ports to realize the moving target defense.

B. *Protocol*

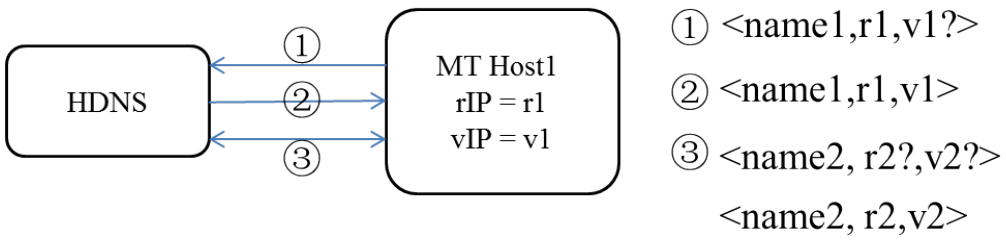

Figure 3 Register before communication

Hopping information is generated by the pseudo-random function, whose general form is $e=f(I, K)$, e is the end-host information, f is the pseudo-random function, I is hopping mode, and K is hopping factor. Hopping period $p=g(c, q, r)$, g is a mapping function, c is the current network traffic condition, q is the network risk coefficient, r is the security requirement of data transmission. The hopping period p significantly affects the feasibility of this technique. When p is too small, that is, the hopping frequency is too fast, the network communication spends much time on establishing and releasing the connection, which affects the communication efficiency. When p is too large, the low hopping frequency will leave sufficient time for the attacker to track the IP address and port, making the end-hopping technology fails to play its due role. According to the network environment, Management platform is used to configure a reasonable hopping period and hopping strategy.

The general algorithm of RHH hopping and update is presented in Algorithm 1.

Algorithm 1 RHH hopping and update algorithm

connection$_k$ < IP_i , IP_j, $Port_i$, $Port_j$, $Policy_k$ >
receive $Policy_k$ from Management platform
determine hopping ranges.
for all packets p_i to $Host_j$ **do**
  while system time t arrival hopping interval T
  do
    if $Policy_k$ is IP hopping **then**
      action IP_i `:= f (I, K)
      update connection < IP_i `, IP_j, $Port_i$, $Port_j$, $Policy_m$ >
      send UPDATE message to HDNS
      send UPDATE message to HOST$_j$
    else if $Policy_k$ is Port hopping **then**
      action $Port_i$ `:= f (I, K)
      update connection < IP_i, IP_j, $Port_i$`, $Port_j$, $Policy_m$ >
      send UPDATE message to HOST$_j$
    endif
  end while
    if $Policy_k$ is IP hopping **then**
      modify IP_i ->IP_i` *in packet* p_i
    else if $Policy_k$ is Port hopping **then**
      modify $Port_i$ ->$Port_i$` *in packet* p_i
    endif
end for

As shown in Fig.3, MT Host1 first registers its IP address with HDNS. MT Host2 is the legal client for installing the defense agent plug-in and is on MT Host1's whitelist. When MT Host1 accesses MT Host2, it first sends the query packet to HDNS to get the IP address of MT Host2. Then MT Host1 establishes a connection with MT Host2 through four handshakes. When the IP address changes(MT Host1 is in the mode of hopping service), UPDATE message is sent to inform MT Host2 of its latest IP address. Next communication uses the new IP address.

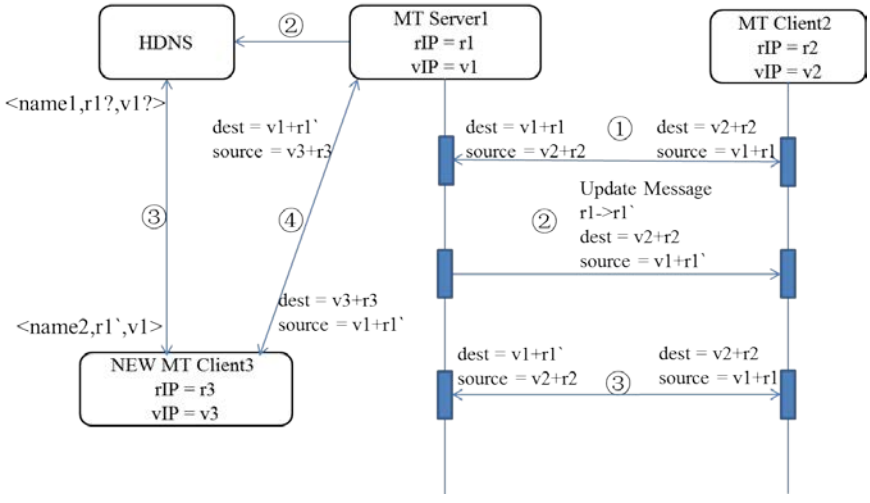

Figure 4 Communicating with moving hosts through IP

An UPDATE message is adopted as a synchronization mechanism. An UPDATE message is similar to ACK message but does not require strict time synchronization. As shown in Fig.4, hopping information is placed in the UPDATE message, which is easy to implement for the session-based end-hopping technology. When the IP address changes, MT Host1 sends UPDATE message

to the established MT Host2 to update the address, to keep the existing connection uninterrupted. Meanwhile, MT Host1 sends the latest IP address to the HDNS to update the address, to ensure that MT Host1 is properly addressed when the new host firstly connects. When port changes, only the UPDATE message is sent to the host that has established the connection. The message contains the hopping factor of the port hopping algorithm, and receiver calculates the new port value according to the hopping factor. The new port is used in the next communication. During synchronization, since the attacker does not deploy the defense plug-in, he will not be able to receive the UPDATE message. Even if the UPDATE message is intercepted, it is difficult for the attacker to decipher the UPDATE message within the effective time because the ciphertext decoding needs time and the port synchronization only transfer the hopping factor.

C. *Defense proxy plug-in*

The defense agent plug-in structure is shown in Fig.5. Communicate with the upper application through the API interface provided up to receive data from user space; Server parses the defense commands from Management platform through the command interface and determines the service mode and hopping strategy. Differently, from Server, there is no command interface in the defense proxy plug-in of Client. The communication interface is used to transfer the processed data to the network protocol stack. The plug-in includes a communication module, end-hopping (processing) module, UPDATE module, and an encryption/authentication module.

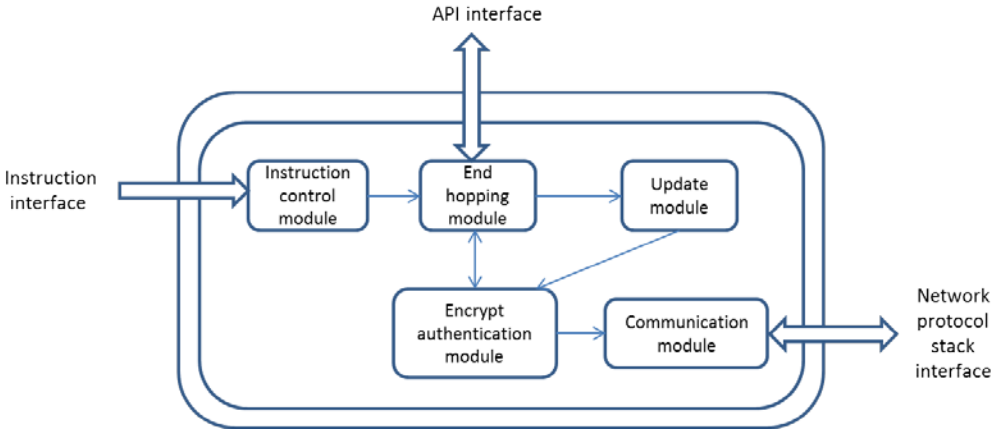

Figure 5 Defense agent plug-in structure

Communication is based on TAP virtual network equipment, which changes the traditional data exchange mode and the underlying communication logic and adds four handshakes to establish the connection and two handshakes to release the connection. The connection must be established before sending the communication data. During the connection process, the identity of the other party is authenticated and the symmetric key used by the encryption module is negotiated.

End-hopping realizes the hopping of IP addresses and ports. The result of the instruction module parsing controls the simultaneous or single hopping of IP address and port. The IP address can be selected as one of the three random factors (time factor, a random number of the system and self-input number) for hopping to change the real IP address of the host dynamically. By modifying the port field in the packet, the dynamic change of the port field in the packet is realized without changing the real port of the host.

UPDATE is responsible for the synchronization of end-host information. When the IP address and/or port changes, UPDATE module is triggered and the UPDATE message is sent to transmit the hopping information.

Encryption/authentication realizes data confidentiality, integrity, and non-repudiation, and cooperates with the end-hopping module. The AES algorithm is used to encrypt UPDATE messages, and the Diffie-Hellman key exchange algorithm is used to determine the symmetric key used in the process of establishing the connection, and the public key of the public/private key pair is used to identify the host uniquely. The sender signs the data with the private key and the receiver verifies the authenticity of the data source with the public key.

SECURITY ANALYSIS

Security is an important index to reflect the availability and effectiveness of this technology. This section analyzes the ability to resist common network attacks and analyzes explicitly the anti-scanning attack and anti-dos attack performance.

We propose a variable network architecture that changes IP addresses or ports of designated moving target (MT) hosts randomly and frequently so that the attackers' premises about the network fail. The goal of hopping is to make hosts untraceable via network reconnaissance attacks. However, developing an efficient and practical scheme that can be deployed on general networks requires careful consideration of tough challenges:(1) end-hopping must be transparent to the end-host to prevent interruption of communication connections; (2) the integrity of end-to-end Internet reachability should be maintained; (3) end-hopping should be fast and unpredictable to cheat attackers by excellently employing the whole available end-information range; (4) end-hopping should avoid service interruptions, delays and security violations; (5) RHM should be suitable to deploy in any existing networks.

Based on the asymmetric key scheme, the two sides of communication verify the identity in both ways to ensure the reliability of established connection and communication content, which is effective to prevent man-in-the-middle attacks and replay attacks. The pseudo-random hopping of end-host information increases the difficulty of continuous scanning or interception. Symmetric encryption of UPDATE message transmission makes it difficult for an attacker to decode the end-host information in a short time even if intercepted.

Outside of RHH, the attacker can sniff out the information of all active hosts in the target area within a certain time. The scanning time required is inversely proportional to the attacker's scanning ability *D* (sniffs per second). Suppose that the end-host information space in RHH is N and the end hopping period is *T*. Under the premise that the sniffer ability of an attacker remains unchanged, the success rate of a sniffer in each period:

$$\rho = \frac{D \times T}{N} \tag{1}$$

Attackers can sniff during the hopping cycle. Outside the domain of RHH, the end-host information does not hop, so the hopping period is infinite. The number of end-host information that an attacker can sniff the active host is N, and the attack success rate is 1. In the domain of RHH, the success rate of scanning can be effectively reduced when the hopping period T is shortened, or the end-host information space N is increased.

According to the result of scanning, the attacker can not attack the target accurately. At this point an attacker can launch a directed blind attack, that is, to launch a Dos attack for all the sniffed end-host information. Suppose the transmission rate of the attack packet is v and the average length of the packet is l. Attack intensity per unit time:

$$s = v \times l \tag{2}$$

Average attack intensity:

$$\hat{s} = v \times l / N \tag{3}$$

It can be seen that when increasing the end-host information space N, the more the end-host information, the smaller the average attack intensity per unit time. Table I describes the essential parameters of our formalization. The following is a description of these constraints.

Table I. Description of parameters

Parameters	Description
b_{ij}	whether range r_j is assigned to host h_i ($b_{ij} \in \{0, 1\}$)
c_{ik}	show if host h_i belongs to subnet s_k
R_i	minimum required hopping rate
r_j	hopping range
T	The interval during which a virtual IP must not be assigned to any host more than once.

Hopping Rate Constraint: Take IP as an example. The total number of hopping virtual IPs of all hosts in subnet s_k during period T must be less than the aggregate size of all ranges assigned to subnet s_k (Eq. 4). The required virtual IPs of a host h_i during one repetition period is $R_i * T$.

$$\forall k, \left(\sum_{1 \le i \le n} c_{ik} R_i \right) * T \le \sum_{1 \le j \le m} b_{jk} \left| r_j \right| \qquad (4)$$

Range Allocation Constraint: Each range must be assigned to precisely one subnet s_k (Eq. 5), because each range must be allocated to at least one subnet, while routing constrains us to assign each range to at most one subnet.

$$\forall j, \sum_{1 \le k \le n} b_{jk} = 1 \qquad (5)$$

IMPLEMENTATION AND EVALUATION

D. *Experimental deployment*

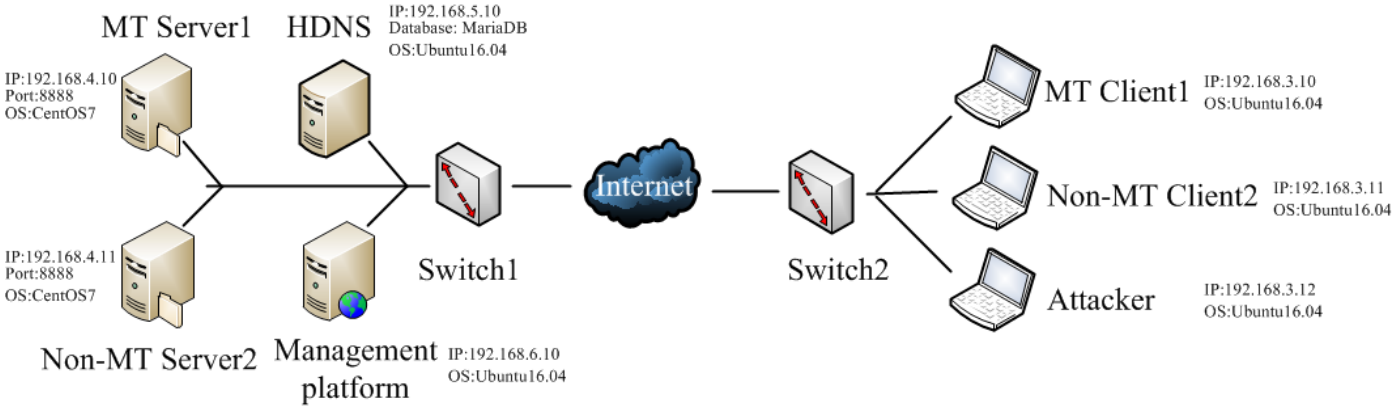

Figure 6 Experimental deployment

The experiment deploys a router and two LAN areas, as shown in fig. 6. Among them, LAN1 deploys 1 switch and 2 server nodes (only Server1 has the ability of moving target defense). LAN2 deploys 1 switch and 3 client nodes (only Host1 has the ability of moving target defense install defense agency plug-in, Host2 is a regular client, Host3 is an attacker). Server1 and Host1 constitute the virtual Intranet and use the Intranet channel for communication. In the above experimental setting, this section carries out three scenarios of experiments, which are whole-network communication experiment, anti-attack ability experiment and impact experiment on the original application performance, respectively testing the ability to resist scanning-based attack and the impact on the original application performance.

E. Whole-network communication experiment

In the experimental design, Server1 in LAN1 starts NC monitoring on port 8888 and starts IP hopping and port hopping. Host1 in LAN2 connects to port 8888 of Server1 for communication. Meanwhile, Host1 turns on Wireshark to sniff local packets.

The captured packets are shown in Table II. When the Serial Numbers in the table are 13 and 722 respectively, the IP address of Server1 is changed from 192.168.4.10 to 192.168.4.122 and 192.168.4.57. Server1 changes from port 8888 to ports 31424 and 31511. Host1 initiates the communication request to Server1 in different network segments. Although Server1 starts the change of IP and port, Host1 and Server1 can interact frequently and the whole network communication is not affected.

Table II. Captures the packet information

Sequence	***Source IP***	***Dest IP***	***Source port***	***Dest port***
13	192.168.3.10	192.168.4.122	14256	31424
722	192.168.3.10	192.168.4.57	14256	31511

F. Anti-attack ability experiment

As the first step of the attack, the first task of the attacker is to sniff the IP address and the open service port number of the active host to get the information for the target host. Server1 starts IP hopping, and Server2 does not. Attacker Host2 performs an Nmap scanning scan on the 192.168.4.0/24 network segment. Two experiments were conducted at different times, and the results are shown in Table III.

Table III. Scanning results

	Time	***Scanning results***	***Current IP***	***Scanning time***
Server1	t1	192.168.4.10	192.168.4.28	3.12s
Server2		192.168.4.11	192.168.4.11	2.91s
Server1	t2	192.168.4.61	192.168.4.102	2.50s
Server2		192.168.4.11	192.168.4.11	2.41s

As can be seen from the experimental results, Server1 starts IP hopping, and Nmap can detect its IP address forthwith. However, due to IP address periodic hopping, when Host2 attacks with this IP address, it is an invalid attack (which is related to the hopping period and preparation time of the attack). Without IP hopping enabled, Nmap can accurately sniff Server2's IP address and allow attacker Host2 to attack Server2 in the next step.

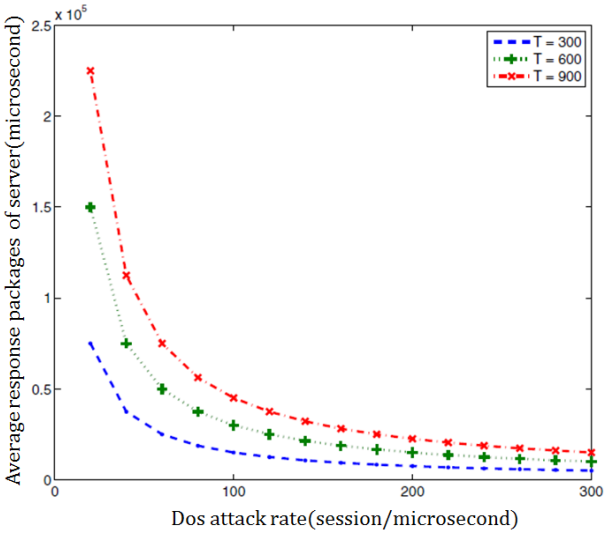

Figure 7 The response of server for DoS attack

Not only can UPDATE messages be encrypted, but the Management platform can also control Server to open encryption function for communication packets' confidentiality protection. The end-host information is hopping and the difficulty of decoding ciphertext significantly increases the complexity of the attacker to obtain the end-host information by intercepting the packet. Therefore, RHH in this paper can prevent sniffer and intercept attacks, and achieves the defense goal of hidden nodes.

In order to simulate the anti-dos attack ability of RHH, it is assumed that the attacker is ready to attack the server by scanning out the Server's end-host information at some time. The jmeter4.0 network tool is used to simulate the DoS attack on Server1 respectively. The server response probability is shown in Fig.7. The unit of *T* is millisecond.

In a connectivity Dos attack on Server1, the server responds fall quickly when jmeter4.0 sends data packets before a rate of 100 / ms. Server1 responds close to 0 when the data packet sending rate reaches 300 /ms. When the attacker launches the attack, the Server's information is still changing. At this time, end-host information is invalid, and the attack could not be successful.

G. *Influence on original application performance experiment*

Jmeter4.0 network tool was used in the experiment, mainly testing indicators such as the response time of Host1 accessing Server1 service in LAN2, and evaluating the impact of end-hopping technology on server response performance. The comparison of experimental results is shown in Fig.8. W stands for request duration.

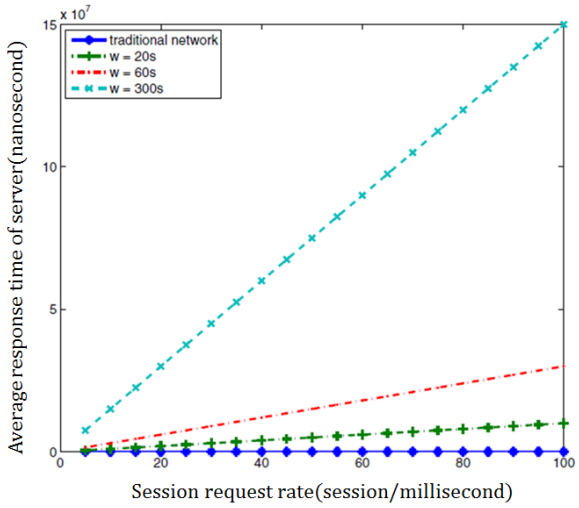

Figure 8 Server response time at different request rates

Under the condition of fixed server performance, a total of 8 tests were conducted for different users, startup time and cycle times. The test results may be different in different network environments and hardware conditions. The experiment shows that end-hopping technology has a certain impact on server performance. The service response time is somewhat improved from the normal response time, with an average impact of 10^{-2}s orders of magnitude. The next step is to improve the evaluation method of the impact of end-hopping technology on the original application performance, increase the network throughput and other evaluation indicators, and improve the end-hopping algorithm to reduce the impact on the original application performance.

CONCLUSION

In order to solve the severe imbalance between the cost of network security defense and the attackers' efforts to break into the network, this paper proposes a new MTD approach in the network layer. With strong adaptability, RHH is compatible with the existing network and does not need to change any intermediate network node. With the WAN communication capability, the hosts in the RHH could communicate securely through the defense agent plug-in, and make Server moving target defense capabilities in RHH by using the end-hopping and authentication technology, so that

the attacker cannot easily identify the information of MT-host. At the same time, this paper has done many experiments. The experiment shows that RHH proposed in this paper is practical and feasible, which can effectively prevent the scanning-based attacks and reduce the risk of network attack. For the future, further research is needed, for example, trap the attackers using expired terminal information with honeypot technology.

Acknowledgments

We would like to thank the office of cyberspace security at the Army Engineering University for their experiment support.

References

[1] F. Al-Shraideh, “Host Identity Protocol,” International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), Morne, Mauritius, 2006, pp. 203-203.

[2] Jajodia Sushil, K. Ghosh Anup, Swarup Vipin, Wang Cliff, and Sean Wang X, “Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats,” Springer Ebooks, New York, 2011, pp. 1-183.

[3] Ang Cui and Salvatore J. Stolfo, “Symbiotes and defensive Mutualism: Moving Target Defense, ” Moving Target Defense, Advances in Information Security, New York, 2011, pp. 99-108.

[4] M. Albanese, A. De Benedictis, S. Jajodia, and Kun Sun, “A moving target defense mechanism for MANETs based on identity virtualization," 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, 2013, pp. 278-286.

[5] Shi l y, jia c f, and lu s w. “Research on active network protection based on end-hopping”, Journal of communications, vol. 29-2, pp. 106-110, Feb. 2008. (in Chinese)

[6] M. Atighetchi, P. Pal, F. Webber, and C. Jones, “Adaptive use of network-centric mechanisms in cyber-defense,” Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2003., Hokkaido, Japan, 2003, pp. 183-192.

[7] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G.Anagnostakis, “Defending against hitlist worms using network address space randomization,” Computer Networks, vol. 51, pp. 3471-3490, Aug. 2007.

[8] D. Kewley, R. Fink, J. Lowry and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01, Anaheim, CA, USA, 2001, pp. 176-185 vol.1.

[9] E. Al-Shaer, Q. Duan, and J. H. Jafarian, “Random Host Mutation for Moving Target Defense,” Security and Privacy in Communication Networks, Springer Berlin Heidelberg, vol. 106, pp. 310-327, July 2012.

[10] Jafarian, Jafar Haadi , E. Al-Shaer, and Q. Duan . “Openflow random host mutation:transparent moving target defense using software defined networking,” Workshop on Hot Topics in Software Defined Networks ACM, Finland, vol. 12, pp. 127-132, August 2012.

[11] N. Mckeown, T. Anderson, H. Balakrishnan, , G. M. Parulkar, and J. S. Turner, “Openflow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol.38, pp. 69-74, April 2008.