A Self-adaptive Hopping Approach of Moving Target Defense to thwart Scanning Attacks

Duohe Ma[1], Cheng Lei[1,2,3(✉)], Liming Wang[1], Hongqi Zhang[2,3], Zhen Xu[1], and Meng Li[4]

[1] State Key Laboratory of Information Security, Institute of Information Engineering of CAS, Beijing, China
{maduohe,wangliming,xuzhen}@iie.ac.cn, leicheng12150@126.com
[2] China National Digital Switching System Engineering and Technological Research Center, Zhengzhou, Henan, China
zhq37922@126.com
[3] Henan Key Laboratory of Information Security, Zhengzhou, Henan, China
[4] Department of Computer Science, Hong Kong Baptist University, Hong Kong, China
mli@comp.hkbu.edu.hk

Abstract. End-point hopping is one of important moving target defense (MTD) mechanisms to kill the attacker's reconnaissance. This method involves periodically changing the network configuration in use by communicating end points. Since without the awareness of attack strategies, existing end-point hopping mechanisms is blind which leads the network defense to low security effectiveness and high overhead. In this paper we propose a novel MTD approach named self-adaptive end-point hopping, which is based on adversary strategy awareness and implemented by Software Defined Networking (SDN) technique. It can greatly counterpoise the defense benefit of end-point hopping and service quality of network system. Directed at the blindness problem of hopping mechanism in the course of defense, hopping trigger based on adversary strategy awareness is proposed for guiding the choice of hopping mode by discriminating the scanning attack strategy, which enhances targeted defense. Aimed at the low availability problem caused by limited network resource and high hopping overhead, satisfiability modulo theories and are used to formally describe the constraints of hopping, so as to ensure the low-overhead of hopping. Theoretical and experimental analysis shows the ability to thwart scanning attacks in a relatively reasonable hopping cost.

Keywords: Moving target defense · Software defined networking · Self-adaptive hopping · Scanning attack strategy

1 Introduction

In current network environment, the static nature of network configuration makes it easy for attackers to detect the target system and find only a single exploitable bug to successfully implement intrusion. Specifically, static and

K.-Y. Lam et al. (Eds.): ICICS 2016, LNCS 9977, pp. 39–53, 2016.
DOI: 10.1007/978-3-319-50011-9_4

fixed IP address allows network scanners to aggregate information in order to construct an accurate and persistent maps of the network. The unvarying nature of this network topology enables adversaries to collaboratively share and reuse their collected reconnaissance information in order to launch a larger attack. In the security battle, time is on the attackers side. Attackers have time to study targeted network to determine potential vulnerabilities and choose the time of attack to cause maximal impact. Once attackers attack and breach a system, they can maintain illegal access privileges for extended periods of time without being detected.

In the opposite, it is difficult for the defender to block all the vulnerabilities and filter all attacks in the case of IT system becoming increasingly complex. Although heavily secured perimeter firewalls and intrusion detection systems are deployed to protect the network from outside attackers, in practice they are not effective for Zero-day attack and Advanced Persistent Threats (APT), and can be avoided by skilled attackers. Without awareness of private information of the opponent, the defender may use static protection mechanisms and spend substantial effort to protect an asset which may not be the target of the attacker.

Moving target defense (MTD) has been proposed to change the game by wresting the advantage from the attacker because it eliminates the availability of constant or slowly-changing vulnerability windows that allow attackers to lie in wait and conduct useful experiments on persistent vulnerabilities [1]. Its purpose is to provide a dynamic, non-deterministic and non-sustained runtime environment [2]. Network MTD (NMTD) breaks the dependency requirements of the attack chains to the deterministic and consistency of network environment by multi-level dynamical changes [4]. As one of the hot spots of NMTD, end-point hopping is one of the effective mechanisms [5,6] to mitigate network attacks.

Although lots of hopping methods have been proposed [7–11,13], existing mechanisms lack the ability to adapt to different reconnaissance strategies, which leads the network defense to blindness. To summarize, there are two major problems in existing end-point hopping researches. First, the benefits from hopping defense decrease due to the inadequate dynamic of network hopping, caused by self-learning insufficiency in reconnaissance attack strategy, leading to the blindness of hopping mechanism selection. Second, due to the limited network resources and high overhead, the availability of hopping mechanism is poor.

To address the above problems, Network Moving Target Defense based on Self-adaptive End-point Hopping Technique (SEHT) is proposed. The key contributions of this paper can be shown in the following aspects:

(1) Directed to the lack of self-adaptive to scanning attack of existing hopping mechanism, hopping trigger based on adversary strategy awareness is designed. It uses hypothesis tests to analyze scanning attack strategy, and guides the choice of hopping strategy, which enhances the defense benefit.
(2) Aimed at limited network resources and high hopping overhead, end-point hopping based on satisfiability modulo theories is proposed. It uses satisfiability modulo theories (SMT) [18] to formally describe the constraints of hopping, so as to ensure the low-overhead of hopping, which increase the availability of hopping mechanism.

2 Background and Related Works

2.1 Category of Network Scanning Attacks

Network scanning is a kind of network reconnaissance technique by means of sending probe packets to selected end-point space range [19]. With different scanning technique constantly springs up, network scanning attack improves its efficiency based on the network structural characteristics and knowledge gained [20]. Accordingly, scanning attack strategy can be classified into three types: blind scanning, half-blind scanning and follow-up scanning:

(1) *Blind scanning strategy:* It is used when an attacker has to scan the entire active end-point. Since the structure of existing network information system has the characteristic of certainty and the static, attackers adopt blind scanning strategy so as to improve its efficiency by evenly scanning without repetition [21].
(2) *Half-blind scanning strategy:* It is used when an attacker knows the node distribution of the selected range of end-point information to scan. Half-blind scanning strategy is adopted so as to achieve higher success rate by unevenly scanning with repetition [22].
(3) *Follow-up scanning strategy:* It is directed at network systems implementing NMTD mechanisms When knowing the node distribution and the use of mutation mechanism, attackers try to obtain the mutation pattern of end-points by spatial compression and scanning frequency change. Based on it, follow-up scanning strategy is adopted so as to follow the hopping of specific end-point by uneven scanning with changeable frequency [23].

The reason to discriminate scanning attack strategy is that network scanning is used as a precondition technique the initial phase of attacks, which plays an important role in network attacks [3,4]. Therefore, this paper discriminates scanning strategy by analyzing behavior characteristic of different scanning strategies, which achieves self-adaptive end-point hopping.

2.2 Research Works About MTD Hopping

In traditional network architecture, Atighetchi *et al.* [7] proposed a hopping mechanism using false IP and port information to confuse scanning attack during net-flow exchange. Lee and Thing [8] proposed a random port hopping mechanism, which calculates next hopping end-point information to evade scanning attack by using pseudo-random function or shared secret key, but the method is vulnerable to network delay interference. MT6D [9] uses large IPv6 address space property to implement end-point information hopping so as to increase the unpredictability. Hari and Dohi [10] introduced a discrete Markov chain based on RPH so as to improve the success rate among communication parties. Lin et al. [11] proposed a novel synchronization method by additionally opening the corresponding end-point information of the previous and the after hopping period. HOPERAA algorithm was designed in [12], eliminating the influence of

linear clock drift on hopping synchronization. The drawback of these methods is hard to implement on network.

Software defined networking (SDN) [13] with the feature of logic control plane being separate from data transfer plane has brought a new solution of effective collaborative management in distributed routing. For that, end-point hopping based on SDN can change hopping period and hopping rules dynamically. NASR [14] prevents connection requests not within the service period by using address transition of packet header and the update of flow table based on DHCP update. SDNA [15] confuses scanning attackers by virtual hopping, which deploys a hypervisor node in each subnet to ensure hopping consistency. OF-RHM [16] proposed virtual end-point mapping mechanism based on Openflow [13]. It converts real IP to virtual IP so as to implement end-point hopping. However, since OF-RHM only implements space hopping, attackers can improve success rate of scanning attack by changing scanning frequency. To address this problem, Jafarian et al. [17] proposed ST-RHM hopping mechanism, which can resist cooperative scanning attack effectively by using temporal-spatial mixed hopping based on SDN. Because of the double hopping in spatial and temporal hopping, it leads to the increase of overhead and the loss of service.

In the rest of this paper, we will give the detail of Self-adaptive End-point Hopping Technique (SEHT) to solve these problems mentioned above. The main notions used in this paper are given below (Table 1).

Table 1. The main notions used in this paper

Character	Description
$SEHT$	Self-adaptive End-point Hopping Technique
SMT	Satisfiability modulo theories
BHR	Base hopping range
$LTHR$	Low-frequency temporal hopping range
$HTHR$	High-frequency temporal hopping range
T_{BHR}	The hopping period of base hopping
T_{LTHR}	The hopping period of low-frequency hopping
T_{HTHR}	The hopping period of high-frequency hopping
T_{EHP}	The hopping period of end-point
hEI	Hopping end-point information, as $<IP, Port>$
m_B, m_L, m_H	The number of hEI range in different layer
N_{fail}	The number of failed requested packet
w_i^{EI}	Weighted value
$C(hR_i)$	The maximum router capacity
C_{j_1,j_2}, b_i^k	Boolean variable
δ_i, B_f	The setting threshold value

3 The Mechanism of Self-adaptive End-Point Hopping

End-point hopping is shown in Fig. 1, it tricks, evades and prevents scanning attack by changing network configuration, such as IP address and port, and status dynamically. Therefore, it increases the usage difficulty of vulnerabilities and backdoors so as to ensure the security of targeted systems. Existing end-point hopping mechanisms mainly adopt random hopping strategy [14,16].

As is shown in solid part in Fig. 1, hopping configuration manager is used to configure end-point hopping on the basis of security objectives. After that, hopping implementation engine is used to implement end-point hopping. However, since random hopping is lack of offensive and defensive situational awareness, the effectiveness and availability of end-point hopping is limited.

Self-adaptive end-point hopping adds analysis engine and hopping trigger engine based on random hopping. Analysis engine is used to perceive and analyze network system security status. According to it, different hopping strategies are triggered in hopping trigger engine which based on adversary strategy awareness, and end-point hopping constraints are generated consequently.

3.1 Adversary Strategy Awareness and Hopping Trigger Engine

According to the behavior characteristics of different network scanning strategies, SEHT adopts Sibson entropy [24] to obtain the distribution of failed requested packets so as to discriminate scanning strategy. Only failed request packets are chosen because successful requests contain both normal packets of

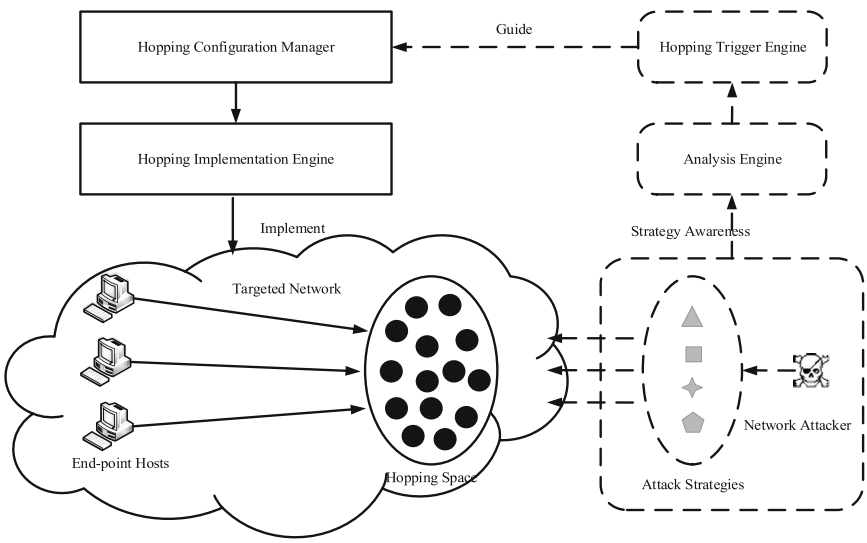


Fig. 1. Traditional hopping V.S self-adaptive of hopping.

legitimate users and the successful probe packets of attackers, but there is only one valid hEI for each end-point in every hopping period.

It has high accuracy and good stability in different anomalous awareness application scenarios [25].

Suppose the total number of failed request packets in the t^{th} mutation period is N_{fail}. The number of failed request packets in the i^{th} divided hEI space is denoted as N^i_{fail}. Equation (1) is used to calculate the probability distribution of the source and the destination address of failed requests in one mutation period denoted as $P_i^{Src}(\pi)$ and $P_i^{Dst}(\pi)$ respectively, with $j \in \{Src, Dst\}$, $\pi \in \{hEI\}$. Based on it, follow-up scanning strategy is discriminated after analyzing source address probability distribution of probe packets in adjacent T_{LTHR}. Besides, blind scanning strategy is then discriminated after analyzing destination address probability distribution of probe packets in each T_{EHP}.

Equation (2) indicates the Sibson entropy of the source address probability distribution of the failed request packets in the two consecutive T_{LTHR} of the i^{th} end-point, in which $D_i(p,q) = \sum_{\pi \in \Pi_i} p(\pi) \cdot \log \frac{p(\pi)}{q(\pi)}$, and $\overline{P^{Src}} = \frac{1}{2}[P_{t-1}^{Src}(\pi) + P_t^{Src}(\pi)]$. In order to prevent the interference of network jitter, Sibson entropy is calculated in two consecutive T_{LTHR} instead of it in two consecutive T_{EHP} of the i^{th} end-point. Based on Eq. (2), whether the scanning is follow-up strategy or not can be discriminated by comparing the Sibson entropy with the setting threshold.

Chauvenet criterion, shown as Eq. (3), is used to eliminate the abnormal high-frequency temporal mutation space. If blind scanning strategy is used, attackers are to scan the entire end-point space. The average number of scanned times of every end-point is $N_{fail}/m_B m_L$ in the ideal condition. However, because attackers might not always complete the scan of the whole end-point space within one T_{EHP}, the Sibson entropy directly calculated based on the distribution of failed probe packets of destination address and that of $N_{fail}/m_B m_L$ in one T_{EHP} will be larger. Therefore, the destination address probability distribution of the failed probe packets in the t^{th} T_{EHP} and its modified Sibson entropy are calculated by using Eq. (4), where $D(p,q) = \sum_{\pi \in \Pi} p(\pi) \cdot \log \frac{p(\pi)}{q(\pi)}$, and $\overline{P_t^{Dst}} = \frac{1}{2}(P_t^{Dst}(\pi) + \frac{n_{fail}}{m'_B m'_L})$. By comparing with the setting threshold, whether blind scanning strategy is adopted or not can be determined. If not adopted, attackers will use half-blind reconnaissance strategy.

$$P_i^j(\pi) = \pi_k \cdot (\sum_{k=1}^{N_{fail}} \pi_k)^{-1} \tag{1}$$

$$D_S(P_{t-1}^{Src}(\pi), P_t^{Src}(\pi)) = \frac{1}{2}\{D_i[P_{t-1}^{Src}(\pi), \overline{P^{Src}}] + D_i[P_t^{Src}(\pi), \overline{P^{Src}}]\} \tag{2}$$

$$\frac{N^i_{fail} - N_{fail}/m_B m_L}{(m_B m_L)^2/12} < -\xi \tag{3}$$

$$D_S(P_t^{Dst}(\pi), \frac{N_{fail}}{m'_B m'_L}) = \frac{1}{2}\{D[P_t^{Dst}(\pi), \overline{P_t^{Dst}}] + D[\frac{N_{fail}}{m'_B m'_L}, \overline{P_t^{Dst}}]\} \tag{4}$$

In order to improve the unpredictability of end-point mutation, SEHT select different hopping strategy according to the discrimination of scanning attack strategy. Consequently, hEI space is generated. The scanning attack strategies can be calculated as following. If there is $\sqrt{D_S(P_{t-1}^{Src}(\pi), P_t^{Src}(\pi))} \leq \delta_1$, follow-up scanning strategy is implemented by attackers. And when $\sqrt{D_S(P_t^{Dst}(\pi), \frac{N_{fail}}{M'})} \leq \delta_2$, blind scanning strategy is implemented by attackers. Otherwise, when $\sqrt{D_S(P_t^{Dst}(\pi), \frac{N_{fail}}{M'})} > \delta_2$ and $\sqrt{D_S(P_{t-1}^{Src}(\pi), P_t^{Src}(\pi))} > \delta_1$ establishes, half-blind scanning strategy is implemented by attackers.

Furthermore, if attackers use mixed scanning strategies, based on the self-learning of scanning strategies, SEHT implements corresponding hopping strategy according to the priority of follow-up scanning, half-blind scanning and blind scanning for efficient defense.

3.2 End-Point Hopping Based on SMT

In order to achieve the manageability and low overhead in the process of hopping implementation, SMT solver is used to obtain the required hEI set, which meets the security and performance constraints in end-point hopping.

Define Boolean variable $b_T^v(k)$ indicates whether hopping switch v forwards the k^{th} net-flow in T_{EHP} or not. If hopping switch v forwards the k^{th} net-flow in T_{EHP}, there is $b_T^v(k) = 1$. Otherwise, there is $b_T^v(k) = 0$. The details of SEHT constraints are shown as follows

(1) Capacity constraint: This constraint is used to select hopping routers that can carry the maximum net-flow table size so as to prevent packet loss caused by data overflow [26].

Equation (5) indicates the exponential function of marginal cost, where $\sigma = 2n$ is a tuning parameter [27]. $1 - \frac{C_v(k)}{C_v}$ indicates the utilization ratio of the forwarding table of v when the forwarding table of the k^{th} net-flow is added. Equation (6) indicates the accumulated cost of added net-flow table should under the maximum net-flow table size C_{max}^v that hopping routers can carry.

Equation (7) reduces route overhead by using route aggregation and adjacent allocation principles in routing update, which prevents the explosion of flow table size. $D_{j_1,j_2}^k = B_{j_1}^k \wedge B_{j_2}^k \wedge C_{j_1,j_2}$ means the assigned end-point information j_1 and j_2 in consecutive T_{EHP} to the same subnet are continuous, in which $B_j^k = \bigvee_{h^i \in s^k} b_j^i$ represents there is at least one end-point node h^i in subnet s_k assigned to hopping space j. Besides, Φ is the lower bound of the number of end-point information in each hopping space.

$$c_v(k) = C_v(\sigma^{1-\frac{C_v(k)}{C_v}} - 1) \tag{5}$$

$$\forall hR_i, \quad C^v_{max} - \sum_{i=1}^{k} b^v_T(i) \cdot c_v(i) \geq C^v_{th}, \quad b^v_T(i) = 1 \tag{6}$$

$$\sum_{k} \sum_{j_1} \sum_{j_1 \neq j_2} B^k_{j_1} \wedge B^k_{j_2} \wedge C_{j_1,j_2} \geq \Phi \tag{7}$$

(2) Hopping space selection constraint: This constraint ensures the unpredictability of SEHT by limiting repetition rate in hEI selection. Equation (8) ensures that every end-point node can be assigned hEI. Equation (9) sets repetition rate threshold δ_3 so as to ensure the repetition of selected hEI not exceed the threshold. Furthermore, Eq. (10) requires that the assigned hEI in the last hopping period won't be assigned in the following hopping period. This constraint ensures every node can be assigned required hEI, and improves the unpredictability of hopping.

$$\sum_{1<j\leq M} b^j_i \geq 1 \tag{8}$$

$$\sum b^j_i \geq \frac{N^i_{LTHR} - 1}{2\delta_3 n_{HTHR}} \tag{9}$$

$$\forall hEI \in F b^j_i = 0 \tag{10}$$

(3) Reachability constraint: This constraint means all net-flows in forwarding routers are reachable to destination end-point nodes. Equation (11) represents that the in-degree and out-degree of each router in the forwarding path is equal. Equation (12) means each router in the forwarding path is physically adjacent to its last hopping router and next hopping router, in which $\chi(hR_i)$ is routing set eliminating source and destination routers in the forwarding path. However, forwarding net-flows from one router to its next physical adjacent router is not enough to guarantee the reachability of net-flow. Equation (13) requires the distance from the next hopping router to destination router is not larger than the distance from the current hopping router to destination router, in which d^{i-Dst}_k represents the distance from router i to destination router.

$$If \quad b^k_T = 1, k \in [1, n], \quad \sum_{i\in I} b^v_T(i) = \sum_{o\in O} b^v_T(o) \tag{11}$$

$$If \quad b^k_i = 1, \forall hR_j \in \chi(hR_i), \quad \sum b^k_j = 2 \tag{12}$$

$$If \quad \forall hR_j \in \{hR | next\text{-}hop \ of \ hR_i\}, \quad d^{j-Dst}_k \leq d^{i-Dst}_k \tag{13}$$

(4) Forwarding path delay constraint: This constraint prevents service performance decrease due to the excessive transmission delay. Since net-flow transmission delay is positively correlated with the number of routing nodes [28], Eq. (14) indicates that the maximum length of forwarding path cannot exceed the threshold $L_{\max}$.

$$\sum b^k_i \leq L_{\max} \quad i \in \{Src, hR_1, ..., Dst\} \tag{14}$$

4 Implementation of SEHT Based on SDN

As is shown in Fig. 2, SEHT uses hopping switch (HS), randomization controller (RC) and the trusted hopping components (THC) of end-point nodes to implement network hopping collaboratively. RC divides $\{hEI\}$ to BHR according to the number of subnet and its scale. HS divides BHR to LTHR according to the number of end-points and their importance. THC selects hEI according to hopping strategy by using shared parameters with HS.

RC mainly consists with hopping trigger, hopping decision engine, and SMT solver of hopping space module. The function of hopping trigger module is to analyze scanning strategy based on hypothesis tests, according to the illegal connection packets reported by HS. Hopping decision engine is to select different hopping strategies according to scanning strategies. While SMT solver is to obtain the required end-point information set according to hopping constraints and global view of SDN. After that, RC updates LTHR to HS.

THC of end-point nodes is used to negotiate mutation with THC in other end-points, and implementing virtual mapping from EI to hEI. THC in SEHT is based on a universal virtual-network kernel driver TAP. In order to be transparent to users' applications, network hopping needs to operate Ethernet frames using TAP under Linux.

In order to ensure the hopping efficiency of SEHT and the stability of network sessions, end-points will store two hEI the first time. One is considered as the active hopping end-point information. The other will be utilized at the next

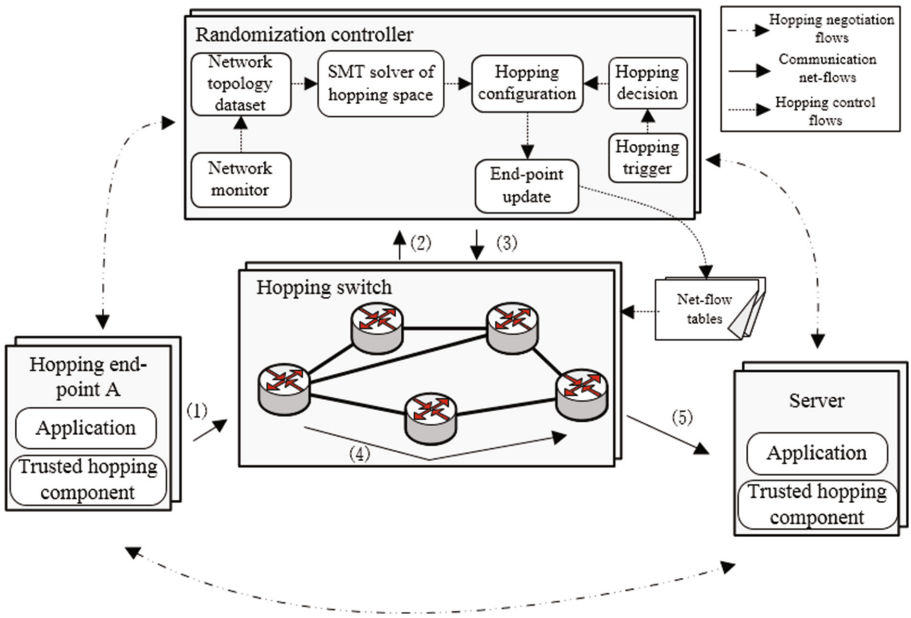


Fig. 2. SEHT Structure based on SDN.

hopping period, which is pre-calculated so as to notice other communicating THCs to be prepared to hopping when T_{EHP} is expired. At the same times, since there are still ongoing sessions in the network during end-point hopping, Change Time To Live (CTTL) is set so that expired hEI is retained to receive packets of existing sessions.

Since the flow tables need to update because of end-point and routing mutation during network communications, it is necessary to prevent the inconsistency of flow table update and packet loss. Directed to this problem, SEHT adopts *delete in sequential order, and add in reverse* update policy.

5 Experiments and Analysis

In order to verify the feasibility and effectiveness of SEHT, we use Mininet to build simulation network topology and adopt Erdos-Renyi model for random network topology generation. We choose OpenVSwitch (OVS) supporting Openflow protocol as HS, and OpenDaylight as RC. SEHT is deployed on OpenDaylight and OVS. Besides, Z3 SMT solver is used to solve the constraints. Linux CentOS 6.5 is used in Web Server and FTP Server. Windows7 is used in client. Besides, hEI is composed of Class B IP address pool and 2^{16} size port pool. The configuration of SEHT is shown in Table 2.

Table 2. Initial parameters of SEHT configuration

Parameter	Signification	Value
σ	Tuning parameter	5
δ_1	Threshold value of follow-up scanning strategy	0.05
δ_2	Threshold value of blind scanning strategy	0.075
δ_3	Threshold value of the repetition of selected hEI	0.005
γ	Ratio of scanning frequency to mutation frequency	0.4
λ	Maximum likelihood estimation	0.02
$L_{\max}$	Maximum length of forwarding path	32
T_{LTHR}	Hopping period of low-frequency hopping	50 s

5.1 Self-adaptive Hopping Overhead

The overhead of static networks, ST-RHM and SEHT hopping is shown in Table 3. It mainly consists of mutation computational complexity, average transmission delay and flow table size.

Assuming the number of host nodes in a subnet is n_t, hEI space is n_m, and EI can be aggregated is n_a. The size of net-flow table size in static network is n_t. Because in each hopping period, hEI is selected from all available hEI set, the size of net-flow table is $1 + n_m m_H$. While with capacity constraints, the size of net-flow table is $1 + m_H n_m / n_a$. Compared with ST-RHM, SEHT can effectively reduce the size of net-flow table.

Table 3. End-point hopping overhead

Hopping mechanism	Computational complex	Average transmission delay	Net-flow table size
Static network	$O(1)$	$t \times L_s$	n_l
OF-RHM	$O(\gamma n_h)$	$t \times L_s$	$1 + n_m/n_s$
ST-RHM	$O((\gamma n_h)^2)$	$t \times L_s$	$1 + n_m m_H$
SEHT	$O((\gamma n_h)^2)$	$t \times L_s$	$1 + m_H n_m/n_a$

5.2 Defend Scanning Attacks Analysis

Suppose there are n_l active end-point nodes in the network, the end-point information space is m, scanning width of attacker is $1/T_{SCN}$, and the scanning frequency is $n_s = w \cdot t/T_{SCN}$. The number of the end-point information scanned by the attack is $n_s = w \cdot t/T_{SCN}$, $n_s \leq m$. The ratio of scanning frequency to mutation frequency is $r = T_{EHP}/T_{SCN}$.

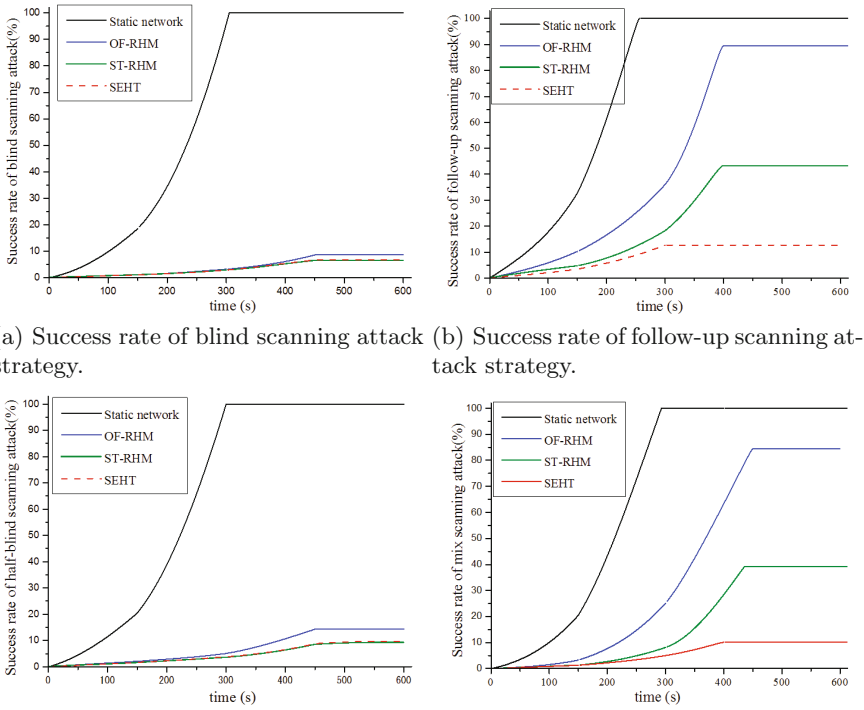
(1) The Capability of Resist Blind Scanning Attack. Since the blind scanning strategy is used to enhance the scanning rate. The success rate of scanning x active end-point nodes by attackers in static network, which can be supposed as $T_{EMP} = \infty$, obeys hypergeometric distribution expressed as $P_b(x) = (C_{n_l}^{x} \cdot C_{m-n_l}^{n_s-x})/C_m^{n_s}$.

Hence, the success rate of attackers in static network is $P_{\text{hb}}^{\text{static}}(x > 0) = 1 - aC_{\varphi m - n_l'}^{n_s/a}/\varphi C_{\varphi m}^{n_s/a}$. In OF-RHM [16], ST-RHM [17], and SEHT network, the probability of successfully scanning x active nodes during one mutation period obeys Bernoulli distribution. The success rate of attackers using blind scanning strategy is $P_b(x > 0) = 1 - [1 - rwn_l/(mn_l + mrw)]^{n_s}$. Particularly when $r = 1$, the scanning attack frequency is the same as the hopping frequency, the probability that an attacker successfully launching blind scanning is $P_b^{static}(x > 0) = 1 - C_{m-n_l}^{n_s}/C_m^{n_s}$. Compared with static network, it can be concluded that OF-RHM, ST-RHM, and SEHT can effectively resist blind scanning strategy, which is consistent with the conclusion in [29].

(2) The Capability of Resist Follow-Up Scanning Attack. When attackers use follow-up scanning strategy, there will be $r \geq 1$ in active scanning. Suppose attackers can repeat scanning b times in one T_{EMP}. The success rate of attackers in OF-RHM is $P_{\text{fu}}(x > 0) = 1 - [1 - bn_l'/(n_l' + \varphi mb)]^{n_s}$, which is consistent with the analysis in [11]. The success rate of attacker in ST-RHM is $P_{fu}(x > 0) = 1 - [1 - (bn_l' - n_\gamma)/(n_l' + \varphi mb)]^{n_s}$. Since SEHT deploys hopping period stretch policy, the hopping rate will lead to $r \leq 1$ after the follow-up scanning strategy is learnt by SEHT. As a result, the success rate of attackers in SEHT is $P_{\text{fu}}(x > 0) = 1 - [1 - (rn_l' - n_\gamma)/(n_l' + \varphi m)]^{n_s}$. Analysis shows that compared with ST-RHM, SEHT can effectively defend the follow-up scanning by combining spatial hopping with hopping period stretch policy.

(3) The Capability of Resist Half-Blind Scanning Attack. Since half-blind scanning strategy is used to actively scan specific range of end-point information which is physically adjacent to scanning source, it can be assumed that attacker can repeat scanning a times, and the scanning range is φm, $\varphi \in (0, 1)$, where there are n_l' active end-point nodes. Since OF-RHM adopts random hopping, the success rate of attackers using half-blind scanning strategy in OF-RHM is $P_{hb}(x > 0) = 1 - a[1 - wrn_l'/(\varphi mn_l' + \varphi mwr)]^{n_s}$. As for ST-RHM, it uses deceiving hopping. It can be assumed that there are n_γ hEI invalid at the end of each hopping period. The success rate of attackers using half-blind scanning strategy in ST-RHM is $P_{\text{hb}}(x > 0) = 1 - a[1 - (wrn_l' - \varphi mn_\gamma)/(\varphi mn_l' + \varphi mwr)]^{n_s}$. Since SEHT deploys random mutation based on weighted value, σ hEI will be selected for the next hopping period in each T_{EHP}. The success rate of half-blind hopping strategy in SEHT is $P_{hb}(x > 0) = 1 - a[1 - \sigma wrn_l'/(\varphi mn_l' + \varphi mwr)]^{n_s}$.

(4) The Capability to Resist Mixed Scanning Attack. In practical environments, the attacker often filtered EI through blind scanning. On this basis, half-blind or follow-up scanning is used in specific EI range. The success rate of mixed scanning attack is shown in Fig. 3(d). Since in static network, the success



(a) Success rate of blind scanning attack strategy.

(b) Success rate of follow-up scanning attack strategy.

(c) Success rate of half-blind scanning attack strategy.

(d) Success rate of mixed scanning attack strategy.

Fig. 3. SEHT Assessments to defend scanning attacks.

rate of attacker increases dramatically when the strategy changes from blind scanning attack to half-blind scanning attack. Since SEHT introduces hopping period stretch policy after discriminate follow-up scanning, it can effectively reduce about 29% scanning attack compared with ST-RHM and can reduce about 75% scanning attack compared with OF-RHM.

6 Conclusion

Without the awareness of attack strategies, existing end-point hopping mechanisms have two major problems. First, the hopping mechanism selection is blindness. Second, high hopping overhead leads the defense system to bad availability. To address these challenges, a novel MTD approach named Self-adaptive End-point Hopping Technique (SEHT) is proposed, which is based on adversary strategy awareness and implemented by Software Defined Networking (SDN). The advantages of this mechanism are represented by two aspects. Hopping trigger based on adversary strategy awareness is proposed for guiding the choice of hopping mode by discriminating the scanning attack strategy. And to ensure the low-overhead of hopping, satisfiability modulo theories and are used to formally describe the constraints of hopping. Theoretical analysis and simulation experiments show that SEHT can resist almost 90% scanning attack even in mixed scanning strategy with low-overhead hopping.

Acknowledgments. This paper is supported by the National Basic Research Program of 973 Program of China (2011CB311801); the National High-Tech Research and Development Plan of China (863 Program) (2012AA012704, 2015AA016106); the Strategic Priority Research Program of the Chinese Academy of Sciences, Grants No. XDA06010701, XDA06010306. Zhengzhou Science and Technology Talents (131PLKRC644).

References

1. Cybersecurity Game-Change Research Development Recommendations. NITRD CSIA IWG (2010). http://www.nitrd.gov/pubs/CSIA-IWG-Cybersecurity-GameChange-RD-Recommendations-20100513.pdf
2. Jajodia, S., Ghosh, A.K., Swarup, V., et al.: Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. Springer Science & Business Media, New York (2011)
3. Kewley, D., Fink, R., Lowry, J., et al.: Dynamic approaches to thwart adversary intelligence gathering. In: Proceedings of DARPA Information Survivability Conference & Exposition II, DISCEX 2001, vol. 1, pp. 176–185. IEEE (2001)
4. Lei, C., Ma, D., Zhang, H.: Moving target network defense effectiveness evaluation based on change-point detection. Math. Probl. Eng. **2016**, 1–11 (2016). Article ID 6391502
5. Xu, J., Guo, P., Zhao, M., et al.: Comparing different moving target defense techniques. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, Arizona, pp. 97–107 (2014)

6. Al-Shaer, E.: Toward network configuration randomization for moving target defense. In: Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., Sean Wang, X. (eds.) Moving Target Defense, pp. 153–159. Springer, New York (2011)
7. Atighetchi, M., Pal, P., Webber, F., et al.: Adaptive use of network-centric mechanisms in cyber-defense. In: Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, pp. 183–192. IEEE (2003)
8. Lee, H.C.J., Thing, V.L.L.: Port hopping for resilient networks. In: 2004 IEEE 60th Vehicular Technology Conference, VTC 2004-Fall, vol. 5, pp. 3291–3295. IEEE (2004)
9. Dunlop, M., Groat, S., Urbanski, W., et al.: MT6D: a moving target IPv6 defense. In: Military Communications Conference, 2011-Milcom, pp. 1321–1326. IEEE (2011)
10. Hari, K., Dohi, T.: Dependability modeling and analysis of random port hopping. In: 2012 9th International Conference on Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), pp. 586–593. IEEE (2012)
11. Lin, K., Jia, C.F., Shi, L.Y.: Improvement of distributed timestamp synchronization. J. Commun. **33**(10), 110–116 (2012)
12. Malathi, P.: Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts. In: 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–6. IEEE (2013)
13. Kirkpatrick, K.: Software-defined networking. Commun. ACM **56**(9), 16–19 (2013)
14. Antonatos, S., Akritidis, P., Markatos, E.P., et al.: Defending against hitlist worms using network address space randomization. Comput. Netw. **51**(12), 3471–3490 (2007)
15. Yackoski, J., Xie, P., Bullen, H., et al.: A self-shielding dynamic network architecture. In: Military Communications Conference, 2011-MILCOM, pp. 1381–1386. IEEE (2011)
16. Jafarian, J.H., Al-Shaer, E., Duan, Q.: Openflow random host mutation: transparent moving target defense using software defined networking. In: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, pp. 127–132. ACM (2012)
17. Jafarian, J.H.H., Al-Shaer, E., Duan, Q.: Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers. In: Proceedings of the First ACM Workshop on Moving Target Defense, pp. 69–78. ACM (2014)
18. Bjner, N., De Moura, L.: Z310: applications, enablers, challenges and directions. In: Sixth International Workshop on Constraints in Formal Verification (2009)
19. Ma, L.B., Li, X., Zhang, L.: On modeling and deploying an effective scan monitoring system. J. Softw. **20**(4), 845–857 (2009)
20. Ma, D., Xu, Z., Lin, D.: Defending blind DDoS attack on SDN based on moving target defense. In: Tian, J., Jing, J., Srivatsa, M. (eds.) SecureComm 2014. LNICSSITE, vol. 152, pp. 463–480. Springer, Heidelberg (2015). doi:10.1007/978-3-319-23829-6_32
21. Wang, Y., Wen, S., Xiang, Y., et al.: Modeling the propagation of worms in networks: a survey. IEEE Commun. Surv. Tutor. **16**(2), 942–960 (2014)
22. Badishi, G., Herzberg, A., Keidar, I.: Keeping denial-of-service attackers in the dark. IEEE Trans. Dependable Secur. Comput. **4**(3), 191–204 (2007)
23. Zhao, C.L., Jia, C.F., Weng, C., et al.: Research on adaptive strategies for end-hopping system. J. Commun. **32**(11A), 7–57 (2013)

24. Sibson, R.: Information radius. Zeitschrift f Wahrscheinlichkeitstheorie und verwandte Gebiete **14**(2), 149–160 (1969)
25. Yu, S., Thapngam, T., Liu, J., et al.: Discriminating DDoS flows from flash crowds using information distance. In: Third International Conference on Network and System Security, NSS 2009, pp. 351–356. IEEE (2009)
26. Kar, K., Kodialam, M., Lakshman, T.V., Tassiulas, L.: Routing for network capacity maximization in energy-constrained ad hoc networks. In: Proceedings of INFOCOM (2003)
27. Huang, M., Liang, W., Xu, Z., et al.: Dynamic routing for network throughput maximization in software-defined networks. In: IEEE INFOCOM The 35th Annual IEEE International Conference on Computer Communications, pp. 978–986. IEEE (2016)
28. Peng, B., Kemp, A.H., Boussakta, S.: QoS routing with bandwidth and hop-count consideration: a performance perspective. J. Commun. **1**(2), 1–11 (2006)
29. Carroll, T.E., Crouse, M., Fulp, E.W., et al.: Analysis of network address shuffling as a moving target defense. 2014 IEEE International Conference on Communications (ICC), pp. 701–706. IEEE (2014)