Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 6391502, 11 pages
http://dx.doi.org/10.1155/2016/6391502

Research Article

Moving Target Network Defense Effectiveness Evaluation Based on Change-Point Detection

Cheng Lei,[1,2] Duo-he Ma,[3] Hong-qi Zhang,[1,2] and Li-ming Wang[3]

[1]*China National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450001, China*
[2]*Henan Key Laboratory of Information Security, Zhengzhou 450001, China*
[3]*State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China*

Correspondence should be addressed to Duo-he Ma; maduohe@iie.ac.cn

Received 5 March 2016; Accepted 9 May 2016

Academic Editor: Jean J. Loiseau

In order to evaluate the effectiveness of moving target network defense, a dynamic effectiveness evaluation approach based on change-point detection is presented. Firstly, the concept of multilayer network resource graph is defined, which helps establish the relationship between the change of resource vulnerability and the transfer of network node state. Secondly, a change-point detection and standardized measurement algorithm is proposed. Consequently, it improves the efficiency of evaluation by measuring the change-point dynamically and enhancing the accuracy of evaluation based on multilayer network resource graph. What's more, in order to evaluate the defense effectiveness comprehensively, defense cost and benefits are set as evaluation indicators. Finally, experimental analysis, represented by MT6D and DNAT, proves the feasibility of the proposed evaluation method and the accuracy of the evaluation results.

1. Introduction

With the rapid development of advanced persistent threat (APT), traditional security defense mechanism is increasingly incompetent for new threats. In order to ensure the advancement of the defense process, network defense mechanism transforms from "active defense" to "reconfigurable defense." Therefore, moving target network defense (MTND) [1] mechanism comes into being. It continuously and dynamically changes the attack surface [2] of a defense system in multilevels, so that the intruded target in the face of a malicious adversary has the characteristics of heterogeneity, randomness, and unpredictability, consequently, improving the defense defectiveness by increasing the uncertainty and complexity of the malicious adversary. However, with the constant emergence of MTND technique, how to evaluate the effectiveness [3] of the proposed moving target network defense technology becomes a key and urgent problem.

Existing MTND effectiveness evaluation method is mainly divided into three categories: (1) empirical analysis based on offense and defense experiments [4], (2) contrastive analysis based on simulations [5–7], and (3) abstract analysis based on mathematical models [8–10]. Among them, empirical analysis is used in [4], which proposes a multistate dynamic model and verifies the validity conjecture of MTND by analyzing a number of offense and defense instances. However, this method is hard to meet the sustained and dynamic characteristics of MTND and, therefore, hard to ensure the timeliness of evaluation results. In order to solve the above problem to some extent, contrastive analysis based on simulation is proposed in [5, 6]. Evaluation indicators of MTND implementation effectiveness by analyzing network kill chain and typical MTND schemes are proposed in [5]. Zhuang et al. in [6] evaluates MTND implementation effectiveness by simulation experiments, which is based on conservative attack graph. However, the studies above do not take the cost produced during MTND implementation into consideration, so it is hard to balance the network system availability and defensive security by comprehensively evaluating the effectiveness of MTND implementation. In addition, evaluating MTND based on attack graph can only analyze the defense benefits of MTND to known attacks, but

not those to unknown attacks such as zero-day attack. Aimed at the first problem, quantitative framework for MTND effectiveness evaluation is proposed in literature [7]. It evaluates the defense cost and benefits on the basis of simulation experiments, which compares the MTND effectiveness between mission representation and attack representation. However, due to the limited scope of different experimental conditions and the nonnormalized quantitative criteria of vulnerability utilization in different network environments, it is difficult to compare the MTND effectiveness evaluated in different application conditions. Aimed at the second problem in [6], Wang et al. in [8] introduce the concept of network resource graph, based on which mathematical model is used to abstractly analyze the effectiveness of MTND in different application conditions. Zhuang et al. in [9] propose a scalable quantitative model, which is used to analyze the effectiveness of defense benefit by calculating attack transition probabilities among network nodes. In literature [10], Carroll et al. propose a performance evaluation method, network address mutation, based on Urn probability model. It evaluates the effectiveness of MTND by calculating the relationship of successful attack probability with network address size, the number of adversary detection, the number of network vulnerabilities, and the frequency of address hopping. However, it only considers the effectiveness of MTND under one single task, which is incompatible with the characteristics of multistep and parallel multitask in actual network systems. What's more, an abstract analysis based on mathematical model is easy to deviate from actual conditions in the process of abstraction.

In conclusion, the evaluation of MTND effectiveness needs (1) to combine the change of network vulnerabilities and the transition of network node security state, so as to ensure the accuracy and comparability of evaluation results in different application conditions, (2) to improve the efficiency of effectiveness evaluation, so as to improve the timeliness of evaluation results, and (3) to consider defense benefits and cost of MTND implementation, so as to ensure the comprehensiveness of evaluation. Hence, aimed at the above problems, we propose an effectiveness evaluation method for moving target network defense based on change-point detection.

2. Basic Architecture of Evaluation

The so-called "change-point" refers to the state and vulnerability of network nodes, whose change is related to malicious adversary intrusion, MTND hopping, and the changes of dependency among different resources and correlation relationship of similar resources. Via multilayer network resource graph (MNRG) (Figure 7), moving target network defense effectiveness evaluation based on change-point detection evaluates the effectiveness of MTND after detecting and measuring the amount of changes of change-point. As shown in Figure 1, its basic architecture consists of three parts: the construction and update of MNRG, change-point detection and standardized measurement, and effectiveness evaluation.

Firstly, aimed at the deficiency of attack graph in presenting unknown attack and the high frequency change of

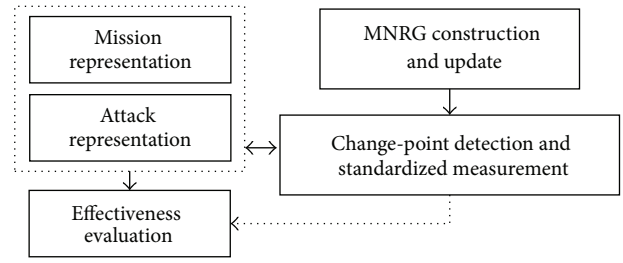

Figure 1: Architecture of the evaluation method.

MTND, the paper introduces a hierarchical thinking into the network resource graph and defines MNRG, thus, not only ensuring the integrity in rendering all kinds of attack paths, but also improving the timeliness in the process of MNRG update. Secondly, aimed at the problem that static measurement is hard to indicate the amount of changes in change-point accurately, change-point detection algorithm is proposed. The method uses graph similarity theory to detect the changes in MNRG before and after MTND implementation. What's more, standardized measurement is used to quantitate and calculate the utilization probability of change-point by a malicious adversary. It combines CVSS with dependency of different types of network resources, correlation relationship of similar resources and network node states in adjacent time, thus, ensuring the unification of metrics and achieving dynamic measurement at the same time. Finally, it calculates the defense benefits and cost of MTND from mission representation and attack representation, respectively, at the stage of MTND effectiveness evaluation, providing guidance for the balance between network system availability and security defense by analyzing the effectiveness of MTND comprehensively.

2.1. Construction and Update of MNRG. Network attack graph is to describe potential attack path by graphically presenting vulnerability dependency and state transition relationship. Existing attack graph is divided into state attack graph [11] and attribute attack graph [12]. In state attack graph, each node represents the state of global network system. With the increase of network size, such problems as low efficiency and space explosion in constructing state attack graph exist. Consequently, Ammann et al. [13] introduce a "monotonic" hypothesis of malicious adversary ability into the construction of attack graph. Attribute attack graph is based on the "monotonic" hypothesis, with a good scalability but no space explosion problem with the increase of the number of network nodes. However, since a malicious adversary will use both known vulnerability and unknown vulnerability of network resources to hit targets, the existing attack graph describes the possible attack path based on prior knowledge of well-known vulnerability. Therefore, it's hard to present possible attack path completely especially in zero-day attack. Thereby, Wang et al. [8] proposes the concept of network resource graph. It is a graphical representation method to depict the dependency of different resources and the transition of node state in network. The formal definition is as follows.

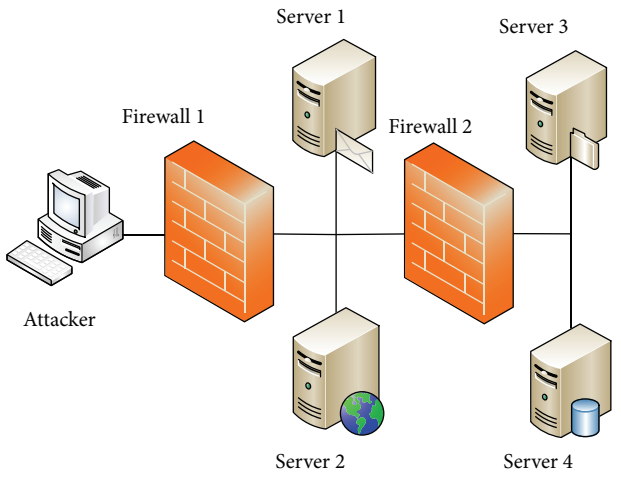

Figure 2: Illustration of network system.

Definition 1. Network resource graph (NRG) is a bilateral directed graph consisting of NRG(N, E). N is a vertex set, which can be presented as $N = N_v \cup N_c, N_v = \{\langle r, h_s, h_d\rangle \mid r \in \text{res}(h_d), h_s, h_d \in H\}$. It is the network resource vulnerability set in host h_d which can be used by host h_s. N_c is a state property set of resource, which can be divided into initial state property and intermediate state property. Initial state property can be presented as $N_{ci}\{n_{ci} \mid \nexists e \in E, \text{s.t.}(N_e, N_{ci}) \in (N_e \times N_c)\}$. Intermediate state property can be presented as $N_c - N_{ci}$. E is the set of directed edge. It can be presented as $E = E_r \cup E_i$, in which $E_r = (N_c \times N_v)$ means the precondition set and $E_i = (N_v \times N_c)$ means the postcondition set.

Figure 3(a) is the NRG of Figure 2. Unlike the exploitation of a known vulnerability which has its unique pre- and postconditions, new kind of attack, such as zero-day, mainly uses the provided services of target hosts to get access and promote privilege so that attackers can invade successfully by transferring the target host to specific state. Therefore, the condition of exploiting network resource vulnerability can be presented as $E = \langle \text{srv}, \text{priv}, \text{conn}\rangle$. It means the needs of services to be open $\text{srv} \in \{\text{srv}(h_d) \to 2^S\}$, the needs of privilege to possess $\text{priv} \in \{\text{priv}(h_d) \to 2^P\}$, and the needs of reachability to have $\text{conn} \in \{\text{conn}(H \times H)\}$, so as to successfully invade target host h_d.

Because of the high frequency change of MTND, scalability and dynamic adjustment problems are the key restraint in evaluating MTND effectiveness in dynamically changing network systems. The update of NRG should be completed in real-time, meanwhile preventing high computational complexity. What's more, on the one hand, MTND mechanism protects network collaboratively by changing network configuration and overall state property of nodes. On the other hand, a malicious adversary implements intrusion by using dependency of different resources. In conclusion, NRG should not only prevent space explosion with the growth of network scalability, but also establish the relationship between the change of resource vulnerability and the transfer of network node state. Considering the above two factors, we introduce a hierarchical thinking [14] into NRG and propose the concept of MNRG. Its formal description is defined in Definition 2. MNRG is divided into resource layer and node layer. In resource layer, it describes all possible partial orders of resource vulnerability exploited by a malicious adversary in different nodes. In node layer, it describes the state transition of different nodes caused by both malicious intrusion and MTND implementation. A tree structure is used to connect resource layer and node layer. For the purpose of illustration and clarity of description, network hosts are between resource layer and node layer in Figure 3(b).

Definition 2. Multilayer network resource graph is a bilateral directed graph consisting of MNRG(N, E). N is a vertex set, which can be presented as $N = N_P \cup N_R$. As N_P is a vertex set in node layer, it represents state property of corresponding network host. N_R is a vertex set in resource layer, which can be presented as $N_R = N_v \cup N_c$. It contains vulnerability and state property of network resources. For any hosts h in network, there is $\forall n_{Pi}^h \in N_P^h \subset N_P$ in node layer, and $\exists N_v^h \subseteq \text{res}(h)$ in resource layer, where $n_{Pi}^h \in N_{ci}^h$ is the initial state property of N_v^h. E is the set of directed edge. It can be presented as $E = E_r \cup E_i$, in which $E_r = (N_c \times N_v)$ means the precondition set and $E_i = (N_v \times N_c)$ means the postcondition set. Directed edges in node layer can be presented as $E_P \subseteq E$, and directed edges in resource layer can be presented as $E_R = E$.

If the number of network hosts is n, with m different types of resources in each host, the computational complex of MNRG construction and update is shown in Table 1. Therefore, compared with NRG, MNRG reduces the computational complex in the process of construction and update without the loss of any relationship of resource dependency.

What's more, we define attack path based on MNRG, whose formal description is shown in Definition 3.

Definition 3. Given MNRG(N, E), attack path is partial order sequence $\text{seq}(n_{vi})$, $i \in [1, n]$, which starts from hosts in one of the initial state $n_{ci} \in N_P$, and ends up with the goal state property of target hosts $n_{cg} \in N_P$. A malicious adversary exploits a series of related resource vulnerabilities n_{vi} by satisfying certain precondition $e_r \in E_r$.

2.2. Change-Point Detection and Standardized Measurement. Because MTND has the characteristics of unpredictable and random hopping, it is difficult for the static measurement of vulnerability to accurately measure the exploitation of vulnerability, which leads to the deviation of effectiveness evaluation of MTND. This paper proposes network-based moving target defense effectiveness evaluation based on change-point detection. It adopts graph similarity theory to detect the differences of change-point in a network system and measure its inherent and variable features in a standardized way, so as to evaluate MTND effectiveness in the next step.

The change-point detection and the standardized measurement algorithm are shown in Algorithm 1, with the input being MNRG_t and MNRG_{t+1}, which is the MNRG before and after one period of attack. It uses the minimum spanning tree algorithm to traverse two MNRGs firstly. If there exists

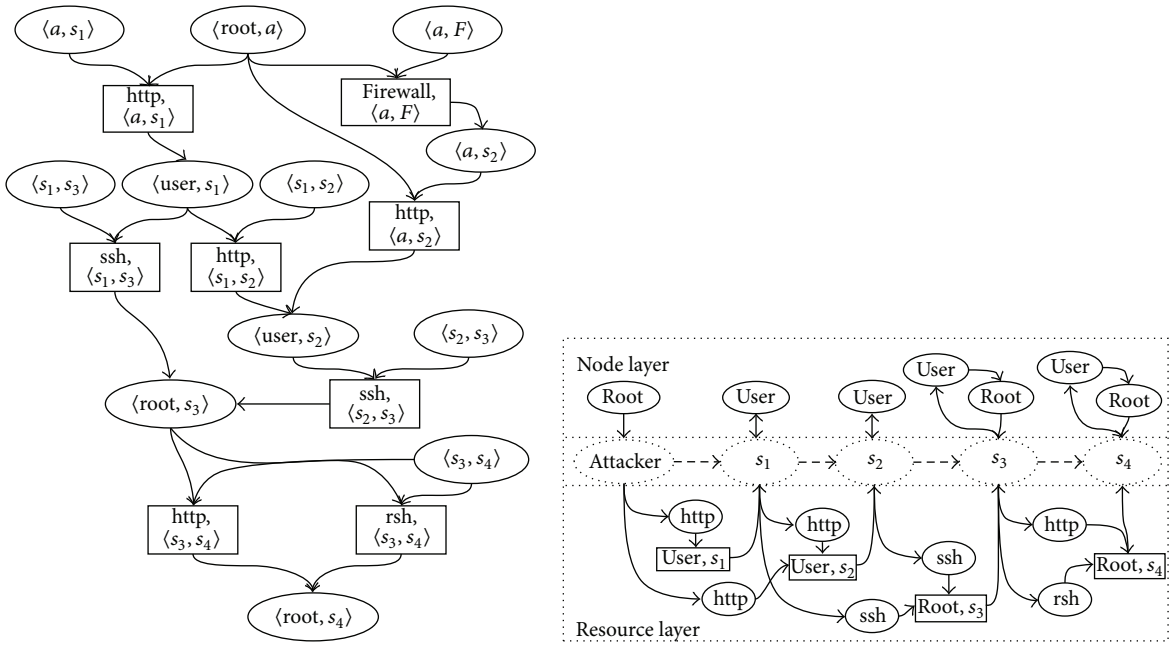

Figure 3: (a) NRG of network system. (b) MNRG of network system.

Table 1: Computational complex in construction and update.

Type of resource graph	Computational complex in construction	Computational complex in update
NRG [8]	$O(m^2n^2)$	$O(mn)$
MNRG	$O(m^2n + n^2)$	Node layer: $O(n)$ Resource layer: $O(m)$

a new kind of network resource after implementing MTND, the influence of inherent feature of the new resource, the relationship of different resource dependency, and the correlation of the same kind of resources on vulnerability exploitation by a malicious adversary should be taken into consideration. In other words, it can be calculated by using (1) to (5). For existing resources, the influence of the change of host state property after MTND hopping on the relationship of different resource dependency and the correlation of the same kind of resources should be considered. The probability of forward-transition, self-transition, and backward-transition can be calculated by using (6) to (10). As a result, the probability of successful intrusion of the malicious adversary can be calculated based on the initial state property. Finally, (11) can be used to calculate the maximum probability of attack path used for successful intrusion.

Because the change of change-point is determined by both its inherent characteristics, such as resource value and vulnerability, and variable characteristics, such as network environment, dependency of different resources, and correlation of the same kind of resources, standardized measurement is to be able to effectively measure the inherent and variable characteristics of change-point. In other words, in order to compare different MTND mechanisms in different implementation cases, it requires a unified standard to measure change-point in different activity models. What's more, the variable characteristics of change-point should be measured dynamically combined with its actual network environment, so as to assure the reliability of the measurement result. Common vulnerability scoring system [15] (CVSS) can achieve metric standardization by using open framework independent of specific applications. However, CVSS does not take the factor of dependency of different resources and correlation of the same kind of resources into consideration, which may lead to the deviation in calculating intrusion probability caused by underestimation of risks. For example, (1) several different types of resource vulnerabilities may have the dependency relationship with one another, among which, if one kind of vulnerability can be easily exploited by a malicious adversary, the possibilities of other resource vulnerabilities being exploited may increase. (2) For the same kind of network resources, if a malicious adversary successfully exploits this kind of vulnerability in one host, then the successful rate will be higher in exploiting the same kind of resource vulnerability in other network nodes. Thus, this algorithm adds the dependency of different resources and the correlation of the same kind of resources into the set of dynamic metrics so as to ensure the reliability of measurement. What's more, since the transition of states obeys Markov chain properties, that is, the state property at time t being only related to the state property at time $t-1$, the factor of state transition of adjacent time should be taken into consideration while calculating the probability of a malicious adversary in successfully meeting the target state.

Input:
$\text{MNRG}_t(V, E)$: MNRG before attack intrusion
$\text{MNRG}_{t+1}(V', E')$: MNRG after attack intrusion
Output:
$Exploit_+ \subseteq (V' - V \cap V')$: new resource vulnerability added in MNRG_{t+1}
$P(n_{cg})$: probability of successfully intrusion after MTND implementation

$\langle V, E\rangle \leftarrow \text{MST}(G_t)$; // Apply minimum spanning tree algorithm (MST) to traverse MNRG.
$\langle V', E'\rangle \leftarrow \text{MST}(G_{t+1})$;
$\langle (V' - V \cap V'), (E' - E \cap E')\rangle \leftarrow G' \setminus G \cap G'$; //Find change-point only belonging to MNRG_{t+1}.
for every $v'_{Ri} \in V'_R$ **do**
{
if (v'_{Ri} in V'_R, $v'_{Ri} \notin V_R$) then //There are new added resource vulnerabilities.
{
add v'_{Ri} to $Exploit_+$
if ($c(v'_{Ri}, v_{Ri}) \neq 0$) //There exists the same kind of resource as those in MNRG_t.
Calculate $p'(v'_{Ri}) = c \cdot p(v_{Ri})$; //Calculate the probability of successful exploiting by using (5).
else //There are not any kind of resource the same as those in MNRG_t.
Calculate $p(v_i \mid \wedge c_I)$; //Calculate the possibility of inherent feature of vulnerability exploiting by using (1).
Calculate PreCondn(v_i) and PostCondn(v_i); //Calculate the pre-condition and post-condition of vulnerability exploiting by using (2)–(4) respectively.
}
else if (v'_{Ri} in V'_R, $v'_{Ri} \in V_R$) //There is no new added resource vulnerabilities in MNRG_{t+1}.
{
Calculate $P(n^t_{Pi} \mid n^{t-1}_{Pi})$; //Calculate state transition from t to $t+1$ by using (6)–(10) respectively
Update PreCondn(v_i) and PostCondn(v_i); //Update the pre-condition and post-condition of vulnerability exploiting.
end if
}
}
end for
Calculate $P(n_{cg})$; //Calculate successful rate of attack intrusion by using (11).
return $P(n_{cg})$ and $Exploit_+$

Algorithm 1: Change-point detection and standardized measurement algorithm.

In conclusion, the process of standardized measurement calculates (1) the influence of dependency of different network resources in possibility of successful intrusion by converting CVSS, (2) the influence of correlation of the same type of network resources via introducing correlativity parameters, and (3) the influence of state transition caused by MTND hopping via proposing transfer factor. Due to the fact that a malicious adversary transfers state property of network hosts by exploiting different types of resource vulnerabilities and its dependency, while MTND transfers state property of network hosts by dynamically hopping the overall hosts, we calculate the influence of dependency of different network resources and correlation of the same type of network resources in possibility of successful intrusion at resource layer and the influence of state transition of adjacent time at node layer. If there are three types of network resource vulnerabilities v_1, v_2, and v_3, its dependency relationship is shown in Figure 4. c_1–c_3 are the initial state properties; c_5 and c_6 are the goal states; T_A is the period of network attack; T_{MTND} is the period of MTND implementation.

In resource layer, if a malicious adversary can exploit resource vulnerability successfully, it must meet the inherent

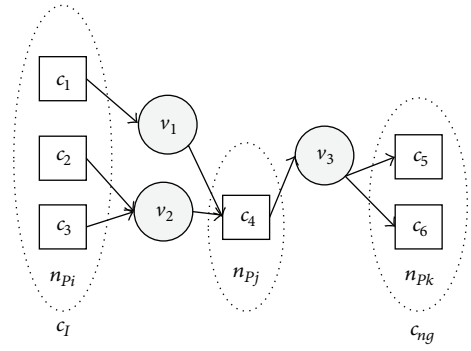

Figure 4: Dependency of different network resources in node x.

character and variable character, the latter of which determines the precondition and postcondition of vulnerability exploitation, at the same time. The probability of inherent characteristics of resource vulnerability exploitation can be expressed by (1). It means the exploitation possibility of resource vulnerability under the circumstance that all its

preconditions are satisfied simultaneously. When there are multiple preconditions to be satisfied, only if all the requirements are met can the malicious adversary exploit vulnerability successfully. Therefore, there exists conjunctive relationship in preconditions, whose probability can be calculated by (2). On the other hand, if one state property can be satisfied by the exploitation of different resource vulnerabilities, the malicious adversary can meet the requirements by only satisfying any one of the corresponding vulnerabilities. Therefore, there exists disjunction relationship in postconditions, whose probability can be calculated by (3). Since the precondition and postcondition are determined by the dependency relationship among different types of resource vulnerabilities, they will change under different network connections and configurations. The dependency of different types of resource vulnerabilities can be calculated by (4):

$$p\left(v_i \mid \wedge c_I\right) = \frac{\mathrm{CVSS}_{\mathrm{BMS}}\left(p_i\right)}{10}, \tag{1}$$

$$\mathrm{PreCondn}\left(v_2\right) = P\left(c_1\right) P\left(c_2\right), \tag{2}$$

$$\begin{aligned}\mathrm{PostCondn}\left(v_1\right) &= \mathrm{PostCondn}\left(v_2\right) \\ &= \left(P\left(v_1\right) + P\left(v_2\right) - P\left(v_1\right) P\left(v_2\right)\right) p\left(c_4\right),\end{aligned} \tag{3}$$

$$p\left(c_i\right) = \frac{\mathrm{CVSS}_{\mathrm{TMS}}\left(p_i\right) \mathrm{CVSS}_{\mathrm{EMS}}\left(p_i\right)}{100}. \tag{4}$$

From the above analysis, the probability of a malicious adversary's successful intrusion by exploiting resource vulnerabilities can be expressed as $p(v_1) = p(c_1)p(v_1 \mid c_1)p(c_4)$ in Figure 4. However, there exists the same type of network resources in different network hosts, such as http service. Once the malicious adversary successfully exploits the vulnerability of such resources in any nodes in network, the successful rate of reusing the same type of vulnerability will increase. The reason is that the inherent characteristics of the same type of resource vulnerability is the same though the configuration is different in different network nodes. Consequently, we introduce the concept of correlativity parameters, whose formal description is shown in Definition 4.

Definition 4. Given MNRG(N, E), $\forall n_{v1}, n_{v2} \in N_v$, if n_{v1} and n_{v2} belong to the same type of resources, the correlativity of n_{v1} and n_{v2} can be presented as $c(n_{v1}, n_{v2}) : [1, x] \times [1, x] \rightarrow [0, 1]$, where x means all the possible configurations of this resource.

The probability of successfully exploiting the same type of resources by a malicious adversary via introducing correlativity parameter can be presented as the following, where $p(v_i) = p(v_i \mid \wedge c_I) \prod p(c_i)$:

$$p'\left(v_i\right) = c \cdot p\left(v_i\right). \tag{5}$$

In node layer, because the transition of state property of nodes is associated with the exploitation of vulnerability by a malicious adversary and the hopping results of MTND, the probability of state transition before and after MTND implementation is shown in (6). It means the state property

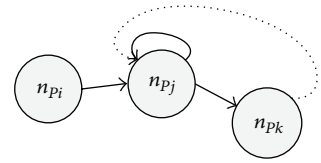

Figure 5: State transition example of node x.

at the moment of t is jointly determined by the state property of its adjacent moment and the transition of state property:

$$P\left(n_{Pi}^{t}\right) = P\left(n_{Pi}^{t} \mid n_{Pi}^{t-1}\right) P\left(n_{Pi}^{t-1}\right). \tag{6}$$

Since the nature of MTND mechanism is to transfer the state property of network hosts by shifting attack surface systematically and dynamically, the malicious adversary may invalid its vested exploitation of resources and privileges, leading to the failure of supporting for further attacks. Therefore, the malicious adversary may be stuck in certain states of network hosts in attack path or even fall back to previous state in any other network nodes in attack path. State transition can be divided into forward-transition, self-transition, and backward-transition as shown in (7). In this paper, "transfer factor" is introduced to calculate the state transition probability of network nodes, and its expression is $\varphi = (1 - k/n)$. It means the probability of state transfer does not occur after one hopping period of MTND, where n is the total number of states variable and k is the number of states actual implementing:

$$P\left(n_P^t \mid n_P^{t-1}\right) \begin{cases} P_{kj}\left(n_{Pk}^{t} \mid n_{Pk}^{t-1}\right) \\ P_{jj}\left(n_{Pj}^{t} \mid n_{Pj}^{t-1}\right) \\ P_{ij}\left(n_{Pi}^{t} \mid n_{Pi}^{t-1}\right). \end{cases} \tag{7}$$

(1) The so-called forward-transition refers to the state property possessed by a malicious adversary falling back to previous state in any network nodes in attack path, since the precondition of the state property a malicious adversary possessed is not satisfied. On the one hand, the construction and update of MNRG follow the monotonic hypothesis, which is the basis for preventing state space explosion. On the other hand, forward-transition will make the construction of MNRG no longer following the monotonic hypothesis. Therefore, we introduce the forward-transition indirectly so as to prevent the occurrence of state space explosion.

In order to explain clearly, Figure 5 only shows the node layer of Figure 4. Since the precondition of n_{Pk} is not satisfied after MTND implementation, the state property n_{Pk} possessed by the malicious adversary falls back to previous state. The probability of forward-transition can be equaled as the joint probability of self-transition of n_{Pj} and backward-transition of n_{Pi}, which is the latest network node state transition that does not occur in attack path. Therefore, forward-transition can be transformed equally by self-transition and backward-transition in order to ensure the obedience by monotonic hypothesis, as shown in

$$P_{kj}\left(n_{Pk}^{t} \mid n_{Pk}^{t-1}\right) = P_{ij}\left(n_{Pi}^{t} \mid n_{Pi}^{t-1}\right) P_{jj}\left(n_{Pj}^{t} \mid n_{Pj}^{t-1}\right) \tag{8}$$

(2) The so-called self-transition refers to the state property possessed by a malicious adversary stuck in certain states of network hosts in attack path. It contains two cases: ① during the period of attack T_A, if the period of MTND is T_{MTND}, the state property n_{Pj} is not transferred after MTND implementation, but its postcondition changes, which leads to the result that the malicious adversary cannot intrude from n_{Pj} to n_{Pk}. Its probability is $\varphi^{T_A/T_{\text{MTND}}}(1 - p(v_3))^{T_A/T_{\text{MTND}}}$. ② During the period of attack T_A, if neither the state property n_{Pj} is transferred nor its postcondition changes, but its adjacent state property n_{Pk} is transferred, the probability is $\varphi^{T_A/T_{\text{MTND}}}(1-\varphi^{T_A/T_{\text{MTND}}})(1-(1-p(v_3))^{T_A/T_{\text{MTND}}})$. In conclusion, the probability of self-transition can be shown in

$$\begin{aligned} P_{jj}\left(n_{Pj}^{t} \mid n_{Pj}^{t-1}\right) &= \varphi^{T_A/T_{\text{MTND}}}\left(1 - p\left(v_3\right)\right)^{T_A/T_{\text{MTND}}} \\ &\quad + \varphi^{T_A/T_{\text{MTND}}}\left(1 - \varphi^{T_A/T_{\text{MTND}}}\right) \\ &\quad \cdot \left(1 - \left(1 - p\left(v_3\right)\right)^{T_A/T_{\text{MTND}}}\right). \end{aligned} \tag{9}$$

(3) The so-called forward-transition refers to a situation where neither the state property possessed by a malicious adversary is transferred nor its precondition is changed. The probability of forward-transition can be presented by

$$\begin{aligned} &P_{jk}\left(n_{Pi}^{t} \mid n_{Pi}^{t-1}\right) \\ &\quad = \varphi^{2T_A/T_{\text{MTND}}}\left(1 - \left(1 - p\left(v_3\right)\right)^{T_A/T_{\text{MTND}}}\right). \end{aligned} \tag{10}$$

What's more, since the malicious adversary can be assumed rational, the attack path which has the character of low attack cost and high exploitation probability will be chosen by attackers. From the above analysis, at the moment t, the maximum probability of attack path chosen by the malicious adversary from certain initial state property to goal state property can be presented by

$$\begin{aligned} P\left(n_{cg}\right) = \operatorname{argmax} \prod_{Pi=1}^{n} &\left\{ P\left(n_{Pi}^{t} \mid n_{Pi}^{t-1}\right) \right. \\ &\left. \cdot \left\{ p\left(c_I\right) \prod_{Ri=\text{source}}^{\text{target}} \left(p\left(v_i\right) p\left(c_i\right)\right) \right\} \right\}. \end{aligned} \tag{11}$$

2.3. Effectiveness Evaluation. The effectiveness of MTND implementation is composed of defense cost and defense benefits. Since the implementation costs of network system deploying MTND can be divided into defense cost of MTND and running expense in performing tasks, the evaluation on defense cost of MTND can be obtained by comparing the amount of change in running expense before and after MTND implementation. Defense benefits of MTND refer to the impact on malicious intrusion after implementing MTND. It can be obtained by comparing the amount of change in probability of successful malicious intrusion. Based on the above analysis, this paper uses mission representation and attack representation, respectively, with [7], before and after MTND implementation to indicate the defense cost and benefits of MTND, as shown in Table 2. As for mission representation, it is a kind of specific activity model depicting the network behavior when performing tasks. Attack representation is a kind of specific activity model depicting invasion behavior of the malicious adversary when intruding specific target.

Table 2: The indicators in MTND evaluation.

	Mission representation	Attack representation
The amount of change in efficiency	ΔProductivity (M)	ΔProductivity (A)
The amount of change in success rate	ΔProductivity (M)	ΔProductivity (A)

As shown in (12), operational efficiency presents how fast the activity model fully implements an activity. In mission representation, productivity (M) indicates how fast the network performs some tasks. In attack representation, productivity (A) indicates how fast the malicious adversary intrudes the target hosts successfully. $\nu : \tau \times t_{\text{duration}} \rightarrow V_P$ is a mapping function from behavior τ and duration time t_{duration} to V_P, where $\tau = \{\tau_1, \tau_2, \ldots, \tau_n\}$, $t_{\text{duration}} = \{t_{\text{duration1}}, \ldots, t_{\text{duration}n}\}$, and $V_P \in [0, 1)$:

$$\text{Productivity}\left(\cdot\right) = \frac{1}{|n|}\sum_{i=1}^{n}\omega_i \nu\left(\tau_i, t_{\text{duration}i}\right). \tag{12}$$

Because the importance of network node depends on the value of resources it possesses and the importance of services it provides, the importance of different network nodes is different. On the one hand, the change of performance in different hosts after MTND implementation will impact the overall network performance. On the other hand, the hosts successfully intruded by the malicious adversary determine the extent of harm of network attack on the entire network system. Therefore, an important factor ω_i is introduced to weigh the importance of hosts in network system, $\omega_i \in [0, 1]$. The success rate of running presents the probability of successfully performing an activity in activity model. In mission representation, success rate indicates that of performing some tasks, as shown in (13). $\nu : T \times A \rightarrow V_S$ is a mapping function from behavior τ and the number of success n_{success} to V_S, where $T = \{\tau_1, \tau_2, \ldots, \tau_n\}$, $A = \{n_{\text{success}\,1}, \ldots, n_{\text{success}n}\}$, and $V_S \in [0, 1)$. In attack representation, success rate indicates that of intrusion by the malicious adversary, as shown in (14):

$$P_{\text{Success}}\left(M\right) = \frac{1}{|n|}\sum_{i=1}^{n}\omega_i \nu\left(\tau_i, n_{\text{success}i}\right), \tag{13}$$

$$\begin{aligned} P_{\text{Success}}\left(A\right) &= \prod_{i=1}^{n}\omega_i P\left(n_{Pi}^{t} \mid n_{Pi}^{t-1}\right) \\ &\quad \cdot \left\{ p\left(c_I\right) \prod_{Ri=\text{source}}^{\text{target}} \left(p\left(v_i\right) p\left(c_i\right)\right) \right\}. \end{aligned} \tag{14}$$

In conclusion, within one attack period T_A, the defense cost is shown in (15). It is determined by the amount of change

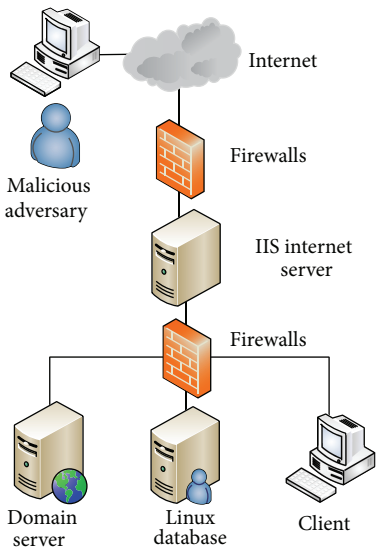

Figure 6: Network topology of experiment.

of efficiency and success rate in performing certain tasks in mission representation. The defense benefit is shown in (16). It is determined by the amount of change of efficiency and success rate in performing certain tasks in attack representation. What's more, because the design of MTND focuses on different parts in network kill chain [16] of APT, it is necessary to evaluate the highest defense benefit in the phase of network kill chain. Equation (17) shows the highest defense benefit of MTND implementation in the phase of network kill chain, where $T_\Phi = \{\tau \mid \nu(\tau, \text{phase}) = \phi\}$, and Φ divides the APT attack into six stages [17], that is, $\Phi = \{R, W, D, E, I, C2, AO\}$:

$$\text{cost} = \sum_{i=0}^{\lfloor T_A/T_{\text{MTND}} \rfloor} \Delta_i \left(\text{Productivity}\,(M) \cdot P_{\text{Success}}\,(M)\right), \quad (15)$$

$$\text{benefit} = \sum_{i=0}^{\lfloor T_A/T_{\text{MTND}} \rfloor} \Delta_i \left(\text{Productivity}\,(A) \cdot P_{\text{Success}}\,(A)\right), \quad (16)$$

$$\text{benefit}_{\text{phase}} = \underset{\phi \in \Phi}{\text{argmax}} \frac{1}{\left|T_\phi\right|} \sum_{\tau \in T_\phi} \Delta \left(\text{Productivity}\,(A) \cdot P_{\text{Success}}\,(A)\right). \quad (17)$$

3. Case Study

In order to verify the feasibility and correctness of the proposed moving target network defense effectiveness evaluation based on change-point detection, the experimental network environment is built by using a typical topology shown in Figure 6. There are four hosts in the network, H_1, H_2, H_3, and H_4, whose basic information is shown in Table 3. The mission representation in the experiment is the request and access of network resources. The attack representation in the experiment is the tampering of sensitive data in the domain server. The MTND mechanism chosen to defend is MT6D and DNAT, respectively. The principle of MT6D

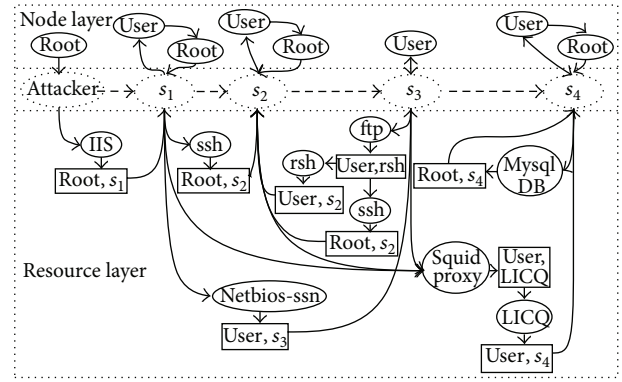

Figure 7: MNRG of experiment topology.

Table 3: The hosts configuration in experiment.

Host name	System information
H_1: IIS internet server	Windows NT 4.0
H_2: Domain server	Windows 2000 SP1
H_3: Client	Windows XP Pro SP2
H_4: Linux database	Red Hat 7.0

Table 4: The list of resource vulnerability.

Number	Host	Service	Port	Vulnerability
A	H_1	IIS network service	80	IIS buffer overflow
B	H_2	ftp	21	ftp rhost overwrite
C	H_2	ssh	22	ssh buffer overflow
D	H_2	rsh	514	rsh login
E	H_3	Netbois-ssn	139	Netbios-ssn nullsession
F	H_3	rsh	514	rsh login
G	H_4	LICQ	5190	LICQ remote-to-user
H	H_4	Squid proxy	80	Squid port scan
I	H_4	Mysql DB	3306	local-setuid-bof

[18] is to defend malicious intrusion by hopping endpoint-information of hosts deployed by MTND. Its hopping is performed in a fixed period which is based on the result of a hash by using the shared key, a value derived from the host's MAC address, and a timestamp. What's more, MT6D uses tunnel encryption technology to prevent attackers from correlating net-flow, thus ensuring that the hopping of endpoint information cannot be tracked. The principle of DNAT [19] is a lightweight MTND mechanism. Its hopping is performed in a fixed period which is based on the collaborative support of NAT and DNS. The NAT device stores state for each established sessions, allowing the DNS server to change addresses and providing a unique response to each new client without disrupting the established sessions.

The important factor of each host in experiments is $\omega_1 = 0.4$, $\omega_2 = 0.55$, $\omega_3 = 0.3$, and $\omega_4 = 0.7$. The resource vulnerabilities scanned by Nessus are shown in Table 4, by which the MNRG is constructed. The experiments are divided into two groups. The first group implements MT6D to defend against

Table 5: The list of attack path.

No.	Attack path	Original success rate	Success rate under MT6D implementation	Success rate under DNAT implementation
1	root $a \to A \to$ root $s_1 \to C \to$ root $s_2 \to G \to H \to$ user $s_4 \to I \to$ root s_4	0.194	0.103	0.11
2	root $a \to A \to$ root $s_1 \to E \to$ user $s_3 \to G \to H \to$ user $s_4 \to I \to$ root s_4	0.216	0.115	0.119
3	root $a \to A \to$ root $s_1 \to E \to$ user $s_3 \to B \to D \to$ user $s_2 \to G \to H \to$ user $s_4 \to I \to$ root s_4	0.097	0.053	0.052
4	root $a \to A \to$ root $s_1 \to E \to$ user $s_3 \to B \to C \to$ root $s_2 \to G \to H \to$ user $s_4 \to I \to$ root s_4	0.128	0.076	0.079

the intrusion of the malicious adversary so as to protect the safety of sensitive data. The second group deploys DNAT to defend against the intrusion of the malicious adversary in order to protect the safety of sensitive data.

3.1. Change-Point Detection and Standardized Measurement. If $T_A = T_{\text{MTD}} = 150$ s, the change-point calculated by using equations above in experiment is shown in Table 5. The original success rate means the probability of successful intrusion of a malicious adversary without implementing MTND, while the success rate under MT6D or DNAT implementation means the probability of successful intrusion of a malicious adversary after implementing MT6D or DNAT, respectively.

By analyzing Table 5, the following conclusion can be drawn. (1) Both MT6D and DNAT can reduce the success rate of a malicious adversary's intrusion effectively by endpoint information hopping. (2) Because the success rate of a malicious adversary's intrusion will decrease with the growth of the length of attack path, compared with the 3th and 4th attack path, the 1st and 2nd attack paths have higher success rates. This is consistent with the principle mentioned in [20] that the safety of communication nodes can be enhanced by adding in one or more intermediate nodes. (3) Under the fixed hopping period, the effectiveness of MT6D is better than DNAT after a period of time. The reason is that MT6D uses tunnel encryption technology to prevent attackers from correlating net-flow, which plays an important role to protect the implementation of MTND so as not to suffer from the following attack.

3.2. Comparative Analysis of Effectiveness Evaluation. Since a malicious adversary usually chooses an attack path with low cost, a short length, and a high success rate, the 2nd attack path will be more easily exploited by the malicious adversary to implement intrusion. If the malicious adversary chooses the 2nd attack path to implement intrusion: root $a \to A \to$ root $s_1 \to E \to$ user $s_3 \to G \to H \to$ user $s_4 \to I \to$ root s_4, the period of attack is $T_A = 150$ s. We change the period of MTND as $T_{\text{MTND}} = 10$ s, 20 s, 30 s, 50 s, 75 s, 100 s, 120 s, 150 s, and 300 s to compare the derivation between evaluation results by proposed method and the effectiveness of practical implementation. Figures 8 and 9 show the defense cost and benefits of MT6D and DNAT, respectively, by calculating and implementing in different hopping periods. The practical

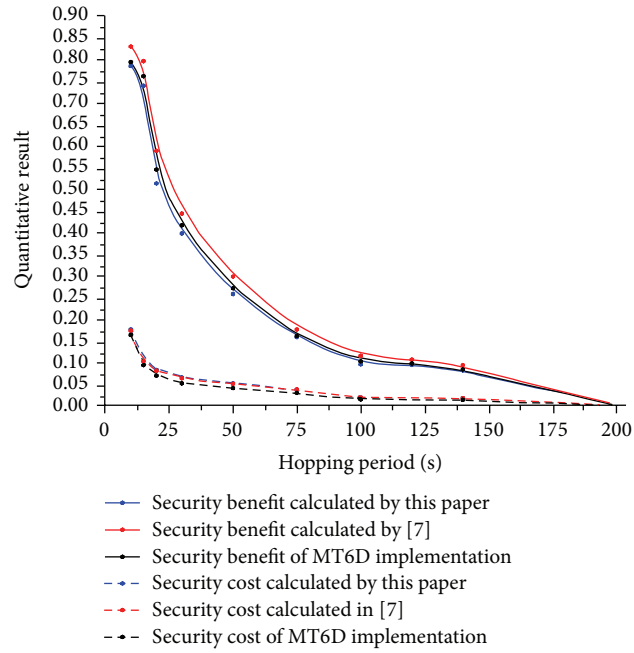

Figure 8: Evaluation comparison of MT6D.

defense cost and benefits are the result of each MTND implementation.

The following conclusion can be drawn after analyzing: (1) both the defense cost and benefits of MT6D and DNAT decrease with the increase of hopping period. Besides, compared with DNAT, MT6D has higher defense benefits, but the defense cost is also high. (2) The maximum defense benefit of MT6D and DNAT is in the phase of reconnaissance (R), which enhances the security of protected network system by increasing the scanning expense of malicious attacks. (3) The calculated evaluation results are almost the same as the actual performance. But compared with the method in [7], the deviation of our proposed method is smaller. (4) In defense benefits, because our proposed method takes the variable character into consideration, the evaluation results of defense benefits are lower than practical benefits. In defense cost, because the method we used is similar to the one in [7], the evaluation results of defense cost are higher than practical cost. Therefore, the proposed evaluation method in this paper

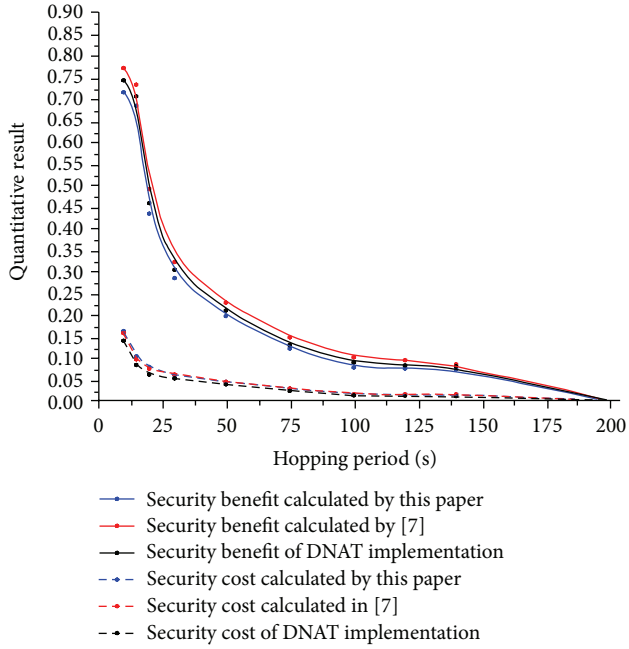

Figure 9: Evaluation comparison of DNAT.

is more conservative than the one in [7]. In conclusion, the proposed network-based moving target defense effectiveness evaluation based on change-point detection can evaluate the implementation of different MTND effectively and comprehensively under the same standard.

4. Conclusion

In order to evaluate the implementation effectiveness of moving target network defense mechanism, an effectiveness evaluation based on change-point detection is proposed. First of all, the paper defines multilayer network resource graph by introducing the hierarchical thinking into network resource graph, thus establishing the relationship between the change of resource vulnerability and the transition of state property of network hosts while depicting the integrity of attack path. Secondly, a change-point detection and standardized measurement algorithm are proposed to detect change-point in real-time and implement metrics dynamically, which not only reduces the deviation of static measurement but also improves the efficiency of evaluation. What's more, based on mission representation and attack representation, the defense cost and benefits of MTND implementation can be obtained for helping evaluate the effectiveness of MTND comprehensively. Finally, the proposed method is used to evaluate the effectiveness of MT6D and DNAT. The case study verifies the feasibility of evaluation method and the validity of evaluation results by comparing with evaluation results of existing evaluation method and the effectiveness results in practical implementation.

Competing Interests

The authors declare that they have no conflict of interests.

Authors' Contributions

All authors drafted the paper and read and approved the final paper.

Acknowledgments

This work is supported by the National Basic Research Program of 973 Program of China (2011CB311801); the National High Technology Research and Development Program of China (2012AA012704, 2015AA016106); Zhengzhou Science and Technology Talents (131PLKRC644) and "Strategic Priority Research Program" of the Chinese Academy of Sciences (Grant No. XDA06010701).

References

[1] J. Xu, P. Guo, M. Zhao, R. F. Erbacher, M. Zhu, and P. Liu, "Comparing different moving target defense techniques," in *Proceedings of the 1st ACM Workshop on Moving Target Defense (MTD '14)*, pp. 97–107, ACM, Scottsdale, Ariz, USA, 2014.

[2] K. Sun and S. Jajodia, "Protecting enterprise networks through attack surface expansion," in *Proceedings of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation (SafeConfig '14)*, pp. 29–32, ACM, Scottsdale, Ariz, USA, 2014.

[3] P. Larsen, S. Brunthaler, and M. Franz, "Security through diversity: are we there yet?" *IEEE Security & Privacy*, vol. 12, no. 2, pp. 28–35, 2014.

[4] D. Evans, A. Nguyen-Tuong, and J. Knight, "Effectiveness of moving target defenses," in *Moving Target Defense*, vol. 54 of *Advances in Information Security*, pp. 29–48, Springer, New York, NY, USA, 2011.

[5] M. Green, D. C. MacFarland, D. R. Smestad, and C. A. Shue, "Characterizing network-based moving target defenses," in *Proceedings of the 2nd ACM Workshop on Moving Target Defense (MTD '15)*, pp. 31–35, ACM, Denver, Colo, USA, October 2015.

[6] R. Zhuang, S. Zhang, S. A. DeLoach et al., "Simulation-based approaches to studying effectiveness of moving-target network defense," in *Proceedings of the National Symposium on Moving Target Research*, pp. 39–44, 2012.

[7] K. Zaffarano, J. Taylor, and S. Hamilton, "A quantitative framework for moving target defense effectiveness evaluation," in *Proceedings of the 2nd ACM Workshop on Moving Target Defense*, pp. 3–10, ACM, Denver, Colo, USA, October 2015.

[8] L. Wang, M. Zhang, S. Jajodia et al., "Modeling network diversity for evaluating the robustness of networks against zero-day attacks," in *Computer Security—ESORICS 2014*, pp. 494–511, Springer, 2014.

[9] R. Zhuang, S. A. DeLoach, and X. Ou, "A model for analyzing the effect of moving target defenses on enterprise networks," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference (CISRC '14)*, pp. 73–76, April 2014.

[10] T. E. Carroll, M. Crouse, E. W. Fulp, and K. S. Berenhaut, "Analysis of network address shuffling as a moving target defense," in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 701–706, IEEE, Sydney, Australia, June 2014.

[11] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 273–284, May 2002.

[12] L. Wang, S. Noel, and S. Jajodia, "Minimum-cost network hardening using attack graphs," *Computer Communications*, vol. 29, no. 18, pp. 3812–3824, 2006.

[13] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 217–224, ACM, Washington, DC, USA, November 2002.

[14] J. B. Hong and D. S. Kim, "Performance analysis of scalable attack representation models," in *Security and Privacy Protection in Information Processing Systems*, pp. 330–343, Springer, Berlin, Germany, 2013.

[15] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[16] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare & Security Research*, vol. 1, pp. 80–85, 2011.

[17] Y. Fu, H. Cheng-Li, X. Ping-Wu et al., "Detecting APT attacks: a survey from the perspective of big data analysis," *Journal on Communications*, vol. 36, no. 11, pp. 1–14, 2015 (Chinese).

[18] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, "MT6D: a moving target IPv6 defense," in *Proceedings of the IEEE Military Communications Conference (MILCOM '11)*, pp. 1321–1326, Baltimore, Md, USA, November 2011.

[19] C. A. Shue, A. J. Kalafut, M. Allman et al., "On building inexpensive network capabilities," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 2, pp. 72–79, 2012.

[20] J. Yackoski, H. Bullen, X. Yu, and J. Li, "Applying self-shielding dynamics to the network architecture," in *Moving Target Defense II*, vol. 100 of *Advances in Information Security*, pp. 97–115, Springer, New York, NY, USA, 2013.