doi:10.11959/j.issn.1000-436x.2017015

基于变点检测的网络移动目标防御效能评估方法

雷程[1,3]，马多贺[2]，张红旗[1,3]，杨英杰[1,3]，王淼[2]

（1. 信息工程大学密码工程学院，河南 郑州 450001；
2. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；
3. 河南省信息安全重点实验室，河南 郑州 450001）

摘 要：提出一种基于变点检测的网络移动目标防御效能评估方法。针对网络资源图无法表示资源脆弱性对节点安全状态影响的问题，定义分层网络资源图，在建立资源脆弱性改变和节点安全状态转换关联关系的同时，提高构建和更新网络资源图的效率。针对静态检测度量无法准确度量网络移动目标防御动态改变的问题，设计变点检测和标准化度量算法，在保证度量标准统一的基础上实现对网络移动目标防御的安全成本和安全收益的实时检测和动态度量，提高评估的准确性和结果的可比性。典型实例分析证明了所提出的网络移动目标防御效能评估方法的可行性和有效性。

关键词：网络移动目标防御；分层网络资源图；变点检测；标准化度量；效能评估

中图分类号：TP393 **文献标识码**：A

Performance assessment approach based on change-point detection for network moving target defense

LEI Cheng[1,3], MA Duo-he[2], ZHANG Hong-qi[1,3], YANG Ying-jie[1,3], WANG Miao[2]

(1. Cryptography Engineering Institute, Information Engineering University, Zhengzhou 450001, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China;
3. Henan Key Laboratory of Information Security, Zhengzhou 450001, China)

Abstract: A performance assessment approach based on change-point detection for network moving target defence was proposed. Directed to the problem of network resource graph not being able to present the effect of network resource vulnerabilities to network nodes, a conversion relationship between resource vulnerability changes and node security states was established by defining the concept of a hierarchical network resource graph and the efficiency of resource graph construction and updating were improved. Furthermore, directed to the problem of static detection algorithm not being able to precisely measure the dynamic change of network moving target defense, a change-point detection algorithm and standard degree measurement algorithm was designed. The security cost and benefit of network moving target defense in real-time and dynamically on the basis of unified metrics were defected and measured, which improved the evaluation accuracy. The analysis result of typical examples has proved the feasibility and the effectiveness of the proposed approach.

Key words: network moving target defense, multi-layer network resource graph, change-point detection, standardized measurement, performance assessment

收稿日期：2016-04-28；**修回日期**：2016-11-12

通信作者：马多贺，maduohe@iie.ac.cn

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2011CB311801）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2012AA012704, No.2015AA016106）；郑州市科技领军人才基金资助项目（No.131PLKRC644）；中国科学院先导专项基金资助项目（No.XDA06010701）

Foundation Items: The National Basic Research Program of China (973 Program) (No.2011CB311801), The National High Technology Research and Development Program of China (863 Program)(No.2012AA012704, No.2015AA016106), Zhengzhou Science and Technology Talents Project (No.131PLKRC644), Strategic Priority Research Program of the Chinese Academy of Sciences (No.XDA06010701)

1　引言

当前的网络系统具有确定性、静态性和同质性的特点，攻击者一旦掌握了特定的漏洞信息，就能在脆弱性时间窗内构造攻击、入侵系统，并能够低成本地复制攻击到更大范围的类似网络系统。日益复杂的攻击手段和层出不穷的零日漏洞，使传统的静态防御方法愈加被动。

为了改变这种攻防不对称的局面，移动目标防御（MTD, moving target defense）[1~3]应运而生，它的核心思想是“创建、评估和部署多样性的、不断转变的和随时间变化的机制与策略，以增加攻击者攻击的复杂性和成本，限制漏洞被暴露和被攻击的机会，并增加系统的弹性”。通过对目标系统的攻击面[4]进行多层次、持续和动态的转变，以增加攻击者的攻击成本和代价，降低入侵成功率直至迫使攻击者放弃攻击，从而提高防御目标的安全性。网络移动目标防御(NMTD, network moving target defense)通过动态、随机化网络属性配置，能够大大提高攻击者探测网络目标的难度，从而有效抵御多种网络攻击。目前，研究者已经提出多种 NMTD 技术和实现方法[5]，而如何有效评估 NMTD 的安全效果成为当前研究的重点和难点之一。

通过对已有 NMTD 研究的分析，可以将已有关于 NMTD 有效性的评估方法分为以下 4 类。

1) 基于攻防实验的实证分析[6]。通过分析若干攻防实例，提出随机多态化防御模型，验证了 NMTD 的有效性猜想。但此方法仅定性地分析了 NMTD 的防御有效性，且受限于实际样本量大的限制，难以用于评估广泛意义上的 NMTD 实施效能。

2) 基于模拟仿真的实证分析[7~9]。Green 等[7]通过分析网络杀伤链和典型的 NMTD 方案，提出了评估 NMTD 有效性的指标；Clark 等[8]则对基于欺骗的 IP 跳变方法进行了评估，通过分析引入的虚假节点数量以及真实节点与虚假节点 IP 的随机化程度，对欺骗型 NMTD 的防御收益进行了评估；Zhuang 等[9]以保守攻击图为基础，通过对 NMTD 方案进行仿真实验定性说明其有效性。基于模拟仿真的实证分析方法由于不依赖于样本数量，可在一定程度上解决评估的通用性问题。然而，由于仿真基于先验知识对攻击行为和系统状态变化进行描绘，无法评估 NMTD 对诸如零日攻击等新型未知攻击的防御有效性。

3) 基于数学模型的抽象分析[10~14]。文献[10]提出了一种基于攻击转移概率关系的可扩展量化模型；Carroll 等[11]提出了一种基于 URN 概率模型的网络地址跳变性能评估方法；文献[12]提出了一种基于攻击面的量化转移评估方法；Okhravi 等[13]提出了基于马尔可夫模型的 NMTD 评估方法；Han 等[14]通过构建传染病动力学模型对 NMTD 的实施进行了建模。然而，基于数学模型的抽象分析方法仅考虑了单一任务下 NMTD 的效能，与实际网络系统多步骤且任务并行的特性不符。其抽象性易与实际网络条件产生偏差。

4) 基于混合方法的分析。混合方法是对上述方法优缺点的一种取长补短的探索组合。Zaffarano 等[15]采用基于混合方法的分析架构，提出了基于活动模型的 NMTD 量化框架，它通过仿真实验对比任务模板和攻击模板下 NMTD 的实施效果，并在此基础上抽象分析了 NMTD 防御实施的成本消耗和安全收益。

通过分析可知，虽然基于攻防实验和模拟仿真的评估方法的评估结果准确性高，但是由于不同实验条件的适用范围有限，且不同环境中脆弱性利用率的量化标准难以统一，导致不同应用环境之间评估的 NMTD 实施效能难以相互比较。基于数学模型的抽象分析方法虽然可以有效比较不同 NMTD 的实施效果，但因为抽象过程中度量的局限性，导致评估结果与实际情况有偏差。

因此，现有评估方法存在以下 2 个问题：1) 由于资源脆弱性的改变和节点安全状态转换之间缺乏映射关系，导致评估过程出现失真；2) 由于现有检测度量方法难以准确刻画攻防双方对资源脆弱性利用难易度的影响，导致评估结果存在偏差。因此，针对以上不足，本文提出基于变点检测的网络移动目标防御效能评估方法。

2　预备知识

2.1　网络攻击图与网络资源图

网络攻击图(AG, attack graph)是一种通过图形表达可能的攻击路径、系统状态转移关系的方法，用以描述潜在入侵路径。现有攻击图主要分为状态攻击图[16]和属性攻击图[17]这 2 类。状态攻击图的每个节点代表系统全局状态，随着网络规模的增大，它存在创建效率低、易引发组合空间爆炸的问题。为此，Ammann[18]等将恶意敌手能力的“单调性”假设引入到分析模型中。属性攻击图就是建立在

“单调性”假设基础上的，它不会随着节点数量的增加而出现空间爆炸的问题，呈现出良好的可扩展性。然而，由于恶意敌手实施入侵会采用未知新型攻击和已知攻击相结合的方法，现有攻击图是基于已知漏洞利用的先验概率，无法完整刻画恶意敌手可能的攻击路径；此外，由于攻击图仅反映了攻击行为和系统状态的变化情况，并未考虑防御策略对系统状态的影响。因此，为了能评估 NMTD 的防御效能，Wang 等[17]在属性攻击图的基础上提出了网络资源图的概念，它是一种通过图形表达资源依赖关系和系统状态转移的方法，其形式化定义如下。

定义 1 网络资源图[17]（NRG, network resource graph）是由 NRG(N, E) 组成的双边有向图。N 是顶点集合，它可以表示为 $N = N_{\mathrm{v}} \bigcup N_{\mathrm{c}}$，$N_{\mathrm{v}} = \{<r, h_{\mathrm{s}}, h_{\mathrm{d}}> | r \in res(h_{\mathrm{d}})$，$h_{\mathrm{s}}, h_{\mathrm{d}} \in H\}$ 是目的节点 h_{d} 中可被源节点 h_{s} 利用的网络资源脆弱性集合；N_{c} 是资源的状态属性集合，它可以分为初始状态属性和中间状态属性，其中，初始状态属性可以表示为 $N_{\mathrm{ci}}\{n_{\mathrm{ci}} | \exists e \in E, \mathrm{s.t.}(e, N_{\mathrm{ci}}) \in (e \times N_{\mathrm{c}})\}$，中间状态属性表示为 $N_{\mathrm{c}} - N_{\mathrm{ci}}$。$E$ 是有向边集合，它可以表示为 $E=E_{\mathrm{r}} \cup E_{\mathrm{i}}$，其中，$E_{\mathrm{r}}=(N_{\mathrm{c}} \times N_{\mathrm{v}})$ 表示前置条件，$E_{\mathrm{i}}=(N_{\mathrm{v}} \times N_{\mathrm{c}})$ 表示后置条件。

不同于已知攻击，未知新型攻击主要通过目标节点提供的服务进行接入和提权，并在此基础上通过让目标节点达到特定状态而成功入侵。因此，网络资源脆弱性的利用 E 可以表示为 $E = <srv, priv, conn>$，它描绘了成功入侵目的节点 h_{d} 所要开启的服务 $srv \in \{srv(h_{\mathrm{d}}) \to 2^{S}\}$、所要拥有的权限 $priv \in \{priv(h_{\mathrm{d}}) \to 2^{P}\}$ 以及入侵节点与目标节点间的连通性 $conn \in \{conn(H \times H)\}$（$H$ 表示网络中的节点集合）。其中，一次脆弱性的利用过程称为原子攻击，它是攻击过程中的最小执行单元，是导致节点状态发生变迁的原因。

然而，恶意敌手是通过侦测不同资源可用性，利用其脆弱性的关联关系和其工作流的缺陷改变节点状态属性以实施入侵的[3]；NMTD 跳变则是基于安全目标定制安全策略，通过限定节点状态属性协同改变资源配置以进行防御的[19]。因此，需要建立节点资源脆弱性利用和节点状态属性改变的映射关系。与此同时，由于 NMTD 具有动态改变的特性，NRG 的更新效率将是其能否有效评估 NMTD 的关键。所以，NRG 的构建与更新应防止由于计算复杂度过高而导致实时性差的问题。

2.2 通用脆弱性评分系统

通用脆弱性评分系统[20](CVSS, common vulnerability scoring system)是一个由公共发起的，旨在度量和量化脆弱性及其影响的平台。CVSS 通过提供全部评估参数细节，让使用者了解总体度量的由来，实现评估架构的广泛开放；通过采用无关应用的框架结构让所有脆弱性度量都可以采用同一个框架，实现评分标准的规范统一；通过动态度量集合结合脆弱性的实际环境，实现对资源脆弱性本体利用难易度的量化。如图 1 所示，CVSS 主要由基本度量集合(BMG, base metric group)、时变度量集合(TMG, temporal metric group)和环境度量集合(EMG, environmental metric group) 3 个部分组成。其中，BMG 度量了资源脆弱性固有的基本属性，它不随时间和环境的改变而改变；TMG 和 EMG 则分别度量了资源脆弱性随时间和环境变化而变化的属性。

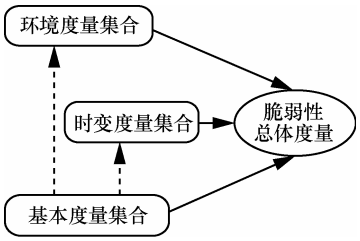


图 1 CVSS 评估架构

虽然 CVSS 为资源脆弱性的不同属性进行了量化赋值以便对其本体利用难易度进行评价，但是由于 CVSS 无法检测度量攻防双方对资源脆弱性利用的影响，导致无法动态评估资源脆弱性利用的难易程度，继而造成评估的结果出现偏差的问题。1) 若不同类资源脆弱性之间存在依赖关系，一旦其中某一种脆弱性交易被恶意敌手利用，则其他与之存在依赖关系的资源脆弱性的利用率将增加；2) 对于相同类型资源的脆弱性，若恶意敌手在某一节点上成功利用该种脆弱性，那么恶意敌手在网络其他节点利用同种脆弱性的成功率将增加；3) 由于网络节点状态属性的转移服从马尔可夫链特性[10]，因此，上一时刻 NMTD 的实施将影响下一时刻资源脆弱性利用的难易度。

3 基于分层资源图的变点检测与标准化度量算法

所谓“变点”[21]是指网络中发生改变的节点，本文所指的变点是随着恶意敌手入侵或 NMTD 跳

变而发生改变的节点安全状态和资源脆弱性。

基于变点检测的网络移动目标防御效能评估方法将分层[22]的思想引入网络资源图，定义了分层网络资源图(MRG, multi-layer network resource graph)，算法以分层网络资源图为基础，通过检测和度量变点的改变量进而分析实施 NMTD 的效能。其整体架构如图 2 所示，它由分层资源图构建与更新、变点检测与标准化度量以及效能评估 3 个部分组成。

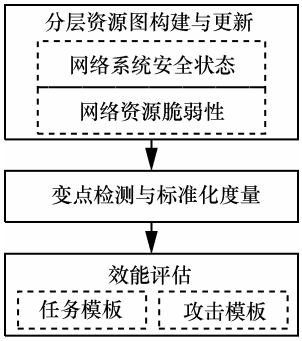


图 2　效能评估整体架构

首先，本文针对现有网络资源图无法建立资源脆弱性和节点安全状态关联的问题，引入分层网络资源图的概念，在构建资源脆弱性改变和节点安全状态转换之间的桥梁的同时提高了更新的实时性。其次，针对静态检测度量资源的改变难以准确描述 NMTD 实施效果的问题，提出变点检测与标准化度量算法。采用图相似理论检测 NMTD 实施前后 MRG 中的变点，并对变点的利用率进行标准化度量和计算。将不同资源依赖关系、同类资源关联度和相邻时刻节点状态属性与 CVSS 量化相结合，从而在保证度量标准统一的同时实现动态度量。最后，效能评估阶段分别从任务模板和攻击模板中计算防御实施的安全成本和收益，综合分析 NMTD 的实施效能，从而为实现系统可用性与 NMTD 防护有效性的平衡提供指导。

3.1　分层网络资源图的构建与更新

针对资源脆弱性的改变和节点安全状态转换之间缺乏映射关系的问题，定义了分层资源图的概念，其形式化描述如定义 2 所示。它将网络资源图分为资源层和节点层，资源层描述了恶意敌手在一个节点内利用脆弱性入侵的所有可能偏序关系；节点层描述了由于恶意敌手入侵或者 NMTD 跳变导致的网络节点状态转移。网络逻辑拓扑示例如图 3 所示。

定义 2　分层网络资源图是由 MRG(N, E) 组成的双边有向图。N 是顶点集合，它可以表示为 $N = N_{\mathrm{P}} \cup N_{\mathrm{R}}$，其中，$N_{\mathrm{P}}$ 是节点层的顶点集合，它表示网络节点的安全状态属性；N_{R} 是资源层中的顶点集合，它可以表示为 $N_{\mathrm{R}}=N_{\mathrm{v}} \cup N_{\mathrm{c}}$，它由资源的脆弱性 N_{v} 和资源的安全状态属性 N_{c} 共同组成。E 是有向边集合，它可以表示为 $E=E_{\mathrm{r}} \cup E_{\mathrm{i}}$，$E_{\mathrm{r}}=(N_{\mathrm{c}} \times N_{\mathrm{v}})$ 为前置条件，$E_{\mathrm{i}}=(N_{\mathrm{v}} \times N_{\mathrm{c}})$ 为后置条件，其中，节点层有向边表示为 $E_{\mathrm{P}} \subseteq E$；资源层有向边表示为 $E_{\mathrm{R}}=E$。

对于网络中任意节点 h，由于它包含了多种资源，因此，在资源层 $res(h)=\{N_{\mathrm{v}}^h | N_{\mathrm{v}}^h \in N_{\mathrm{v}}\}$，它表示节点 h 中所包含的资源脆弱性。相应地，节点 h 的状态属性是节点所含资源的状态属性集合[1]，它可表示为 $N_{\mathrm{P}}^h=\{N_{\mathrm{c}}^h | N_{\mathrm{c}}^h \in N_{\mathrm{c}}\}$，所以节点层中 $\forall n_{\mathrm{P}i}^h \in N_{\mathrm{P}}^h \subset N_{\mathrm{P}}$，资源层 $\exists N_{\mathrm{v}}^h \subseteq res(h)$，使 $n_{\mathrm{P}i}^h \subseteq \{N_{\mathrm{c}}^h\}$。由图 4 所示实例可知，图 4(b)是在图 4(a)基础上转

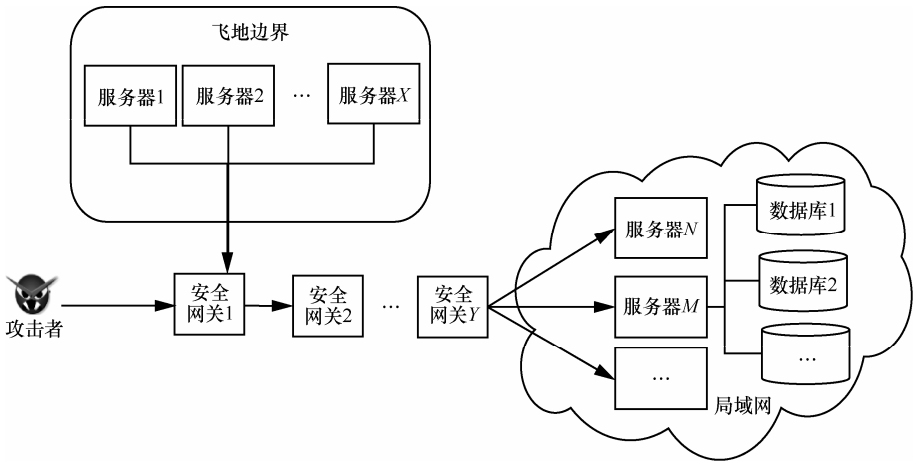


图 3　网络逻辑拓扑示例

化生成的分层网络资源图，其中，元素 a、F 分别表示可连通、防火墙。由此可知，MRG 实现了节点资源脆弱性利用的抽象化与节点状态转移的具体化，建立了节点资源脆弱性利用和节点状态属性改变的映射关系。

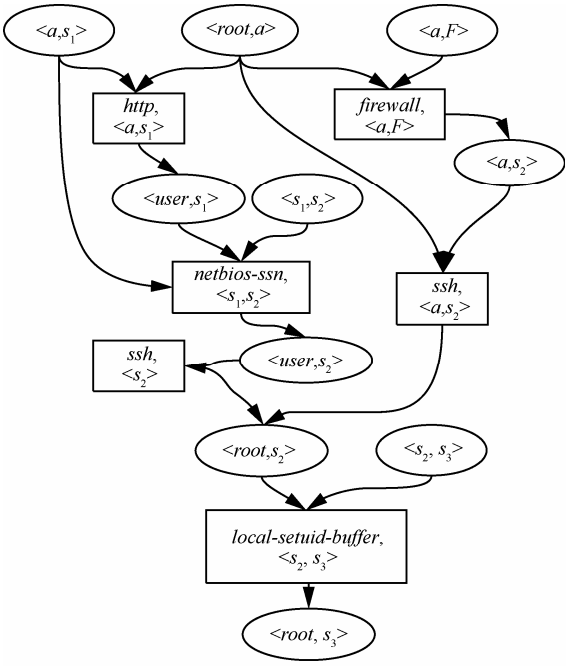


图 4　资源图与分层资源图示例

图 4 中椭圆代表网络节点的安全状态；方形代表资源的脆弱性；五边形代表资源的安全状态属性；< >表示连通性；（ ）表示用户的权限。

此外，为了能够较完备地刻画已知或未知攻击的攻击路径，在 MRG 的基础上定义了攻击路径的概念，其形式化描述如定义 3 所示。

定义 3　攻击路径(AP, attack path)是分层资源图 MRG(N, E) 中的原子攻击序列，若该序列满足以下约束，则称它为一条攻击路径。

1) 后面任意原子攻击的前提条件都是前面原子攻击的后果或者是初始状态属性。

2) 前面任意原子攻击的后果都是后面原子攻击的前提。

3) 该序列的最后一个原子攻击产生的后果是目标状态集合$\{n_{\mathrm{cg}}\}$的子集。

3.2　变点检测与标准化度量

针对现有度量方法难以准确刻画攻防双方对资源脆弱性利用影响的问题，提出变点检测与标准化度量算法，通过采用图相似理论检测 NMTD 实施前后 MRG 中的变点，并对其固有特性和可变特性进行标准化度量，以提供给下一步效能分析。算法具体流程如下所示。

算法 1　变点检测算法

输入：

$\mathrm{MRG}_t(N,E)$ //攻击实施前的 MRG

$\mathrm{MRG}_{t+1}(N',E')$ //一个攻击周期后的 MRG

输出：

$Exploit_+ \subseteq (N'-N\bigcap N')$// MRG_{t+1} 中增加的资源脆弱性

$P(n_{\mathrm{cg}})$ //实施跳变后恶意敌手成功入侵节点的概率

$<N,E>\leftarrow MST(G_t)$; //遍历 MRG

$<N',E'>\leftarrow MST(G_{t+1})$;

$<(N'-N\bigcap N'),(E'-E\bigcap E')>\leftarrow G'\setminus G\bigcap G'$;

for every $v'_{\mathrm{R}i}\in N'_{\mathrm{R}}$ do

{

if($v'_{\mathrm{R}i}$ in N'_{R}, $v'_{\mathrm{R}i}\notin N_{\mathrm{R}}$) then //为新增的资源

{

add $v'_{\mathrm{R}i}$ to $Exploit_+$

if there exists the same kind of resource as former resource

Calculate $P'(v_i)$;

else

Calculate $p(v_i|\wedge c_{\mathrm{I}})$, $PreCondn(v_i)$, $Post\text{-}Condn(v_i)$; //c_{I}表示初始状态属性

}

else if ($v'_{\mathrm{R}i}$ in N'_{R}, $v'_{\mathrm{R}i}\in N_{\mathrm{R}}$)//资源未被完全转移

{

Calculate $P(n^t_{\mathrm{P}i}|n^{t-1}_{\mathrm{P}i})$;//计算状态转移概率

Calculate $p(v_i|\wedge c_i)$, $PreCondn(v_i)$ and $PostCondn(v_i)$; //c_i表示泛在的状态属性

}}

end for

Calculate $P(n_{cg})$; //计算攻击路径最大成功概率

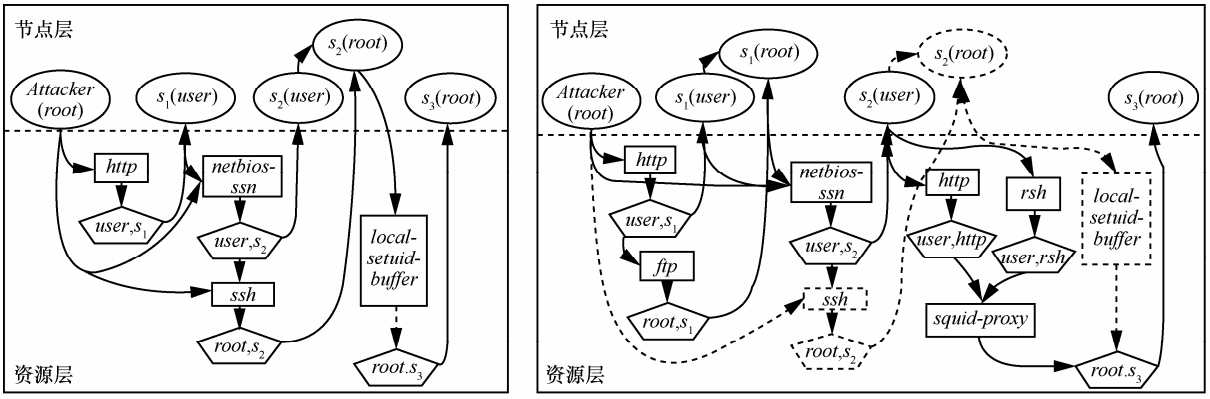
return $P(n_{cg})$ and $Exploit_{+}$

分别输入一段时间前后的分层网络资源图 MRG_t 和 MRG_{t+1}。利用最小生成树算法对 2 个 MRG 图进行遍历，若 MRG 中实施 NMTD 的变点存在新增资源，则只需考虑新增资源的固有特性与不同类型资源的依赖关系和与同类资源的关联度对恶意敌手资源利用的影响，并利用式(1)~式(5)计算恶意敌手利用资源的成功率；对于现有资源，则要通过检测节点层 (N_P, E_P) 和 (N'_P, E'_P) 的相似度，考虑随着 NMTD 跳变或恶意敌手攻击能力的改变，不同节点状态属性的改变对不同类型资源依赖关系和与同类资源关联度的影响，利用式(6)~式(10)计算节点前向转移、自转移和后向转移概率，并以转移后节点的状态属性作为初始状态计算节点中恶意敌手利用资源的成功率。最后，利用式(11)获得恶意敌手实施攻击的最大成功率及相应的攻击路径。

网络移动目标防御中防御策略转换是通过改变目标系统的网络属性来实现的，可以通过 MRG 的资源“变点”来进行抽象和评估。如图 5 所示，虚线表示已经被转移的变点(即资源脆弱性与节点状态属性)，由变点检测算法可知，$t+\Delta t$ 时刻 MRG 中资源层新增的资源脆弱性为 $Exploit_{+}=\{ftp,rsh,http,squid\text{-}proxy\}$，转移的资源脆弱性为 $Exploit_{-}=\{ssh,local\text{-}setuid\text{-}buffer\}$（如虚线部分所示）。其中，由于 s_1 中新增了 *ftp*，导致节点层中 s_1 增加了 $s_1(root)$ 状态属性；s_2 中转移了 *ssh*，导致节点层中 s_2 减少了 $s_2(root)$ 状态属性；而转移的资源脆弱性 *local-setuid-buffer* 与新增的资源脆弱性 *rsh*、*http* 和 *squid-proxy* 并未导致节点状态属性的改变。通过变点检测算法可知，由于在 $t+\Delta t$ 时刻，MRG 中资源脆弱性的改变，恶意敌手原有攻击路径 $ssh \rightarrow local\text{-}setuid\text{-}buffer$、$netbios\text{-}ssn \rightarrow ssh \rightarrow local\text{-}setuid\text{-}buffer$ 和 $http \rightarrow netbios\text{-}ssn \rightarrow ssh \rightarrow local\text{-}setuid\text{-}buffer$ 失效。但可通过 $http \rightarrow ftp \rightarrow netbios\text{-}ssn \rightarrow rsh \rightarrow squid\text{-}proxy$、$netbios\text{-}ssn \rightarrow rsh \rightarrow squid\text{-}proxy$、$http \rightarrow netbios\text{-}ssn \rightarrow rsh \rightarrow squid\text{-}proxy$、$http \rightarrow ftp \rightarrow netbios\text{-}ssn \rightarrow http \rightarrow squid\text{-}proxy$、$netbios\text{-}ssn \rightarrow http \rightarrow squid\text{-}proxy$ 和 $http \rightarrow netbios\text{-}ssn \rightarrow http \rightarrow squid\text{-}proxy$ 路径实施入侵。

由于变点的改变是由其固有特性（如资源的价值、资源存在的脆弱性等）和可变特性（如网络环境、不同资源的依赖和同类资源的关联度等）共同决定的，因此，标准化度量要能够有效度量变点的固有特性和可变特性。这就要求标准化度量满足以下 2 点：1) 在统一标准下对不同活动模型中的资源实施度量，从而为下一步评估和比较不同 NMTD 机制实施的效能提供归一化数据；2) 要结合资源所处的实际环境，动态度量其可变特性，以保证度量数据的可靠。

因此，本文算法在 CVSS 的基础上通过将攻防双方对资源脆弱性的影响因素加入到可变特性中，以保证评估数据的有效性。它主要体现在以下 2 个方面：1) 资源脆弱性的关联和依赖关系对攻击实施的影响，即不同类型资源间的依赖关系和相同类型资源间的关联关系对攻击实施的影响；2) 采取的防御措施对资源脆弱性利用的削弱和影响，即上一时



(a) *t*时刻的MRG　　(b) *t*+Δ*t*时刻的MRG

图 5　*t* 和 *t*+Δ*t* 时刻的 MRG

刻 NMTD 的实施对下一时刻攻击利用资源脆弱性难易度的影响。

标准化度量通过转换 CVSS 中 TMG 和 EMG，以实现量化资源脆弱性的关联和依赖关系对攻击实施的影响；通过引入关联度参数，以计算相同类型资源的关联关系对攻击成功率的影响。对于防御措施对资源脆弱性利用的削弱和影响，通过引入转移因子以计算每次跳变后节点状态转移对攻击成功率的影响。由于恶意敌手是通过利用不同资源脆弱性使节点状态发生转移的；NMTD 跳变则是使网络节点整体状态发生转移。因此，MRG 在资源层中计算不同资源的依赖关系和同类资源的关联度；在节点层计算相邻时刻节点状态属性的转移。如图 6 所示，假设节点 h 中有 3 种不同类型资源脆弱性 v_1、v_2 和 v_3，其依赖关系如图。$c_1 \sim c_3$ 为初始状态属性(c_1)，c_5 和 c_6 为目标状态属性(c_{ng})。T_{A} 为网络攻击持续的周期，T_{MTD} 为节点实施 NMTD 的周期。

在资源层，恶意敌手若能成功利用资源脆弱性，必须同时满足固有特性、前置条件和后置条件，其中，前置条件和后置条件又由资源可变特性决定。资源脆弱性的固有特性被成功利用的概率计算如式(1)所示，它表示在前置条件同时被满足的条件下，资源脆弱性的可利用概率。当资源脆弱性存在多个前置条件需要满足时，只有所有的前置条件被同时满足，恶意敌手才能够成功利用该资源脆弱性。因此，脆弱性 v_2 的前置条件存在多条件合取关系，其概率计算如式(2)所示。对于资源的后置条件，当某一状态属性可通过利用多种资源脆弱性被满足时，恶意敌手只要成功利用其中任意资源脆弱性即可达到该后置条件。因此，后置条件 c_4 存在多脆弱性析取关系，其概率计算如式(3)所示。不同资源间的前置和后置条件是由不同资源的依赖关系决定的，它随着网络连通性、配置信息等因素的变化而改变。因此，不同资源的依赖关系如式(4)所示。

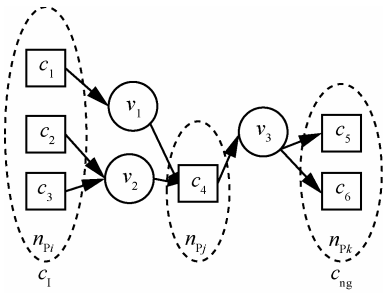


图 6 节点 h 中不同资源依赖关系

$$P(v_i|\wedge c_1)=\frac{\mathrm{CVSS}_{\mathrm{BMS}}(p_i)}{10} \tag{1}$$

$$PreCondn(v_2)=P(c_1)P(c_2) \tag{2}$$

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

$$P(c_i)=\frac{\mathrm{CVSS}_{\mathrm{TMS}}(p_i)\mathrm{CVSS}_{\mathrm{EMS}}(p_i)}{100} \tag{4}$$

由以上分析可知，恶意敌手在成功利用节点 h 中资源脆弱性 v_1 的概率为 $P(v_1)=P(c_1)P(v_1|c_1)P(c_4)$。然而，由于不同网络节点中存在相同的资源类型，如不同网络节点都提供了 *http* 服务，一旦恶意敌手在某一节点成功利用了 *http* 的脆弱性，之后再利用该类资源脆弱性时的成功率将提高。这是因为对于相同类型的资源脆弱性，虽然其在不同网络节点中的配置信息不尽相同，但是其脆弱性的固有特性是相同的，因此，一旦恶意敌手成功利用了某类资源的脆弱性，其之后利用同类资源脆弱性的成功率将提高。本文引入了关联度参数的概念，其形式化描述如定义 4 所示。

定义 4 给定分层资源图 MRG(N,E)，对于 $\forall n_{v1},n_{v2}\in N_{\mathrm{v}}$，若 n_{v1}、n_{v2} 属于相同类型的资源，那么 n_{v1}、n_{v2} 的关联度(correlativity)为 $c(n_{v1},n_{v2}):[1,x]\times[1,x]\rightarrow[0,1]$。其中，$x$ 表示资源所有可能的配置。

在引入关联度参数的基础上，同类型脆弱性被反复利用满足的条件概率如式(5)所示。其中，$P(v_i)=P(v_i|\wedge c_i)\prod P(c_i)$。

$$P'(v_i)=cP(v_i) \tag{5}$$

在节点层，由于节点的状态属性与恶意敌手在节点中资源脆弱性的利用和该节点上一周期跳变的结果相关，因此，节点在 t 时刻的状态转移概率如式(6)所示。它表示 t 时刻 $n_{\mathrm{P}i}$ 节点的状态属性是由 $t-1$ 时刻该节点的状态属性和转移的状态属性共同决定的。

$$P(n_{\mathrm{P}i}^t)=P(n_{\mathrm{P}i}^t|n_{\mathrm{P}i}^{t-1})P(n_{\mathrm{P}i}^{t-1}) \tag{6}$$

由于 NMTD 的本质是通过系统、动态地转移攻击面而改变节点的状态属性，使恶意敌手的既得资源和特权失效，无法为其实施进一步的攻击提供支持。因此，恶意敌手可能会滞留在攻击路径的某一节点的状态属性，甚至回退到当前攻击路径上其他节点的任意状态属性。以图 7 为例，节点的状态转移可分为前向转移、自转移和后向转移，具体如

式(7)所示。本文通过引入“转移因子”以计算节点的状态转移概率，可表示为 $\varphi = 1 - \frac{m}{n}$。它表示一次跳变周期后状态属性未发生转移的概率，其中，n 表示可变的状态总数， m 表示实际实施跳变的状态个数。

$$P(n_{\mathrm{P}}^{t}|n_{\mathrm{P}}^{t-1})\begin{cases} P_{kj}(n_{\mathrm{P}k}^{t}|n_{\mathrm{P}k}^{t-1}) \\ P_{jj}(n_{\mathrm{P}j}^{t}\mid n_{\mathrm{P}j}^{t-1}) \\ P_{ij}(n_{\mathrm{P}i}^{t}|n_{\mathrm{P}i}^{t-1}) \end{cases} \tag{7}$$

1) 所谓前向转移是指恶意敌手所处节点状态属性的前置条件由于发生跳变而导致恶意敌手回退到该攻击路径上其他节点的状态属性。由于MRG的构建遵循“单调性假设”，它是保证 MRG 不发生状态空间爆炸的基础；而前向转移会导致在 MRG 构建中无法再遵循“单调性假设”。因此，通过自转移和后向转移间接引入前向转移以防止状态空间爆炸的问题。

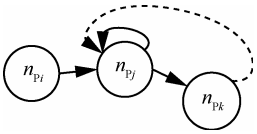


图 7　节点 h 状态转移示例

为了便于观察，将图 6 中节点状态转移抽象如图 7 所示。由于跳变后 $n_{\mathrm{P}k}$ 的前置条件中存在资源和特权失效， $n_{\mathrm{P}k}$ 会发生前向转移。它的前向转移概率可以看作是该条攻击路径上距此节点最近的未发生状态改变的节点 $n_{\mathrm{P}i}$ 的后向转移概率与失效节点 $n_{\mathrm{P}i}$ 的自转移概率的联合概率。因此，如式(8)所示，前向转移概率可利用自转移概率和后向转移概率对进行等价转换，以保证攻击图构建遵循“单调性假设”。

$$P_{kj}(n_{\mathrm{P}k}^{t}|n_{\mathrm{P}k}^{t-1}) = P_{ij}(n_{\mathrm{P}i}^{t}|n_{\mathrm{P}i}^{t-1})P_{jj}(n_{\mathrm{P}j}^{t}\mid n_{\mathrm{P}j}^{t-1}) \tag{8}$$

2) 所谓自转移是指恶意敌手所处的节点状态属性由于发生跳变而导致恶意敌手滞留在该节点其他的状态属性。它包含 2 种情况：① 在攻击持续时间 T_{A} 内，若 NMTD 跳变周期为 T_{MTD}，跳变后节点状态 $n_{\mathrm{P}j}$ 没有发生改变，但其后置条件发生改变导致恶意敌手无法实施入侵进而将节点状态从 $n_{\mathrm{P}j}$ 转移到 $n_{\mathrm{P}k}$，其概率为 $\varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}(1-P(v_3))^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}$；② 在攻击持续时间 T_{A} 内，若 NMTD 跳变周期为 T_{MTD}，节点状态 $n_{\mathrm{P}j}$ 及其后置条件都没有改变，但与其邻接的节点状态 $n_{\mathrm{P}k}$ 发生跳变，从而导致节点状态的自转移。其概率为 $\varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}(1-\varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}})(1-(1-P(v_3))^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}})$。由此，自转移概率如式(9)所示。

$$P_{jj}(n_{\mathrm{P}j}^{t}\mid n_{\mathrm{P}j}^{t-1}) = \varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}(1-P(v_3))^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}} + \varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}(1-\varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}})(1-(1-P(v_3))^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}) \tag{9}$$

3) 所谓后向转移是指恶意敌手所处的节点状态属性和其前置条件在发生跳变时均未发生改变，其转移概率如式(10)所示。若 $n_{\mathrm{P}j} \in N_{ci}$，后向转移概率可表示为 $\varphi^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}P(v_3)$。

$$P_{jk}(n_{\mathrm{P}i}^{t}|n_{\mathrm{P}i}^{t-1}) = \varphi^{\frac{2T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}(1-(1-P(v_3))^{\frac{T_{\mathrm{A}}}{T_{\mathrm{MTD}}}}) \tag{10}$$

以图 5 为例，恶意敌手在 t 时刻从初始状态条件到目标节点状态属性所有可能的路径如表 1 所示，其中，最短攻击路径为路径 5 和 6；利用不同资源脆弱性最少的攻击路径是路径 1、5 和 6。由于现有评估方法[21]常通过分析最短攻击路径的成功率判断恶意敌手成功入侵的最大概率，因此，易导致评估结果出现偏差。如当攻击路径 1 中恶意敌手成功利用 *http* 资源脆弱性的概率为 0.35，c=0.8；攻击路径 5 中恶意敌手成功利用 *http* 资源脆弱性的概

表 1　　**攻击路径**

编号	入侵路径	入侵步骤	存在资源脆弱性类型/种
1	$rootA \to http \to user,s_1 \to netbios\text{-}ssn \to user,s_2 \to http \to squid\text{-}proxy \to root,s_3$	4	3
2	$rootA \to http \to user,s_1 \to netbios\_ssn \to user,s_2 \to rsh \to squid\text{-}proxy \to root,s_3$	4	4
3	$rootA \to http \to user,s_1 \to ftp \to root,s_1 \to netbios\text{-}ssn \to user,s_2 \to http \to squid\text{-}proxy \to root,s_3$	5	4
4	$rootA \to http \to user,s_1 \to ftp \to root,s_1 \to netbios\text{-}ssn \to user,s_2 \to rsh \to squid\text{-}proxy \to root,s_3$	5	5
5	$rootA \to netbios\text{-}ssn \to user,s_2 \to http \to squid\text{-}proxy \to root,s_3$	3	3
6	$rootA \to netbios\text{-}ssn \to user,s_2 \to rsh \to squid\text{-}proxy \to root,s_3$	3	3

率为 0.22；攻击路径 6 中恶意敌手成功利用 *rsh* 资源脆弱性的概率为 0.17，剩余资源脆弱性利用率相同。则恶意敌手入侵概率最大的攻击路径是路径 1。这是因为可假设恶意敌手是理性的，它会在所有可能的入侵路径中选择攻击成本低、成功率高的脆弱性包含在攻击路径中。因此，如式(11)所示，通过综合分析入侵步骤、资源脆弱性利用率和不同脆弱性数量得到某条攻击路径的成功率，其中，c_1 为初始状态属性。

$$P(n_{\text{cg}})=\operatorname{argmax}\prod_{\text{P}i=1}^{n}\left\{P(n_{\text{P}_i}^{t}|n_{\text{P}_i}^{t-1})\left\{P(c_1)\prod_{i=\text{source}}^{\text{target}}(cP(v_i)P(c_i))\right\}\right\} \tag{11}$$

假设网络中有 u 个节点，每个节点有 v 种不同类型的资源，基于分层资源图的变点检测算法的计算复杂度如表 2 所示。

表 2 算法计算复杂度

资源图类型	构建计算复杂度	更新计算复杂度	遍历
NRG	$O(m^2n^2)$	$O(mn)$	$O(u!v!^u)$
MRG	$O(m^2n+n^2)$	节点层：$O(n)$ 资源层：$O(m)$	$O(u!v!)$

相较于 NRG[17]，该算法在不改变资源的依赖关系的同时有效降低资源图构建和更新的计算复杂度，具有良好的可扩展性和实时性。表 2 给出了 NRG 算法与 MRG 算法在构建、更新和遍历 3 个维度上的计算复杂度对比，从算法分析的角度论证了本文算法的优势。

4 效能评估

NMTD 的效能是由实施防御的安全成本和产生的安全收益共同组成的，本文仅考虑与攻防行为相关的代价和回报[23]。NMTD 实施成本主要是指防御策略对系统可用性的影响以及防御实施消耗的软硬件资源。由于在部署 NMTD 的网络系统中运行成本可分为 NMTD 的实施成本和网络执行任务时的运行开销，因此，对 NMTD 安全成本的评估可通过对比分析实施 NMTD 前后网络执行某项任务时运行效率和成功率的改变量获得。NMTD 的安全收益是指 NMTD 实施前后对恶意敌手实施某种入侵的影响。它可分为直接防御收益和间接防御收益，直接防御收益是指通过实施防御减少的攻击收益；间接防御收益则是指通过实施防御增加的攻击成本。因此，可通过分析恶意敌手入侵成功率和入侵效率的改变量共同决定。

基于以上分析，本文借鉴活动模板[7]的思想，分别利用 NMTD 实施前后任务模板和攻击模板中攻防成本和收益的改变量描述 NMTD 实施的安全成本和安全收益，具体如表 3 所示。活动模板是由任务实施的行为集合和行为属性集合共同组成的，可形式化表示为 $<T,A>$。其中，$T=\{\tau_1,\tau_2,\cdots,\tau_n\}$ 表示行为集合；$A=\{\alpha_1,\cdots,\alpha_m\}$ 表示行为属性集合。活动模板中一次“执行”被抽象为一个从任务实施行为和行为属性到行为属性量化值域的映射，可表示为 $\nu:T\times A\to V$。本文任务模板是描述执行某项任务时网络行为的具体活动模板；攻击模板则是描述恶意敌手具体入侵某个目标时攻击行为的活动模型。

表 3 NMTD 实施的评估指标

模板类型	任务模板	攻击模板	
未实施 NMTD	性能开销基线	攻击成本基线	攻击收益基线
实施 NMTD	综合性能开销	攻击成本	攻击收益

运行效率描述了活动模板完全实施某项活动的快慢程度。任务模板中运行效率 Productivity(M) 如式(12)所示，它描述了网络运行某项任务的快慢程度。其中，$\nu:\tau\times t_{\text{duration}}\to V_{\text{Productivity}}$ 是运行某项任务的一系列行为 τ 和每个行为的运行持续时间 t_{duration} 到量化值域 $V_{\text{Productivity}}$ 的映射，$V_{\text{Productivity}}\in[0,1)$。攻击模板中运行效率 Productivity($A$) 如式(13)所示，它描述了恶意敌手在网络杀伤链各阶段入侵目标节点的平均快慢程度。其中，$\nu:\tau\times t_{\text{duration}}\to V_{\text{Productivity}}$ 是某一阶段的一系列攻击行为 τ 和每个攻击行为持续时间 t_{duration} 到量化值域 $V_{\text{Productivity}}$ 的映射，$V_{\text{Productivity}}\in[0,1)$。

$$\text{Productivity}(M)=\frac{1}{|n|}\sum_{i=1}^{n}\nu(\tau_i,t_{\text{duration}}^{i}) \tag{12}$$

$$\text{Productivity}(A)=\frac{1}{|n|}\sum_{j=R}^{AO}\sum_{i=1}^{n}j\nu(\tau_i,t_{\text{durationi}}) \tag{13}$$

运行成功率描述了活动模型成功实施某项活动的概率。由于所拥有的资源价值及所提供服务的重要程度不同，所以节点的重要程度就不同。不同节点实施 NMTD 后性能的改变将会导致对整个网络性能的影响不同；且恶意敌手成功入侵的节点重

要性决定了该攻击对整个网络产生的危害程度。因此，在计算运行成功率时引入危害系数 ω_i，$\omega_i \in [0,1]$，它刻画了节点在网络系统中的重要程度。任务模板描述了执行某项任务的成功率，如式(14)所示。$\nu: T \times A \to V_{\mathrm{S}}$ 是运行某项任务的一系列行为 τ 和每个行为执行成功率 $\frac{n_{\mathrm{success}}}{n_{\mathrm{total}}}$ 到量化值 V_{S} 的一个映射，$V_{\mathrm{S}} \in [0,1)$。攻击模板描述了恶意敌手成功入侵目标节点的危害程度，具体如式(15)所示。

$$P_{\mathrm{success}}(M) = \frac{1}{|n|}\sum_{i=1}^{n}\omega_i \nu\left(\tau_i, \frac{n_{\mathrm{success}}^i}{n_{\mathrm{total}}^i}\right) \tag{14}$$

$$P_{\mathrm{success}}(A) = \prod_{i=1}^{n}\omega_i P(n_{\mathrm{P}i}^t | n_{\mathrm{P}i}^{t-1})\left\{P(c_{\mathrm{I}})\prod_{Ri=\mathrm{source}}^{\mathrm{target}}(P(v_i)P(c_i))\right\} \tag{15}$$

NMTD 防御成本是指采用防御策略所耗费的资源（$Cost_{\mathrm{security}}$），以及实施防御导致的服务质量下降（$Cost_{\mathrm{perf}}$）。因此，如式(16)所示，利用任务模板中实施 NMTD 防御前后的性能改变度量。其中，性能开销基线是指在未实施 NMTD 条件下网络系统运行某项任务的开销，它由网络运行某项任务的运行效率和运行成功率共同组成；综合性能开销是指在实施 NMTD 条件下网络系统运行某项任务的开销，它由网络运行某项任务的运行效率和运行成功率共同组成。由于在一次攻击周期 T_{A} 内，NMTD 的防御成本与运行成功率和运行效率成反比，因此，可表示为

$$D_{\mathrm{cost}} = \sum_{i=0}^{\left\lfloor \frac{T_{\mathrm{A}}}{T_{\mathrm{NMTD}}} \right\rfloor} \Delta\left[\frac{\mathrm{Productivity}(M)}{P_{\mathrm{Success}}(M)}\right]$$

$$D_{\mathrm{cost}} = \Delta[Cost_{\mathrm{perf}} + Cost_{\mathrm{security}}] \tag{16}$$

NMTD 防御收益是指采用防御策略后降低的攻击成功率，以及实施防御导致的攻击成本增加。因此，如式(17)所示，利用攻击模板中实施 NMTD 防御后的直接防御收益（DDR, defense direct reward）和间接防御收益（DIR, defense indirect reward）度量。其中，*DDR* 是通过实施某种防御策略降低的攻击收益。攻击的收益则是指 NMTD 防御前后成功实施某种攻击所导致的危害程度，即 $DDR = A_{\mathrm{benefit}} = \Delta P_{\mathrm{success}}(A)$。*DIR* 是通过实施某防御策略增加的攻击实施成本。攻击的实施成本是指 NMTD 防御前后成功实施某种攻击的开销，它由恶意敌手实施某种攻击的入侵效率和入侵最大成功率共同组成，即 $DIR = A_{\mathrm{cost}} = \frac{\Delta \mathrm{Productivity}(A)}{P(n_{\mathrm{cg}})}$。因此，在一次攻击周期 T_{A} 内，NMTD 的防御收益具体可表示为

$$D_{\mathrm{benefit}} = \sum_{i=0}^{\left\lfloor \frac{T_{\mathrm{A}}}{T_{\mathrm{NMTD}}} \right\rfloor} -\Delta(A_{\mathrm{cost}} + A_{\mathrm{benefit}})$$

$$D_{\mathrm{benefit}} = DIR + DDR \tag{17}$$

此外，由于 NMTD 的设计并非能够针对网络杀伤链[24]中的每个攻击环节进行有效防御。因此，针对不同 NMTD 对网络杀伤链中各阶段所提供防护能力的不同，式(18)描述了 NMTD 在网络杀伤链中安全收益最高的阶段，即恶意敌手在实施 NMTD 的网络系统中损失最大的阶段，$T_{\Phi} = \{\tau \,|\, \nu(\tau, phase) = \phi\}$。为了实现对不同攻击阶段 NMTD 防御的标准化度量[25]，将网络杀伤链归结为 5 个阶段，即 $\Phi = \{R, W\&D, E\&I, C2, AO\}$。

1) 侦测攻击对象（*R*, reconnaissance）。对被攻击目标身份的确认和脆弱性等相关信息的收集。网络侦测通常由端扫描和流量监听配合实施，它是恶意敌手探测攻防环境的关键和实施后续攻击的前提。

2) 研制武器化工具和传输入侵武器（W&D, weaponi- zation & delivery）。针对侦测获得的脆弱性定制入侵工具，并将研制的入侵工具传输到被攻击的目标网络环境中。恶意敌手可通过直接或间接的方式传播到目标网络系统中。

3) 执行脆弱性利用和安装后门程式（E&I, exploitation & installation）。入侵工具在传输到目标网络节点后执行对目标节点脆弱性的利用，并在利用脆弱性的基础上将特定的程式安装在被攻击的网络系统中，为后续指挥和控制目标节点打下基础。

4) 指挥与控制（*C*2, command and control）。成功安装后门程式后对目标节点进行长期有效的控制，以备后续攻击所用。

5) 打击入侵目标（*AO*, actions on targets）。恶意敌手在有效控制目标节点的基础上，依据不同攻击目的实施网络攻击，对目标节点进行敏感信息窃取或网络系统毁瘫等。

$$D_{\max(\mathrm{phase})} = \arg\max_{\phi \in \Phi} \frac{1}{|T_\phi|}\sum_{i=0}^{\left\lfloor \frac{T_{\mathrm{A}}}{T_{\mathrm{NMTD}}} \right\rfloor}\sum_{\tau \in T_\phi} -\Delta(A_{\mathrm{cost}} + A_{\mathrm{benefit}}) \tag{18}$$

5 实例分析

为了验证基于变点检测的网络移动目标防御效能评估方法的可行性与正确性，利用如图 8 所示的典型拓扑[10, 17]构建实验网络环境。

图 8 网络中实线所示的 4 台主机 H_1、H_2、H_3 和 H_4 的基本配置信息和危害程度如表 4 所示，防火墙策略如表 5 所示；符号“−”表示 2 个节点之间不存在连通关系。实验的任务模板为网络资源请求与获取，攻击模板为敏感数据窃取攻击。分别采用 Adaptive-EH[26]和 DNAT[27]2 种 NMTD 方案进行防御。Adaptive-EH 首先对恶意敌手实施的攻击策略进行判别，并由此选取简单随机跳变或时空混合跳变策略，以通过自适应跳变的方式对被保护的目标服务器实施防御。其中，简单随机跳变是在固定的跳变周期内对共享密钥和时间戳等信息进行散列以得到跳变端信息；时空混合跳变则是在此基础上通过拉伸跳变周期以提高跳变的随机性。

DNAT 方案则是一种轻量级的 NMTD 技术，它通过 NAT 对 DNS 提供的域名信息进行空间跳变。NAT 设备通过存储每个已经建立连接的会话状态，在 DNS 服务器实施地址跳变的时候，通过发送特殊指令给相关网络节点，从而在保证现有会话不被中断的情况下实施地址跳变。

表 4 主机节点配置

节点名称	系统信息	危害程度
H_1：网络服务器	Windows NT 4.0	ω_1=0.4
H_2：域内服务器	Windows 2000 SP1	ω_2=0.55
H_3：客户端	Windows XP Pro SP2	ω_3=0.3
H_4：Linux 数据库	Red Hat 7.0	ω_4=0.7

表 5 防火墙策略

节点	恶意敌手	H_1	H_2	H_3	H_4
恶意敌手	本地	所有	—	—	—
H_1	所有	本地	所有	所有	Squid LICQ
H_2	所有	IIS	本地	所有	Squid LICQ
H_3	所有	IIS	所有	本地	Squid LICQ
H_4	所有	IIS	所有	所有	本地

如表 6 所示，实验利用 Nessus 扫描获得的节点脆弱性结果构建 MRG，如图 9 所示。整个实验分为 2 组，一组采用 Adaptive-EH 防御恶意敌手入侵 Linux 数据库，以防止其获取节点的 *root* 权限而窃取敏感数据；另一组则采用 DNAT 对入侵 Linux 数据库的恶意敌手实施防御，以防止其获取节点的 *root* 权限而窃取敏感数据。

表 6 节点资源脆弱性

编号	节点	资源	端口号	资源脆弱性
A	H_1	IIS 网络服务	80	IIS *buffer overflow*
B	H_1	FTP	21	*ftp rhost overwrite*
C	H_2	FTP	21	*ftp rhost overwrite*
D	H_2	SSH	22	*ssh buffer overflow*
E	H_2	RSH	514	*rsh login*
F	H_3	Netbois-ssn	139	*netbios-ssn nullsession*
G	H_4	LICQ	5190	LICQ *remote-to-user*
H	H_4	Squid 代理	80	*squid port scan*
I	H_4	Mysql DB	3306	*local-setuid-buffer*

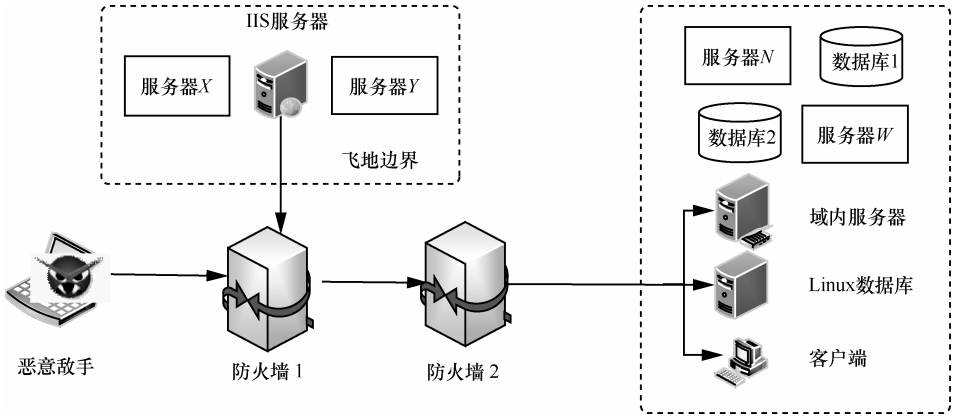


图 8 实验拓扑

5.1　基于分层网络资源图的变点检测与标准化度量

通过变点检测算法和标准化度量计算得到的攻击路径成功率如表 7 所示。

通过分析表 7 可得到以下结论。

1) 恶意敌手攻击的成功率随着攻击路径的增长而降低，因此，第 3 条和第 9 条攻击路径的成功率较高。这与文献[28]中所描述的通信节点可通过一个或更多中间节点增强安全性的原理相一致。

2) 在入侵步骤相同的条件下，恶意敌手入侵的成功率随着不同资源脆弱性数量的增加而降低，因此，相较于第 1 条和第 6 条攻击路径，第 7 条和第 12 条攻击路径成功率更高。

3) 在入侵步骤和资源脆弱性数量相同的条件下，恶意敌手对不同脆弱性的成功利用率决定了攻击路径的成功率。如第 3 条和第 9 条攻击路径，由于恶意敌手成功利用 *ftp rhost overwrite* 的概率高于

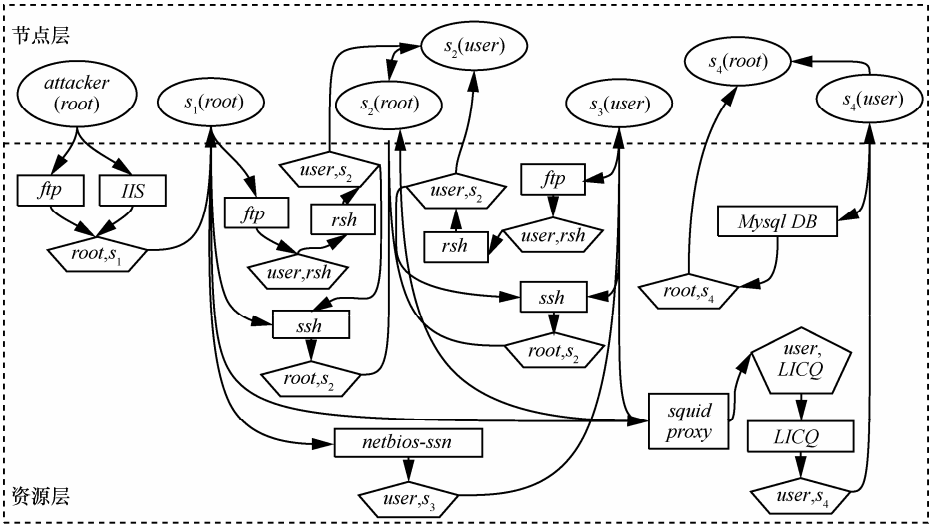


图 9　构建的 MRG

表 7　　攻击路径成功率

编号	攻击路径	攻击步骤	存在脆弱性类型/种	攻击成功率
1	$root,a \to \mathrm{A} \to root,s_1 \to \mathrm{C} \to \mathrm{E} \to user,s_2 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	7	7	0.095
2	$root,a \to \mathrm{A} \to root,s_1 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	5	5	0.194
3	$root,a \to \mathrm{A} \to root,s_1 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	4	4	0.231
4	$root,a \to \mathrm{A} \to root,s_1 \to \mathrm{F} \to user,s_3 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	5	5	0.212
5	$root,a \to \mathrm{A} \to root,s_1 \to \mathrm{F} \to user,s_3 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	6	6	0.147
6	$root,a \to \mathrm{A} \to root,s_1 \to \mathrm{F} \to user,s_3 \to \mathrm{C} \to \mathrm{E} \to user,s_2 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	8	8	0.084
7	$root,a \to \mathrm{B} \to root,s_1 \to \mathrm{C} \to \mathrm{E} \to user,s_2 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	7	6	0.103
8	$root,a \to \mathrm{B} \to root,s_1 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	5	5	0.210
9	$root,a \to \mathrm{B} \to root,s_1 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	4	4	0.251
10	$root,a \to \mathrm{B} \to root,s_1 \to \mathrm{F} \to user,s_3 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	5	5	0.229
11	$root,a \to \mathrm{B} \to root,s_1 \to \mathrm{F} \to user,s_3 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	6	6	0.159
12	$root,a \to \mathrm{B} \to root,s_1 \to \mathrm{F} \to user,s_3 \to \mathrm{C} \to \mathrm{E} \to user,s_2 \to \mathrm{D} \to root,s_2 \to \mathrm{G} \to \mathrm{H} \to user,s_4 \to \mathrm{I} \to root,s_4$	8	7	0.091

利用 IIS *buffer overflow* 的概率，因此，第 9 条攻击路径成功率最高。

5.2 效能评估与分析

由于恶意敌手通常会选取攻击成本低、攻击路径短、成功率高的路径，因此，第 9 条攻击路径更易被恶意敌手利用以实施入侵。假设恶意敌手利用第 9 条路径 $root,a\to \mathrm{B}\to root,s_1\to \mathrm{G}\to \mathrm{H}\to user,s_4\to \mathrm{I}\to root,s_4$ 进行攻击，攻击周期为 $T_{\mathrm{A}}=150$ s。分别设定 NMTD 跳变周期为 T_{MTD} = 10 s、20 s、30 s、50 s、75 s、100 s、120 s、140 s、200 s，其中，$T_{\mathrm{MTD}}=200$ s 表示在一次攻击周期内并没有实施 NMTD 跳变。通过改变 NMTD 跳变周期，从而比较提出的评估方法与现有评估方法[15]、NMTD 实际跳变结果之间的差异。图 10 和图 11 分别表示不同跳变周期情况下，计算和实施 Adaptive-EH 与 DNAT 的安全成本和安全收益，表 8 分析了本文与文献[15]评估结果的偏差。此外，图 12 给出了 $T_{\mathrm{MTD}}=20$ s、50 s 时 Adaptive-EH 和 DNAT 在网络杀伤链中各阶段的安全收益。

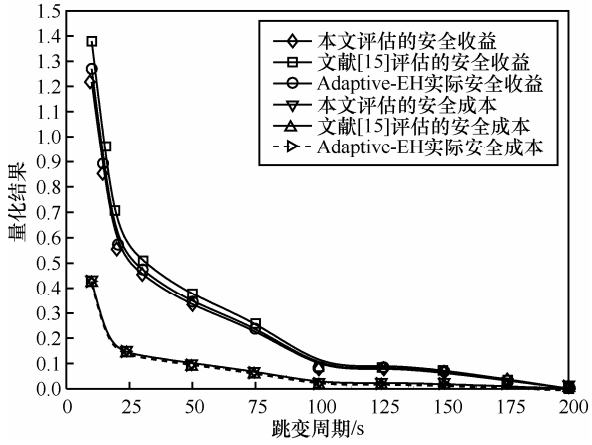


图 10 Adaptive-EH 的安全成本和收益

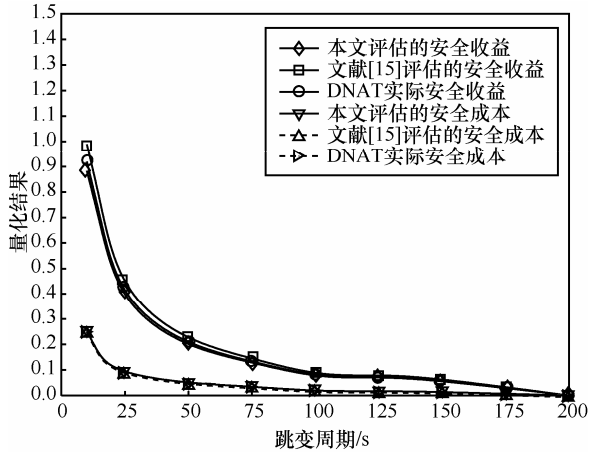


图 11 DNAT 的安全成本和收益

表 8 评估与实际防御效能偏差

方法	最大标准差		平均标准差	
	Adaptive-EH	DNAT	Adaptive-EH	DNAT
本文方法	4.44%	4.59%	3.88%	3.93%
文献[15]方法	9.73%	9.02%	8.77%	8.42%

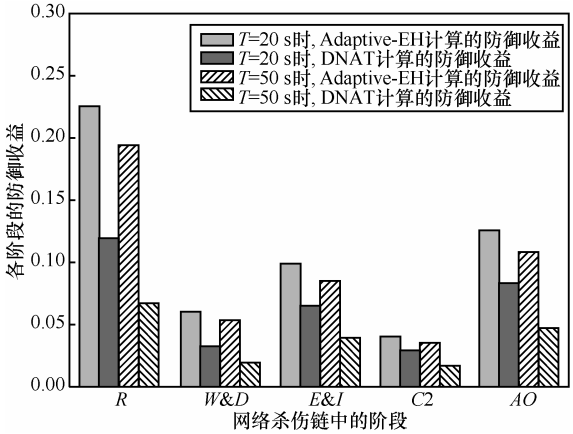


图 12 Adaptive-EH 和 DNAT 的各阶段收益

由以上图表分析可得到如下结论。

1) Adaptive-EH 和 DNAT 2 种网络移动目标防御方案都可以有效降低恶意敌手的入侵成功率。

2) 2 种 NMTD 方案的安全成本和安全收益都随着跳变周期的增加而减小。相较于 DNAT，Adaptive-EH 由于采用了自适应跳变的方法，因此，具有良好的抗攻击性和可用性。

3) 利用提出的评估方法和文献[15]中方法所评估的结果与实际 NMTD 实施的效能结果大体保持一致。但是本文评估结果与实际防御效能的平均标准差约为 3.9%；文献[15]评估结果与实际防御效能的平均标准差则约为 8.6%，因此，本文评估结果存在的偏差更小。这是因为在安全收益评估方面，本文提出的评估方法将变点的可变特性考虑在内，因此，评估的结果更加准确。

4) Adaptive-EH 和 DNAT 2 种 NMTD 方案收益的最高阶段是侦测(R)阶段。这是因为 Adaptive-EH 和 DNAT 都是通过增加恶意敌手侦查阶段的成本从而提高目标节点的安全性的。相较于 DNAT，Adaptive-EH 在侦测阶段的防御收益更高。

综上所述，基于变点检测的网络移动目标防御效能评估方法能在统一的标准下准确地对不同 NMTD 方案进行综合评估和比较分析。

6　结束语

针对现有 NMTD 效能评估方法存在的评估过程失真和评估结果存在偏差的问题，本文提出了一种新的网络移动目标防御效能评估方法。该方法基于资源脆弱性的变点检测，通过分层网络资源图将网络资源图抽象为节点层和资源层，在建立资源脆弱性改变和节点安全状态转换关联关系的同时，保证了网络资源图构建和更新的高效。该评估方法设计了变点检测与标准化度量算法，通过对目标网络中任务模板和攻击模板的变点进行实时检测，并将攻防双方对资源脆弱性的影响因素加入到可变特性中进行动态度量，从而提高评估的准确性。

安全评估对于论证 NMTD 模型的可行性和提高防御系统实现的有效性都具有重要意义，是当前移动目标防御的重要研究内容。本文提出的评估方法对于现有 4 类评估方法存在的共性缺点进行了改进和优化，实例分析表明该方法能够通过安全成本和安全收益的计算，有效评估多种网络移动目标防御系统的效能。

参考文献：

[1] Cybersecurity game-change research & development recommendations[EB/OL]. http://www.nitrd.gov/ pubs/CSIA_IWG_Cybersecurity_GameChange_RD_Recommendations_20100513.pdf.

[2] ZHANG M, WANG L, JAJODIA S, et al. Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 1071-1086.

[3] ZHUANG R, BARDAS A G, DELOACH S A, et al. A theory of cyber attacks: a step towards analyzing MTD systems[C]//The Second ACM Workshop on Moving Target Defense. ACM, 2015: 11-20.

[4] SUN K, JAJODIA S. Protecting enterprise networks through attack surface expansion[C]//The 2014 Workshop on Cyber Security Analytics, Intelligence and Automation. ACM, 2014: 29-32.

[5] 石乐义, 贾春福, 吕述望. 基于端信息跳变的主动网络防护研究[J]. 通信学报, 2008, 29(2): 106-110.
SHI L Y, JIA C F, LYU S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2): 106-110.

[6] EVANS D, NGUYEN-TUONG A, KNIGHT J. Effectiveness of moving target defenses[M]. Moving Target Defense I: Creating Asymmetric Uncertainty for Cyber Threats. New York, Springer, 2011: 29-48.

[7] GREEN M, MACFARLAND D C, SMESTAD D R, et al. Characterizing network-based moving target defenses[C]//ACM CCS Workshop on Moving Target Defense (MTD). 2015.

[8] CLARK A, SUN K, BUSHNELL L, et al. A game-theoretic approach to IP address randomization in decoy-based cyber defense[C]// International Conference on Decision and Game Theory for Security. Springer International Publishing, 2015: 3-21.

[9] ZHUANG R, ZHANG S, DELOACH S A, et al. Simulation-based approaches to studying effectiveness of moving target network defense[C]//In National Symposium on Moving Target Research, Annapolis, 2012: 21-26.

[10] ZHUANG R, DELOACH S A, OU X. A model for analyzing the effect of moving target defenses on enterprise networks[C]//The 9th Annual Cyber and Information Security Research Conference. ACM, 2014: 73-76.

[11] CARROLL T E, CROUSE M, FULP E W, et al. Analysis of network address shuffling as a moving target defense[C]//Communications (ICC), 2014 IEEE International Conference on, Sydney, 2014: 701-706.

[12] MANADHATA P K. Game theoretic approaches to attack surface shifting[M]. Moving Target Defense II: Application of Game Theory and Adversarial Modeling. New York, Springer, 2013: 1-13.

[13] OKHRAVI H, RIORDAN J, CARTER K. Quantitative evaluation of dynamic platform techniques as a defensive mechanism[M]. Research in Attacks, Intrusions and Defenses. New York, Springer, 2014: 405-425.

[14] HAN Y, LU W, XU S. Characterizing the power of moving target defense via cyber epidemic dynamics[C]//The 2014 Symposium and Bootcamp on the Science of Security, Raleigh, 2014: 23-33.

[15] ZAFFARANO K, TAYLOR J, HAMILTON S. A quantitative framework for moving target defense effectiveness evaluation[C]//The Second ACM Workshop on Moving Target Defense. ACM, 2015: 3-10.

[16] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs[C]//Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. IEEE, 2002: 273-284.

[17] WANG L, NOEL S, JAJODIA S. Minimum-cost network hardening using attack graphs[J]. Computer Communications, 2006, 29(18): 3812-3824.

[18] AMMANN P, WIJESEKERA D, KAUSHIK S. Scalable, graph-based network vulnerability analysis[C]//The 9th ACM Conference on Computer and Communications Security. ACM, 2002: 217-224.

[19] LARSEN P, BRUNTHALER S, FRANZ M. Security through diversity: are we there yet?[J]. IEEE Security & Privacy, 2014, 12(2): 28-35.

[20] MELL P, SCARFONE K, ROMANOSKY S. Common vulnerability scoring system[J]. Security & Privacy, IEEE, 2006, 4(6): 85-89.

[21] FINK G A, HAACK J N, Mckinnon A D, et al. Defense on the move: ant-based cyber defense[J]. Security & Privacy, IEEE, 2014, 12(2): 36-43.

[22] HONG J B, KIM D S. Performance analysis of scalable attack representation models[M]//Security and Privacy Protection in Information Processing Systems. Springer Berlin Heidelberg, 2013: 330-343.

[23] 王元卓, 林闯, 程学旗, 等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报, 2010, 33(9): 1748-1762.
WANG Y Z, LIN C, CHENG X Q, et al Analysis for network at-

tack-defense based on stochastic game model[J]. Chinses Journal of Computers, 2010,33(9):1748-1762.

[24] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. Leading Issues in Information Warfare & Security Research, 2011, 1: 80.

[25] 付钰, 李洪成, 吴晓平, 等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1-14.
FU Y, LI H C, WU X P, et al. Detecting APT attacks: a survey from the perspective of big data analysis[J]. Journal of Communications, 2015, 36(11): 1-14.

[26] 赵春蕾, 贾春福, 翁臣, 等. 端信息跳变系统自适应策略研究[J]. 通信学报, 2011 (11A): 47-57.
ZHAO C L, JIA C F, WENG C, et al. Research on adaptive strategies for end-hopping system[J]. Journal on Communications, 2011(11A): 47-57.

[27] SHUE C A, KALAFUT A J, ALLMAN M, et al. On building inexpensive network capabilities[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(2): 72-79.

[28] YACKOSKI J, BULLEN H, YU X, et al. Applying self-shielding dynamics to the network architecture[M]//Moving Target Defense II: Application of Game Theory and Adversarial Modeling. New York, Springer, 2013: 97-115.

作者简介：

雷程（1989-），男，北京人，信息工程大学博士生，主要研究方向为网络信息安全、数据安全交换、移动目标防御。

马多贺（1982-），男，安徽六安人，博士，中国科学院信息工程研究所助理研究员，主要研究方向为应用安全、移动目标防御、云安全、网络与系统安全等。

张红旗（1962-），男，河北遵化人，博士，信息工程大学教授、博士生导师，主要研究方向为网络安全、等级保护和信息安全管理。

杨英杰（1971-），男，河南郑州人，信息工程大学教授、硕士生导师，主要研究方向为数据挖掘、态势感知和信息安全管理。

王淼（1991-），女，河北廊坊人，中国科学院信息工程研究所硕士生，主要研究方向为移动目标防御、网络与系统安全和云安全。