基于主机安全状态迁移模型的动态网络防御有效性评估

刘 江* 张红旗 杨英杰 王义功
(解放军信息工程大学 郑州 450001)
(河南省信息安全重点实验室 郑州 450001)

摘 要：为了进行动态网络防御有效性评估，该文提出动态网络防御环境下的主机安全状态转移图生成算法，构建了主机安全状态迁移模型，基于状态转移概率给出了动态网络防御有效性的定量评估方法，为动态网络防御策略设计提供了有益参考。最后，通过一个典型网络实例说明和验证了上述模型和方法的可行性和有效性。

关键词：动态网络防御；主机安全状态迁移；转移概率；有效性评估
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2017)03-0509-09
DOI: 10.11999/JEIT160513

Effectiveness Evaluation of Moving Network Defense Based on Host Security State Transition Model

LIU Jiang ZHANG Hongqi YANG Yingjie WANG Yigong
(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)
(*Henan Key Laboratory of Information Security*, *Zhengzhou* 450001, *China*)

Abstract: To evaluate the effectiveness of moving network defense, this paper presents the host security state deduce graph construction algorithm in moving network defense environment. The host security state transition model is constructed, the quantitative effectiveness evaluation method is proposed for moving network defense based on host state transition probability, and a useful reference is provided for the design of moving network defense policy. Finally, feasibility and effectiveness of the proposed model and method are illustrated and verified in a representative network example.

Key words: Moving network defense; Host security state transition; Transition probability; Effectiveness evaluation

1 引言

动态目标防御 (Moving Target Defense, MTD) 是在部署和运行网络系统时，通过有效降低其相似性、确定性和静态性，增加其多样性、随机性和动态性来构建持续变化、不相似、不确定的网络系统，以增加攻击难度和成本的一种网络安全机制[1]。动态目标防御的目的不是构建一个没有脆弱性的系统，而是通过不断改变攻击面，减少攻击时间窗口，提升网络主动防御能力[2]。

动态目标防御机制可在多个层面以多种不同的方式实现，在网络层被称为动态网络防御[3](Moving Network Defense, MND)，指在保持网络运行和服务完整性和连续性的前提下，通过改变或隐藏的方式动态改变主机 IP 地址和端口[4]、路由器、防火墙等网络节点配置信息，增加攻击者获取有效网络指纹和漏洞信息的难度，进而阻止攻击发生。动态网络防御的研究涉及两个方面：一是动态网络防御体系的构建和动态网络防御机制的实现，其为网络空间主动防御体系构建提供了新思路；二是动态网络防御的有效性评估，其为设计防御效果更好、防御收益更高的动态网络防御策略提供了重要参考，这也是本文的研究内容。

目前，已经有部分研究进行动态目标防御的有效性评估。文献[5]提出动态多态化防御模型，分析了几个攻防实例的安全特性，给出了动态目标防御有效性的几个猜想。文献[6]对攻击面转移进行量化分析，将动态目标防御视为安全性与可用性之间的一种平衡，利用博弈论计算最优策略，但未给出具体的计算方法。文献[7]基于构建的动态网络防御系统和 CAG(Conservative Attack Graph)攻击图，利用仿真实验分析了网络配置改变对攻击成功率的影

收稿日期：2016-05-19；改回日期：2016-09-09；网络出版：2016-11-17
*通信作者：刘江 liujiang2333@163.com
基金项目：国家 863 计划项目(2012AA012704)，郑州市科技领军人才项目(131PLJRC644)
Foundation Items: The National 863 Program of China (2012AA 012704), The Scientific and Technological Leading Talent Project of Zhengzhou (131PLJRC644)

响，定性说明了动态目标防御的有效性。文献[8]采用马尔科夫模型刻画了系统安全状态分布及其转移关系，评估了系统动态变化的防御效果，但仅适用于动态平台 DP(Dynamic Platform)策略。文献[9]利用节点间的状态转移概率关系分析了动态目标防御的有效性，但未考虑回退概率且存在状态节点空间“爆炸”的弊端。文献[10]利用传染病动力学模型对动态目标防御的效能进行了系统分析和定量描述，使用网络攻防结构图刻画动态目标防御特征，以获取最优动态目标防御策略，但是作为描述网络攻防能力的模型传染系数的确定是一个难题。文献[11]阐述了基于 urn 概率模型的网络地址跳变性能评估方法，定量分析了端信息规模、探测速率、脆弱性数量和跳变频率对攻击成功率的影响，但网络攻击是一个复杂的多步骤过程，考虑单一节点跳变对攻击成功率的影响存在较大的局限性。文献[12]提出层次攻击描述模型 HARM(Hierarchical Attack Representation Model)，从随机性、多样性和冗余性 3 个角度对动态目标防御有效性进行评估，但未考虑动态目标防御的动态特性及不同动态目标防御策略的防御成本。

针对以上问题，本文提出基于主机安全状态迁移模型的动态网络防御有效性评估方法。第 2 节提出主机安全状态转移图生成算法；第 3 节描述主机安全状态迁移模型，给出前向转移、自转移和后向转移概率的含义和计算方法；第 4 节基于上述 3 种转移概率计算动态网络防御对入侵成功率的影响及其防御收益；第 5 节构建实验网络并验证所提模型和方法的可行性和有效性；第 6 节总结全文并对未来研究进行展望。

2 主机安全状态转移图

2.1 基本思想

网络攻防对抗的实质是网络安全状态的相互转换。主机安全状态转移图中的节点表示主机安全状态，边表示威胁事件的发生或者防御策略的实施引起主机安全状态的转移。从初始安全状态出发，依据网络连接关系，利用威胁模式库中的潜在威胁描述生成威胁事件。如果两个主机间具有连通关系，同时满足威胁事件发生所需的所有前提条件，则增加从源主机到目的主机的边；如果防御策略实施改变了主机的连通关系或者入侵者的既有权限，则增加从目的主机到源主机的边。主机安全状态转移图的构造过程如图 1 所示。

(1)网络安全要素： 通常使用主机服务信息 F、主机漏洞信息 V、主机资产信息 Z、访问权限 P、网络连接关系 $\boldsymbol{C}$ 描述网络安全要素。其中，$F=<\text{host},\text{service},\text{port}>$ 表示主机 host 上开启服务 service 并在端口 port 监听； $V=<\text{host},\text{service},\text{cveid}>$ 表示主机 host 上的服务 service 存在脆弱性 cveid； $Z=<\text{host},\text{value}>$ 表示主机 host 的资产价值为 value， value 的值越大代表资产越敏感和重要；$P=<\text{host},\text{privilege}>$ 表示入侵者在主机 host 上拥有 privilege 访问权限，privilege=$\{\text{none},\text{user},\text{root}\}$ 分别表示不具有任何权限、具有普通用户权限、具有 root 用户权限；矩阵 $\boldsymbol{C}$ 描述主机之间的连接关系，矩阵的行表示源主机 shost，矩阵的列表示目的主机 dhost，矩阵元素表示 shost 到 dhost 的端口 port 访问关系，当 port 为空时，表示 shost 与 dhost 之间不存在连接关系。

(2)威胁模式库： 威胁模式库 W 是对具有相似前提和结果的一类脆弱性利用的描述， $W=<\text{tid},\text{prec},\text{postc},\text{cveidset}>$。其中，tid 表示威胁模式标识；$\text{prec}=<\text{privilege},\text{cveid},\boldsymbol{C}>$ 表示威胁发生时所需的网络安全要素集合，包括入侵者在源主机上具有的初始访问权限 privilege、目的主机的脆弱性 cveid、网络连接关系 $\boldsymbol{C}$； $\text{postc}=<\text{privilege},\boldsymbol{C},\text{sd}>$ 表示威胁发生后的结果，包括入侵者在目的主机上获得的权限提升 privilege、网络连接关系 $\boldsymbol{C}$ 的变化、服务破坏 sd 等； cveidset 表示适用于该威胁模式的漏洞编号集合。威胁模式是对一类脆弱性利用的抽象定义，在构造主机安全状态转移图时需要将其进行实例化操作。

(3)防御策略库： 防御策略库 D 是防御者在识

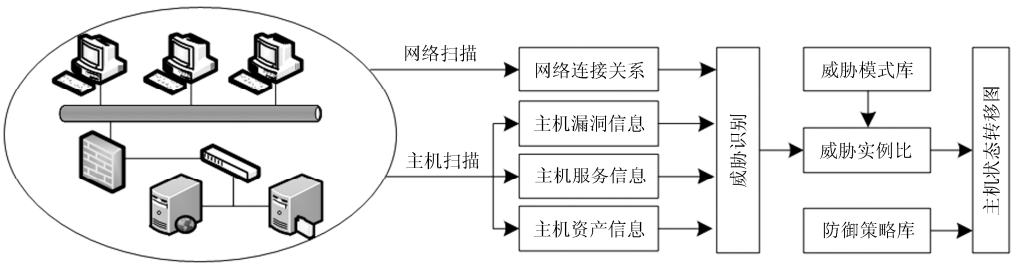

图 1 主机安全状态转移图构建

别威胁后采取的响应措施， D=<tid, dset> 。其中，tid 表示威胁模式标识； $\text{dset}=\{<d_1,p_1,c_1>,\cdots,<d_m,p_m,c_m>\}$ 是应对特定威胁模式的防御策略集，d_i 是防御策略标识， p_i 是防御策略对网络安全要素的影响结果， c_i 是防御策略成本。本文仅考虑动态网络防御策略，如端信息跳变、数据库访问接口改变策略。防御成本包括操作成本和负面成本[13–15]，其具体定义参考文献[13]。其中，防御成本量化可用 DoS 攻击的系统损失为基准，设基准值为 δ ，根据防御策略操作的复杂程度给出其相对等级，如可设地址跳变和端口跳变的操作成本分别为 $0.50\,\delta$ 和 $0.25\,\delta$ ，负面成本分别为 $1.20\,\delta$ 和 $0.75\,\delta$ 。

主机安全状态转移图是一个状态转移系统 $T=(S,t,s_0,S_{\mathrm{G}})$ 。其中， $S=\{s_1,s_2,\cdots,s_n\}$ 是主机安全状态集合，$s_i=<\text{host},\text{privilege}>$； $\tau=S\times S$ 是状态转移关系集合，由安全威胁、防御策略等决定； $s_0\in S$ 是主机初始安全状态； $S_{\mathrm{G}}\subseteq S$ 是目标状态集合。对于每个节点 $s_i\in S$, $\mathbb{R}^+(s_i)=\{s_m\in S:(s_i,s_m)\subset\tau\}$ 表示节点 s_i 的所有出节点， $\mathbb{R}^-(s_i)=\{s_n\in S:(s_n,s_i)\subset\tau\}$ 表示节点 s_i 的所有入节点。为了将主机安全状态转移图应用于动态目标防御有效性评估中，引入状态转移权重概念，即若存在原子威胁事件 e_i 使得入侵者能够由节点 s_m 到达 s_n ，则状态转移权重 $w_{mn}=p_i$ 。其中， p_i 表示 e_i 发生的先验概率，根据通用漏洞评估系统 CVSS(Common Vulnerability Scoring System)计算威胁事件发生的先验概率。

2.2 算法描述

主机安全状态转移图生成过程中，首先根据 V , $\boldsymbol{C}$ 进行威胁识别和实例化，生成威胁发生产生的新网络安全要素(第 2 至第 14 行)；然后得出防御策略生效对网络安全要素的影响(第 15 至第 25 行)；最后输出主机安全状态转移图和相应的节点及边的集合。采用正向广度优先算法，具体如表 1 所示。

主机安全状态转移图与普通攻击图相比，增加了防御策略对状态转移的影响分析，更全面地反映了网络攻防对抗，能够更好地为用户选取防御策略提供依据。同时，主机安全状态转移图中的节点仅描述主机安全状态，可有效压缩状态转移图的规模，抑制“状态爆炸”的发生，更有利于进行安全分析。

2.3 复杂度分析

主机安全状态转移图生成算法的时间复杂度不仅与网络规模、网络连接关系的数目有关，而且与主机漏洞数目有关。假设目标网络的主机数为 n ，每个主机的漏洞个数为 v ，分析每两个主机之间连接关系的计算复杂度为 $O(n^2-n)$ ，对每个主机的漏洞与每个连接关系进行匹配，在最坏的情况下需要的计算复杂度为 $O(v(n^2-n))$ ，主机安全状态转移图中的节点数目最多为 $3n$ ，在每个主机实施防御策略后，遍历其所有节点的出入节点的计算复杂度为 $O(9n^2-3n)$ 。最终，该算法的计算复杂度为 $O(n^2)$ 数量级。

表 1　主机安全状态转移图生成算法

算法：	主机安全状态转移图生成算法
输入：	网络连接关系 $\boldsymbol{C}$ ，主机漏洞信息 V ，威胁模式库 W ，防御策略库 D
输出：	节点集合 S ，边集合 E ，主机安全状态转移图 T
(1)	$S\leftarrow\varnothing, E\leftarrow\varnothing$;
(2)	**for each** $\boldsymbol{C}$ **do**
(3)	**if** V.host == $\boldsymbol{C}$.dhost and V.cveid $\cap$ W.cveidset == $\varnothing$
(4)	**return**; //威胁模式库中未识别出主机漏洞
(5)	**else if** P.host == $\boldsymbol{C}$.shost and P.privilege $\geq$ W.prec
(6)	s_u.host = $\boldsymbol{C}$.shost;
(7)	s_u.previlege = P.privilege;
(8)	s_v.host = $\boldsymbol{C}$.dhost;
(9)	s_v.previlege = (W.postc).privilege;
(10)	$S\leftarrow S\cup\{s_u,s_v\}$; //将节点 s_u,s_v 加入节点集合 S
(11)	$E\leftarrow E\cup(s_u\rightarrow s_v)$; //将边 $s_u\rightarrow s_v$ 加入边集合 E
(12)	**end if**
(13)	**end if**
(14)	**end for**
(15)	**for each** $s_i\in S$ and $d_i\in D$
(16)	**for each** $s_r\in\mathbb{R}^-(s_i)$
(17)	$E\leftarrow E\cup(s_i\rightarrow s_r)$; //将边 $s_i\rightarrow s_r$ 加入边集合 E
(18)	**end for**
(19)	**for each** $s_t\in\mathbb{R}^+(s_i)$
(20)	$E\leftarrow E-(s_i\rightarrow s_t)$; //将边 $s_i\rightarrow s_t$ 从边集合 E 中删除
(21)	**end for**
(22)	**if** $\mathbb{R}^-(s_i)==\varnothing$ and $\mathbb{R}^+(s_i)==\varnothing$
(23)	$S\leftarrow S-s_i$; //将孤立节点 s_i 从节点集合 S 中删除
(24)	**end if**
(25)	**end for**
(26)	**return** S, E, T

3　主机安全状态迁移模型

3.1 模型基本元素

主机安全状态迁移模型以有限状态机模型为基础表示入侵和防御过程。入侵者的渗透过程是从初始有限特权开始，利用系统漏洞不断提升用户权限的过程；防御者的保护过程则是实施防御策略，消

除漏洞或者减少漏洞被利用的机会，降低用户权限的过程。

给定主机安全状态转移图 $T=(S,t,s_1,S_G)$，$s_m \in s_G$，$e_i(i=1,2,\cdots,n)$ 是原子威胁事件，$V_a=\{s_1,s_2,\cdots,s_i,\cdots,s_m\}$ 是所有主机状态节点集合，$E_a=\{s_1 \to s_2,\cdots,s_{i-1} \to s_i,\cdots,s_{m-1} \to s_m\}$ 是原子威胁事件发生引起的主机安全状态迁移，$F_a=\{s_2 \to s_1,s_3 \to s_1,\cdots,s_m \to s_1,\cdots,s_{i-1} \to s_i,\cdots,s_m \to s_{m-1}\}$ 是防御策略实施引起的主机安全状态迁移，威胁路径 $P_a=\{s_1,e_1,s_2,e_2,s_3,\cdots e_i,s_i \cdots,s_m\}$ 是一组从初始状态 s_1 到目标状态 s_m 的原子威胁事件序列。p_{ij} 是主机状态节点的后向转移概率，威胁事件发生使得入侵者逐步达到提升权限的目的。p_{ii} 和 $p_{ij}^{'}$ 分别是主机状态节点的自转移概率和前向转移概率，防御策略的实施使得入侵者的既得资源和特权失效，入侵者可能会滞留在在入侵路径的某一状态节点，甚至回退到当前状态节点之前的某一状态节点。主机安全状态迁移模型如图 2 所示，节点表示主机安全状态，边表示状态节点的后向转移、自转移和前向转移。

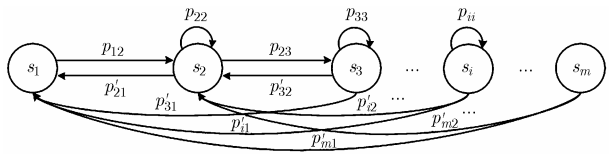

图 2 主机安全状态迁移模型

3.2 转移概率

设入侵周期 T_a，防御策略调整周期 T_h，可调整状态节点数 n，真正实施调整的节点数为 k ($0 \le k \le n$)，则 T_a 内任一状态节点发生防御策略调整的概率为 $\alpha=k/n$，从状态节点 s_1 到状态节点 s_t 的入侵成功概率为 P_t ($1 \le t \le m$)。为简化分析，假设防御策略实施能够成功应对当前状态节点面临安全威胁的概率为 1。

(1)前向转移概率 $p_{ij}^{'}$：假设入侵者处于状态节点 s_i，在 T_a 内目标网络节点动态实施防御策略迫使其回退到该威胁路径上距离状态节点 s_i 最近且未发生防御策略调整的状态节点 s_j ($j<i$)的概率称为前向转移概率，即 $s_i,s_{i-1},\cdots,s_{j+1}$ 均进行防御策略调整，s_j 未进行防御策略调整，状态节点 s_i 到状态节点 s_j 的前向转移概率为 $p_{ij}^{'}$。

$$p_{ij}^{'}=\left[1-(1-\alpha)^{T_a/T_h}\right]^{i-j}(1-\alpha)^{T_a/T_h},\ s_i \in V_a,\ s_j \in V_a,\ s_i \to s_j \in F_a,\ 1<j<i \le m \quad (1)$$

其中，状态节点 s_j 在跳变周期内未进行防御策略调整的概率为 $1-\alpha$，则 $(1-\alpha)^{T_a/T_h}$ 表示在 T_a 内状态节点 s_j 均未进行防御策略调整的概率，$[1-(1-\alpha)^{T_a/T_h}]^{i-j}$ 表示在 T_a 内 $s_i,s_{i-1},\cdots,s_{j+1}$ 均进行防御策略调整的概率。

设 $V_a=\{s_j,s_{j+1},\cdots,s_{i-1},s_i\}$，$E_a=\{s_j \to s_{j+1},s_{j+1} \to s_{j+2},\cdots,s_{i-1} \to s_i\}$，$1<j<i \le m$，当在状态节点上不实施动态网络防御策略时，入侵成功率只与原子威胁事件相关，其处于威胁路径上状态节点 s_i 的概率为 α_i。

$$\alpha_i=\prod_{u=j}^{i-1}w_{u(u+1)}\Bigg/\left[1+\sum_{k=j}^{i-1}\left(\prod_{u=j}^{k}w_{u(u+1)}\right)\right],\ s_i \in V_a,\ s_j \in V_a,s_i \to s_j \in F_a,1<j<k<i \le m \quad (2)$$

其中，$\prod_{u=j}^{i-1}w_{u(u+1)}$ 表示入侵者成功从状态节点 s_j 入侵到状态节点 s_i 的概率，$1+\sum_{k=j}^{i-1}\left(\prod_{u=j}^{k}w_{u(u+1)}\right)$ 表示入侵者处于从状态节点 s_j 到状态节点 s_i 的威胁路径上的各状态节点的概率之和。

在不限制状态节点防御策略调整数目的情况下，即任一状态节点在 T_a 内都可以进行 T_a/T_h 次策略调整，入侵者可能处于威胁路径上的任一状态节点，其回退到状态节点 s_j 的概率之和为 $\sum_{i=2}^{m}p_{ij}^{'}$，则状态节点 s_j 的平均前向转移概率 $p_j^{'}$ 为

$$p_j^{'}=\sum_{i=2}^{m}\alpha_i p_{ij}^{'},\ s_i \in V_a,s_j \in V_a,s_i \to s_j \in F_a,\ 1<j<i \le m \quad (3)$$

(2)自转移概率 p_{ii}：对于状态节点 s_i 而言，入侵者在一个威胁周期 T_a 后仍处于状态节点 s_i，称为状态节点 s_i 的自转移概率。状态节点 s_i 的自转移概率 p_{ii} 由两部分组成：一是入侵者未能成功地从状态节点 s_i 入侵到状态节点 s_{i+1}，且状态节点 s_i 未进行防御策略调整；二是入侵者成功地从状态节点 s_i 入侵到状态节点 s_{i+1}，但状态节点 s_{i+1} 进行防御策略调整且状态节点 s_i 未进行防御策略调整。

$$\begin{aligned}p_{ii}&=\left(1-w_{ij}\right)^{T_h/T_a}(1-\alpha)^{T_a/T_h}+\left(1-\left(1-w_{ij}\right)^{T_h/T_a}\right)\cdot(1-\alpha)^{T_a/T_h}\left(1-(1-\alpha)^{T_a/T_h}\right)\\&=(1-\alpha)^{T_a/T_h}-\left(1-\left(1-w_{ij}\right)^{T_h/T_a}\right)(1-\alpha)^{2T_a/T_h},\\&\quad s_i \in V_a,\ s_{i+1} \in V_a,\ s_i \to s_{i+1} \in F_a,1<i \le m\end{aligned} \quad (4)$$

(3)后向转移概率 p_{ij}：对于状态节点 s_i 而言，当入侵者成功地从状态节点 s_i 入侵到状态节点 s_j，且状态节点 s_i 和状态节点 s_j 均未进行防御策略调整，入侵者在一个入侵周期 T_a 后处于状态节点 s_j，称为状态节点 s_i 的后向转移概率。后向转移概率实际上就是状态转移图中某一威胁路径的成功概率。

$$p_{ij}=\left(1-\left(1-w_{ij}\right)^{T_{\mathrm{h}}/T_{\mathrm{a}}}\right)(1-\alpha)^{2T_{\mathrm{a}}/T_{\mathrm{h}}},\ s_i\in V_{\mathrm{a}},\ s_j\in V_{\mathrm{a}},s_j\to s_i\in E_{\mathrm{a}},1<j<i\le m \tag{5}$$

4　动态网络防御有效性

文献[6]将动态网络环境下的攻防对抗建模为二人博弈模型，借鉴该思想，本文认为动态网络防御策略的有效性可以通过其对入侵成功率和防御收益的影响进行衡量。

4.1 入侵成功率

入侵成功率指主机安全状态迁移模型中，入侵者到达某一节点状态的难易程度或获取不同节点访问特权的概率。假设主机安全状态迁移模型中存在一条从初始状态节点 s_1 到目标状态节点 s_m 的完整威胁路径 $P_{\mathrm{a}}=\{s_1,e_1,s_2,e_2,s_3,\cdots e_i,s_i\cdots,s_m\}$，当不进行动态网络防御策略调整时，入侵成功概率 P_{u}

$$P_{\mathrm{u}}=\prod_{k=j}^{i-1}p_{k(k+1)},\ s_i\in V_{\mathrm{a}},\ j\ne m,\ s_j\in V_{\mathrm{a}},\ s_j\to s_i\in E_{\mathrm{a}},\ 1<j<k<i<m \tag{6}$$

当进行动态网络防御策略调整时，结合主机安全状态转换图中的状态转移权重和主机状态迁移模型中定义的 3 类转移概率，计算入侵成功概率 P_t

$$P_t=\prod_{k=j}^{i-1}\left(p_k^{'}p_{k(k+1)}\right)\sum_{r=0}^{\infty}\left(p_k^{'}p_{kk}\right)^r=\prod_{k=j}^{i-1}\left(p_k^{'}p_{k(k+1)}\right)\left(1-p_k^{'}p_{kk}\right)^{-1} \tag{7}$$

其中，$s_i\in V_{\mathrm{a}},j\ne m,s_j\in V_{\mathrm{a}},s_j\to s_k\in E_{\mathrm{a}},s_k\to s_j\in F_{\mathrm{a}},1<j<k<i<m$，$p_k^{'}p_{k(k+1)}$ 表示在动态防御策略下状态节点 s_k 成功转移到状态节点 s_{k+1} 的概率，$\sum_{r=0}^{\infty}\left(p_k^{'}p_{kk}\right)^r$ 表示在动态防御策略下状态节点 s_k 的自转移概率，当 $0<p_k^{'}p_{kk}<1$ 时，$\sum_{r=0}^{\infty}\left(p_k^{'}p_{kk}\right)^r=\left(1-p_k^{'}p_{kk}\right)^{-1}$。显然，网络防御策略的动态调整降低了入侵成功率，$P_t$ 与 α 成正比，即进行动态网络防御策略调整的状态节点数目占总状态节点数目的比例越高，入侵成功率越低；P_t 与 $T_{\mathrm{a}}/T_{\mathrm{h}}$ 成反比，即入侵周期越长，防御策略调整周期越短，入侵成功率也越低。

4.2 剩余损失

主机安全状态转移图中，同一状态节点存在多条入边和出边，只有当所有入边都失效时，该状态节点才会失效；而当状态节点失效时，该状态节点的所有出边也会失效。防御覆盖面 $\mathrm{DS}_i=\{\mathrm{ds}_i^k\mid\mathrm{ds}_i^k\in V_{\mathrm{a}}\}$ 表示 d_i 实施导致不可达的主机状态节点集合；防御覆盖路径 $\mathrm{DP}_i=\{P_a\mid P_a\cap\mathrm{DS}_i\ne\varnothing\}$ 表示 d_i 影响到的威胁路径集合。

潜在损失 PL(Potential Loss)是在威胁路径入侵成功率为 1 的情况下，目标节点遭受攻击造成的损失。攻击者在不同状态节点可以获取不同权限，进而发动不同类型的攻击。文献[13]给出了获取 root 权限、发动 DoS 等攻击类型的致命度，体现了攻击的固有危害。借鉴该思想，同时出于对统一量纲的考虑，使用 DoS 攻击的系统损失值为基准设置其他攻击的损失值，如可设获取 root 权限的潜在损失为 5δ。

剩余损失 RL(Residual Loss)是动态网络防御策略实施后，目标节点仍未消除的威胁及其存在的损失。通过主机安全状态迁移模型，推断入侵成功率的变化，即可分析攻击发生对信息系统造成的剩余损失。设初始状态节点 s_1 到目标状态节点 s_t 存在多条入侵路径，其潜在损失为 PL_t，防御策略 d_i 的防御覆盖路径数目为 $|\mathrm{DP}_i|$，第 k 条防御覆盖路径的入侵成功率为 P_t^k，则剩余损失为

$$\mathrm{RL}_i=\sum_{k=1}^{|\mathrm{DP}_i|}\left(\mathrm{PL}_tP_t^k\right) \tag{8}$$

4.3 防御收益

防御收益 DR(Defense Reward)是防御者采取防御策略能够有效避免的价值损失与防御成本的差值。防御策略 d_i 的剩余损失为 RL_i，防御成本为 c_i，则防御收益为

$$\mathrm{DR}_i=|\mathrm{DP}_i|\mathrm{PL}_t-\mathrm{RL}_i-c_i=\sum_{k=1}^{|\mathrm{DP}_i|}(\mathrm{PL}_t(1-P_t^k))-c_i \tag{9}$$

动态网络防御策略调整的状态节点数目越多，调整的周期越短，剩余损失越小，但是防御成本也越大。不计代价的防御策略显然是不合理的，应该在防御成本和收益之间寻求一种均衡，以最大化防御收益。

4.4 对比分析

通过对现有动态目标防御有效性评估方法的分析，结合动态目标防御策略的特点，选取评估性质、是否考虑跳变频率等 7 个指标将本文方法和其他文献的方法进行对比分析，结果如表 2 所示。方法的通用性指评估方法是否能够适用于多种类型动态防御策略。其中，文献[8]只能对动态平台策略有效性进行评估，文献[11]只能对端信息跳变策略有效性进行评估，其通用性较差；文献[10]中传染病动力学模型中的传染系数随网络对抗环境的改变而改变，其通用性较一般。

表 2 不同方法比较结果

方法	评估性质	理论基础	是否考虑跳变频率	是否考虑防御成本	计算方法	通用性	具体应用
文献[6]	定量	博弈论	否	是	无	好	策略选取
文献[8]	定量	马尔科夫	否	否	详细	差	效能评估
文献[9]	定量	攻击图	是	否	详细	好	效能评估
文献[10]	定量	传染病动力学	是	是	详细	中	策略选取
文献[11]	定量	概率论	是	否	详细	差	效能评估
文献[12]	定量	层次攻击图	否	否	详细	好	效能评估
本文	定量	攻击图	是	是	详细	好	效能评估

本文方法不仅考虑了动态网络防御的动态性，即跳变频率对防御有效性的影响，而且考虑了动态网络防御策略的防御成本，使得防御有效性评估值更加合理。另外，使用攻击图进行有效性评估，可以适用于多种类型的动态目标防御策略，具有良好的通用性。

5 实例分析

为验证评估方法的可行性和有效性，借鉴 Sheyner 构建的经典实验网络[16]，设计了一个类似的实验目标网络环境，其拓扑结构如图 3 所示。

安全威胁来自外网，Web 服务器和堡垒主机 H1 部署在非隔离区 DMZ(DeMilitarized Zone)，内网由文件服务器、数据库服务器及主机 H2 组成。防火墙的安全策略为仅允许外部用户访问 Web 服务器的 HTTP 和 FTP 服务，以及堡垒主机 H1 上的 SMTP 服务，其他网络节点和端口均进行阻断。使用 Nessus 工具进行扫描，挖掘设备脆弱性信息，同时利用 CVSS 计算脆弱性利用的先验概率，及其被利用后的潜在损失量化值，如表 3 所示。

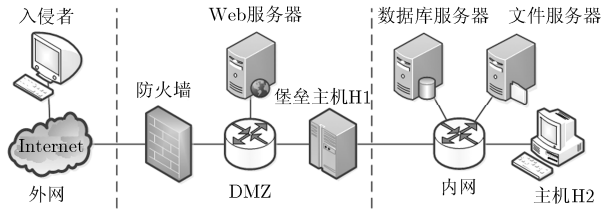

图 3 实验目标网络拓扑结构

根据算法 1，得出实验目标网络的主机安全状态转移图。为了更加清楚地进行展示和描述，将主机安全状态转移图拆分为威胁视角主机安全状态转移图和防御视角主机安全状态转移图，分别如图 4，图 5 所示。图中，A 表示入侵主机，W 表示 Web 服务器，F 表示文件服务器，D 表示数据库服务器，H1 表示堡垒主机，H2 表示内网主机，S_i(host, previlege) 表示第 i 种主机安全状态下攻击者对主机 host 具有 previlege 权限。

威胁视角主机安全状态转移图的每条边上注明了引起主机安全状态转移的威胁发生时所依赖的服务漏洞，tid_1 表示利用 FTP 服务的 Write $home /.rhost 漏洞，$\text{tid}_2$ 表示利用 AP 服务的 Apache Chunked-Enc 漏洞，tid_3 表示利用 IIS 服务的 HTTP.sys 漏洞，tid_4 表示利用 SMTP 服务的 Remote buffer overflow 漏洞，tid_5 表示利用 RPC 服务的 Code Injection 漏洞，tid_6 表示利用 Mysql 服务的 Local buffer overflow 漏洞。

防御视角主机安全状态转移图的每条边上注明

表 3 设备脆弱性信息

序号	主机	服务	脆弱性	CVE 编号	初始权限	目标权限	先验概率	潜在损失
C_1	Web 服务器	AP	Apache Chunked-Enc	CVE-2002-0392	user	root	0.3	5.0 δ
C_2	Web 服务器	IIS	HTTP.sys	CVE-2015-1635	user	root	0.6	5.0 δ
C_3	Web 服务器	FTP	Write $home/.rhost	CVE-2011-4800	user	user	0.4	2.5 δ
C_4	堡垒主机 H1	SMTP	Remote buffer overflow	CVE-2005-0560	user	root	0.5	5.0 δ
C_5	主机 H2	RPC	Code Injection	CVE-2008-4250	user	root	0.6	5.0 δ
C_6	文件服务器	FTP	Write $home/.rhost	CVE-2011-4800	user	user	0.4	2.5 δ
C_7	数据库服务器	FTP	Write $home/.rhost	CVE-2011-4800	user	user	0.4	2.5 δ
C_8	数据库服务器	Mysql	Local buffer overflow	CVE-2005-2558	user	root	0.6	5.0 δ

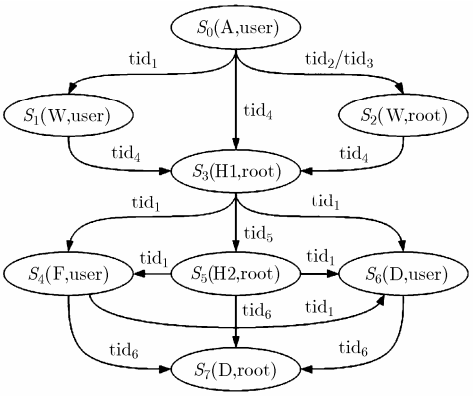

图 4　威胁视角主机安全状态转移图

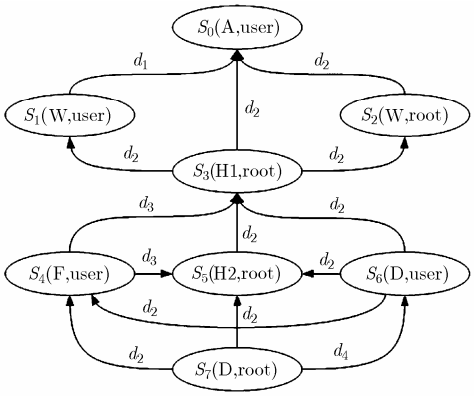

图 5　防御视角主机安全状态转移图

了引起主机安全状态转移的具体防御策略，d_1 表示将服务器操作系统更新为 Linux，d_2 表示进行服务器 IP 地址跳变，d_3 表示进行服务器通信端口跳变，d_4 表示随机化数据库访问接口函数。动态防御策略的成本量化值如表 4 所示。

表 4　动态防御策略成本量化

序号	防御策略	操作成本	负面成本
1	更新操作系统	$1.00\,\delta$	$1.50\,\delta$
2	IP 地址跳变	$0.50\,\delta$	$1.20\,\delta$
3	端口跳变	$0.25\,\delta$	$0.75\,\delta$
4	随机化数据库访问接口函数	$0.80\,\delta$	$1.00\,\delta$

(1)入侵成功率对比分析：　设 $T_{\mathrm{a}}=T_{\mathrm{h}}=100$ s，$\alpha=1/7$，为求解完整威胁路径的成功率，在计算前向转移概率时只需计算状态节点 s_0 的平均前向转移概率 p_0' 即可。通过对图 4 和图 5 所示的主机安全状态转移图进行分析，发现存在 28 条从初始状态节点 s_0 到目标状态节点 s_7 的威胁路径。将网络防御策略不进行动态调整时的攻击成功率称为原始成功率，其与进行网络防御策略动态调整的入侵成功率进行对比，结果如表 5 所示。

通过对表 5 进行分析发现，(a)动态网络防御策略可以有效降低入侵成功率，平均幅度约为 30%；(b)威胁路径越长，入侵成功率越低，这与文献[17]中要求所有通信节点必须通过一个或更多的中间节点以增强安全性的原理是一致的；(c)威胁路径“$s_0\to C_4\to s_3\to C_5\to s_5\to C_8\to s_7$”的入侵成功率最高，防御者应该优先在该威胁路径上实施防御。

(2)防御周期调整对防御收益的影响：　设 $T_{\mathrm{a}}=100$ s，$\alpha=1/7$，改变防御策略调整周期 T_{h} 分别为 20 s, 40 s, 60 s, 80 s, 100 s, 200 s, 500 s，选取威胁路径“$s_0\to C_4\to s_3\to C_6\to s_4\to C_8\to s_7$”为目标测试路径进行实验，对数据库访问端口进行跳变，分别计算其防御收益，结果如表 6 所示。

通过对表 6 进行分析发现，(a)随着端口跳变周期的增大，威胁路径“$s_0\to C_4\to s_3\to C_6\to s_4\to C_8\to s_7$”的入侵成功率不断提升，因为跳变周期越小，防御者探测端口并实施攻击的有效时间窗口越小；(b)随着端口跳变周期的增大，防御收益先增大后减小，因为跳变周期越小，单位时间的跳变次数越多，防御成本越大，而跳变周期越大，入侵成功率越高，剩余损失越大；(c)本实验网络中，当数据库访问端口的跳变周期为 100 s 时，针对威胁路径“$s_0\to C_4\to s_3\to C_6\to s_4\to C_8\to s_7$”的防御收益最大。

(3)不同防御策略对防御收益的影响：　设 $T_{\mathrm{a}}=T_{\mathrm{h}}=100$ s，$\alpha=1/7$，在状态节点 s_4 处进行 IP 地址跳变和 FTP 服务端口跳变，防御覆盖路径共有 12 条，计算其防御收益，结果如表 7 所示。

由表 7 可以看出 IP 地址跳变在跳变周期为 100 s 时的防御收益最大，端口跳变在跳变周期为 20 s 时防御收益最大，说明不同防御策略收益最大时的跳变周期不一定相同。因此，在最大化防御收益时，应该综合考虑防御策略类型和防御跳变周期。

6　结束语

本文根据主机安全状态转移图构建了动态网络防御环境下的主机安全状态迁移模型，利用前向转移、自转移和后向转移 3 种转移概率计算入侵成功率，并结合动态网络防御成本对其有效性进行了定量评估。与现有方法相比，本文方法将动态网络防御的动态特性和防御成本纳入评估因素进行考虑，使得评估结果更加合理。典型网络拓扑中的实验分析，说明和验证了动态网络防御策略对入侵成功率和防御收益的影响规律。下一步研究中，拟在大规

表 5 威胁路径入侵成功率对比

序号	威胁路径状态转移	原始成功率	$p_0^{'}$	MND 成功率
1	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_6 \to s_4 \to C_8 \to s_7$	0.048	0.614	0.033
2	$s_0 \to C_4 \to s_3 \to C_6 \to s_4 \to C_8 \to s_7$	0.120	0.591	0.088
3	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_6 \to s_4 \to C_8 \to s_7$	0.036	0.677	0.027
4	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_6 \to s_4 \to C_8 \to s_7$	0.072	0.527	0.040
5	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.019	0.649	0.014
6	$s_0 \to C_4 \to s_3 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.048	0.627	0.031
7	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.014	0.672	0.010
8	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.028	0.548	0.016
9	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_8 \to s_7$	0.029	0.636	0.019
10	$s_0 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_8 \to s_7$	0.072	0.541	0.041
11	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_8 \to s_7$	0.022	0.682	0.015
12	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_8 \to s_7$	0.044	0.516	0.025
13	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.012	0.642	0.009
14	$s_0 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.029	0.567	0.018
15	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.009	0.690	0.007
16	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_6 \to s_4 \to C_7 \to s_6 \to C_8 \to s_7$	0.018	0.521	0.010
17	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_5 \to s_5 \to C_8 \to s_7$	0.072	0.618	0.047
18	$s_0 \to C_4 \to s_3 \to C_5 \to s_5 \to C_8 \to s_7$	0.180	0.533	0.112
19	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_8 \to s_7$	0.054	0.675	0.037
20	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_8 \to s_7$	0.108	0.505	0.056
21	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_5 \to s_5 \to C_7 \to s_6 \to C_8 \to s_7$	0.029	0.636	0.019
22	$s_0 \to C_4 \to s_3 \to C_5 \to s_5 \to C_7 \to s_6 \to C_8 \to s_7$	0.072	0.541	0.041
23	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_7 \to s_6 \to C_8 \to s_7$	0.022	0.682	0.015
24	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_5 \to s_5 \to C_7 \to s_6 \to C_8 \to s_7$	0.044	0.516	0.025
25	$s_0 \to C_3 \to s_1 \to C_4 \to s_3 \to C_7 \to s_6 \to C_8 \to s_7$	0.072	0.541	0.041
26	$s_0 \to C_4 \to s_3 \to C_7 \to s_6 \to C_8 \to s_7$	0.120	0.591	0.088
27	$s_0 \to C_1 \to s_2 \to C_4 \to s_3 \to C_7 \to s_6 \to C_8 \to s_7$	0.036	0.677	0.027
28	$s_0 \to C_2 \to s_2 \to C_4 \to s_3 \to C_7 \to s_6 \to C_8 \to s_7$	0.072	0.527	0.040

模网络环境下对动态网络防御策略的操作成本和负面成本进行实验和分析，为大规模网络环境下的动态网络防御策略设计和部署提供有益参考。

表 6 不同跳变周期下的防御收益对比

序号	T_{h}	原始成功率	$p_0^{'}$	MND 成功率	跳变概率	防御收益
1	20 s	0.120	0.591	0.007	0.537	3.998 δ
2	40 s	0.120	0.591	0.045	0.320	4.199 δ
3	60 s	0.120	0.591	0.061	0.266	4.216 δ
4	80 s	0.120	0.591	0.082	0.175	4.275 δ
5	100 s	0.120	0.591	0.088	0.143	4.303 δ
6	200 s	0.120	0.591	0.106	0.118	4.256 δ
7	500 s	0.120	0.591	0.114	0.089	4.228 δ

表 7 不同防御策略的防御收益对比

序号	T_{h}	跳变概率	防御收益	
			IP 地址跳变	端口跳变
1	20 s	0.537	51.274 δ	54.873 δ
2	40 s	0.320	53.716 δ	52.165 δ
3	100 s	0.143	56.180 δ	49.988 δ
4	200 s	0.118	52.928 δ	48.284 δ

参 考 文 献

[1] PRAKASH A and WELLMAN M P. Empirical game-theoretic analysis for moving target defense[C]. Proceedings of the Second ACM Workshop on Moving Target

Defense, Denver, Colorado, USA, 2015: 57–65.

[2] ZHUANG Rui, BARDAS A G, DELOACH S A, *et al*. A theory of cyber attacks: a step towards analyzing MTD systems[C]. Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, Colorado, USA, 2015: 11–20.

[3] GREEN M, MACFARLAND D C, SMESTAD D R, *et al*. Characterizing network-based moving target defenses[C]. Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, Colorado, USA, 2015: 31–35.

[4] JAFARIAN J H, AL-SHAER E, and QI Duan. An effective address mutation approach for disrupting reconnaissance attacks[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(12): 2562–2577. doi: 10.1109/TIFS.2015.2467358.

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

[6] MANADHATA P K. Game Theoretic Approaches to Attack Surface Shifting[M]. New York: Moving Target Defense II: Application of Game Theory and Adversarial Modeling, Springer, 2013: 1–13.

[7] ZHUANG Rui, ZHANG Su, 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, MD, USA, 2012: 21–26.

[8] OKHRAVI H, RIORDAN J, and CARTER K. Quantitative Evaluation of Dynamic Platform Techniques as a Defensive Mechanism[M]. New York: Research in Attacks, Intrusions and Defenses, Springer, 2014: 405–425.

[9] ZHUANG Rui, DELOACH S A, and OU Xinming. A model for analyzing the effect of moving target defenses on enterprise networks[C]. Procee dings of the 9th Annual Cyber and Information Security Research Conference, Tennessee, USA, 2014: 73–76.

[10] HAN Yujuan, LU Wenlian, and XU Shouhuai. Characterizing the power of moving target defense via cyber epidemic dynamics[C]. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security, Raleigh, NC, USA, 2014: 23–33.

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

[12] HONG J B and KIM D S. Assessing the effectiveness of moving target defenses using security models[J]. *IEEE Transactions on Dependable and Secure Computing*, 2015, 13(2): 163–177. doi: 10.1109/TDSC.2015.2443790.

[13] 姜伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报, 2009, 32(4): 817–827. doi: 10.3724/SP.J.1016.2009.00817.

JIANG Wei, FANG Binxing, TIAN Zhihong, *et al*. Evaluating network security and optimal active defense based on attack-defense game model[J]. *Chinese Journal of Computers*, 2009, 32(4): 817–827. doi: 10.3724/SP.J.1016.2009.00817.

[14] VAN LEEUWEN B, STOUT W, and URIAS V. Operational cost of deploying moving target defenses defensive work factors[C]. 2015 IEEE Military Communications Conference, Tampa, FL, USA, 2015: 966–971.

[15] ZAFFARANO K, TAYLOR J, and HAMILTON S. A quantitative framework for moving target defense effectiveness evaluation[C]. Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, Colorado, USA, 2015: 3–10.

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

[17] YACKOSKI J, BULLEN H, YU Xiang, *et al*. Applying Self-shielding Dynamics to the Network Architecture[M]. New York: Moving Target Defense II: Application of Game Theory and Adversarial Modeling, Springer, 2013: 97–115.

刘　江：男，1988 年生，博士生，研究方向为动态目标防御、安全策略管理.

张红旗：男，1962 年生，教授，博士生导师，研究方向为网络信息安全、安全管理.

杨英杰：男，1971 年生，教授，硕士生导师，研究方向为数据挖掘、态势感知.

王义功：男，1987 年生，硕士，讲师，研究方向为安全策略管理.