基于脆弱性变换的网络动态防御有效性分析方法

李立勋[1,2],张 斌[1,2],董书琴[1,2],唐慧林[1,2]
(1. 信息工程大学,河南郑州 450001;2. 河南省信息安全重点实验室,河南郑州 450001)

摘 要: 有效性分析对合理制订最优网络动态防御策略至关重要.首先利用随机抽样模型从脆弱性变换角度给出入侵成功概率计算公式,用于刻画变换空间、变换周期及脆弱性数量对网络入侵过程的影响;然后针对单、多脆弱性变换两种情况,分别给出相应的入侵成功概率极限定理并予以证明,同时给出两种情况下的最优变换空间计算方法;仿真结果表明,增大单条入侵路径上依次攻击的脆弱性数量、减小变换周期可持续提高网络动态防御有效性,而增大变换空间初始可以提升网络动态防御有效性,但是由于入侵成功概率会随变换空间的持续增大而逐渐收敛,在入侵成功概率收敛时,有效性无法持续提高.

关键词: 网络安全;网络动态防御;安全策略分析;入侵成功概率;动态变换;脆弱性变换;随机抽样
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2018)12-3014-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.12.027

Effectiveness Analysis Approach Based on Vulnerability Mutation for Network Dynamic Defense

LI Li-xun[1,2], ZHANG Bin[1,2], DONG Shu-qin[1,2], TANG Hui-lin[1,2]
(1. *Information and Engineering University, Zhengzhou, Henan* 450001, *China*;
2. *Key Laboratory of Information Security, Zhengzhou, Henan* 450001, *China*)

Abstract: Effectiveness analysis is critical for making optimal network dynamic defense (NDD) strategies. Firstly, the attack success probability formula is derived by constructing the random sampling model from the perspective of vulnerability mutation, which can depict the influence caused by the mutation space, the mutation period and the number of vulnerabilities on the process of network attack. Then, two limit theorems of attack success probability are given and proved in single and multiple vulnerabilities cases respectively, and the calculating methods of optimal mutation space are given according to the two theorems. The simulation results show that the NDD's effectiveness improves with the mutation period reducing and the number of vulnerability attacked successively on a single attack path growing, meanwhile, although enlarging the mutation space is beneficial to improving the NDD's effectiveness in the beginning, the attack success probability would converge with the persistent enlargement of mutation space, which limits the continuous improvement of NDD's effectiveness.

Key words: cyber security; network dynamic defense; security policy analysis; attack success probability; dynamic mutation; vulnerability mutation; random sampling

1 引言

为应对日益复杂的网络攻击,研究人员提出移动目标防御和拟态防御等网络动态防御(Network Dynamic Defense,NDD)思想,旨在通过对安全目标及其对外呈现形式实施空间和时间上的规律性或驱动性变化从而降低信息系统确定性、静态性和同构性,增大入侵者探测、利用系统脆弱性和维持已有渗透成果的成本和难度,进而降低入侵成功概率[1,2].为科学设置动态变换空间和变换周期,合理制订最优 NDD 策略,需要进行 NDD 有效性分析.

目前针对 NDD 有效性分析的研究工作主要分为以下四个方面:(1) 基于模拟仿真的方法,在仿真平台模拟 NDD 体系下的网络攻防过程,并通过网络和系统的状态变化分析不同 NDD 技术对网络入侵的防御效果[3~5],此类方法难以定量分析变换空间和变换周期对防御有效性的影响.(2) 基于图论的方法,利用有向图对 NDD 体系下入侵者状态及系统资源转移过程和攻击步骤间的依赖关系进行建模,从入侵成功概率和攻击

收稿日期:2017-11-28;修回日期:2018-01-25;责任编辑:覃怀银
基金项目:河南省基础与前沿技术研究计划项目(No. 2014302903);信息保障技术重点实验室开放基金项目(No. KJ-15-109);信息工程大学新兴科研方向培育基金(No. 2016604703)

成本角度分析 NDD 有效性[6~8],此类方法主要关注动态变换周期对防御有效性的影响,未同时分析变换空间与防御有效性的关系.(3) 基于博弈论的方法,建立 NDD 体系下的攻防博弈模型,从防御效费比角度开展有效性分析[9~11].(4) 基于瓮模型的方法,利用瓮模型对网络嗅探过程建模,研究地址变换和端口跳变对嗅探攻击的防御有效性,但是其方法只适用于单脆弱性变换场景的 NDD 有效性分析[12,13]. 基于博弈论和基于瓮模型的方法虽然在构建 NDD 数学模型时同时考虑了变换周期与变换空间对防御有效性的影响,但是未给出所提变换策略下的最优变换空间计算方法.

本文首先对 NDD 体系下的网络入侵过程进行分析,指出其会因为脆弱性变换而具有非马尔可夫特性,进而导致入侵成功概率求解困难. 为此,在随机抽样模型中引入时间概率密度函数,从脆弱性变换角度推导出 NDD 体系下入侵者的入侵成功概率计算公式. 然后,分别给出单、多脆弱性变换条件下的入侵成功概率极限定理,并通过入侵成功概率计算公式极限变换的形式对定理进行证明,同时基于这两条定理给出单、多脆弱性变换情况下动态变换的最优变换空间计算方法. 最后,通过仿真实验对文章的结论进行验证.

2　系统脆弱性相关定义

NDD 机制实施动态变换的对象包括硬件平台、软件版本等,而变换时机包括随机变换、定时变换和驱动性变换[1]. 因此,为刻画 NDD 机制的变换对象、变换时机与系统脆弱性的关系,给出 NDD 体系下的系统脆弱性定义如下:

定义 1　网络动态防御体系下的系统脆弱性(简称为脆弱性),记为 mvul,$\text{mvul}=\langle \text{id},\langle P_1,\Delta t_1\rangle,\langle P_2,\Delta t_2\rangle,\cdots,\langle P_n,\Delta t_n\rangle\rangle$,$n\in N$($N$ 为自然数),其中 id 为脆弱性标识,$P_i(1\leqslant i\leqslant n)$表示针对该脆弱性实施入侵所利用的系统属性,同时也是 NDD 机制的变换对象;$\Delta t_i(1\leqslant i\leqslant n)$表示 NDD 技术对 P_i 属性实施变换的变换周期.

定义 2　网络动态防御体系下的系统脆弱性状态(简称为脆弱性状态). 对于脆弱性 mvul,记 mvul 在 t 时刻的状态为 $\text{mvul}(t)$,$\text{mvul}(t)=\langle \text{id},p_1,p_2,\cdots,p_n\rangle$,$n\in N$,其中 id 为脆弱性标识,$p_i(1\leqslant i\leqslant n)$表示脆弱性 P_i 属性的当前取值.

定义 3　网络动态防御体系下的系统脆弱性变换(简称为脆弱性变换). 对于脆弱性 mvul,给定两个时刻 t_1 和 t_2,$t_2>t_1$,若 $\text{mvul}(t_2)\neq\text{mvul}(t_1)$,则称脆弱性 mvul 发生了变换.

将脆弱性 mvul 的变换周期记为 interval,根据定义 3,$\text{interval}=\min\{\Delta t_i\}$. 将该脆弱性的变换空间记为 W,根据笛卡尔积定义,$W=P_1\times P_2\times\cdots\times P_n$,将 W 大小记为 $|W|$,则 $|W|=|P_1|\cdot|P_2|\cdot\cdots\cdot|P_n|$,其中 $|P_i|(1\leqslant i\leqslant n)$为第 i 个属性的值域空间大小.

3　NDD 体系下的入侵过程

3.1　非马尔可夫特性分析

在静态防御体系中利用多个脆弱性入侵时,入侵路径上各脆弱性的 P_i 属性保持不变,下一步入侵可视为对上一步结果的扩展延伸. 因此,文献[14]提出可利用攻击图的马尔可夫特性分析静态防御体系下的网络入侵过程,并指出入侵者“将来”攻击目标和入侵结果只与“当前”所处状态有关,而不受“过去”入侵过程的影响.

然而在 NDD 体系下,软件版本、服务端口等属性的动态变化可能导致入侵路径上的脆弱性发生动态变换,从而改变入侵者“当前”状态和“过去”入侵结果,进而影响“将来”入侵过程,本文将此现象称为 NDD 体系下入侵过程的非马尔可夫特性. 如,在图 1 所示的入侵场景中,假定入侵者计划的入侵路径为“$A\rightarrow B\rightarrow C\rightarrow D$”,在 t_0 时刻已经实现“$A\rightarrow B\rightarrow C$”的入侵,并准备在 t_1 时刻发起“$C\rightarrow D$”的渗透. 如果节点 B 在 t_0 到 t_1 中间某个时刻动态变换了 IP 地址,导致入侵者失去对 B 和 C 的控制,进而无法在原有入侵成果的基础上进一步实施针对 D 的入侵.

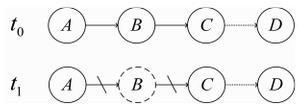


图1　NDD体系下网络入侵过程的非马尔可夫特性

3.2　基于脆弱性变换的入侵成功概率计算

在静态防御体系下,系统脆弱性一般保持不变,若入侵者有能力针对系统脆弱性的变换空间发起穷举性入侵,则入侵成功概率(attack success probability, asp) asp = 1. 然而在 NDD 体系下,脆弱性会因为 P_i 属性的变换而呈现不确定性,因此即使实施穷举性入侵,也不一定确保入侵成功. 下面利用随机抽样模型计算 NDD 体系下的入侵成功概率.

假设在入侵者的单条入侵路径上存在 n 个脆弱性,而入侵者必须依次攻击每个脆弱性才能达成攻击目标(若实施并行攻击则视为存在多条入侵路径),每个脆弱性 $\text{mvul}_i(1\leqslant i\leqslant n)$以变换周期 $\text{interval}_i(1\leqslant i\leqslant n)$独立变换,变换空间大小为 $|W|_i(1\leqslant i\leqslant n)$. 称 n 个脆弱性同时保持不变的时间间隔为入侵时间窗口,记为 T. 根据 NDD 体系下网络入侵的非马尔可夫特性,入侵者要想入侵成功,需在 T 内逐个探测每个脆弱性的当前状态并实施入侵. 当 $n=1$ 时,表示利用单一脆弱性实施入侵,此时 $T=\text{interval}_1$;当 $n>1$ 时,表示利用多个脆弱性实施入侵,此时 NDD 体系下网络入侵的非马尔可夫特性导致 T 是一个随机变量,$T\in[0,\min\{\text{interval}_i\}\ ](1\leqslant i\leqslant n)$,因此引

入概率密度函数 $f(T)$ 表示 T 的分布规律.

假设入侵者依次攻击单条入侵路径上的 n 个脆弱性的过程中,相邻两次攻击之间无时间间隔,且完成对任意一个脆弱性攻击所需要的时间周期均为 τ,则突破单条路径上的 n 个脆弱性所需的总时间周期为 $n\tau$. 将入侵者在 T 内通过具有 n 个脆弱性的单条入侵路径实施入侵的次数记为 k,则

$$k=\frac{T}{n\tau} \tag{1}$$

因为存在 k 不等于整数的情况,所以随机抽样时先对 k 取整. 根据首次入侵发起时间点 $t_1(0\leqslant t_1<n\tau)$ 与起点 t_0 的相对关系,入侵者在 T 内实际可完成的入侵次数为 $[k]$ 或 $[k]-1$. 如,在图 2 所示入侵场景中,$T=3.6n\tau$,$t_0=0$,若 $t_1=0.3n\tau$,则实际可完成的入侵次数为 $[k]=3$;若 $t_1=0.8n\tau$,则实际可完成的入侵次数为 $[k]-1=2$.

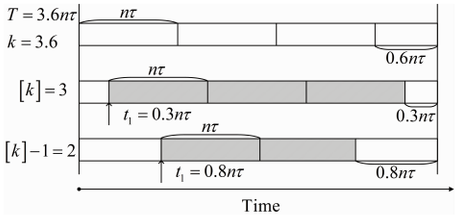


图2 完整入侵次数计算示意图

对于任意 T,当 $0\leqslant t_1<T-[k]n\tau$ 时,入侵者实际可完成的入侵次数为 $[k]$;当 $T-[k]n\tau\leqslant t_1<n\tau$ 时,入侵者实际可完成的入侵次数为 $[k]-1$. 假设 t_1 在 $[0,n\tau)$ 服从均匀分布,那么入侵者实际可完成的入侵次数为 $[k]$ 和 $[k]-1$ 时的概率分别为

$$P_{[k]}=(T-[k]n\tau)/(n\tau) \tag{2}$$

$$P_{[k]-1}=[(1+[k])n\tau-T]/(n\tau) \tag{3}$$

下面给出 T 内的入侵成功概率 $\mathrm{asp}(T)$ 计算方法. 记 n 个脆弱性的总变换空间大小为 S,则 $S=\prod_{i=1}^{n}|W|_i(1\leqslant i\leqslant n)$. 根据式(1~3),当 $0\leqslant T\leqslant n\tau$ 时,$k\leqslant 1$,且当 $k=1$ 时,$P_{[k]}=P_{[1]}=0$,所以 $\mathrm{asp}(T)=0$;当 $T\geqslant(S+1)n\tau$ 时,$k\geqslant S+1$,且当 $k=S+1$ 时,$P_{[k]-1}=P_{[S]}=1$,所以 $\mathrm{asp}(T)=1$;当 $n\tau<T<(S+1)n\tau$ 时,入侵者的入侵过程可抽象为不放回随机抽样事件,此时的入侵成功概率

$$\mathrm{asp}(T)=P_{[k]}\cdot\left(1-\frac{C_{S-1}^{[k]}}{C_S^{[k]}}\right)+P_{[k]-1}\cdot\left(1-\frac{C_{S-1}^{[k]-1}}{C_S^{[k]-1}}\right)$$

$$=\frac{T}{n\tau S}-\frac{1}{S} \tag{4}$$

其中,$C_S^{[k]}$ 表示入侵者对总变换空间 S 完成 $[k]$ 次入侵后的所有结果数,$C_{S-1}^{[k]}$ 表示入侵者的 $[k]$ 次入侵均失败的所有结果数,$\frac{C_{S-1}^{[k]}}{C_S^{[k]}}$ 表示入侵者攻击失败的概率,以此类推可得其余符号的含义.

当 $n=1$ 时,因为 $T=\mathrm{interval}_1$ 是一个定值,此时的入侵成功概率

$$\mathrm{asp}(\mathrm{interval}_1)=\begin{cases}0, & 0\leqslant\mathrm{interval}_1\leqslant\tau\\ \dfrac{\mathrm{interval}_1}{\tau\cdot|W|_1}-\dfrac{1}{|W|_1}, & \tau<\mathrm{interval}_1<(|W|_1+1)\tau\\ 1, & \mathrm{interval}_1\geqslant(|W|_1+1)\tau\end{cases} \tag{5}$$

而当 $n>1$ 时,因为 T 在区间 $[0,\min\{\mathrm{interval}_i\}]$ 内随机分布,此时入侵成功概率 $\mathrm{asp}(\min\{\mathrm{interval}_i\})$ 为 $\mathrm{asp}(T)$ 的期望 $\mathrm{E}(\mathrm{asp}(T))$,即

$$\mathrm{asp}(\min\{\mathrm{interval}_i\})=\mathrm{E}(\mathrm{asp}(T))=\int_0^{\min\{\mathrm{interval}\}}\mathrm{asp}(T)\cdot f(T)\,\mathrm{d}T \tag{6}$$

其中,$f(T)$ 的具体表达形式与脆弱性数量 n、脆弱性变换周期 $\mathrm{interval}_i(1\leqslant i\leqslant n)$ 以及变换的相对时间关系有关,在实际 NDD 体系中,可结合动态安全策略部署情况确定 n 和 $\mathrm{interval}_i(1\leqslant i\leqslant n)$,并通过概率分布拟合的方式得出 $f(T)$ 的表达式.

显然,当 $0<\min\{\mathrm{interval}_i\}\leqslant n\tau$ 时,$\mathrm{asp}(\min\{\mathrm{interval}_i\})=0$;当 $n\tau<\min\{\mathrm{interval}_i\}<(S+1)n\tau$ 时,

$$\mathrm{asp}(\min\{\mathrm{interval}_i\})=\int_{n\tau}^{\min\{\mathrm{interval}\}}\left(\frac{T}{n\tau S}-\frac{1}{S}\right)\cdot f(T)\,\mathrm{d}T \tag{7}$$

当 $\min\{\mathrm{interval}_i\}\geqslant(S+1)n\tau$ 时,

$$\mathrm{asp}(\min\{\mathrm{interval}_i\})=\int_{n\tau}^{(S+1)n\tau}\left(\frac{T}{n\tau S}-\frac{1}{S}\right)\cdot f(T)\,\mathrm{d}T+\int_{(S+1)n\tau}^{\min\{\mathrm{interval}\}}f(T)\,\mathrm{d}T \tag{8}$$

当脆弱性数量 $n>1$ 时,入侵者在 T 内的入侵成功概率

$$\mathrm{asp}(\min\{\mathrm{interval}_i\})=\begin{cases}0, & 0\leqslant\min\{\mathrm{interval}_i\}\leqslant n\tau\\ \displaystyle\int_{n\tau}^{\min\{\mathrm{interval}\}}\left(\frac{T}{n\tau S}-\frac{1}{S}\right)\cdot f(T)\,\mathrm{d}T, & n\tau<\min\{\mathrm{interval}_i\}<(S+1)n\tau\\ \displaystyle\int_{n\tau}^{(S+1)n\tau}\left(\frac{T}{n\tau S}-\frac{1}{S}\right)\cdot f(T)\,\mathrm{d}T+\int_{(S+1)n\tau}^{\min\{\mathrm{interval}\}}f(T)\,\mathrm{d}T, & \min\{\mathrm{interval}_i\}\geqslant(S+1)n\tau\end{cases} \tag{9}$$

假设入侵者在达成攻击目标之前,会针对脆弱性总变换空间 S 发起穷举性攻击,直到入侵成功. 根据式

(4),当 $n\tau < T < (S+1)n\tau$ 时,在穷举性攻击过程中,入侵者共需经历 S/k 次脆弱性变换. 每次脆弱性变换后,入侵者并不能继续利用先前的入侵结果,因此在 S/k 次变换过程中,入侵事件可抽象为放回随机抽样事件,而入侵者只要有一次入侵成功就算达成攻击目标,所以入侵成功概率

$$\mathrm{asp} = 1 - P_{\mathrm{fail}} \tag{10}$$

其中 P_{fail} 表示入侵者在每个变换周期内都攻击失败的概率

$$P_{\mathrm{fail}} = [1 - \mathrm{asp}(T)]^{\frac{S}{k}} \tag{11}$$

特别地,当 $n=1$ 时,$T = \mathrm{interval}_1$,

$$\mathrm{asp} = 1 - \left(1 - \frac{\mathrm{interval}_1}{\tau \cdot |W|_1} + \frac{1}{|W|_1}\right)^{\frac{\tau \cdot |W|}{\mathrm{interval}_1}} \tag{12}$$

然而当 $n>1$ 时,入侵时间窗口 T 也是一个随机变量,进而无法确定 T 内最大入侵次数 k 的准确取值. 但是因为 $k = \dfrac{T}{n\tau}$,所以与式(6)同理,可求得 k 的期望为

$$E(k) = \int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T \tag{13}$$

通过归纳总结典型 NDD 技术[1] 特点,发现其变换周期(单位:s)通常不超过 10^3 数量级,而变换空间大小通常不低于 10^4 数量级,因此本文主要研究 $n\tau < \min\{\mathrm{interval}_i\} < (S+1)n\tau$ 时的入侵成功概率计算式. 与式(10)同理,当 $n>1$,$n\tau < \min\{\mathrm{interval}_i\} < (S+1)n\tau$ 时,入侵者在穷举性入侵过程中,入侵成功概率

$$\mathrm{asp} = 1 - \left[1 - \int_{n\tau}^{\min\{\mathrm{interval}\}} \left(\frac{T}{n\tau S} - \frac{1}{S}\right) \cdot f(T)\,\mathrm{d}T\right]^{\frac{S}{\int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T}} \tag{14}$$

4 NDD 动态变换对象的最优变换空间

4.1 单脆弱性变换下最优变换空间计算

定理 1　给定脆弱性变换周期 interval 和入侵者攻击单个脆弱性所需的时间周期 τ(假定攻击不同脆弱性所需的时间周期相同),当脆弱性数量 $n=1$ 时,入侵成功概率随脆弱性变换空间大小 $|W|$ 的持续增大而存在极限.

证明　当脆弱性数量 $n=1$ 时,令脆弱性变换空间大小 $|W| \to \infty$,对式(12)求极限得:

$$\lim_{|W|\to\infty} \mathrm{asp}_{n=1} = \lim_{|W|\to\infty} \left[1 - \left(1 - \frac{\mathrm{interval}}{\tau \cdot |W|} + \frac{1}{|W|}\right)^{\frac{\tau \cdot |W|}{\mathrm{interval}}}\right]$$

$$= \lim_{|W|\to\infty} \left[1 - \left(1 + \frac{1}{\frac{|W|}{\frac{\tau - \mathrm{interval}}{\tau}}}\right)^{\frac{|W|}{\tau - \mathrm{interval}} \cdot \frac{\tau - \mathrm{interval}}{\tau}}\right]$$

$$= 1 - \mathrm{e}^{\frac{\tau - \mathrm{interval}}{\mathrm{interval}}} \tag{15}$$

根据式(15),在单脆弱性变换情况下,当 $|W| \to \infty$ 时,asp 的极限只与 interval 和 τ 的取值有关. 证毕

由定理 1 可知,当给定 interval 和 τ 时,持续增大变换空间并不能一直降低入侵成功概率. 因此,在单脆弱性变换情况下,为了获得最佳动态防御效果,同时降低防御成本和部署复杂度,NDD 的最优变换空间大小应设置为

$$|W|_{\mathrm{optimal}} = \min\{|W| \mid 1 - \left(1 - \frac{\mathrm{interval}}{\tau \cdot |W|} + \frac{1}{|W|}\right)^{\frac{\tau \cdot |W|}{\mathrm{interval}}} = 1 - \mathrm{e}^{\frac{\tau - \mathrm{interval}}{\mathrm{interval}}}\} \tag{16}$$

4.2 多脆弱性变换下最优变换空间计算

定理 2　给定脆弱性变换周期 $\mathrm{interval}_i$、单条入侵路径上依次攻击的脆弱性数量 n、入侵者攻击单个脆弱性所需的时间周期 τ(假定攻击不同脆弱性所需的时间周期相同)和入侵时间窗口概率密度函数 $f(T)$,对于脆弱性总变换空间大小 S,当 $n>1$,$n\tau < \min\{\mathrm{interval}_i\} < (S+1)n\tau$ 时,入侵成功概率随 S 的持续增大而存在极限.

证明　当脆弱性数量 $n>1$ 时,令脆弱性总变换空间大小 $S \to \infty$,对式(14)求极限得:

$$\lim_{S\to\infty} \mathrm{asp}_{n>1} = \lim_{S\to\infty} \left\{1 - \left[1 - \int_{n\tau}^{\min\{\mathrm{interval}\}} \left(\frac{T}{n\tau S} - \frac{1}{S}\right) \cdot f(T)\,\mathrm{d}T\right]^{\frac{S}{\int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T}}\right\} = \lim_{S\to\infty} \left[1 - \left(1 + \frac{1}{\frac{S}{\int_{n\tau}^{\min\{\mathrm{interval}\}} \frac{n\tau - T}{n\tau} \cdot f(T)\,\mathrm{d}T}}\right)^{\frac{S}{\int_{n\tau}^{\min\{\mathrm{interval}\}} \frac{n\tau - T}{n\tau} \cdot f(T)\,\mathrm{d}T} \cdot \frac{\int_{n\tau}^{\min\{\mathrm{interval}\}} \frac{n\tau - T}{n\tau} \cdot f(T)\,\mathrm{d}T}{\int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T}}\right]$$

$$= 1 - \mathrm{e}^{\frac{\int_{n\tau}^{\min\{\mathrm{interval}\}} \frac{n\tau - T}{n\tau} \cdot f(T)\,\mathrm{d}T}{\int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T}} \tag{17}$$

根据式(17),在多脆弱性变换情况下,当 $S \to \infty$ 时,asp 的极限只与 interval 、n、τ 和 $f(T)$ 的取值有关. 证毕

由定理 2 可知,与单脆弱性变换的情况类似,当给定 $\mathrm{interval}_i$、n、τ 和 $f(T)$ 时,持续增大总变换空间大小 S 并不能一直提高动态防御有效性. 因此,在多脆弱性变换情况下 NDD 的最优总变换空间大小应设置为

$$S_{\mathrm{optimal}} = \min\{S \mid 1 - \left[1 - \int_{n\tau}^{\min\{\mathrm{interval}_i\}} \left(\frac{T}{n\tau S} - \frac{1}{S}\right) \cdot f(T)\,\mathrm{d}T\right]^{\frac{S}{\int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T}} = 1 - \mathrm{e}^{\frac{\int_{n\tau}^{\min\{\mathrm{interval}\}} \frac{n\tau - T}{n\tau} \cdot f(T)\,\mathrm{d}T}{\int_0^{\min\{\mathrm{interval}\}} \frac{T}{n\tau} \cdot f(T)\,\mathrm{d}T}}\} \tag{18}$$

5 NDD 有效性分析

参照文献[7]中的实验网络拓扑,利用防火墙将典型企业网络隔离为允许外网直接访问的 DMZ 区和不允许外网直接访问的内网办公区,其中 DMZ 区部署 1 台 Web 服务器,内网办公区部署 1 台数据库服务器和 3 台办公主机,允许 Web 服务器访问内网办公区的数据库服务. 下面通过 MATLAB 仿真分析单、多脆弱性变换下,脆弱性数量、变换周期及变换空间与 NDD 有效性的关系.

5.1 单脆弱性变换场景

Web 服务器采用 Web 服务多态化技术[15],通过动态轮换多个虚拟 Web 服务器给入侵者呈现不断变换的系统攻击面,增大入侵者利用系统脆弱性的难度. 在其中 1 台虚拟 Web 服务器上设置远程溢出漏洞(CVE-2015-1635),入侵者可利用该脆弱性远程获取 Web 服务器 root 权限. 下面根据式(12)仿真分析脆弱性变换周期 interval 和变换空间 $|W|$ 对 asp 的影响. 图 3 中 interval = $(0,100\tau)$, $|W|=(0,100)$.

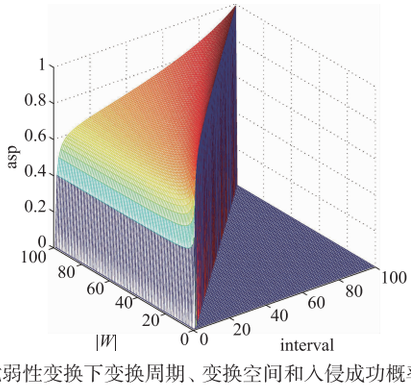
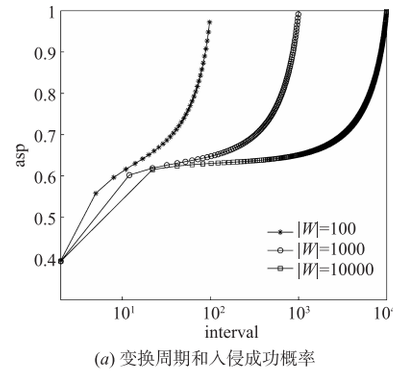


图3 单脆弱性变换下变换周期、变换空间和入侵成功概率的关系

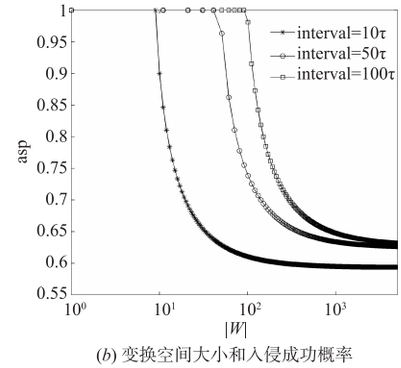
由图 3 可知,当 $\tau<\text{interval}<(|W|+1)\tau$ 时,令 $|W|$ 保持不变,则 asp 随 interval 的增大先迅速增大然后缓慢增大;令 interval 保持不变,则 asp 随 $|W|$ 的增大而减小. 为进一步直观分析 asp 随 interval 及 $|W|$ 的变化而呈现的变化规律,分别固定 $|W|$ 和 interval 再进行仿真,结果如图 4(*a*)和图 4(*b*)所示. 图 4(*a*)中分别取 $|W|=100,1000,10000$, interval = $(\tau,10000\tau)$;图 4(*b*)中分别取 interval = $10\tau,50\tau,100\tau$, $|W|=(1,1500)$.

由图 4(*a*)可知,当 $\tau<\text{interval}<(|W|+1)\tau$ 时,对于相同 $|W|$,asp 随 interval 的减小而非线性降低,其曲线首尾"陡峭",中间"平缓",表明可通过减小变换周期提高动态防御有效性.

由图 4(*b*)可知,asp 随 $|W|$ 的增加而迅速降低,并随 $|W|$ 的继续增大而逐渐收敛于特定值. 当 interval = $10\tau,50\tau,100\tau$ 时,若 $|W|\to\infty$,根据式(15)计算的



(*a*) 变换周期和入侵成功概率



(*b*) 变换空间大小和入侵成功概率

图4 单脆弱性变换下入侵成功概率

asp 极限值分别等于 0.5934,0.6247,0.6284,而图 4(*b*)中的 asp 分别约等于 0.5938,0.6265,0.6303,误差小于 0.002,因此,图 4(*b*)的仿真结果与定理 1 相吻合.

5.2 多脆弱性变换场景

多脆弱性变换场景设置如下:数据库服务器采用数据库接口随机化技术[15]减小入侵者实施 SQL 注入的成功概率,同时在数据库服务器上设置 SQL 远程代码注入漏洞(CVE-2015-1762). 由于防火墙安全规则限制,为获取内网办公主机的 root 权限,入侵者首先需要利用 CVE-2015-1635 获取 Web 服务器的 root 权限,再以 Web 服务器为跳板,利用 CVE-2015-1762 获取数据库服务器的 root 权限,然后以数据库服务器为跳板,利用内网办公主机的脆弱性实施进一步渗透. 在此入侵过程中,Web 服务多态化技术会对入侵者利用 CVE-2015-1635 时依赖的 Web 服务软件实行动态变换,数据库接口随机化技术会对入侵者利用 CVE-2015-1762 时依赖的数据库接口实行动态变换,因此构成一个多脆弱性变换场景.

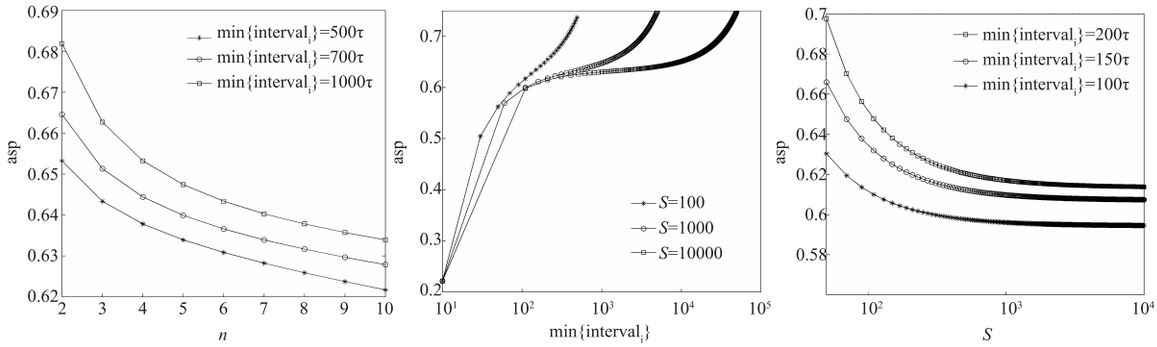
以 T 在区间 $[0,\min\{\text{interval}_i\})$ 服从均匀分布的情况为例仿真分析多脆弱性变换情况下 NDD 有效性,其余分布情况下的分析方法与下文类似. 当 T 服从均匀分布时,

$$F(T)=\begin{cases}\dfrac{1}{\min\{\text{interval}_i\}}, & 0<T<\min\{\text{interval}_i\}\\ 0, & \text{其他}\end{cases} \tag{19}$$

将式(19)代入式(14),可得当 $n\tau<\min\{\text{interval}_i\}<(S+1)n\tau$ 时的入侵成功概率

$$\text{asp}=1-\left\{1-\left[\frac{1}{\min\{\text{interval}_i\}}\left(\frac{\min\{\text{interval}_i\}^2+n^2\tau^2-2n\tau\min\{\text{interval}_i\}}{2n\tau S}\right)\right]\right\}^{\frac{2n\tau S}{\min\{\text{interval}_i\}}} \tag{20}$$

下面根据式(20)仿真分析 n、$\min\{\text{interval}_i\}$、$S$ 对 asp 的影响. 因为在入侵者单条入侵路径上利用的脆弱性数量一般不超过 10[16],所以下文的分析中取 $n\in[2,10]$. 图 5(a)中 $\min\{\text{interval}_i\}=500\tau,700\tau,1000\tau$,$S=1000$,$n=[2,10]$;图 5($b$)中 $S=100,1000,10000$,$n=5$,$\min\{\text{interval}_i\}=[10\tau,50000\tau]$;图 5($c$)中 $\min\{\text{interval}_i\}=100\tau,150\tau,200\tau$,$n=5$,$S=[50,10000]$.



(a) 脆弱性数量与穷举性入侵成功概率　(b) 最小变换周期与穷举性入侵成功概率　(c) 总变换空间大小与穷举性入侵成功概率

图5　多脆弱性变换下穷举性入侵成功概率

由图 5(a)可知,当 $\min\{\text{interval}_i\}$ 和 S 一定时,asp 随 n 的增大而减小,表明可通过增加入侵者在单条入侵路径上所必须顺序攻击的脆弱性数量来提高动态防御有效性.

由图 5(b)可知,当 S 和 n 一定时,与单脆弱性变换情况类似,asp 随 $\min\{\text{interval}_i\}$ 的减小而非线性降低,表明多脆弱性变换情况下,同样可通过减小变换周期而提高动态防御有效性. 特别地,当 $\min\{\text{interval}_i\}=Sn\tau$ 时,$\text{asp}\approx 0.75$. 这是因为当 $\min\{\text{interval}_i\}=Sn\tau$ 时,根据式(9)可知此时的入侵成功概率 $\text{asp}(\min\{\text{interval}_i\})\approx 0.5$,同时根据式(13)可知入侵者在单个入侵窗口内平均可发起的入侵次数 $E(k)=S/2$,因此入侵者平均需要经历 2 次脆弱性变换才能实施穷举性入侵,所以入侵成功概率 $\text{asp}\approx 1-0.5^2=0.75$.

由图 5(c)可知,asp 随 S 的增加而迅速降低,并随 S 的继续增大而逐渐收敛于特定值. 将式(19)代入式(17)可得

$$\lim_{S\to\infty}\text{asp}_{n>1}=1-\mathrm{e}^{\frac{2n\tau\min\{\text{interval}_i\}-n^2\tau^2-\min\{\text{interval}_i\}^2}{\min\{\text{interval}_i\}^2}} \tag{21}$$

当 $\min\{\text{interval}_i\}=100\tau,150\tau,200\tau$ 时,若 $S\to\infty$,根据式(21)计算的 asp 极限值分别等于 0.5944,0.6072,0.6135,而图 5(c)中的 asp 分别等于 0.5946,0.6075,0.6139,误差小于 0.0005,因此,图 5(c)的仿真结果与定理 2 相吻合.

6　结束语

本文从时间和空间维度定义 NDD 体系下的脆弱性及其相关定义,结合时间概率密度函数和随机抽样模型给出 NDD 体系下的入侵成功概率计算公式,在此基础上,提出并证明单、多脆弱性变换场景下的入侵成功概率极限定理,并据此给出相应的最优变换空间计算公式. 下一步我们将继续研究当入侵时间窗口服从其它分布规律时的最优变换空间大小计算方法.

参考文献

[1] 蔡桂林,王宝生,王天佐,等. 移动目标防御技术研究进展[J]. 计算机研究与发展,2016,53(5):968-987.
CAI Gui-lin, WANG Bao-sheng, WANG Tian-zuo, et al. Research and development of moving target defense technology[J]. Journal of Computer Research and Development, 2016, 53(5): 968-987. (in Chinese)

[2] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学,2014,30(7):1-7.
WU Jiang-xing. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7): 1-7. (in Chinese)

[3] ESKRIDGE T C, CARVALHO M M, STONER E, et al.

VINE-A cyber emulation environment for MTD experimentation[A]. George C. Proceedings of the Second ACM Workshop on Moving Target Defense[C]. Denver, Colorado, USA: ACM, 2015. 43 – 47.

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

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

[6] ZHUANG R, DELOACH S A, OU X. A model for analyzing the effect of moving target defenses on enterprise networks [A]. Robert K A. Cyber and Information Security Research Conference[C]. Oak Ridge, TN, USA: ACM, 2014. 73 – 76.

[7] 雷程,马多贺,张红旗,等. 基于变点检测的网络移动目标防御效能评估方法[J]. 通信学报,2017,38(1):126 – 140.
LEI Cheng, MA Duo-he, ZHANG Hong-qi, et, al. Performance assessment approach based on change-point detection for network moving target defense[J]. Journal on Communications, 2017, 38(1): 126 – 140. (in Chinese)

[8] HAMLET J R, LAMB C C. Dependency graph analysis and moving target defense selection[A]. Peng Liu. Proceedings of the 2016 ACM Workshop on Moving Target Defense [C]. Vienna, Austria: ACM, 2016. 105 – 116.

[9] CARTER K M, RIORDAN J F, OKHRAVI H. A game theoretic approach to strategy determination for dynamic platform defenses[A]. Sushil J. Proceedings of the First ACM Workshop on Moving Target Defense[C]. Scottsdale, Arizona, USA: ACM, 2014. 21 – 30.

[10] HODA M, SAEED V, WILLIAM K, et al. Markov modeling of moving target defense games[A]. Peng Liu. Proceedings of the 2016 ACM Workshop on Moving Target Defense[C]. Vienna, Austria: ACM, 2016. 81 – 92.

[11] MASON W, SRIDHAR V, MASSIMILIANO A, et al. Moving target defense against DDoS attacks: an empirical game-theoretic analysis[A]. Peng Liu. Proceedings of the 2016 ACM Workshop on Moving Target Defense[C]. Vienna, Austria: ACM, 2016. 93 – 104.

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

[13] LUO Y B, WANG B S, CAI G L. Effectiveness of port hopping as a moving target defense[A]. Yong-ik Y. International Conference on Security Technology[C]. Hainan, China: IEEE, 2014. 7 – 10.

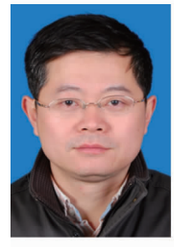
[14] 程叶霞,姜文,薛质,等. 基于攻击图模型的多目标网络安全评估研究[J]. 计算机研究与发展,2012,49:23 – 31.
CHENG Ye-xia, JIANG Wen, XUE Zhi, et al. Multi-objective network security evaluation based on attack graph model[J]. Journal of Computer Research and Development, 2012, 49: 23 – 31. (in Chinese)

[15] SUSHIL J, ANUP K G, VIPIN S, et al. Moving Target Defense-Creating Asymmetric Uncertainty for Cyber Threats [M] New York: Springer, 2011. 117 – 151.

[16] 陈锋,张怡,苏金树,等. 攻击图的两种形式化分析[J]. 软件学报,2010,21(4):838 – 848.
CHEN Feng, ZHANG Yi, SU Jin-shu, et all. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4): 838 – 848. (in Chinese)

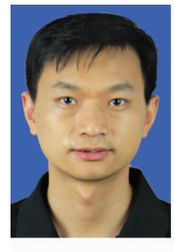
作者简介

李立勋 男,1994 年生于四川都江堰. 现为信息工程大学硕士研究生. 主要研究方向为网络动态防御.
E-mail: lilixun_1994@126.com



张 斌 男,1969 年生于河南许昌. 现为信息工程大学教授、博士生导师. 主要研究方向为网络空间安全.
E-mail: zhangbin1969@sohu.com

董书琴 男,1990 年生于河北邢台. 现为信息工程大学博士研究生. 主要研究方向网络安全态势感知.
E-mail: dongshuqin377@126.com



唐慧林 男,1981 年生于安徽枞阳. 现为信息工程大学讲师. 主要研究方向为网络安全.
E-mail: gogowithsnow@126.com