基于马尔可夫的有限自动机入侵容忍系统模型

罗智勇，杨旭，孙广路，谢志强，刘嘉辉
（哈尔滨理工大学计算机科学与技术学院，黑龙江 哈尔滨 150080）

摘 要：为保证区域网被入侵时，系统仍然能为合法用户提供正常服务，设计了一种有限自动机入侵容忍模型。该模型在马尔可夫的理论基础上，通过建立状态转移概率矩阵来描述系统提供服务的状态变换关系，将转移状态进行量化求解，发现系统中关键结点。通过对关键结点的维护可以增强系统的容忍能力和提高服务的可靠性。实验对比表明，该模型不但具备很强的入侵容忍能力，在保障系统受到入侵时的完整性也具有明显优势。

关键词：网络安全；入侵容忍；有限自动机；状态转移；马尔可夫过程
中图分类号：TP393.4
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019196

Finite automaton intrusion tolerance system model based on Markov

LUO Zhiyong, YANG Xu, SUN Guanglu, XIE Zhiqiang, LIU Jiahui
School of Computer Science and Technology, Harbin University of Science and Technology, Heilongjiang 150080, China

Abstract: To ensure that the system could still provide normal service for legitimate users when the LAN being invaded, a finite automaton intrusion tolerance model was designed. Based on Markov's theory, the state transformation relationship of the service provided by the system by establishing the state transition probability matrix was described, quantified the transition state and found the key nodes in the system. The maintenance of key nodes could enhance the tolerance of the system and improve the reliability of the service. Experimental comparison shows that this model not only has strong intrusion tolerance, but also has obvious advantages in the integrity of the security system when it is invaded.

Key words: network security, invasion tolerance, finite automaton, state transition, Markov process

1 引言

区域网的基础设施通常由大量相互依赖的系统节点组成，这使网络具有一定的开放性，也使网络的入侵变得更加容易且具有隐蔽性[1]。日益复杂的网络攻击通常遵循一系列长期步骤和行动，被称为多阶段攻击，因此很难预测[2]。所以除了在防火墙和访问控制机制等软件系统中使用传统的安全解决方案外，现代网络还需要使用入侵容忍技术。作为第三代网络安全保障技术，入侵容忍融合了容错技术和加密技术[3]，在攻击无法被避免的情况下，系统针对受损情况的不同采取不同的响应策略，通过降级服务争取分析时间，一边学习一边提供网络服务，最终保证系统的稳定运行。在现有入侵容忍系统的文献中，普遍采用定量分析法来形式化服务器系统的各个安全属性，通过建模进一步寻找系统潜在的弱点，针对这些弱点制定不同的应对策略，让系统提供降级服务增强容忍能力及自我修正能力，进而达到延长系统平稳运行时间的目的[4]。

邢云菲等[5]根据入侵容忍系统的状态转移模型的定量分析以及各状态下的概率计算，结合系统遭到入侵之后所采取的进程迁移策略，建立了一种比

收稿日期：2019−03−22；**修回日期**：2019−07−27
基金项目：国家自然科学基金资助项目（No.61772160）；黑龙江省留学归国人员科学基金资助项目（No.LC2018030）
Foundation Items: The National Natural Science Foundation of China (No.61772160), The Scientific Research Starting Foundation for Returned Overseas of Heilongjiang Province (No.LC2018030)

较完善的入侵容忍网络系统。刘进[6]基于高分子链病毒优化分析方法，将入侵容忍系统状态数据和线性规划技术相融合，提出了入侵容忍系统病毒吸附算法。徐晓斌等[7]为了实现对某一单个节点数据的信任评估，设计了一种异常数据过滤方法，其原理是基于节点数据的时空相关性，将定量数据和定性知识做不确定性转换，进而提升系统的入侵容忍能力。孙蔚[8]将网络管理系统和入侵检测系统相结合，提出了一种包含检测、报告和响应等多种功能的层次化入侵检测模型。国外众多研究者提出隐马尔可夫入侵检测模型，如 Divya 等[9]将遗传算法和隐马尔可夫模型相结合，利用遗传算法推导出有效的入侵检测规则，然后使用隐马尔可夫模型来预测攻击者的下一个攻击类，对攻击进行精确检测。Kholidy 等[10]提出了一种有限状态隐马尔可夫预测模型，该模型采用自适应风险方法预测多阶段云攻击。风险模型考虑到威胁的发生概率，衡量威胁对系统的潜在影响，将攻击预测模型与自主云入侵检测框架相集成，攻击来临前对控制器发出早期预警，进而在攻击对系统构成严重安全风险之前采取主动的纠正行动。Holgado 等[11]和 Ahmadian 等[12]所述模型在分析输入输出关系和基于训练数据集生成转移概率矩阵方面具有易处理的数学形式。它通过状态之间的转移概率来处理顺序数据，以此来跟踪多阶段攻击的进度。

上述研究建立了不同的入侵容忍模型，但是通常建模复杂，计算量大，处理入侵行为耗时长。且当入侵行为发生时，上述模型的解决办法多为检测当前入侵行为，预测下一步攻击，面对当前模型无法预测的更加复杂的入侵，并不能保证系统的入侵容忍能力，当系统因为入侵完全失控时，模型中也没有给出相应的解决办法。本文基于马尔可夫理论，提出一种优化的有限自动机入侵容忍模型，主要工作及创新如下。

1) 建立了优化的入侵容忍模型，并在模型中增加了学习状态，系统在遭受攻击后可以不断改进，增强自身稳定性。

2) 利用马尔可夫过程（MP, Markov process）模型参数求解算法，得到系统在不同状态下的平均损坏时间（ADT, average damage time）。

3) 通过分析容忍系统，找出 ADT 关键节点，维护这些关键节点，达到增强系统可用性和可靠性的目的。

4) 分析不同入侵因素对系统容忍能力的影响，提出增强系统容忍能力的解决办法。

2 马尔可夫过程模型

俄国数学家马尔可夫于 1907 年提出了马尔可夫模型（Markov model）[13]。设 $X(t)$为一个随机过程，如果该随机过程 $X(t)$在某一时刻 t_0 的状态已知，则之后任意时刻 $t(t>t_0)$所表现的状态与 $X(t)$在 t_0 时刻之前的状态无关，那么称 $X(t)$具有无后效性，具有无后效性的随机过程就是马尔可夫过程。马尔可夫过程中状态和时间既可以是离散的，也可以是非离散的。状态离散、时间离散的马尔可夫过程称为马尔可夫链。马尔可夫链中，各个时刻状态之间的转移由状态转移的概率矩阵 $\boldsymbol{P}$ 来控制。

马尔可夫模型可以表示为 $\lambda=\{S,\boldsymbol{P},\boldsymbol{G}\}$，其中 λ 为模型名，其余参数含义如下。

1) S 是系统的状态空间，是由系统所有可能状态所组成的非空的状态集。

2) $\boldsymbol{P}=\left[p_{ij}\left(t,t+k\right)\right]_{n\times n}$ 为系统的状态转移概率矩阵，是一个 n 阶方阵，n 为状态空间中所有可能的数量，$p_{ij}\left(t,t+k\right)=\boldsymbol{P}\{X_{t+k}=j\,|\,X_t=i\}$，$i,j\in S$ 表示系统在时刻 t 处于状态 i，但经过 k 步之后状态转移至 j 的概率，其中 X_t 表示系统在 t 时刻的状态，且存在对于任意 $i\in S$，满足约束 $\sum_{j=1}^{n}p_{ij}\left(t,t+k\right)=1$，$0\leqslant p_{ij}\left(t,t+k\right)\leqslant 1,\ i,j\in S$。

3) $\boldsymbol{G}=[g_1,g_2,g_3,\cdots,g_n]$是系统的初始概率分布矩阵，$g_i$ 表示系统在初始时刻处于状态 i 的概率，且满足约束 $\sum_{i=1}^{n}g_i=1$。

对于 $0\leqslant p_{ij}\left(t,t+k\right)\leqslant 1$，$i,j\in S$，当 $k=1$ 时，称 $p_{ij}\left(t,t+1\right)=p_{ij}\left(1\right)$ 为时刻 t 的一步状态转移概率。

通常，使用马尔可夫链进行预测是在当前状态已知的情况下，通过确定一步转移概率矩阵 $\boldsymbol{P}$（即 $k=1$），得到下一状态的概率分布，得到的概率值越大，则下一步处于该状态的可能性越大。

3 优化的容忍系统状态转移模型

由于容忍系统可以保护的对象是多样性的，因此每个容忍系统的目标设定采用的整体框架、实现系统的安全算法都不尽相同。本文为了表现出入侵容忍系统在不同状态的抽象行为，创建了优化的系

统状态转移模型（SSTM, system state transition model），其结构如图 1 所示。

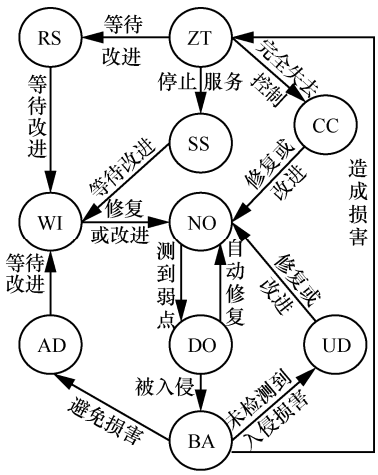


图 1　系统状态转移模型

SSTM 描述了多数容忍系统在遭受入侵后可能处于的状态和在不同状态下的处理方式，即系统中可能发生的事件。模型中各状态的转换方式如下。

步骤 1　开始系统处于正常运行（NO, normal operation）状态。

步骤 2　当系统中存在的弱点被入侵者检测到并利用时，系统处于危险运行（DO, dangerous operation）状态。

步骤 3　如果系统发现自身弱点并及时修复了该弱点，则系统回归正常运行。

步骤 4　如果入侵者成功入侵了系统，则系统处于被入侵（BA, being attacked）状态。

步骤 5　若系统可以避免入侵造成的损害，则系统处于避免损害（AD, avoid damage）状态。

步骤 6　这时，系统将进入等待改进（WI, waiting for improving）状态。

步骤 7　若系统没有检测到入侵，也未触发容忍系统，则系统处于未发现威胁（UD, unknown damage）状态。

步骤 8　若入侵对系统造成了损害但是系统成功触发有限自动机系统，则系统进入零容忍（ZT, zero tolerance）状态。

步骤 9　此时，系统将评估当前所受损害及运行状态，若系统可以降低服务等级继续运行，则系统处于降低服务等级（RS, reduce the service）状态。

步骤 10　若评估后发现系统不能继续运行，则系统处于停止服务（SS, stop the service）状态。无论是处于 RS 状态还是处于 SS 状态，系统都将进入 WI 状态，等待改进。

步骤 11　若系统受到入侵后，完全失去控制，则系统处于失控（CC, can't be control）状态，这时系统需要管理员修复或改进后才能继续运行。

SSTM 根据入侵受损情况被划分为若干状态等级，当系统与已知状态相似，则可以使用该状态转移模型进行处理。由于各状态之间的转换不受前一状态的影响，符合马尔可夫过程。因此，可以采用马尔可夫对模型进行分析。

4　容忍系统的有限自动机分析

有限自动机是一种控制状态有限、符号集有限的自动机，分为确定有限自动机和非确定有限自动机。

如图 1 所示，随着入侵容忍系统的运行，系统从一个状态转换为另一个状态，这些状态可能为健康状态，也可能为带病工作状态，不同的系统状态代表不同的含义。某一时刻，均存在某种确定的状态与系统相对应，系统无论如何运行最终均将处于终止状态，因此系统的状态是有限的，故可用有限自动机对容忍系统进行描述。又由于容忍系统具有非确定有限自动机的特点，即在给定状态和符号的情况下，不能唯一地确定下一个状态。所以，本文采用非确定有限自动机理论来研究容忍系统的形式化描述方法。

定义 1　一个非确定有限自动机 NDFSA 是一个五元组，即 NDFSA=(S_{space}, Σ, Map, N_0, N_D)，各元素定义如下。

S_{space} 是一个非空有限状态空间，它的每个元素称为一个状态。

Σ 是一个非空有限输入字母表，它的每个元素称为一个输入字符。

Map 是映射函数，可表示为 $S_{\text{space}}\Sigma\rightarrow S_{\text{space}}$ 的子集，即 Map 是一个多值映射，若当自动机处于状态 s，并输入字符 δ 后，系统转换到状态 s'，则表示为：Map(s,δ)= s'。

$N_0 \subseteq S_{\text{space}}$ 是非空初始状态集。

$N_D \subseteq S_{\text{space}}$ 是 S_{space} 终止状态集，可取空值。

根据图 1，可以将容忍系统模型抽象为非确定性有限自动机 NDFSA=(S_{space},Σ,Map,N_0,N_D)，其中 S_{space} = {NO,DO,BA,AD,UD,WI,ZT,RS,SS,CC}；

Σ={0,1,τ}，1 和 0 分别表示容忍系统安全策略的成功和失败，τ 表示空移；N_0={N}；N_D={N}。

映射 Map：$S_{\text{space}}\Sigma \rightarrow S_{\text{space}}$ 为

$\text{Map}(\text{NO},0)=\text{DO}$，$\text{Map}(\text{NO},1)=\text{NO}$；

$\text{Map}(\text{DO},1)=\text{NO}$，$\text{Map}(\text{DO},\tau)=\text{BA}$；

$\text{Map}(\text{BA},0)=\text{UD}$，$\text{Map}(\text{BA},1)=[\text{AD},\text{ZT}]$；

$\text{Map}(\text{AD},0)=\text{WI}$，$\text{Map}(\text{AD},1)=\text{WI}$；

$\text{Map}(\text{UD},1)=\text{NO}$；$\text{Map}(\text{WI},1)=\text{NO}$；

$\text{Map}(\text{ZT},0)=\text{CC}$，$\text{Map}(\text{ZT},1)=[\text{RS},\text{SS}]$；

$\text{Map}(\text{RS},0)=\text{WI}$，$\text{Map}(\text{RS},1)=\text{WI}$；

$\text{Map}(\text{SS},1)=\text{WI}$；$\text{Map}(\text{CC},1)=\text{WI}$

该容忍系统模型的非确定有限自动机状态转换表如表 1 所示。基于图 1 的系统状态转移模型，建立该容忍系统模型的非确定有限自动机状态转换模型，如图 2 所示。图 2 反映了入侵容忍系统不同状态之间的动态转换框架，状态转换模型表现了系统遭受的入侵行为和系统实际安全需求二者之间的相应措施。

表 1　容忍系统的非确定有限自动机状态转换表

状态 s	输入字母表 Σ		
	0	1	τ
NO	DO	NO	—
DO	—	NO	BA
BA	UD	[AD,ZT]	—
AD	WI	WI	—
UD	—	NO	—
ZT	CC	[RS,SS]	—
RS	WI	WI	—
SS	—	WI	—
CC	—	NO	—
WI	—	NO	—

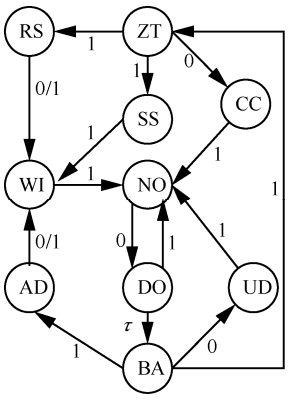


图 2　容忍系统非确定有限自动机状态转换模型

5　有限自动机的马尔可夫量化过程

由于图 2 所示的有限自动机容忍系统的状态空间为 S_{space} = {NO,DO,BA,AD,UD,WI,ZT,RS,SS,CC}，且转换状态满足马尔可夫过程，因此可以将其量化，并使用马尔可夫理论对有限自动机容忍模型进行分析，该模型被称之为 MP 模型。

定义 2　MPSTP（Markov process state transition probability）矩阵是指结合马尔可夫过程，在离散的时间点将状态空间中各节点一次转换成下一状态的概率值组成一个矩阵，则该矩阵称为 MPSTP 矩阵，用 $\boldsymbol{P}$ 表示。

使用概率符号 P_{n}、P_{nd}、P_{db}、P_{bs}、P_{bu}、P_{aw}、P_{un}、P_1、P_2、P_{zr}、P_{zs}、P_{rw}、P_{sw}、P_3、P_{wn}、P_{cn} 表示各状态之间的一次转换概率，其含义如表 2 所示。

将状态空间中各节点一次转换成下一状态的概率值代入图 2 的非确定有限自动机状态转换模型进行量化，得出 MPSTP 模型如图 3 所示。

图 3 的 MPSTP 模型展示了该容忍系统不同状态之间相互转移的可能性，其中稳定的概率值可由入侵注入的方式测定或者由网络管理员根据经验确定，本文采用第一种方式，通过入侵注入行为实验，测得实验数据。

将状态空间中各节点一次转换成下一状态的概率值建立成一个矩阵，得到 MPSTP 矩阵 $\boldsymbol{P}$ 为

$$\boldsymbol{P}=\begin{array}{c} \\ \text{NO} \\ \text{DO} \\ \text{BA} \\ \text{AD} \\ \text{UD} \\ \text{WI} \\ \text{ZT} \\ \text{RS} \\ \text{SS} \\ \text{CC} \end{array}\begin{array}{c}\begin{array}{cccccccccc}\text{NO} & \text{DO} & \text{BA} & \text{AD} & \text{UD} & \text{WI} & \text{ZT} & \text{RS} & \text{SS} & \text{CC}\end{array}\\ \begin{bmatrix} P_{\text{n}} & P_{\text{nd}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_1 & 0 & P_{\text{ba}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & P_{\text{ba}} & P_{\text{bu}} & 0 & P_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & P_{\text{aw}} & 0 & 0 & 0 & 0 \\ P_{\text{un}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{\text{wn}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{\text{zr}} & P_{\text{zs}} & P_3 \\ 0 & 0 & 0 & 0 & 0 & P_{\text{rw}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & P_{\text{sw}} & 0 & 0 & 0 & 0 \\ P_{\text{cn}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}\end{array}$$

定义 3　DoS（duration of state）矩阵是指有限自动机容忍系统中各状态的持续停留时间所组成的矩阵，用 $\boldsymbol{T}$ 表示，则 $\boldsymbol{T}$=[t_{NO},t_{DO},t_{BA},t_{AD},t_{UD}, t_{WI},t_{ZT}, t_{RS},t_{SS},t_{CC}]。

6　MP 模型量化及分析

MP 模型的量化分析可以指导管理员有针对性地维护系统，达到增强系统入侵容忍能力的目

表 2　　MP 模型各符号及功能描述

符号	功能	功能描述
P_{n}	NO→NO	系统正常工作的概率
P_{nd}	NO→DO	系统中的弱点被入侵行为发现的概率
P_{db}	DO→BA	系统被成功入侵的概率
P_{ba}	BA→AD	系统发现了入侵行为，且屏蔽了入侵损害的概率
P_{bu}	BA→UD	入侵没有被发现的概率
P_{aw}	AD→WI	系统屏蔽了入侵损害但需要进行改进的概率
P_{un}	UD→NO	系统未发现入侵，一段时间后进行改进或修复重新运行的概率
P_1=1−P_{w}−P_{a}	DO→NO	系统检测到自身弱点并及时修复的概率
P_2=1−P_{s}−P_{u}	BA→ZT	成功触发自动机的概率
P_{zr}	ZT→RS	系统能够运行但却需要降级服务的概率
P_{zs}	ZT→SS	系统无法运行自主停止系统的概率
P_{rw}	RS→WI	系统能够提供降级服务运行但需要进行改进的概率
P_{sw}	SS→WI	系统被安全停止运行后需要进行改进的概率
P_3=1−P_{d}−P_{h}	ZT→CC	系统因为入侵故障被迫停止运行的概率
P_{wn}	WI→NO	系统处改进或完善状态后经过改进重返正常运行的概率
P_{cn}	CC→NO	系统处于完全失控状态但经改进或修复后重返正常运行的概率

的。为了简化和准确的量化 MP 模型，本文给出如下定义。

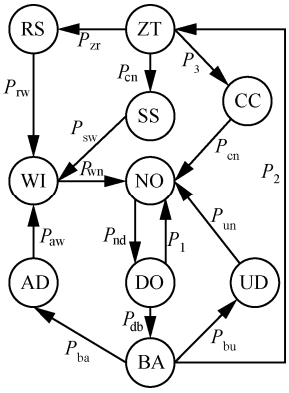


图 3　MPSTP 模型

定义 4　有限机 MP 模型的具体值，是指系统进入 MP 模型各状态的概率。用矩阵 $\boldsymbol{K}$ 表示，则 $\boldsymbol{K}$=[k_{NO},k_{DO},k_{BA},k_{AD},k_{UD},k_{WI},k_{ZT},k_{RS},k_{SS},k_{CC}]，k_i 表示系统进入 MP 模型各状态的概率值，i∈S_{space}。

MP 模型各状态的稳定概率主要有 2 种输入参数：1) 各状态的 MPSTP 矩阵 $\boldsymbol{P}$；2) 各状态的 DoS 矩阵 $\boldsymbol{T}$。

图 3 所示模型中各状态的概率值矩阵 $\boldsymbol{K}$ 可通过式(1)计算。

$$\begin{cases} K' = \boldsymbol{KP} \\ \sum\limits_{i \in S_{\mathrm{space}}} k_i = 1 \end{cases} \tag{1}$$

定义 5　有限自动机的 MP 稳定概率，是指整个系统模型中各个状态持续时间所占的比，用 $\boldsymbol{G}$ 来表示，则 $\boldsymbol{G}$=[g_{NO},g_{DO},g_{BA},g_{AD},g_{UD},g_{WI},g_{ZT},g_{RS},g_{SS},g_{CC}]，其中 g_i 为状态 i 的 MP 稳定概率，g_i 可通过式(2)计算。

$$g_i = \frac{k_i t_i}{\sum\limits_j k_j t_j}, i, j \in S_{\mathrm{space}} \tag{2}$$

6.1　MP 模型安全属性

图 3 所示的状态节点空间 S_{space} 共分为 2 个子集。

1) 系统遭受入侵者入侵的行为节点空间 S_{I}，则 S_{I}={NO,DO,BA}。

2) 入侵发生以后，系统所采取的行为节点空间 S_{R}，则 S_{R}={AD,UD,ZT,RS,SS,CC,WI}。

在空间 S_{R} 中，1) 当系统处于某些状态时，MP 模型的安全属性会受到损坏，这些状态形成了安全受损空间 S_{D}；2) 当系统处于另一些状态时，MP 模型的安全属性不会受到损失，这些状态形成了安全未受损空间 S_{U}。

MP 模型的安全属性可从 3 个方面进行考虑。

1) 可用性（availability），即模型可为合法用户提供正常服务的能力，其概率用 P_{A} 表示。

由于系统在 UD、SS、CC 这 3 种状态下处于非运行状态，因此无法向用户提供任何服务。因此，系统的安全损坏状态 S_{D}={UD,SS,CC}，安全未损坏

状态 S_U={AD,ZT,RS,WI}。MP 模型的系统可用性概率 P_A=1−k_{UD}−k_{SS}−k_{CC}。

2) 机密性（confidentiality），是指系统保证数据安全的能力，其概率用 P_C 表示。

在 UD、CC 状态下，由于系统被入侵行为破坏导致非安全停止运行，将无法保证数据的安全。因此，系统的安全损坏状态 S_D={UD,CC}，安全未损坏状态 S_U={AD,ZT,RS,SS,WI}。MP 模型的系统机密性概率 P_C=1−k_{UD}−k_{CC}。

3) 完整性（integrity），即系统不会被入侵者修改的能力，其概率用 P_I 表示。

在 UD、SS、CC、AD、RS 状态下，由于入侵者的行为，系统将可能不再完整，即完整性受到破坏。因此，系统的安全损坏状态 S_D={UD,SS, CC,AD,RS}，安全未损坏状态 S_U={ZT, WI}。MP 模型的系统完整性概率 P_I=1−k_{UD}−k_{SS}−k_{CC}−k_{AD}−k_{RS}。

由分析可知，MP 模型的 3 个安全属性概率与各个状态节点的稳定概率相关。

综上所述，MP 模型的安全属性概率可通过式(3)计算。

$$P_a = 1 - \sum_{j \in S_D} k_j, a = \mathrm{A,C,I} \tag{3}$$

从式(3)可知，MP 模型安全属性与安全受损空间状态的稳定概率 k_j 成反比关系。

6.2 MP 系统平均损坏时间

定义 6 系统平均损坏时间 ADT，是指系统开始处于MP模型的某状态到系统由于入侵造成的损坏并导致最终停止运行二者之间消耗的平均时长。

平均损坏时间是检测入侵容忍系统抵御入侵行为能力的重要指标。平均损坏时间的值越大，表示系统在该状态受到入侵导致其非正常停止运行的时间就越长，入侵代价也就越大，则系统的安全性也越高。

分析图 3 所示的 MP 模型，发现有些状态是系统被入侵行为损坏后非正常停止运行的状态，该类状态系统需由网络管理人员进行手动修复或改进后才能重新正常运行，将此类状态组成的状态集合，称为停止运行状态集，用 S_E 表示。用 S_M 表示此类状态之外的状态集合，称为中间状态集。

Trivedi[14]的研究表明，ADT 的计算式为

$$\mathrm{ADT} = \sum_{i \in S_M} C_i t_i \tag{4}$$

其中，C_i 表示该容忍系统在最终进入停止状态前通过其他状态 i 的总次数，t_i 是状态 i 的持续时间。

系统总是由正常状态 NO 开始运行，因此首先要算出 C_{NO}。分析图 3，系统通过状态 NO 的概率由流入概率 P_{in} 和流出概率 P_{out} 二者共同决定，且 P_{in}+P_{out}=1。由于 C_{NO} 是系统非正常停止运行前通过正常状态 NO 的总次数，因此 $C_{NO} = \dfrac{1}{P_{in}} = \dfrac{1}{1 - P_{out}}$。

在 MP 模型中，影响状态 NO 流入概率 P_{in} 的因素很多且比较难确定，因此本文采用通过计算流出概率 P_{out} 来确定 C_{NO}。

经分析，系统由状态 NO 进入停止状态的路径共有 5 条，即 NO—DO—BA—AD—WI，NO—DO—BA—UD，NO—DO—BA—ZT—CC，NO—DO—BA—ZT—RS—WI 和 NO—DO—BA—ZT—RS—WI。观察这 5 条状态转换路径发现，在 MP 模型中，系统经过状态 BA 之后最终都将进入停止状态，需由管理员修复或改进后重新回到正常状态 NO，因此状态 NO 的流出概率 P_{out}=$P_{db}P_{nd}$。

7 实验分析与优化评估

7.1 实验环境设计

为验证 MP 模型的优化评估过程，本文组建了如图 4 所示的实验环境。图 4 给出了网络拓扑结构及各服务器存在的漏洞，其中，容忍系统有由服务器 IP_1、IP_2 和 IP_3 组成，它可以对不同主机提供相对应的服务，不同域间的访问策略如下。

1) 该入侵容忍系统中的各服务器与域 D_1 和域 D_2 内的各个网络设备可以相互访问，但不可访问域 D_3 中的网络设备。

2) 域 D_1 中的网络设备 IP 和域 D_2 中的网络设备 IP_9 都可以访问域 D_3 的数据库服务器。

3) 域 D_1 中的网络设备 IP_4 可以和域 D_2 中的网络设备 IP_7 相互访问。

4) 每个域内的网络设备之间可以相互访问。

5) 区域网内部设备必须通过容忍系统中的服务器才可以与 Internet 之间交换数据。

6) 其他网络设备之间如果跨域访问都将被禁止。

7.2 实验数据计算、优化与评估

为绕开企业防火墙安全策略，入侵者普遍采取先入侵内网主机后入侵容忍系统的攻击策略。实验

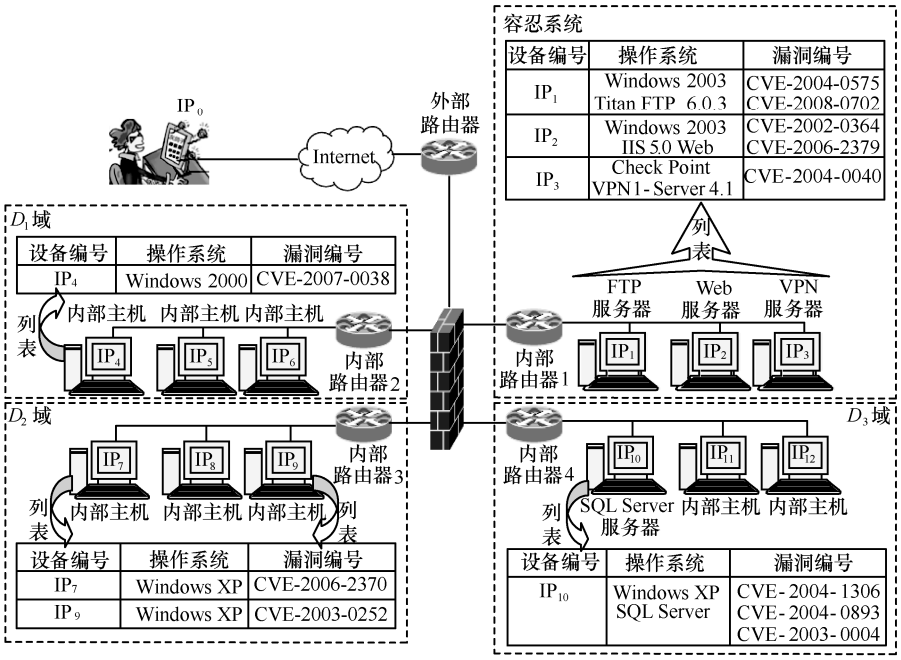


图 4　MP 模型的网络拓扑结构及各服务器存在的漏洞

正是在这种入侵策略下，对图 4 所示容忍系统进行了模拟攻击测试。考虑到不同的操作系统存在不同的漏洞，而不同的漏洞决定了入侵成功的概率，进而影响容忍系统的服务能力。为此，实验分别模拟入侵者在完全控制域 D_1 和域 D_2 内的主机 IP_4、主机 IP_7 和主机 IP_9 的情况下，直接或间接（即通过域 D_3 中数据库服务器）对容忍系统进行攻击。将每种攻击路径所造成容忍系统无法提供服务的数据进行分析统计，得出该容忍系统中各参数的平均值如下。

1) 系统开始正常运行，所以 P_n=1；

2) 系统发生故障，管理员对系统维护后，系统将重新运行，因此 P_{aw}=P_{sw}=P_{rw}=P_{wn}=P_{un}=P_{cn}=1。

3) 系统中的弱点被发现的概率 P_{nd}=0.2。

4) 系统中存在的弱点被入侵者发现后，入侵者入侵成功的概率 P_{db}=0.6。

5) 系统检测到自身弱点并及时修复的概率 P_1=1−P_{nd}−P_{db}=0.2。

6) 入侵被发现且被屏蔽的概率 P_{ba}=0.3。

7) 入侵没有被发现的概率 P_{bu}=0.1。

8) 成功触发自动机的概率 P_2=1−P_{ba}−P_{bu}=0.6。

9) 系统能够运行但却需要降级服务的概率 P_{zr}=0.6。

10) 系统无法运行自主停止概率 P_{zs}=0.3。

11) 系统因为入侵故障被迫停止运行的概率 P_3=1−P_{zr}−P_{zs}=0.1。

由测试可知，系统处于降级服务运行的时间最长，处于容忍触发的时间最短，处于正常运行和未发现入侵继续运行的时间相当，处于屏蔽该入侵行为运行和处于学习改进的时间相当，其他各状态的时间不等。基于实验数据，将系统处于各状态的时间（单位为天）定为：t_{NO}=1，t_{DO}=0.8，t_{BA}=0.3，t_{AD}=0.4，t_{UD}=1.2，t_{ZT}=0.1，t_{RS}=3，t_{SS}=2，t_{CC}=1.5，t_{WI}=1.5。

本文所设定的数据均来自本次实验，现实中不同网络设备存在操作系统、漏洞、网络拥挤程度的差异，所以具体的数据可由网络管理员针对系统的不同进行设置。

7.2.1　MPSTP 矩阵

依据定义 4 的式(1)，可以计算出系统进入 MP 模型各状态的概率值 k_i，如式(5)所示。

$$\begin{cases} k_{NO}=P_n k_{NO}+P_1 k_{DO}+P_{un} k_{UD}+P_{cn} k_{CC}+P_{wn} k_{WI}= \\ \left(P_n+P_1 P_{nd}+P_{un} P_{bu} P_{db} P_{nd}+P_{cn} P_3 P_2 P_{db} P_{nd}+P_{wn}\cdot\right. \\ \left.(P_{aw} P_{ba} P_{db} P_{nd}+P_{rw} P_{zr} P_2 P_{db} P_{nd}+P_{sw} P_{zs} P_2 P_{db} P_{nd})\right) k_{NO}, \\ k_{DO}=P_{nd} k_{NO}, k_{BA}=P_{db} k_{DO}=P_{db} P_{nd} k_{NO}, \\ k_{AD}=P_{ba} k_{BA}=P_{ba} P_{db} P_{nd} k_{NO}, k_{ZT}=P_2 k_{BA}=P_2 P_{db} P_{nd} k_{NO}, \\ k_{UD}=P_{bu} k_{BA}=P_{bu} P_{db} P_{nd} k_{NO}, k_{SS}=P_{zs} k_{ZT}=P_{zs} P_2 P_{db} P_{nd} k_{NO}, \\ k_{RS}=P_{zr} k_{ZT}=P_{zr} P_2 P_{db} P_{nd} k_{NO}, k_{CC}=P_3 k_{ZT}=P_3 P P_{db} P_{nd} k_{NO}, \\ \kappa_{WI}=P_{aw} k_{AD}+P_{rw} k_{RS}+P_{sw} k_{SS}= \\ \left(P_{aw} P_{ba} P_{db} P_{nd}+P_{rw} P_{zr} P_2 P_{db} P_{nd}+P_{sw} P_{zs} P P_{db} P_{nd}\right) k_{NO} \end{cases} \tag{5}$$

将式(5)代入该等式 $\sum_{i\in S_{\text{space}}} k_i = 1$，得出状态 NO 的概率值 k_{NO}，如式(6)所示。

$$\begin{aligned} k_{\text{NO}} = &\Big[\big(P_{\text{n}}+P_{\text{l}}P_{\text{nd}}+P_{\text{un}}P_{\text{bu}}P_{\text{db}}P_{\text{nd}}+P_{\text{cn}}P_3P_2P_{\text{db}}P_{\text{nd}}+\\ &P_{\text{wn}}(P_{\text{aw}}P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+P_{\text{rw}}P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+P_{\text{sw}}P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}})\big)+\\ &P_{\text{nd}}+P_{\text{db}}P_{\text{nd}}+P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+P_{\text{bu}}P_{\text{db}}P_{\text{nd}}+P_2P_{\text{db}}P_{\text{nd}}+\\ &P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}+P_3P_2P_{\text{db}}P_{\text{nd}}+\\ &(P_{\text{aw}}P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+P_{\text{rw}}P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+P_{\text{sw}}P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}})\Big]^{-1} \end{aligned} \tag{6}$$

将式(6)代入式(5)并结合实验所得数据，计算出系统进入 MP 模型各状态的概率值 k_i，如图 5 所示。

利用系统各概率值 k_i 和式(3)，可以得到系统的可用性概率 P_{A}=0.992 1，机密性概率 P_{C}=0.993 4，完整性概率 P_{I}=0.939 4。

7.2.2 MP 稳定概率

将系统进入 MP 模型各状态的概率矩阵 $\boldsymbol{K}$ 和处于各个状态的时间矩阵 $\boldsymbol{T}$ 代入式(2)，得出 MP 模型各状态的稳定概率 g_i，如式(7)所示。

$$\begin{cases} \text{Sum} = \sum_{j\in S_{\text{space}}} k_j t_j = \\ \big(t_{\text{NO}}+t_{\text{DO}}P_{\text{nd}}+t_{\text{BA}}P_{\text{db}}P_{\text{nd}}+t_{\text{AD}}P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+\\ t_{\text{UD}}P_{\text{bu}}P_{\text{db}}P_{\text{nd}}+t_{\text{ZT}}P_2P_{\text{db}}P_{\text{nd}}+t_{\text{RS}}P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+\\ t_{\text{SS}}P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}+t_{\text{CC}}P_3P_2P_{\text{db}}P_{\text{nd}}+\\ t_{\text{WI}}\big(P_{\text{aw}}P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+P_{\text{rw}}P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+P_{\text{sw}}P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}\big)\big)k_{\text{NO}},\\ g_{\text{NO}}=\dfrac{t_{\text{NO}}k_{\text{NO}}}{\text{Sum}},g_{\text{DO}}=\dfrac{t_{\text{DO}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},g_{\text{BA}}=\dfrac{t_{\text{BA}}P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},\\ g_{\text{AD}}=\dfrac{t_{\text{AD}}P_{\text{ba}}P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},g_{\text{UD}}=\dfrac{t_{\text{UD}}P_{\text{bu}}P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},\\ g_{\text{ZT}}=\dfrac{t_{\text{ZT}}P_2P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},g_{\text{RS}}=\dfrac{t_{\text{RS}}P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},\\ g_{\text{SS}}=\dfrac{t_{\text{SS}}P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},g_{\text{CC}}=\dfrac{t_{\text{CC}}P_3P_2P_{\text{db}}P_{\text{nd}}k_{\text{NO}}}{\text{Sum}},\\ g_{\text{WI}}=\dfrac{t_{\text{WI}}\big(P_{\text{aw}}P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+P_{\text{rw}}P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+P_{\text{sw}}P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}\big)k_{\text{NO}}}{\text{Sum}} \end{cases} \tag{7}$$

将实验得到的各状态转移概率 P_i 值和持续时间 t_i 值及计算所得到的 k_i 值代入式(7)，得到各状态的稳定概率 g_i，g_i 的分布轨迹如图 6 所示。

7.2.3 各状态访问次数

由 6.2 节分析，先求出容忍系统最终进入停止状态前通过正常状态的总次数 CNO，然后通过各个状态之间的状态转移概率求出不同状态的 C_i，

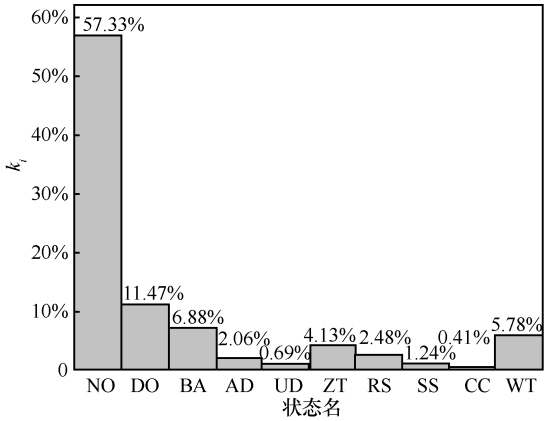


图 5 MP 模型进入各状态的概率

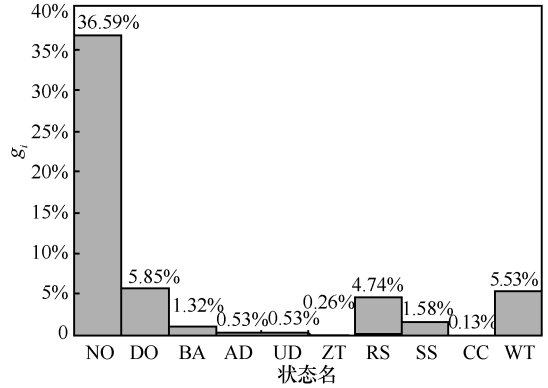


图 6 MP 模型各状态稳定概率

最终可求出系统的平均损坏时间 ADT，可通过式(8)计算。

$$\begin{cases} C_{\text{NO}} = \dfrac{1}{1-P_{\text{db}}P_{\text{nd}}}, C_{\text{DO}} = P_{\text{nd}}C_{\text{NO}},\\ C_{\text{BA}}=P_{\text{db}}P_{\text{nd}}C_{\text{NO}}, C_{\text{AD}}=P_{\text{ba}}P_{\text{db}}P_{\text{nd}}C_{\text{NO}},\\ C_{\text{UD}}=P_{\text{bu}}P_{\text{db}}P_{\text{nd}}C_{\text{NO}}, C_{\text{ZT}}=P_2P_{\text{db}}P_{\text{nd}}C_{\text{NO}},\\ C_{\text{RS}}=P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}C_{\text{NO}}, C_{\text{SS}}=P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}C_{\text{NO}},\\ C_{\text{CC}}=P_3P_2P_{\text{db}}P_{\text{nd}}C_{\text{NO}},\\ C_{\text{WI}}=\big(P_{\text{ba}}P_{\text{db}}P_{\text{nd}}+P_{\text{zr}}P_2P_{\text{db}}P_{\text{nd}}+P_{\text{zs}}P_2P_{\text{db}}P_{\text{nd}}\big)C_{\text{NO}},\\ \text{ADT} = \sum_{i\in S_{\text{M}}} \text{C}_i t_i \end{cases} \tag{8}$$

把实验得到的 P_{db} 和 P_{nd} 代入式(8)，求出 C_{NO} 的数据值，进一步求得每个状态的 C_i 值，其分布条形图如图 7 所示。

ADT 代表着入侵者所付出的入侵代价，所以 ADT 是系统安全可靠的重要指标。增大 ADT 可以增加入侵者的入侵代价从而保障系统的安全。然而，ADT 的增加又与 C_i 和 t_i 有关。一个确定入侵容忍系统，其各状态的 C_i 值基本固定，因此可以通过增加各状态的持续时间 t_i 来达到增大 ADT 的目

的。进一步分析式(8)，可以得出 MP 模型中各中间状态的 ADT 值，其分布情况如图 8 所示。

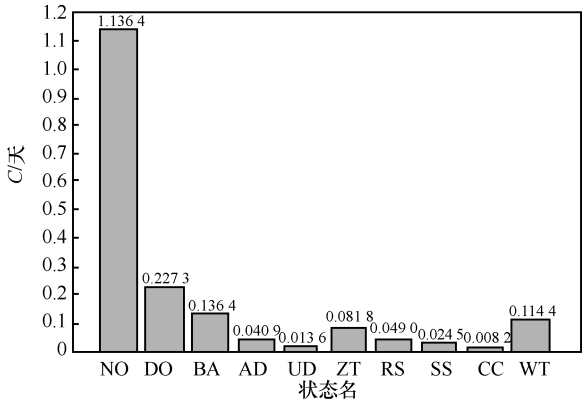


图 7　各状态访问次数

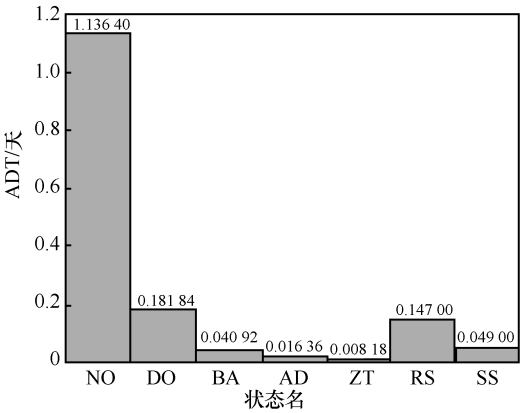


图 8　各中间状态 ADT 变化轨迹

从图 8 中可以看出，各中间状态的持续时间对系统总体 ADT 影响从大到小的顺序为{NO,DO,RS,SS,BA,AD,ZT}。若增大中间状态{NO,DO,RS}的持续时间，则可以有效地提高系统的 ADT，同时也增加了入侵代价，增强了系统的可靠性。

7.3　入侵因素对系统性能的影响

本文主要从容忍系统关键节点的平均故障时间、系统的可用性、机密性和完整性等方面分析了系统的性能。在图 4 所示的实验环境中，假设容忍系统的服务器数量为 $N(N=1,2,\cdots)$，容忍系统的可用性、机密性和完整性定义为：在给定时间周期内，仍有 $\left\lceil \frac{N}{2} \right\rceil$ 个服务器可以提供正常提供服务且数据未泄密和未被篡改的概率。

本文通过使用网络仿真软件 GNS3 模拟网络入侵数据分组，基于实验数据，得出了容忍系统中各关键节点在不同入侵速度 V 下 ADT 的分布轨迹如图 9 所示。

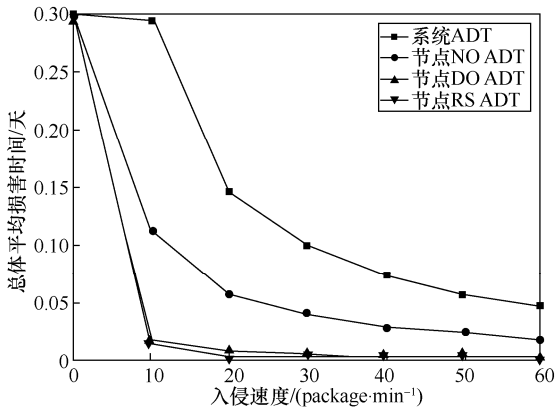


图 9　总体平均损害时间与入侵速度的关系

图 9 表明，容忍系统各总体的平均损害时间与网络入侵速度 V 基本成反比，即入侵速度增加平均损害时间降低。呈现这种关系的主要原因为：随着网络入侵速度的加快，容忍系统中出现故障的服务器数增多，造成系统各关键节点及总体的 ADT 下降。可通过增加容忍系统服务器数量 N 来提高系统的 ADT 值，这是因为在出现故障节点相同的前提下，提供服务的节点数越多，系统的可用性越强。

基于实验中的数据，把容忍系统不同状态的持续时间（单位为天）设定为：$t_{NO}=1$，$t_{DO}=0.8$，$t_{BA}=0.3$，$t_{AD}=0.4$，$t_{UD}=1.2$，$t_{ZT}=0.1$，$t_{RS}=3$，$t_{SS}=2$，$t_{CC}=1.5$，$t_{WI}=1.5$，进而模拟在不同网络入侵成功概率下，系统可用性概率 P_A、机密性概率 P_C 和完整性概率 P_I 之间的轨迹分布，如图 10 所示。

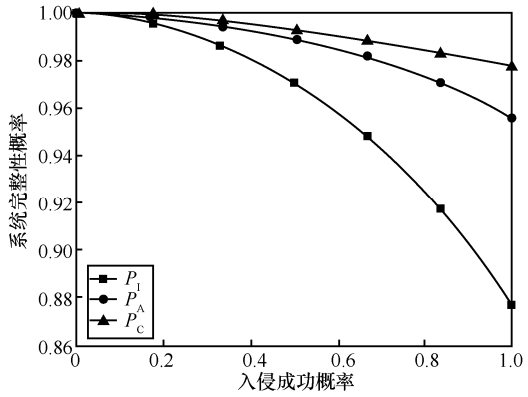


图 10　系统性能概率与入侵成功概率的关系

图 10 的数据表明容忍系统的可用性概率 P_A、机密性概率 P_C 和完整性概率 P_I 随着网络入侵成功概率的增加而明显降低。这主要是因为：入侵成功概率的增加表明入侵的隐蔽性增高，被发现的概率减小，对系统破坏的能力增强，容忍系统服务器被

破坏的数量增多，因此性能下降。图 10 还表明，系统性能概率在入侵成功概率为[0.4, 0.6]时比较好，可通过在给定时间周期 T 内对重点服务器加强入侵防护来提高系统总体的容忍能力。

7.4 模型对比

当系统遭受无法避免的入侵后，容忍能力是评判容忍系统优劣的重要指标。由于本文使用 ADT 来量化系统的容忍能力，ADT 越大，说明系统的带病工作时间越长，容忍能力越高。图 11 给出了本文模型与文献[5]模型在不同的入侵速度下，容忍系统 ADT 的分布轨迹。从图 11 可以看到，本文模型的容忍能力明显高于文献[5]。这是因为文献[5]中的系统在检测到入侵后，立即采取降级服务的安全策略，当入侵速度加快时，系统采用进程迁移策略，但是同时也消耗了计算机资源和时间，随着入侵速度不断增加，超过容忍系统承受能力之后，模型中没有给出解决办法，容忍能力不断下降。本文模型通过增加学习状态，系统遭受攻击后会不断学习修复自身，以提高自身容忍能力。

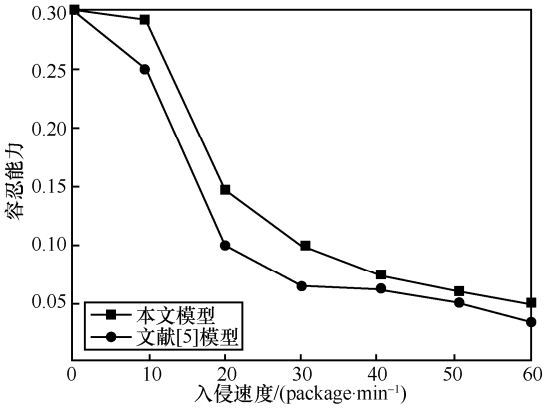


图 11 容忍能力对比

完整性是系统容忍能力的进一步提高的体现。本文分别利用魏柯等[15]建立的模型和本文模型进行试验。在不同攻击速度下，将 2 种模型的完整性进行对比，结果如图 12 所示。

随着攻击速度的增加，攻击成功率明显增加，导致 2 种模型的完整性整体上都呈下降趋势，但是本文模型完整性明显优于文献[15]的模型。这是因为文献[15]的模型在使用马尔可夫过程进行量化时，状态等级划分不够明确导致入侵检测准确率下降，且建模复杂，本文模型很好地克服了这一缺点。

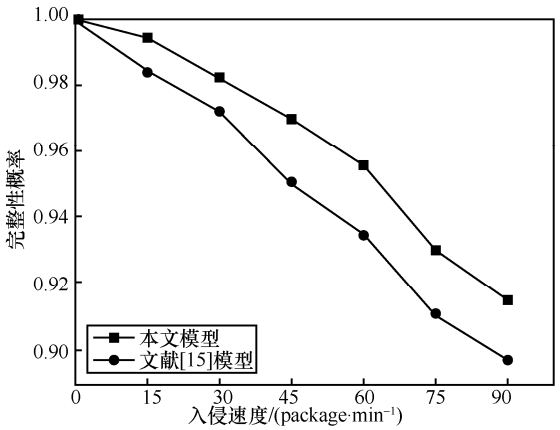


图 12 完整性对比

8 结束语

入侵容忍技术是网络安全管理的重要技术，它保障了系统在入侵发生后能够继续运行[16]。本文创建了优化的 SSTM，由于模型中不同状态之间转换符合有限自动机的原理，因此首先通过该原理对模型进行初步分析，进而使用马尔可夫理论进行定量，给出模型中各状态的转移概率。通过对该模型进行的分析，计算出系统中不同状态的概率值和各状态的访问次数，比较不同状态 ADT 分布情况，得出延长模型处于中间状态{NO,DO,RS}的时间可以增加入侵难度的结论。同时，本文还分析了入侵速度、入侵成功概率与系统容忍能力的对应关系，给出了提高系统容忍能力的方案。最后，本文从容忍能力和完整性 2 个方面和其他文献的入侵容忍模型进行对比，验证了 SSTM 的优越性。下一步将研究在模型中增加联机修复功能，达到提高系统在线入侵容忍能力的目的。

参考文献：

[1] JAJODIA S, ALBANESE M. An integrated framework for cyber situation awareness[M]//Theory and Models for Cyber Situation Awareness. Berlin: Springer, 2017:29-46.

[2] LUKTARHAN N, JIA X, HU L. Multi-stage attack detection algorithm based on hidden Markov model[C]//International Conference on Web Information Systems and Mining. Springer, 2012:275-282.

[3] 罗世亮,程良伦. 面向复杂工业环境的信息物理融合系统可靠性[J]. 北京理工大学学报. 2015, 35(9):973-979.
LUO S L, CHENG L L. Reliability research on cyber-physical systems for the complicated industrial environment[J]. Transactions of Beijing Institute of Technology, 2015, 35(9):973-979.

[4] 席荣荣,云晓春,张永铮.一种改进的网络安全态势量化评估方法[J]. 计算机学报,2015, 38(4):749-758.
XI R R, YUN X C, ZHANG Y Z. An improved quantitative evaluation method for network security[J].Chinese Journal of Computers, 2015,

38(4):749-758.

[5] 邢云菲,栾春玉. 一种改进的对入侵容忍系统的容忍度量化分析[J]. 情报科学, 2015,33(8):55-58,78.
XING Y F, LUAN C Y. A quantitative analysis and detection of intrusion tolerance system model[J]. Information Science, 2015, 33(8): 55-58, 78.

[6] 刘进．基于高分子链的入侵容忍系统病毒吸附算法[J]．科技通报,2014(10): 103-105.
LIU J. Virus adsorption optimization algorithm of intrusion tolerance system based on polymer chain[J]. Bulletin of Science and Technology, 2014(10):103-105.

[7] 徐晓斌,张光卫,王尚广. 基于群体信任的 WSN 异常数据过滤方法[J]. 通信学报, 2014, 35(5): 108-117.
XU X B, ZHANG G W, WANG S G. Abnormal date filtering approach based on collective trust for WSN[J]. Journal on Communications, 2014, 35(5): 108-117.

[8] 孙蔚．基于网管系统的分布式入侵检测模型研究[J]. 电子设计工程, 2014, 22(1): 165-167.
SUN W. Research of distributed intrusion detection based on network management system[J]. Electronic Design Engineering, 2014, 22(1): 165-167.

[9] DIVYA T, MUNIASAMY K. Real-time intrusion prediction using hidden Markov model with genetic algorithm[M]//Artificial intelligence and evolutionary algorithms in engineering systems. Berlin: Springer, 2015: 731-736.

[10] KHOLIDY H A, ERRADI A, ABDELWAHED S, et al. A finite state hidden markov model for predicting multistage attacks in cloud systems[C]// IEEE 12th International Conference on Dependable, Autonomic and Secure Computing. IEEE, 2014: 14-19.

[11] HOLGADOP , VILLAGRA V A , VAZQUEZ L . Real-time multistep attack prediction based on Hidden Markov models[J].IEEE Transactions on Dependable & Secure Computing, 2017, PP(99):1.

[12] AHMADIAN R A, RASOOLZADEGAN A, JAVAN J A. A systematic review on intrusion detection based on the hidden Markov model[J]. Statistical Analysis and Data Mining: The ASA Data Science Journal, 2018, 11(3): 111-134.

[13] 王笑,戚湧,李千目. 基于时变加权马尔可夫链的网络异常检测模型[J]. 计算机科学,2017,44(9):136-14.
WANG X, QI Y, LI Q M. Network anomaly detection model based on time-varying weighted Markov chain[J]. Computer Science, 2017, 44(9):136-14.

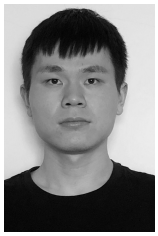
[14] TRIVEDI K S. Probability and statistics with reliability queuing , and computer science applications[M].2nd ed. New York: John Wiley and Sons, 2002.

[15] 魏柯, 张帆.基于马尔可夫的网络容忍入侵能力评估建模[J]. 计算机仿真, 2016, 33(7): 289-292.
WEI K, ZHANG F. Based on Markov network tolerate invasion ability evaluation model[J]. Computer Simulation, 2016, 33(7): 289-292.

[16] 罗智勇, 尤波, 刘嘉辉.基于半马尔可夫的入侵容忍状态转移系统研究[J]. 北京理工大学学报, 2016, 36(7): 712-717.
LUO Z Y, YOU B, LIU J H. Research of the intrusion tolerance state transition system based on semi-Markov[J]. Transactions of Beijing Institute of Technology, 2016, 36(7): 712-717.

[作者简介]

罗智勇（1978− ），男，山东平度人，博士，哈尔滨理工大学教授，主要研究方向为计算机网络与信息安全、网络优化。



杨旭（1995− ），男，安徽合肥人，哈尔滨理工大学硕士生，主要研究方向为计算机网络与信息安全、网络优化。

孙广路（1979− ），男，黑龙江哈尔滨人，博士，哈尔滨理工大学教授，主要研究方向为计算机网络与信息安全、机器学习与智能信息处理。

谢志强（1962− ），男，博士，黑龙江哈尔滨人，哈尔滨理工大学教授，主要研究方向为企业智能计算与调度系统、数据处理、网络优化。

刘嘉辉（1974− ），男，博士，黑龙江牡丹江人，哈尔滨理工大学教授，主要研究方向为计算机网络与信息安全、网络优化。