入侵容忍系统安全属性分析

殷丽华 方滨兴
(哈尔滨工业大学计算机网络与信息安全技术研究中心 哈尔滨 150001)

摘 要 首先提出一个优化的系统状态转移模型,用以描述具有自我演进能力的入侵容忍系统的动态行为,并提高了对攻击行为的描述能力,以该模型为基础,建立 SMP 模型并对系统安全属性及可执行性进行定量分析,进而计算出系统平均安全故障时间(MTTSF);最后给出数值分析结果,并通过计算模型中时间参数的敏感度,得出入侵容忍技术研究的关键点.

关键词 入侵容忍;安全属性;MTTSF;SMP 模型;可执行性
中图法分类号 TP309

Security Attributes Analysis for Intrusion Tolerant Systems

YIN Li-Hua FANG Bin-Xing
(*Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin* 150001)

Abstract It is significant to analyze security attributes of intrusion tolerant system while we research the effects of intrusion tolerance technologies. The paper puts forward an optimized states transition model to characterize dynamic actions of the intrusion tolerant systems with self-evolutional capability. The model improves the capability to describe attack actions and characterizes the modality of systems efficiently. The authors build a semi-Markov process based on the embedded Markov chain of the states transition model. Security attributes including availability and confidentiality and integrality are analyzed by computing steady states probability of Markov model. Associating a reward rate with every state of the model, performability of the system is also computed quantitatively. The mean time to security failure MTTSF is calculated afterwards by computing the visit counts and mean sojourn times of non-absorbing states in SMP model. Finally, numerical results are presented and sensitivity analysis of time parameters in the model is reckoned in order to reduce the key research points of intrusion tolerance technology.

Keywords intrusion tolerance; security attribute; mean time to security failure; semi-Markov process model; performability

1 引 言

网络的开放性使网络系统承受着潜在的巨大威胁[1],现有安全技术不能保护网络系统完全不受攻击,因此需要研究入侵容忍技术以保证系统在攻击存在的情况下能够持续不间断地提供关键服务.入侵容忍的概念最早由 Fraga 和 Powell[2] 在 1985 年提出,但直到近几年才随着 OASIS 和 MAFTIA 项目的研发得以迅猛发展.入侵容忍系统的目的是保证系统即使在发生故障的情况下能够正确运转,当系统由于故障原因不能工作时,应以一种无害的、非

收稿日期:2006-04-05;修改稿收到日期:2006-06-04.本课题得到国家十五预研项目基金(41315.7.3)资助.殷丽华,女,1973 年生,博士研究生,助理研究员,主要研究方向为计算机网络与信息安全.E-mail:yinlh@hit.edu.cn.方滨兴,男,1960 年生,教授,博士生导师,中国工程院院士,主要研究领域为计算机网络与信息安全、并行计算等.

灾难性的方式停止. 其和容错技术区别在于, 容错技术关注的是随机发生的自然故障; 而入侵容忍关注的是人为的恶意攻击, 具有智能性和不可控性.

入侵容忍是一种新的安全方法, 任何安全机制在被接受能为系统提供保护之前, 评估它的性能都非常必要. 对计算机系统进行评估分析的目的主要是为了选择、改进和设计, 对于入侵容忍系统而言, 分析其安全属性能够对未来设计的系统进行性能预测, 找出在入侵容忍系统中关键性能之所在, 增加或提高关键部件对入侵的抵抗和容忍能力, 以实现系统在开放网络环境下的不间断运行.

近年来, 定量的安全分析开始受到研究者们的重视. Jonsson 等人[3] 提出了一个基于攻击者行为的入侵过程的定量模型, 将攻击者行为分为不同阶段. Gong 等人[4] 根据攻击的影响而不是引发攻击的弱点构建了状态模型, 以描述入侵容忍系统的状态转换. Jha 和 Wing[5] 将状态机模型、形式逻辑以及贝叶斯分析方法应用在对系统可生存性的分析上. Ortalo 等人[6,7] 使用特权图对系统中已知弱点模型化得到攻击图, 应用马尔可夫技术对攻击图进行分析. Wang[8] 等人使用随机回报网 SRN 模型对入侵容忍系统进行了分析. Madan[9] 采用 SMP 对软件系统的安全性进行定量分析.

入侵容忍系统应具备自我演进增强的能力, 已有的状态转移模型不能描述系统的这种能力, 且对于攻击的描述能力较弱, 由此影响到模型分析结果的准确性. 本文提出了优化的系统状态转移模型, 能够描述系统的演进增强能力, 针对攻击手段的差异, 提高了对攻击行为的表述能力, 并以此为基础建立 SMP 模型, 对系统的不同安全属性进行了定量分析.

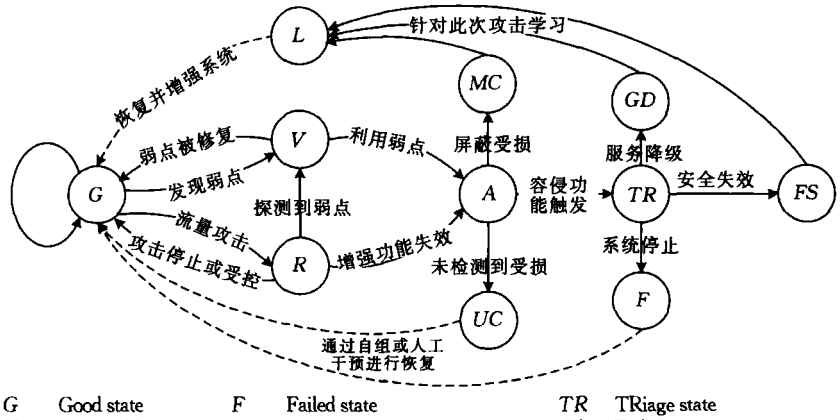
本文第 2 节介绍了优化的状态转移模型及系统 SMP 模型的建立; 第 3 节给出系统可用性及可执行性的分析; 第 4 节计算系统的平均安全故障时间 MTTSF; 第 5 节给出数值分析结果及模型中时间参数的敏感度分析; 第 6 节给出结论.

2 入侵容忍系统的 SMP 模型

一个入侵容忍系统必须具备识别入侵、自动配置以降低入侵的影响及自我演进增强的能力, 对其安全属性的分析, 除了要考虑攻击者的行为, 还必然要考虑系统对安全入侵的响应行为, 因此, 建立系统的安全模型时需要将这两种因素融合在一起.

2.1 通用状态转移模型

根据网络攻击手段的不同, 可将攻击分为两个大类: 基于流量的攻击和基于弱点的攻击. 针对这两类攻击方法, 入侵容忍系统采用完全不同的响应策略, 因此, 我们提出了优化的系统状态转移模型, 描述入侵容忍系统在不安全网络环境下的系统行为, 包括攻击引起的系统状态变化和系统采用不同策略应对攻击时各种可能的系统状态. 模型具有一般性, 能够描述和分析多种攻击行为, 如图 1 所示.



G	Good state	*F*	Failed state	*TR*	TRiage state
V	Vulnerable state	*L*	Learn state	*FS*	Fail-Secure state
R	Resist state	*UC*	Undetected Compromised state	*GD*	Graceful Degradation state
A	Active attack state	*MC*	Masked Compromised state		

图 1 入侵容忍系统状态转换模型

系统初始工作时处于 *G*(Good)状态, 当弱点被发现或攻击者获得系统权限, 系统处于易受攻击的 *V* 状态, 若弱点在攻击成功之前被检测到并进行修补, 则系统由 *V* 状态回到 *G* 状态; 若攻击成功则系统进入 *A*(Active attack)状态. 系统处于 *G* 状态时, 若受到流量攻击, 将转移到 *R*(Resistant)状态, 当攻

击从源头被遏制或在较大范围内被屏蔽，系统回到 G 状态；若攻击强度超过处理能力，系统转入 A 状态；若系统能够通过冗余等措施将入侵成功屏蔽，系统处于 MC(Masked) 状态. 若攻击未被检测到，系统将进入 UC(Undetected) 状态. 若检测到攻击将触发入侵容忍机制，系统进入 TR(Triage) 状态，评估入侵造成的损失并根据响应措施转移到不同的状态：安全停止状态 FS、降级服务状态 GD 或系统失效状态 F，需要人工干预将系统恢复到 G 状态. 当系统由 FS，GD 和 MC 状态回到 G 状态时，通过 L 状态的在线学习，识别此次攻击并进而阻止下一次可能的入侵，使系统处于 G 状态的时间延长.

从系统工作状态转换模型可知，系统在各状态之间的转移满足马尔可夫特性，即系统将要处于的状态只受当前所处状态影响，而与过去状态无关，因此可采用马尔可夫理论对整个系统进行分析. 为简化分析，将系统视为一个整体，并假定多个攻击不会同时存在.

2.2　SMP 模型的建立

为分析系统的安全属性，需要考虑攻击者的攻击行为. 对系统实施入侵，攻击者必然会付出相应代价，例如时间、技术及经济因素等. 通常可将攻击代价视为一个随机变量，此变量与攻击者经验及系统状态相关，可采用不同的随机分布概率模型. 为简化分析，将所有代价均视为时间代价.

将系统状态转移模型进一步抽象，得到嵌入离散时间马尔可夫链 DTMC，其状态空间 $X_s=\{G, R, V, A, MC, UC, TR, FS, GD, L, F\}$，DTMC 描述了各状态之间的转移概率，如图 2 所示.

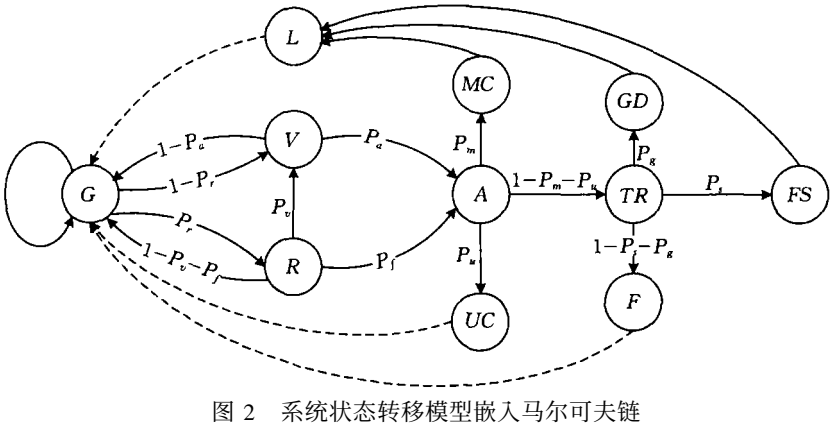


图 2　系统状态转移模型嵌入马尔可夫链

2.2.1　状态转移矩阵

转移概率矩阵 $\boldsymbol{P}$ 描述系统在各状态之间转移的可能性，其中概率值可由先验知识确定或通过入侵注入实验方式测定，本文不做具体研究. 下面分别说明各转移概率所表示的含义：

p_r：$G\to R$，系统遭受流量攻击的概率；

p_v：$R\to V$，系统对流量攻击抵抗失败的概率；

p_a：$V\to A$，系统在弱点状态攻击成功的概率；

p_f：$R\to A$，系统在抵抗状态攻击成功的概率；

p_m：$A\to MC$，系统成功屏蔽攻击的概率；

p_u：$A\to UC$，攻击未被发现的概率；

p_g：$TR\to GD$，系统降级服务的概率；

p_s：$TR\to FS$，系统主动安全关闭的概率；

$p_1=1-p_r$：$G\to V$，系统弱点被发现的概率；

$p_2=1-p_a$：$V\to G$，在入侵成功前系统检测到并排除弱点的概率；

$p_3=1-p_f-p_v$：$R\to G$，系统成功抵挡流量攻击的概率；

$p_4=1-p_m-p_u$：$A\to TR$，系统检测到攻击从而触发容侵机制的概率；

$p_5=1-p_g-p_s$：$TR\to F$，系统最终故障停止的概率.

$$\boldsymbol{P}=\begin{array}{c} \\ G \\ V \\ R \\ A \\ TR \\ MC \\ UC \\ GD \\ FS \\ F \\ L \end{array}\begin{array}{c}\begin{array}{ccccccccccc} G & V & R & A & TR & MC & UC & GD & FS & F & L \end{array}\\ \begin{bmatrix} 0 & p_1 & p_r & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_2 & 0 & 0 & p_a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_3 & p_v & 0 & p_f & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_4 & p_m & p_u & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_g & p_s & p_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}\end{array}.$$

2.2.2　状态保持时间

SMP 模型的另一组参数是各状态的保持时间，

用 h_i 表示系统在状态 i 的保持时间, $i\in\{G, R, V, A, MC, UC, TR, FS, GD, L, F\}$. 由于网络攻击的不可控性, SMP 模型各状态的保持时间分布函数是非指数的, 实际上, h_i 与具体攻击行为以及攻击者技术水平相关联, 随机性较大, 故在分析中采用平均保持时间, 不同于实际的保持时间分布. 下面给出各状态保持时间的含义:

h_G 为系统未遭受 DoS 攻击及弱点未被探测到的时间; h_V 为系统在弱点被探测到而攻击尚未成功期间所费的时间; h_R 为系统抵抗流量攻击并能够提供服务的时间; h_A 为系统检测到攻击行为并开启触发行为所费的时间; h_{TR} 为系统评估采用何种策略处理攻击所费的时间; h_{MC} 为系统在攻击存在并被屏蔽状态的运行时间; h_{UC} 为系统在攻击未被发现并造成破坏状态的运行时间; h_{GD} 为系统发现攻击存在并采取降级处理时的运行时间; h_L 为系统学习本次攻击行为所用的时间; h_{FS}: 系统在安全失败状态的时间; h_F 为系统处在完全失败状态的时间.

3 模型分析

基于 SMP 模型分析的核心思想是先计算稳态概率, 即系统在稳定工作状态下各状态的分布概率, 系统稳态时处于好状态的概率之和作为系统安全性的量化描述. 系统处于好状态的概率越大, 系统就越安全, 例如一个提供 www 服务的入侵容忍系统, 系统处于 F 或 FS 状态时无法提供服务, 处于 UC 状态时提供的服务不可靠, 因此 $\{F, FS, UC\}$ 三个状态为不安全状态, 此时系统的可用性 $Avail=1-\pi_F-\pi_{FS}-\pi_{UC}$, 由于 FS 状态是安全停止, 故系统的机密性 $Con=1-\pi_F-\pi_{UC}$. 同理可计算出其它安全属性值.

模型参数的估计对分析结果非常必要, 由于本文主要讨论宏观分析方法以获得研究入侵容忍技术的关键点, 因此, 参数估计在此不做讨论, 而在结果分析时讨论不同参数对模型结果的敏感度.

3.1 SMP 稳态概率

为计算模型的可用性, 首先需要计算 SMP 各状态的稳态概率, 用 π_i 表示系统稳态时处于状态 i 的概率, $i\in X_s$, $\sum\pi_i=1$. π_i 的计算方法如下[10]:

$$\pi_i=\frac{v_i h_i}{\sum_i v_j h_j},\quad i, j\in X_s \tag{1}$$

其中 v_i 为 DTMC 的稳态概率, h_i 为状态 i 的平均保持时间. v_i 满足如下关系: $\vec{v}=\vec{v}\cdot\boldsymbol{P}$, 其中 $\vec{v}=[v_G, v_V, v_R, v_A, v_{TR}, v_{MC}, v_{UC}, v_{GD}, v_{FS}, v_F, v_L]$, $\sum v_i=1$, $i\in X_s$, $\boldsymbol{P}$ 为 DTMC 状态转移概率矩阵.

状态平均保持时间 h_i 是计算 π_i 的另一要素, 很明显 h_i 由模型在该状态所有的随机时间决定, 而这些时间又是由攻击者的能力、技术水平及系统所采用的技术手段等决定, 因此采用平均状态保持时间以简化模型分析, 令 $\{h_G, h_V, h_R, h_A, h_{MC}, h_{UC}, h_{TR}, h_{GD}, h_{FS}, h_F, h_L\}$ 分别为状态 $\{G, V, R, A, MC, UC, TR, GD, FS, F, L\}$ 的平均保持时间. 令 H 为系统在全部状态的保持时间, 根据式(1)计算各稳态概率 π_i 如下:

$$\begin{aligned}
H&=h_G+p_r h_R+((1-p_r)+p_r p_v)h_V+\\
&((p_r p_v+(1-p_r))p_a+p_r p_f)(h_A+p_m(h_{MC}+h_L)+\\
&p_u h_{UC}+(1-p_m-p_u)(h_{TR}+p_s(h_{FS}+h_L)+\\
&p_g(h_{GD}+h_L)+(1-p_g-p_s)h_F)),\\
\pi_G&=h_G/H,\\
\pi_R&=p_r\cdot h_R/H,\\
\pi_V&=(p_r p_v+(1-p_r))\cdot h_V/H,\\
\pi_A&=((p_r p_v+(1-p_r))p_a+p_r p_f)\cdot h_A/H,\\
\pi_{MC}&=((p_r p_v+(1-p_r))p_a+p_r p_f)p_m\cdot h_{MC}/H,\\
\pi_{UC}&=((p_r p_v+(1-p_r))p_a+p_r p_f)p_u\cdot h_{UC}/H,\\
\pi_{TR}&=((p_r p_v+(1-p_r))p_a+p_r p_f)\cdot\\
&\quad(1-p_m-p_u)\cdot h_{TR}/H,\\
\pi_{GD}&=((p_r p_v+(1-p_r))p_a+p_r p_f)\cdot\\
&\quad(1-p_m-p_u)p_g\cdot h_{GD}/H,\\
\pi_{FS}&=((p_r p_v+(1-p_r))p_a+p_r p_f)\cdot\\
&\quad(1-p_m-p_u)p_s\cdot h_{FS}/H,\\
\pi_F&=((p_r p_v+(1-p_r))p_a+p_r p_f)\cdot\\
&\quad(1-p_m-p_u)(1-p_s-p_g)\cdot h_F/H,\\
\pi_L&=((p_r p_v+(1-p_r))p_a+p_r p_f)\cdot\\
&\quad(p_m+(1-p_m-p_u)(p_s+p_g))\cdot h_L/H.
\end{aligned}$$

3.2 安全属性分析

状态转移模型中包括两种状态, 分别描述攻击行为和系统遭受攻击后的响应行为, $\{G, V, A\}$ 三种状态为攻击不同阶段系统所处状态, 亦即描述攻击者的行为变化; $\{R, UC, MC, TR, FS, GD, F, L\}$ 八种状态为系统采取某一策略后所处状态, 即描述系统的响应行为. 在系统响应状态中某些状态表明特定安全属性受损, 用集合 X_f 表示受损状态集合, X_n 表示未受损状态集合.

计算系统可用性时, 系统在 F, FS, UC 三个状态下不能提供服务, 此时 $X_f=\{UC, FS, F\}$, 系统可

用性为 $Avail=1-\pi_F-\pi_{FS}-\pi_{UC}$. 计算机密性属性时, FS 状态为安全保护状态, 系统在 UC 和 F 状态下数据可能被窃取, 则 $X_f=\{UC, F\}$, 系统机密性为 $Conf=1-\pi_F-\pi_{UC}$. 对完整性属性来说, UC, FS 和 F 状态下的数据完整性都有可能遭到破坏, 因此 $X_f=\{UC, FS, F\}$, $Integ=1-\pi_{UC}-\pi_{FS}-\pi_F$.

上述安全属性的计算为通常状况, 对于不同的攻击, 具体的计算会有所变化, 例如若系统遭受流量 DoS 攻击, $X_n=\{G, R, A, TR, GD\}$, 系统可用性为 $Avail=\pi_G+\pi_R+\pi_A+\pi_{TR}+\pi_{GD}$.

综上, 安全属性的计算公式为

$$Avail/Integ/Conf=\sum_{i\in X_n}\pi_i=1-\sum_{i\in X_f}\pi_i \quad (2)$$

从式(2)可知, 若增大系统安全属性, 可通过增大未受损状态的稳态概率 π_i 来实现, 其中 $i\in X_n$, 从 π_i 计算公式可知, 若增大 π_i, 可通过增大 h_i 来实现.

3.3　可执行性分析

可执行性是指系统连续工作的能力, 单纯的可用性指标不能评价系统在不同状态下执行能力的不同, 可执行性指标用来评价高可靠系统在故障存在时能够继续执行任务的能力. 为系统状态转移图中每一状态增加回报率参数, 反映系统在该状态时的性能级别, 例如, 当系统处于状态 G 时, 具有最佳性能, 则 G 状态对应回报率最大; 系统在 FS 和 F 状态已经停止服务, 则其回报率为 0; 其它状态下, 系统具备不同程度的性能降低, 因此其回报率亦不相同.

令 r_i 为状态 i 的回报率, 表示系统在状态 i 单位时间内所获回报值, π_i 表示状态 i 的稳态概率, $Z=[r_i]^{-1}=[r_G, r_V, r_R, r_{MC}, r_{GD}, r_A, r_{TR}, r_L, r_{UC}, r_{FS}, r_F]^{-1}$ 为系统回报率, 其中 $i\in X_s$, 则模型稳态回报率[10]为 $E[Z]=\sum_{i\in X_s}r_i\pi_i$, 称之为计算可用性.

设 $X(t)$ 为系统状态转移函数, $Z(t)$ 为系统回报率函数, 令 $Y(t)$ 为系统在区间 $[0, t)$ 内的累积回报值, 亦即系统在 $[0, t)$ 时刻内完成任务总量, $Y(t)=\int_0^t Z(\tau)\mathrm{d}\tau$. 通过计算 $Y(t)$, 获得系统随时间变化的累积回报以及系统在不同状态的保持时间对整体性能的影响情况.

4　平均安全故障时间(MTTSF)分析

作为系统可靠性的评价指标, 平均故障时间(MTTF)表示系统从某工作状态开始运行直到最终到达某故障状态的平均时间. 与之类似, 在安全分析中采用平均安全故障时间(MTTSF)作为评价入侵容忍系统从 G 状态开始直到到达故障状态的平均时间. 从攻击者的角度来说, 即从攻击开始到最终系统不能正常工作为止, 所需花费的时间代价. MTTSF 越大, 表明入侵容忍系统对攻击的抵抗容忍能力越强, 或者说系统的安全可靠性越高.

修改 SMP 嵌入链 DTMC, 将其中的失败状态和安全受损状态归为吸收状态, 去掉由吸收状态引出的弧, 也就是说吸收状态只有入弧, 没有出弧, 其余状态归为瞬时状态. 这样模型中所有状态被归为两大类: 吸收状态集 X_a 和瞬时状态集 X_t.

X_a 和 X_t 随攻击的不同而有所变化, 如图 2 所示 DTMC 中, 有 $X_t=\{G, R, V, A, MC, TR, FS, GD\}$, $X_a=\{UC, F, L\}$. 将系统状态重新划分归类后, 对系统状态转移矩阵进行调整, 可写成如图 3 的形式:

$$\boldsymbol{P}=\left[\begin{array}{c|c}\boldsymbol{Q} & \boldsymbol{C}\\ \hline \boldsymbol{0} & \boldsymbol{I}\end{array}\right]$$

图 3　变换后矩阵

图 3 中, $\boldsymbol{Q}$ 表示瞬时状态之间的转移概率, $\boldsymbol{C}$ 表示瞬时状态到吸收状态的转移概率, $\boldsymbol{I}$ 表示单位阵, 即吸收状态到它自身的转移概率为 1. 采用 Trivedi[10] 提出的方法, 得到 MTTSF 的计算公式如下:

$$MTTSF=\sum_i V_i h_i,\quad i\in X_t \quad (3)$$

其中 V_i 表示在 DTMC 中进入吸收状态前经过状态 i 的次数, h_i 表示在状态 i 的平均保持时间, V_i 可由式(2)计算得到.

$$V_i=q_i+\sum V_j Q_{ji},\quad i, j\in X_t \quad (4)$$

式中 q_i 表示系统从状态 i 开始的可能性, 令 $q=[q_i]=[1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$, 表明系统从状态 G 开始运行.

若攻击者入侵成功, 系统最终将到达某一吸收状态从而不可用, 图 2 所示 DTMC 中吸收状态集合 $X_a=\{UC, F, L\}$, 令 b_{ij} 表示系统由状态 $i\in X_t$ 开始最后进入状态 $j\in X_a$ 的概率, 则 SMP 的吸收状态概率矩阵[11] 表示为

$$\boldsymbol{B}=[b_{ij}]=(\boldsymbol{I}-\boldsymbol{Q})^{-1}\boldsymbol{C}$$

当 $i=1$ 时即系统从 G 状态开始运行到各吸收状态的转移概率可由下述公式计算得出

$$b_{1j}=\sum V_i C_{ij},\quad i\in X_t,\ j\in X_a \quad (5)$$

按照式(3)~(5)可分别得出 V_i, $MTTSF$ 和 b_{1j} 的计算公式下:

$$V_G=1/(1-p_a((1-p_r)+p_r p_v)-p_r p_f),$$

$$V_V=((1-p_r)+p_rp_v)\cdot V_G,$$
$$V_R=p_r\cdot V_G,$$
$$V_A=(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot V_G,$$
$$V_{TR}=(1-p_m-p_u)(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot V_G,$$
$$V_{MC}=p_m(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot V_G,$$
$$V_{GD}=p_g(1-p_m-p_u)(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot V_G,$$
$$V_{FS}=p_s(1-p_m-p_u)(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot VG,$$
$$MTTSF=\sum_i V_ih_i,\quad i\in X_t,$$
$$b_{1UC}=p_u(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot V_G,$$
$$b_{1F}=(1-p_s-p_g)(1-p_m-p_u)(p_a((1-p_r)+p_rp_v)+p_rp_f)\cdot V_G,$$
$$b_{1L}=V_{GD}+V_{MC}+V_{FS}.$$

MTTSF 表明系统的安全可靠性,增大 *MTTSF*,也就增加了攻击成功需要付出的代价,可通过增大 V_i 或 h_i 来实现,对于确定的系统,各状态的 V_i 基本固定,因此可增大 V_i 较大状态的保持时间 h_i 以达到增大 *MTTSF* 的目的.

5 数值分析结果

在分析了系统安全性、可执行性和 *MTTSF* 后,给出一个具体数值评估结果的实例. 由于模型参数的实际取值需通过实验观测分析得到,因此采用估计的参数值,所用参数值如下:

状态转移概率. 假定系统遭受流量攻击进入状态 *R* 的概率为 $p_r=0.4$,系统弱点被探测进入 *V* 状态的概率为 $1-p_r=0.6$,流量攻击中探测到弱点的概率为 $p_v=0.1$,攻击成功的概率为 $p_a=0.4$,流量攻击容忍失效的概率为 $p_f=0.2$,攻击发生后系统成功屏蔽攻击的概率为 $p_m=0.3$,系统未发现攻击存在的概率为 $p_u=0.2$,攻击被发现并触发入侵容忍机制的概率为 $1-p_m-p_u=0.5$,从 *TR* 状态系统进入 *GD* 和 *FS* 的概率分别为 $p_g=0.6$ 和 $p_s=0.3$,系统无法处理攻击从而报警停止的概率为 $1-p_g-p_s=0.1$.

平均保持时间. 由经验可知,系统工作在 *G* 状态的时间相对较长,而针对流量攻击的容忍机制使得系统在遭受流量攻击时更多的工作在 *R* 状态而不是进入 *A* 状态,分别设 $h_G=1$, $h_V=1/3$, $h_R=1.5$;当系统发现入侵后分别转移到 *MC*, *UC* 和 *TR* 状态, *MC* 状态通过学习转至 *G*, *UC* 状态下需要人工干预转至 *G*,令 $h_A=0.5$, $h_{MC}=0.5$, $h_{UC}=1$, $h_L=0.4$; *TR* 状态根据入侵容忍策略判定系统的转移方向,因此设 $h_{TR}=1/6$, $h_{GD}=3$, $h_{FS}=1$, $h_F=2$. 需注意的是,所有 h_i 的度量均为时间单位(time units).

回报率. 根据系统的任务执行能力设置各状态的回报率, *G* 和 *V* 状态下系统工作不受影响,具有最大的回报率,设 $r_G=r_V=1$; *R* 和 *MC*, *GD* 状态系统执行能力有所降低,设 $r_R=r_{MC}=0.8$, $r_{GD}=0.6$; *A* 和 *UC* 状态下可能存在不确定因素,因此设 $r_A=0.3$, $r_{UC}=0.2$; *TR* 和 *L* 状态时系统对入侵行为进行相应处理,任务执行能力较低,令 $r_{TR}=r_L=0.1$;而在 *FS* 和 *F* 状态系统停止工作,因此令 $r_{FS}=r_F=0$.

(1) DTMC 稳态概率:

$v_G=0.2928$, $v_R=0.1464$, $v_V=0.1611$,
$v_A=0.123$, $v_{MC}=0.0369$, $v_{UC}=0.0246$,
$v_{TR}=0.0615$, $v_{FS}=0.0184$, $v_{GD}=0.037$,
$v_F=0.0061$, $v_L=0.0922$.

(2) SMP 稳态概率:

$\pi_G=0.3408$, $\pi_R=0.2556$, $\pi_V=0.0625$,
$\pi_A=0.0716$, $\pi_{MC}=0.0215$, $\pi_{UC}=0.0286$,
$\pi_{TR}=0.0119$, $\pi_{FS}=0.0215$, $\pi_{GD}=0.1288$,
$\pi_F=0.0143$, $\pi_L=0.0429$.

(3) DTMC 中到达吸收状态前状态被访问的平均次数:

$V_G=1.7241$, $V_R=0.8621$, $V_V=0.9483$,
$V_A=0.7241$, $V_{MC}=0.2172$, $V_{TR}=0.3621$,
$V_{FS}=0.1086$, $V_{GD}=0.2172$.

设状态 *FS*、*UC* 和 *F* 为系统不可用状态,则 DTMC 的稳态可用性为 $Avail=0.9509$, SMP 的稳态可用性为 $Avail=0.9356$,稳态回报率 $E(Z)=0.7349$,设 *UC*、*F* 和 *L* 状态为吸收状态,则平均安全故障时间 $MTTSF=4.6247$,吸收概率分别为 $b_{1F}=0.0362$, $b_{1UC}=0.1448$, $b_{1L}=0.5431$.

(4) 参数敏感度分析

敏感度分析通常用于评估参数对模型结果的影响能力,以指出模型中的重要参数并进而指导数据收集、最佳运行点及合理分配资源等. 改变输入参数 α 为 $\alpha+\Delta\alpha$,获得模型结果的变化值 ΔM,令 $\Delta\alpha/\alpha$ 表示 α 变化的百分比,则函数 *F* 中参数 α 的半相对敏感度计算公式[12]为 $S_\alpha=\alpha_0|\partial F/\partial\alpha|$. 表 1 列出了不同安全属性的参数敏感度.

表 1　参数敏感度

	MTTSF	可用性	可执行性
S_{h_G}	1.7241	0.2209	0.2431
S_{h_R}	1.2931	0.1879	0.1981
S_{h_V}	0.3161	0.0584	0.0775
S_{h_A}	0.3621	0.0662	0.0283
$S_{h_{GD}}$	0.6517	0.1115	0.0936
$S_{h_{MC}}$	0.1086	0.021	0.0228
$S_{h_{TR}}$	0.0603	0.0118	0.0016
$S_{h_{UC}}$		0.0278	0.0077
S_{h_F}	0.1086	0.0141	0.0
$S_{h_{FS}}$		0.021	0.0
S_{h_L}		0.041	0.0058

对于模型的 *MTTSF*、可用性和可执行性，各状态保持时间对其结果影响力大小按降序排列分别为{h_G, h_R, h_{GD}, h_A, h_V, (h_{MC}, h_F), h_{TR}}，{h_G, h_R, h_{GD}, h_A, h_V, h_L, h_{UC}, (h_{MC}, h_{FS}), h_F, h_{TR}}和{h_G, h_R, h_{GD}, h_V, h_A, h_{MC}, h_{UC}, h_L, h_{TR}}，若增大{*G*, *R*, *V*, *GD*}状态的保持时间，系统的可用性、*MTTSF* 和可执行性都有较大程度的提高.

(5) 累积回报值 $Y(t)$

设状态转移序列为{*G*, *R*, *G*, *V*, *G*, *V*, *A*, *TR*, *GD*, *L*, *G*, *V*, *A*, *MC*, *L*, *G*, *R*, *A*, *TR*, *F* }，此序列模拟系统的实际执行状态，状态保持时间序列为{2.5, 6, 5, 1, 2, 1, 1, 0.5, 5, 0.5, 5, 1.5, 0.5, 0.5, 0.5, 0.5, 5, 7.5, 0.5, 0.5, 5, 0}，所得 $Y(t)$ 值记为 *Y*0，在此时间序列基础上，增加各状态保持时间，得 $Y(t)$ 值如图 4 所示，图中 A_y, B_y, C_y, D_y 分别表示增加 1/2, 1, 3/2, 2 倍时间系统的累积回报值.

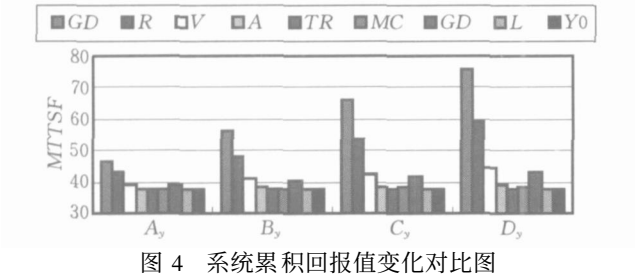


图 4　系统累积回报值变化对比图

由图 4 可知，在同比例增大保持时间的情况下，对累积回报值影响能力强弱的顺序为{*G*, *R*, *V*, *GD*, *A*, *MC*, *TR*, *L*}，可以看出，增加{*G*, *R*, *V*, *GD*}状态的保持时间，可以获得更大的累积回报，亦即提高系统整体的执行能力. 而这些状态也具备较高的回报率，其保持时间的增加，使系统服务质量得以提高，因此具备更好的可执行性能.

6　结　论

已有的网络安全技术不能防范所有入侵，因此需要研究入侵容忍技术. 本文首先提出一个优化的系统状态转移模型，用以描述具有自我演进能力的入侵容忍系统的动态行为. 由于系统状态转移满足马尔可夫特性，故采用 SMP 模型对系统安全属性进行分析，进而计算出平均安全故障时间，系统在不同的工作状态其性能也有差异，将每一状态赋予回报率，系统回报率表示系统的可执行性，累积回报率则表明系统在一段时间内完成任务总量.

最后给出数值分析结果，并通过计算模型中时间参数的敏感度，得出入侵容忍技术研究的关键点. 对于从 *G* 状态开始运行的入侵容忍系统，增大{*G*, *R*, *GD*, *V*}状态的平均保持时间，将在较大范围内提高系统的安全特性及性能，而 *L* 状态能够对遭受的攻击进行学习反馈，从而增强系统. 因此，下一步将研究入侵容忍技术及攻击在线学习，以提高上述状态的保持时间.

参　考　文　献

1 Allen J., Christie A., Fithen W. *et al*. State of the practice of intrusion detection technologies. Carnegie Mellon, SEI, Technical Report: CMU/SEI-99-TR-028, 2000

2 Fraga J. S., Powell D.. A fault- and intrusion-tolerant file system. In: Proceedings of the 3rd International Conference on Computer Security, Dublin, Ireland, 1985, 203~218

3 Jonsson E., Olovsson T.. A quantitative model of the security intrusion process based on attacker behavior. IEEE Transactions on Software Engineering, 1997, 23(4): 235~245

4 Gong F., Goseva-Popstojanova K., Wang F., Wang R., Vaidyanathan K., Trivedi K., Muthusamy B.. Characterizing intrusion tolerant systems using a state transition model. In: Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX Ⅱ), 2001, 2: 211~221

5 Jha S., Wing J. M.. Survivability analysis of networked systems. In: Proceedings of the 23rd International Conference on Software Engineering, Toronto, Canada, 2001, 307~317

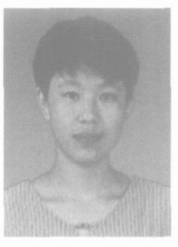
6 Ortalo R., Deswarte Y., Kaaniche M.. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 1999, 25(5): 633~650

7 Sheyner O., Haines J., Jha S., Lippmann R., Wing J. M.. Automated generation and analysis of attack graphs. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, USA, 2002, 273~284

8 Wang D. Z., Madan B. B., Trivedi K. S.. Modeling SITAR system security. In: Proceedings of the 14th IEEE International Symposium on Software Reliability Engineering, 2003, Denver, USA, C-2 Fast Abstracts

9 Madan B. B., Goseva-Popstojanova K., Vaidyanathan K., Trivedi K. S.. A method for modeling and quantifying the se

curity attributes of intrusion tolerant systems. Performance Evaluation, 2004, 56(1~4): 167~186
10 Trivedi K.S.. Probability and Statistics with Reliability, Queuing, and Computer Science Applications. 2nd Edition. New York: John Wiley & Sons, 2002
11 Medhi J.. Stochastic Processes. New Delhi: Wiley Eastern, 1994
12 Karnavas W.J., Sanchez P., Bahill A.T.. Sensitivity analyses of continuous and discrete systems in the time and frequency domains. IEEE Transactions on Systems, Man and Cybernetics, 1993, 23(2): 488~501



YIN Li Hua, born in 1973, Ph. D. candidate, assistant professor. Her major research interests include computer network and information security technology.

FANG Bin Xing, born in 1960, professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His research interests include network and information security, parallel computing etc.

Background

Intrusion tolerance is the last line of defense in depth network security framework and a hot topic in computer network security in recent years. Intrusion tolerance technologies guarantee the critical missions of information systems keep running while the systems suffer the successful intrusions or attacks. It is significant that to research the description model of intrusion tolerance systems and to analyze security attributes of the systems. They can point the development direction of intrusion tolerance technologies. Presently, the security attributes analysis of intrusion tolerance systems is in the phase of exploration and some of researchers who are engaged in this field have achieved available results.

This subject is supported by Defense Pre Research Project of the 'Tenth Five Year Plan' of China whose name is "Security Attributes Analysis Technologies" and grant number is No. 41315.7.1. The project focuses on research and development of network security analysis. The team has made a lot of progress in the area of network security analysis and published nearly 20 papers in international and domestic journals or conference proceedings. Some analysis methods are proposed and Markov theory has been used to analyze the attack graph generated from the real network. An optimized states transition model is put forward to characterize intrusion tolerant systems with self evolutional capability. This paper builds a semi Markov process based on the model and analyzes security attributes of intrusion systems quantitatively. That is one of security analysis methods in the whole research project and directs the key points of intrusion tolerance technology research.