基于博弈论的入侵容忍系统安全性分析模型

周 华* 周海军 马建锋
(西安通信学院 西安 710106)

摘 要：入侵容忍是一种新的网络安全方法，在其被接受能为系统提供保护之前，分析和评估它的安全性能是非常重要的。该文提出基于博弈论的入侵容忍系统安全性分析模型，将网络攻击和入侵容忍之间的过程抽象为一个 2 人零和随机博弈。通过对博弈双方的最优行动策略和预期收益的研究，从安全属性平均失效时间的角度分析了入侵容忍系统的可用性、机密性和完整性，同时对影响攻击者选择行动策略的因素进行了分析，得出了攻击意愿、行动收益和行动策略之间的相互关系。研究结果揭示了入侵容忍系统与攻击者之间的内在联系，为更好地防御网络攻击和入侵提供了决策依据。

关键词：网络安全；入侵容忍；博弈论；随机博弈；安全属性；平均失效时间
中图分类号：TP309.2 **文献标识码**： A **文章编号**：1009-5896(2013)08-1933-07
DOI：10.3724/SP.J.1146.2012.01081

Security Analysis Model of Intrusion Tolerant Systems Based on Game Theory

Zhou Hua Zhou Hai-jun Ma Jian-feng
(*Xi'an Communications Institute*, *Xi'an* 710106, *China*)

Abstract: Intrusion tolerance is a new mechanism used to build secure computer networks. Therefore, it's very important to analyze and evaluate the security performance of intrusion tolerant networks before intrusion tolerance is absolutely adopted. Thus, a security analysis model of intrusion tolerant systems based on game theory is proposed in this paper. According to the analysis model, the processes between attacking and tolerating intrusions are considered as a two-player zero-sum stochastic game, in which the optimal action strategies and expected payoffs of the two parties are studied. By using the study results, this paper analyzes the availability, confidentiality and integrality of intrusion-tolerance systems from the perspective of mean time to failure. Meanwhile, it analyzes the factors that will affect the attackers' choices about action strategies, and obtains the relationships between attack will, payoff and action strategy. The results present the underlying interconnections between intrusion tolerant systems and attackers, which will provide helpful references to withstand the network attacks and intrusions.

Key words: Network security; Intrusion tolerance; Game theory; Stochastic game; Security attribute; Mean time to failure

1 引言

入侵容忍是一种新的安全技术，它的主要思想就是承认系统中存在可以被攻击者利用的脆弱点，并构建一种可以容忍一定数量故障(包括攻击或入侵)的系统。

近年来，入侵容忍系统安全性的定量评估分析受到了越来越多研究者的重视。文献[1]将入侵行为和系统容忍行为建模为一个随机过程，从系统的可用性、机密性和完整性等方面对入侵容忍系统进行了量化分析；文献[2]优化了入侵容忍系统状态转移模型，并根据该模型对系统安全性进行了定量分析；文献[3]利用随机行为网络模型对入侵容忍系统进行了定量分析；文献[4]根据网络系统的层次结构提出了基于威胁传播模型的网络安全评估方法。但是，上述文献侧重研究了网络系统自身的防御措施以及系统状态的变化，没有考虑到攻击手段与网络系统防御措施之间的相互影响。文献[5]利用随机博弈对攻击者和系统管理员的行为进行建模，求解出博弈者的最佳策略以及在此策略下网络系统的安全性；

2012-08-23 收到，2013-04-15 改回
陕西省自然科学基金(2011JQ8039)资助课题
*通信作者：周华 zhoumiaomiao_2005@126.com

文献[6]利用博弈论方法对系统综合的安全性和可靠性进行评估，分析了收益和攻击代价对攻击者期望行为的影响；文献[7]在云计算环境下提出了基于动态博弈的用户行为模型；文献[8]提出了基于博弈论的信息安全技术评价模型，并重点对入侵检测系统进行了综合分析和评价。

本文根据网络攻击(入侵)行为与入侵容忍系统之间的交互过程建立一个 2 人零和随机博弈模型，研究博弈双方所采取的行动策略，求解出该模型下双方的最优行动策略和预期收益，以此为基础分析入侵容忍系统的安全属性和影响攻击者行为的因素。

2 博弈模型描述

在攻击者和入侵容忍系统的博弈过程中，攻击者通过各种手段试图获取自己所需的信息资源或对系统造成直接的破坏，而入侵容忍系统则采取相应的容忍策略试图最大程度地减小攻击行为带来的损害。因此，在博弈过程中，入侵容忍系统所预期的结果以及采取的入侵容忍策略不仅取决于自身，还取决于攻击者的行为[9]。所以，研究入侵容忍系统在面临攻击行为情况下的安全性问题就可以采用博弈论方法。

由于攻击者和入侵容忍系统的博弈是一个非合作博弈过程，且各自行为存在完全的互斥性，因此该博弈是一个零和博弈，也不存在纯策略的纳什均衡，需要求解混合策略的纳什均衡[10]。博弈双方的收益使用统一的单位(比如金钱、时间等)。本文博弈模型中的要素具体描述如下：

(1)系统状态集合。入侵容忍系统可以用一组有限状态集合来表示，即 $S=\{s_1,\cdots,s_i\}$。

(2)攻击者在系统状态 s_i 时的攻击行为集合：$A_i=\{a_1,\cdots,a_m\}$，$\phi\in A_i$ 表示攻击者不采取任何攻击行为。

(3)攻击者在系统状态 s_i 时攻击行为的概率分布：$\Pi_i=(\pi_i(a_1),\cdots,\pi_i(a_m))$，其中 $\pi_i(a_1)$ 表示攻击者选择攻击行为 a_1 的概率。

(4)在系统状态 s_i 时攻击行为收益集合为：$R_i=\{r_1,\cdots,r_m\}$。

(5)入侵容忍系统在系统状态 s_i 时防御措施集合：$D_i=\{d_1,\cdots,d_m\}$，$\phi\in D_i$ 表示入侵容忍系统不采取任何防御措施。

(6)入侵容忍系统在系统状态 s_i 时防御措施的概率分布：$\Theta_i=(\theta_i(d_1),\cdots,\theta_i(d_m))$，其中 $\theta_i(d_1)$ 表示入侵容忍系统采取防御措施 d_1 的概率。

(7)在系统状态 s_i 时入侵容忍系统实施防御措施的收益集合为：$L_i=\{l_1,\cdots,l_m\}$。

在系统状态 s_i 时，攻击者与入侵容忍系统的博弈过程称为一个博弈元素，用 $\boldsymbol{\Gamma}_i$ 表示，则博弈双方的收益矩阵如图 1 所示。

入侵者 \ 容侵系统	d_1	$\cdots$	d_m
a_1	r_{11}, l_{11}	$\cdots$	r_{1m}, l_{1m}
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_m	r_{m1}, l_{m1}	$\cdots$	r_{mm}, l_{mm}

图 1 博弈收益矩阵

其中 r_{kl} 表示攻击者采取 a_k，入侵容忍系统采取防御措施 d_l 时的收益；l_{kl} 表示入侵容忍系统遭受 a_k 攻击，并采取防御措施 d_l 时的收益，其中 $1\le k,l\le m$。由于博弈模型为 2 人零和博弈，所以有 $r_{kl}=-l_{kl}$。博弈元素 $\boldsymbol{\Gamma}_i$ 如式(1)所示：

$$\boldsymbol{\Gamma}_i=\begin{array}{c} \\ a_1 \\ \vdots \\ a_m \end{array}\begin{array}{c} \begin{array}{ccc} d_1 & \cdots & d_m \end{array} \\ \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1m} \\ \vdots & \ddots & \vdots \\ \gamma_{m1} & \cdots & \gamma_{mm} \end{bmatrix} \end{array} \tag{1}$$

其中 $\gamma_{kl}=r_{kl}+\sum_{\forall\boldsymbol{\Gamma}_j}P_{ij}(a_k,d_l)\boldsymbol{\Gamma}_j$，$0<P_{ij}(a_k,d_l)<1$ 表示攻击者采取 a_k，入侵容忍系统采取 d_l 时系统由状态 s_i 转移到 s_j 的概率。γ_{kl} 表示攻击者获取的后续收益。

攻击者预期获取的收益可以表示为

$$E(\Pi_i,\Theta_i)=\sum_{\forall a_k\in A_i}\sum_{\forall d_l\in D_i}\pi_i(a_k)\theta_i(d_l)\gamma_{kl}$$

入侵容忍系统预期的收益表示

$$E(\Theta_i,\Pi_i)=\sum_{\forall d_l\in D_i}\sum_{\forall a_k\in A_i}\theta_i(d_l)\pi_i(a_k)l_{kl}$$

攻击者的目标是最大化自身的收益，入侵容忍系统则需要最小化攻击者的收益，即 $\min\limits_{\Theta_i}\max\limits_{\Pi_i}E(\Pi_i,\Theta_i)$；同时，攻击者的目标还要最小化入侵容忍系统的收益，入侵容忍系统则需要最大化自身的收益，即 $\max\limits_{\Pi_i}\min\limits_{\Theta_i}E(\Theta_i,\Pi_i)$。因此，在系统状态 s_i 下，双方采取的最优策略达到纳什均衡，攻击者和入侵容忍系统的策略分别为 Π_i^* 和 Θ_i^*，则有 $E(\Pi_i^*,\Theta_i^*)=-E(\Theta_i^*,\Pi_i^*)$。

3　博弈模型分析

假定系统由 s_i，s_j，s_k，s_l，s_m 5 个状态组成，博弈状态和转移过程如图 2 所示。

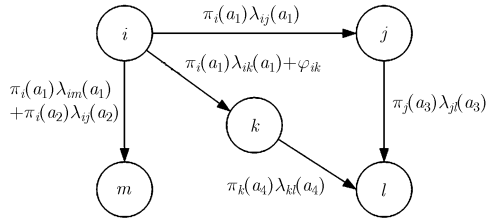


图 2 博弈状态与状态转移

其中 $\lambda_{ij}(a_1)$ 表示在单位时间内攻击者采取 a_1 成功使系统状态由 s_i 转移至 s_j 的次数，$\lambda_{ij}^{-1}(a_1)$ 则表示由 s_i 转移至 s_j 所需要的时间；φ_{ik} 表示单位时间内入侵容忍系统采取防御措施的次数。单位时间设定为 1 h。那么，系统状态由 s_i 转移至 s_j 的概率为

$$P_{ij}=\frac{\lambda_{ij}(a_1)}{\lambda_{ij}(a_1)+\lambda_{im}(a_1)+\lambda_{ik}(a_1)+\varphi_{ik}}$$

博弈元素 $\boldsymbol{\Gamma}_i$ 如式(2)所示：

$$\boldsymbol{\Gamma}_i=\begin{array}{c}\\ \phi \\ a_1\end{array}\begin{array}{c}\begin{array}{cc}\phi & d_1\end{array}\\ \begin{bmatrix}\Delta_i & \gamma_{12}\\ \gamma_{21} & \gamma_{22}\end{bmatrix}\end{array} \tag{2}$$

Δ_i 表示入侵容忍系统在状态 s_i 下没有采取防御措施，而攻击者停止攻击后其自身的预期损失(用负数表示)，它体现了攻击者的攻击意愿，其数值越小，攻击意愿越大。如果攻击者没有攻击，而入侵容忍系统采取了防御措施，攻击者则间接获了收益。

在混合策略纳什均衡下，攻击者以概率 $\pi_i^*(\phi)$ 选择 ϕ，以 $\pi_i^*(a_1)$ 选择攻击行为 a_1，攻击者在系统状态 s_i 下最优策略为

$$\begin{aligned}\Pi_i^*&=\left(\pi_i^*(\phi),\pi_i^*(a_1)\right)\\&=\left(\frac{\gamma_{22}-\gamma_{21}}{\Delta_i-\gamma_{12}+\gamma_{22}-\gamma_{21}},\frac{\Delta_i-\gamma_{12}}{\Delta_i-\gamma_{12}+\gamma_{22}-\gamma_{21}}\right)\end{aligned} \tag{3}$$

入侵容忍系统在状态 s_i 下最优策略为

$$\begin{aligned}D_i^*&=\left(\theta_i^*(\phi),\theta_i^*(d_1)\right)\\&=\left(\frac{\gamma_{22}-\gamma_{12}}{\Delta_i-\gamma_{12}+\gamma_{22}-\gamma_{21}},\frac{\Delta_i-\gamma_{21}}{\Delta_i-\gamma_{12}+\gamma_{22}-\gamma_{22}}\right)\end{aligned} \tag{4}$$

攻击者预期的收益为

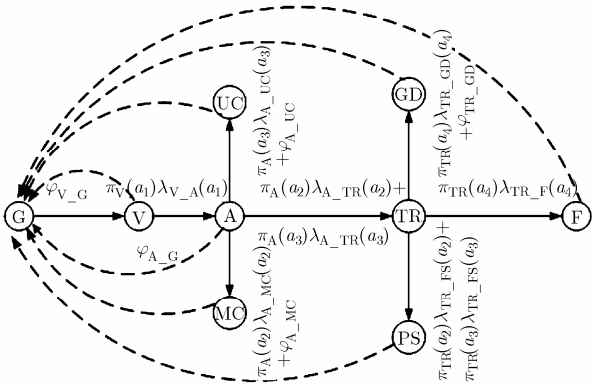
$$E\left(\Pi_i^*,\Theta_i^*\right)=-E\left(\Theta_i^*,\Pi_i^*\right)=\frac{\gamma_{22}\Delta_i-\gamma_{21}\gamma_{12}}{\Delta_i-\gamma_{12}+\gamma_{22}-\gamma_{21}} \tag{5}$$

如果入侵容忍系统从状态 s_i 转移到状态 s_j 会导致某一个安全属性失效，那么该安全属性的平均失效时间(Mean Time To Failure, MTTF)为 MTTF $=(\pi_i^*(a_1)\lambda_{ij}(a_1))^{-1}$。

4　入侵容忍系统的安全属性分析

本文主要从可用性、完整性与机密性的平均失效时间来分析入侵容忍系统的安全属性，分别表示为 A_{MTTF}，I_{MTTF} 和 C_{MTTF}。

根据入侵容忍系统的状态转移模型[1]，其博弈状态与转移过程如图 3 所示。



G：正常状态(Good state)
V：脆弱状态(Vulnerable state)
A：被攻击状态(Active attack)
UC：未知损害状态(Undetected Compromised state)
MC：屏蔽错误状态(Masked Compromised state)
TR：应急分类状态(TRiage state)
GD：降级状态(Graceful Degradation state)
FS：安全停止状态(Fail Secure state)
F：失效状态(Failed state)

图 3 博弈状态与状态转移图

其中，攻击者的全部攻击行为集合为 $A=\{\phi,a_1,a_2,a_3,a_4\}=\{\phi,\mathrm{Probing,U2R,R2L,DOS}\}$[1]。在不同系统状态下，攻击者所采取的攻击行为集合分别为：$A_{\mathrm{V}}=\{\phi,\ a_1\}$；$A_{\mathrm{A}}=\{\phi,a_2,a_3\}$；$A_{\mathrm{TR}}=\{\phi,a_2,a_3,a_4\}$；$A_{\mathrm{UC}}=\{\phi,a_3\}$；$A_{\mathrm{MC}}=\{\phi,a_2\}$；$A_{\mathrm{GD}}=\{\phi,\ a_4\}$；$A_{\mathrm{FS}}=\{\phi,a_2,a_3\}$；$A_{\mathrm{F}}=\{\phi,a_4\}$。

入侵容忍系统的全部防御措施集合为 $D=\{\phi,\ d_1,\ d_2,\ d_3,\ d_4,\ d_5,\ d_6\}=\{\phi,$ repair_vul, block_atta, redundant_data, check_para, degrade, reboot$\}$，分别表示不采取防御、修复系统脆弱点、阻断攻击行为、对文件数据进行冗余备份、对网络行为或应用程序进行参数检查、采取降级服务、重新启动系统等措施。在不同系统状态下，入侵容忍系统的防御措施集合分别为：$D_{\mathrm{V}}=\{\phi,d_1\}$; $D_{\mathrm{A}}=\{\phi,d_2,d_3,d_4\}$；$D_{\mathrm{A}}=\{\phi,d_2,d_3,d_5\}$；$D_{\mathrm{UC}}=\{\phi,d_1\}$；$D_{\mathrm{MC}}=\{\phi,d_1\}$；$D_{\mathrm{GD}}=\{\phi,d_6\}$；$D_{\mathrm{F}}=\{\phi,d_6\}$；$D_{\mathrm{FS}}=\{\phi,d_3,d_6\}$。

在图 3 中，博弈模型的各个博弈元素分别为

$$\boldsymbol{\Gamma}_{\mathrm{V}}=\begin{array}{c} \\ \phi \\ a_1 \end{array}\begin{array}{c} \begin{array}{cc} \phi & d_1 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{V}} & r_{12}^{\mathrm{V}} \\ r_{21}^{\mathrm{V}}+P_{\mathrm{V\_G}}(a_1,d_1)\boldsymbol{\Gamma}_{\mathrm{A}} & r_{22}^{\mathrm{V}} \end{bmatrix} \end{array}$$

$$\boldsymbol{\Gamma}_{\mathrm{A}}=\begin{array}{c} \\ \phi \\ a_2 \\ a_3 \end{array}\begin{array}{c} \begin{array}{ccc} \phi & d_2 & d_3 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{A}} & r_{12}^{\mathrm{A}} & r_{13}^{\mathrm{A}} \\ r_{21}^{\mathrm{A}}+P_{\mathrm{A\_MC}}(a_2,\phi)\boldsymbol{\Gamma}_{\mathrm{MC}} & r_{22}^{\mathrm{A}} & r_{23}^{\mathrm{A}} \\ r_{31}^{\mathrm{A}}+P_{\mathrm{A\_UC}}(a_3,\phi)\boldsymbol{\Gamma}_{\mathrm{UC}} & r_{32}^{\mathrm{A}} & r_{33}^{\mathrm{A}}+P_{\mathrm{A\_TR}}(a_3,d_3)\boldsymbol{\Gamma}_{TR} \end{bmatrix} \end{array}\begin{array}{c} \begin{array}{c} d_4 \end{array} \\ \begin{bmatrix} r_{14}^{\mathrm{A}} \\ r_{24}^{\mathrm{A}}+P_{\mathrm{A\_TR}}(a_2,d_4)\boldsymbol{\Gamma}_{\mathrm{TR}} \\ r_{34}^{\mathrm{A}} \end{bmatrix} \end{array}$$

$$\boldsymbol{\Gamma}_{\mathrm{TR}}=\begin{array}{c} \\ \phi \\ a_2 \\ a_3 \\ a_4 \end{array}\begin{array}{c} \begin{array}{ccc} \phi & d_2 & d_3 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{TR}} & r_{12}^{\mathrm{TR}} & r_{13}^{\mathrm{TR}} \\ r_{21}^{\mathrm{TR}}+P_{\mathrm{TR\_FS}}(a_2,\phi)\boldsymbol{\Gamma}_{\mathrm{FS}} & r_{22}^{\mathrm{TR}} & r_{23}^{\mathrm{TR}} \\ r_{31}^{\mathrm{TR}}+P_{\mathrm{TR\_FS}}(a_3,\phi)\boldsymbol{\Gamma}_{\mathrm{FS}} & r_{32}^{\mathrm{TR}} & r_{33}^{\mathrm{TR}}+P_{\mathrm{TR\_FS}}(a_3,d_3)\boldsymbol{\Gamma}_{\mathrm{FS}} \\ r_{41}^{\mathrm{TR}}+P_{\mathrm{TR\_F}}(a_4,\phi)\boldsymbol{\Gamma}_{\mathrm{F}} & r_{42}^{\mathrm{TR}} & r_{43}^{\mathrm{TR}}+P_{\mathrm{TR\_F}}a_4,d_3\boldsymbol{\Gamma}_{\mathrm{F}} \end{bmatrix} \end{array}\begin{array}{c} \begin{array}{c} d_5 \end{array} \\ \begin{bmatrix} r_{14}^{\mathrm{TR}} \\ r_{24}^{\mathrm{TR}}+P_{\mathrm{TR\_GD}}(a_2,d_5)\boldsymbol{\Gamma}_{\mathrm{GD}} \\ r_{34}^{\mathrm{TR}}+P_{\mathrm{TR\_GD}}(a_3,d_5)\boldsymbol{\Gamma}_{\mathrm{GD}} \\ r_{44}^{\mathrm{TR}} \end{bmatrix} \end{array}$$

$$\boldsymbol{\Gamma}_{\mathrm{UC}}=\begin{array}{c} \\ \phi \\ a_3 \end{array}\begin{array}{c} \begin{array}{cc} \phi & d_1 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{UC}} & r_{12}^{\mathrm{UC}} \\ r_{21}^{\mathrm{UC}} & r_{22}^{\mathrm{UC}} \end{bmatrix} \end{array},\quad \boldsymbol{\Gamma}_{\mathrm{MC}}=\begin{array}{c} \\ \phi \\ a_2 \end{array}\begin{array}{c} \begin{array}{cc} \phi & d_1 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{MC}} & r_{12}^{\mathrm{MC}} \\ r_{21}^{\mathrm{MC}} & r_{22}^{\mathrm{MC}} \end{bmatrix} \end{array},\quad \boldsymbol{\Gamma}_{\mathrm{GD}}=\begin{array}{c} \\ \phi \\ a_4 \end{array}\begin{array}{c} \begin{array}{cc} \phi & d_6 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{GD}} & r_{12}^{\mathrm{GD}} \\ r_{21}^{\mathrm{GD}} & r_{22}^{\mathrm{GD}} \end{bmatrix} \end{array}$$

$$\boldsymbol{\Gamma}_{\mathrm{FS}}=\begin{array}{c} \\ \phi \\ a_2 \\ a_3 \end{array}\begin{array}{c} \begin{array}{ccc} \phi & d_3 & d_6 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{FS}} & r_{12}^{\mathrm{FS}} & r_{13}^{\mathrm{FS}} \\ r_{21}^{\mathrm{FS}} & r_{22}^{\mathrm{FS}} & r_{23}^{\mathrm{FS}} \\ r_{31}^{\mathrm{FS}} & r_{32}^{\mathrm{FS}} & r_{33}^{\mathrm{FS}} \end{bmatrix} \end{array},\qquad \boldsymbol{\Gamma}_{\mathrm{F}}=\begin{array}{c} \\ \phi \\ a_4 \end{array}\begin{array}{c} \begin{array}{cc} \phi & d_6 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{F}} & r_{12}^{\mathrm{F}} \\ r_{21}^{\mathrm{F}} & r_{22}^{\mathrm{F}} \end{bmatrix} \end{array}$$

为了对入侵容忍系统进行量化分析，模型参数采用估计的方法设定，各个参数赋值及其含义见附录 1。在博弈双方达到纳什均衡后，攻击者与入侵容忍系统在各个状态的最优行动策略组合、预期收益以及入侵容忍系统安全属性的平均失效时间如表 1 所示。

表 1 结果表明，系统处于在 V 状态时攻击者的攻击意愿较小，此时攻击者的收益也很小。由于 Probing 攻击不会对系统的安全造成实质性的危害，因而从状态 V 转移至状态 A 不会影响系统的安全属性。在 A 状态，随着攻击者的攻击逐步深入，其收益也开始增加，从 A 状态转移至 TR 状态，入侵容忍系统的机密性和完整性平均失效时间为 0.44 h。在 TR 状态，攻击者的收益迅速增加；在 UC 状态，系统处于未知错误状态，攻击者的收益增加，并且希望维持该状态，以期获取持续的后期收益，因而不采取继续攻击的概率增加到 0.78，此时机密性和完整性的平均失效时间缩短为 0.33 h。在 MC 状态，系统屏蔽了攻击者的攻击行为，此时入侵容忍系统的安全属性平均失效时间增加至 0.95 h，表明系统在单位时间内基本上可以提供正常服务；在 GD, FS 和 F 状态，入侵容忍系统的安全性受到严重的威胁，尽管继续攻击后的收益更大，但攻击者希望维持现状，攻击者不采取继续攻击的概率都非常高。在 GD 状态，入侵容忍系统的可用性平均失效时间缩短为 0.28 h，表明在此状态下，需要采取恢复措施使系统恢复至正常状态；在 F 状态，入侵容忍系统受到强烈的 DOS 攻击，导致系统可用性平均失效时间急剧缩短为 0.03 h，表明系统已经基本失效。在 UC 状态，由于系统处于未知错误状态，不能有效触发相应的防御措施，所以系统不采取任何防御措施的概率高达 0.44。

5 攻击者行为分析

影响攻击者的攻击行为有许多因素，本文博弈模型中主要包括攻击意愿大小，攻击者的预期收益

以及攻击行为被检测之后收益变化等。以 A 状态为例(假定向各个状态转移概率均为 0)，博弈元素如式(6)所示。

$$\boldsymbol{\Gamma}_{\mathrm{A}}=\begin{array}{c} \\ \phi \\ a_2 \\ a_3 \end{array}\begin{array}{c} \begin{array}{cccc} \phi & d_2 & d_3 & d_4 \end{array} \\ \begin{bmatrix} \Delta_{\mathrm{A}} & 5 & 5 & 5 \\ 8 & 0 & r_{23}^{\mathrm{A}} & 10 \\ 8 & 0 & 7 & r_{34}^{\mathrm{A}} \end{bmatrix} \end{array} \tag{6}$$

图 4 结果表明，当攻击意愿值一定时，攻击者选择攻击行为 a_2 的概率随着该行为被检测后所获得的收益值增加而增加，同时也随着攻击行为 a_3 被检测后所获得的收益值减小而增加。图 5 所示结果表明攻击者选择攻击行为 a_3 概率变化具有与图 4 相同的趋势。图 4 和图 5 共同说明了攻击者在选择攻击行为时会考虑各个攻击行为被检测后的收益值大小，并倾向于选择收益值较高的攻击行为。从图 6 可以看出，当攻击行为 a_2 被检测后攻击者的收益值一定时，选择 a_2 的概率随着攻击意愿的增加而增加，

表 1 博弈双方最优行动策略组合、预期收益及安全属性平均失效时间(h)

状态	参　量						
	Π_i^*	Θ_i^*	$E(\Pi_i^*,\Theta_i^*)$	$E(\Theta_i^*,\Pi_i^*)$	A_{MTTF}	I_{MTTF}	C_{MTTF}
V	(0.47, 0.53, 0, 0, 0)	(0.26, 0.74, 0, 0, 0, 0, 0)	0.87	−0.87	–	–	–
A	(0.24, 0, 0.35, 0.41, 0)	(0.15, 0, 0.25, 0.32.0.28, 0, 0)	1.2	−1.2	–	–	–
TR	(0.22, 0, 0.36, 0.06, 0.36)	(0.06, 0, 0.5, 0, 0, 0.44, 0)	4.08	−4.08	–	0.44	0.44
UC	(0.78, 0, 0, 0.22, 0)	(0.44, 0.56, 0, 0, 0, 0, 0)	4.4	−4.4	–	0.33	0.33
MC	(0.42, 0, 0.58, 0, 0)	(0.24, 0.76, 0, 0, 0, 0, 0)	−1.12	1.12	–	0.95	0.95
GD	(0.86, 0, 0, 0, 0.14)	(0.28, 0, 0, 0, 0, 0, 0.72)	7.14	−7.14	0.28	–	–
FS	(0.83, 0, 0.12, 0.05, 0)	(0.33, 0, 0, 0, 0, 0, 0.67)	6.67	−6.67	–	0.40	0.40
F	(0.86, 0, 0, 0, 0.14)	(0.28, 0, 0, 0, 0, 0, 0.72)	7.14	−7.14	0.03	–	–

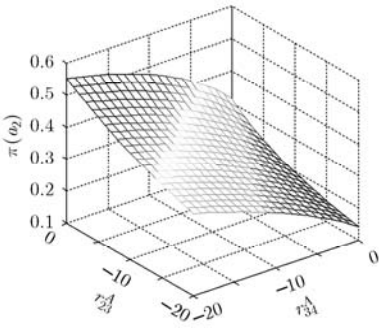


图 4　$\Delta_A=-20$, $\pi(a_2)$ 与 r_{23}^{A} 和 r_{34}^{A} 变化关系

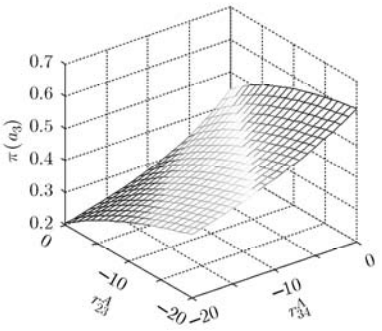


图 5　$\Delta_A=-20$, $\pi(a_3)$ 与 r_{23}^{A} 和 r_{34}^{A} 变化关系

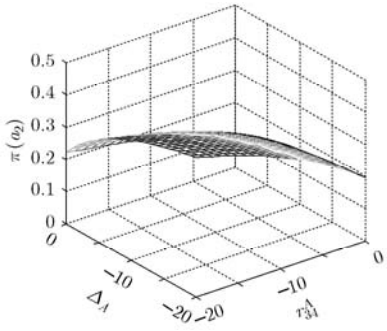


图 6　$r_{23}^{\mathrm{A}}=-10$, $\pi(a_2)$ 与 Δ_A 和 r_{34}^{A} 变化关系

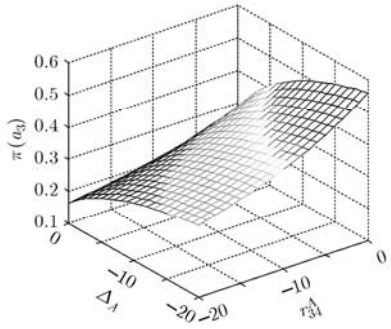


图 7　$r_{23}^{\mathrm{A}}=-10$，$\pi(a_3)$ 与 Δ_A 和 r_{34}^{A} 变化关系

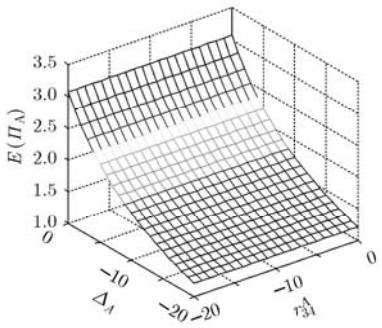


图 8　$r_{23}^{\mathrm{A}}=-10$，$E(\Pi_A)$ 与 Δ_A 和 r_{34}^{A} 变化关系

同时随着 a_3 被检测后获取的收益值减小而增加。同理，选择 a_3 的概率也随着攻击意愿的增大而增加，随着选择 a_3 被检测后获取的收益值增加而增加，如图 7 所示。图 8 表明，攻击者的预期收益只与攻击意愿有关，攻击意愿越大，预期收益越小。因此，入侵容忍系统需要加强系统安全，使得攻击者继续攻击的意愿降低，从而阻止其进一步攻击。虽然在此状态攻击者的预期收益增加了，但是阻止了攻击者继续攻击而获取后续的收益，避免了对系统造成更大的损失。

6 结束语

本文提出了基于博弈论的入侵容忍系统安全性分析模型，将网络攻击和入侵容忍之间的过程抽象为一个 2 人零和随机博弈。从安全属性平均失效时间的角度出发，对入侵容忍系统在各个状态纳什均衡点的安全性进行了分析。最后，分析了影响攻击者行动策略和预期收益的相关因素。上述分析结果为更好地防御网络攻击和入侵提供了一定的决策依据。本文假设了博弈双方都是完全理性的，对相关参数的设定存在一定的主观性。因此，在下一步工作中将着重研究有限理性条件下攻击者和入侵容忍系统的博弈模型，并通过实验数据来设定参数，进一步提高分析和评估结果的准确性。

附录 1 博弈模型参数设定

设定 $\lambda_{\mathrm{V\_A}}(a_1)=20$，表示系统非常容易被攻击者使用 Probing 攻击发现脆弱点；

$$\lambda_{\mathrm{A\_MC}}(a_2)=\lambda_{\mathrm{A\_UC}}\ (a_3)=1$$

表示系统在状态 A 受到 U2R 和 R2L 的攻击程度较轻；$\lambda_{\mathrm{A\_TR}}(a_2)=\lambda_{\mathrm{A\_TR}}(a_3)=3$，表示系统在状态 A 受到 U2R 和 R2L 的攻击程度严重；$\lambda_{\mathrm{TR\_FS}}(a_2)=\lambda_{\mathrm{TR\_FS}}(a_3)=6$，系统在 TR 状态继续受到程度更严重的攻击，系统会进入 FS 状态；$\lambda_{\mathrm{TR\_GD}}(a_4)=10$，表示在 TR 状态受到较轻的 DOS 攻击；$\lambda_{\mathrm{TR\_F}}(a_4)=100$；表示在 TR 状态受到严重的 DOS 攻击，系统入侵容忍措施失效，因而进入 F 状态。$\varphi_{\mathrm{V\_G}}=1/24$，表示在 V 状态，入侵容忍系统每 24 h 对系统的脆弱点进行一次修复；$\varphi_{\mathrm{A\_G}}=0.5$，表示在 A 状态，入侵容忍系统会成功阻断一部分攻击行为；$\varphi_{\mathrm{A\_MC}}=\varphi_{\mathrm{A\_UC}}=1$，表示在 A 状态，采取入侵容忍措施使系统进入 UC 和 MC 状态；$\varphi_{\mathrm{TR\_GD}}=8$，表示采取一定的抗 DOS 攻击措施，可以使得系统进入 GD 状态。

根据上述参数值可以计算出相应的状态转移概率分别为

$$P_{\mathrm{V\_G}}(a_1,d_1)=20/21,\ \ P_{\mathrm{A\_MC}}(a_2,\phi)=2/13$$
$$P_{\mathrm{A\_TR}}(a_2,d_4)=6/13,\ \ P_{\mathrm{A\_UC}}(a_3,\phi)=2/13$$
$$P_{\mathrm{A\_TR}}(a_3,d_3)=6/13,\ \ P_{\mathrm{TR\_FS}}(a_2,\phi)=3/7$$
$$P_{\mathrm{TR\_FS}}(a_3,\phi)=3/7,\ \ P_{\mathrm{TR\_F}}(a_4,\phi)=50/59$$
$$P_{\mathrm{TR\_FS}}(a_3,d_3)=3/7,\ \ P_{\mathrm{TR\_F}}(a_4,d_3)=50/5$$
$$P_{\mathrm{TR\_GD}}(a_2,d_5)=0,\ \ P_{\mathrm{TR\_GD}}(a_3,d_5)=0$$

设定 $\Delta_{\mathrm{V}}=-5$ 表明在 V 状态时攻击者攻击的意愿比较小；$\Delta_{\mathrm{A}}=-20$ 表明攻击者继续攻击的意愿变大；$\Delta_{\mathrm{MC}}=-30,\Delta_{\mathrm{TR}}=-40$ 表明随着入侵的不断深入，攻击者继续攻击的意愿越来越大。入侵容忍系统处于 UC, GD, FS 和 F 状态时，攻击者获取的收益较大，攻击者希望维持这种状态，因为进一步攻击则会导致入侵容忍系统采取防御措施对系统进行恢复或重构，重新进入正常状态 G，那么攻击行为将无法获取持续的收益，所以攻击者继续攻击的意愿非常小，设定 $\Delta_{\mathrm{UC}}=\Delta_{\mathrm{GD}}=\Delta_{\mathrm{FS}}=\Delta_{\mathrm{F}}=0$。

各个状态攻击者的收益如下：

$r_{12}^{\mathrm{V}}=3,\ r_{22}^{\mathrm{V}}=-1,\ r_{21}^{\mathrm{V}}=5;\ r_{12}^{\mathrm{A}}=r_{13}^{\mathrm{A}}=r_{14}^{\mathrm{A}}=5,\ r_{21}^{\mathrm{A}}=8,\ r_{22}^{\mathrm{A}}=0,\ r_{23}^{\mathrm{A}}=-10,\ r_{24}^{\mathrm{A}}=10,\ r_{31}^{\mathrm{A}}=8,\ r_{32}^{\mathrm{A}}=0,\ r_{33}^{\mathrm{A}}=7,\ r_{34}^{\mathrm{A}}=-10;\ r_{12}^{\mathrm{TR}}=r_{13}^{\mathrm{TR}}=6,\ r_{14}^{\mathrm{TR}}=8,\ r_{21}^{\mathrm{TR}}=10,\ r_{22}^{\mathrm{TR}}=-2,\ r_{23}^{\mathrm{TR}}=-15,\ r_{24}^{\mathrm{TR}}=10,\ r_{31}^{\mathrm{TR}}=10,\ r_{32}^{\mathrm{TR}}=-2,\ r_{33}^{\mathrm{TR}}=10,\ r_{34}^{\mathrm{TR}}=10,\ r_{41}^{\mathrm{TR}}=15,\ r_{42}^{\mathrm{TR}}=10,\ r_{43}^{\mathrm{TR}}=15,\ r_{44}^{\mathrm{TR}}=-5;\ r_{12}^{\mathrm{UC}}=8,r_{21}^{\mathrm{UC}}=20,r_{22}^{\mathrm{UC}}=-8;\ r_{12}^{\mathrm{MC}}=8,r_{21}^{\mathrm{MC}}=20,\ r_{22}^{\mathrm{MC}}=-8;\ r_{12}^{\mathrm{GD}}=10,r_{21}^{\mathrm{GD}}=50,r_{22}^{\mathrm{GD}}=-10;\ r_{12}^{\mathrm{FS}}=8,r_{13}^{\mathrm{FS}}=10,r_{21}^{\mathrm{FS}}=40,r_{22}^{\mathrm{FS}}=-15,r_{23}^{\mathrm{FS}}=-10,r_{31}^{\mathrm{FS}}=r_{32}^{\mathrm{FS}}=40,r_{33}^{\mathrm{FS}}=-10;r_{12}^{\mathrm{F}}=10,r_{21}^{\mathrm{F}}=50,r_{22}^{\mathrm{F}}=-10$。

参 考 文 献

[1] Madan B B, Goševa-Popstojanova K, Vaidyanathan K, *et al*.. A method for modeling and quantifying the security attributes of intrusion tolerant system[J]. *Performance Evaluation*, 2004, 56(1-4): 167-186.

[2] 殷丽华, 方滨兴. 入侵容忍系统安全属性分析[J]. 计算机学报, 2006, 29(8): 1505-1512.
Yin Li-hu and Fang Bin-xing. Security attributes analysis for intrusion tolerant systems[J]. *Chinese Journal of Computers*, 2006, 29(8): 1505-1512.

[3] Singh S, Cukier M, and Sanders W. Probabilistic validation of an intrusion tolerant replication system[C]. Proceedings of International Conference on Dependable Systems and Networks, San Francisco, CA, 2003: 615-624.

[4] 陈锋, 刘德辉, 张怡, 等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展, 2011, 48(6): 945-954.
Chen Feng, Liu De-hui, Zhang Yi, *et al*.. A hierarchical evaluation approach for network security based on threat spread model[J]. *Journal of Computer Research and Development*, 2011, 48(6): 945-954.

[5] Lye K-w and Wing J. Game strategies in network security[J]. *International Journal of Information Security*, 2005, 4(1/2):

71–86.

[6] Sallhammar K, Helvik B E, and Knapskog S J. A game-theoretic approach to stochastic security and dependability evaluation[C]. Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, USA, 2006: 61–68.

[7] 陈亚睿, 田立勤, 杨扬. 云计算环境下基于动态博弈论的用户行为模型与分析[J]. 电子学报, 2011, 39(8): 1818–1823.
Chen Ya-rui, Tian Li-qin, and Yang Yang. Model and analysis of user behavior based on dynamic game theory in cloud computing[J]. *Acta Electronica Sinica*, 2011, 39(8): 1818–1823.

[8] 朱建明, Srinivassan Raghunathan. 基于博弈论的信息安全技术评价模型[J]. 计算机学报, 2009, 32(4): 828–834.
Zhu Jian-ming and Srinivassan Raghunathan. Evaluation Model of information security technologies based on game theoretic[J]. *Chinese Journal of Computers*, 2009, 32(4): 828–834.

[9] 李奕男, 钱志鸿, 刘影, 等. 基于博弈论的移动 Ad hoc 网络入侵检测模型[J]. 电子与信息学报, 2010, 32(9): 2245–2248.
Li Yi-nan, Qian Zhi-hong, Liu Ying, *et al*.. An intrusion detection model of mobile Ad hoc networks based on game theory[J]. *Journal of Electronics & Information Technology*, 2010, 32(9): 2245–2248.

[10] 王志文, 卢柯, 王晓飞. 基于博弈论的信息系统生存性提升方法研究[J]. 计算机科学, 2010, 37(9): 81–84.
Wang Zhi-wen, Lu Ke, and Wang Xiao-fei. Approach on promoting survivability for information system based on game-theory[J]. *Computer Science*, 2010, 37(9): 81–84.

周　华：　男，1981 年生，博士，讲师，主要研究方向为计算机网络与信息安全.

周海军：　男，1974 年生，讲师，主要研究方向为网络安全协议、密码算法等.

马建锋：　男，1980 年生，讲师，主要研究方向为计算机网络通信、软件工程等.