基于博弈模型的网络安全失效分析方法研究

谭凌鸿,何选森
TAN Ling-hong,HE Xuan-sen

湖南大学 计算机与通信学院,长沙 410082
College of Computer and Communication,Hunan University,Changsha 410082,China
E-mail:leehom_tan@sina.com.cn

TAN Ling-hong,HE Xuan-sen.Research on failure analysis methods of network security based on game model.Computer Engineering and Applications,2008,44(31):139-141.

Abstract: A method for analyzing the failure of the network security based on game model is proposed.The failure process of the unrepairable network system can be considered as a single-controller stochastic game.The attacker's total utility and best strategy are analyzed and calculated,and the result verifies that the attacker will not change his choice when the expected pay-offs change in a certain range.

Key words: network security;single-controller stochastic game;linear programming

摘 要:提出了一种基于博弈模型的网络安全性失效的分析方法。针对不可修复的网络系统,安全失效过程被看作一个攻击方控制状态转移的随机博弈过程。从攻击的角度计算分析了在此过程中攻击方的总收益和最优策略,结果表明当支付期望值在一定的范围内变化时,攻击者将不改变其行动选择。

关键词:网络安全;单方控制的随机博弈;线性规划
DOI:10.3778/j.issn.1002-8331.2008.31.040 **文章编号:**1002-8331(2008)31-0139-03 **文献标识码:**A **中图分类号:**TP393

网络安全性能是指在不安全因素干扰下的网络可靠性能,包括信息的机密性、数据的完整性、对合法用户的可用性[1]。目前对网络安全性能的研究大多采用随机模型来描述攻击行为及系统安全状态,如 Griffin 和 Madan 等人在文献[2]中分析了在攻击环境下入侵容忍系统的安全失效过程,提出采用半马尔可夫模型分析方法对安全指标进行定量计算;文献[3]中研究了随机 Petri 网对网络系统可信赖性建模分析的方法,着重描述了系统的服务失效模型和容错模型;Walid Hneiti 和 Naim A-jlouni 在文献[4]中针对 Infrastructure 模式的 WLAN,分析了射频信号阻塞对可用性失效的影响,提出通过增加一个接入点以增加系统可靠性的方法。另外,博弈理论(game theory)也被引入对网络攻击行为的分析中,如文献[5]中将攻防双方看作非零和随机博弈中的两个局中人,从攻、防两个方面分析了不同情况下系统状态转移的过程,并计算了双方的最优响应策略;Karin 等人在文献[6]中假定一方的策略固定不变,采用零和随机博弈理论预测某一状态攻击行为发生的概率,并通过仿真分析了代价参数对攻击发生概率的影响。

与文献[2,5]类似,本文对不可修复网络系统的安全失效过程建立了攻、防双方多阶段随机博弈模型,攻击方控制系统状态转移,每个阶段攻击方进行一次行动决策,根据其选择的行动,博弈进入下一阶段或者终止。攻击方的收益只取决于博弈结束时的收益,其瞬态阶段收益为零,因此博弈求解是一个线性规划问题。

1 安全失效的随机博弈模型

通常,"故障-异常-失效(fault-error-failure)"链被用来表示安全失效过程中系统所处的状态,"故障"是自然或者人为引起的;"异常"指系统出现异常行为;"失效"指系统服务失效。安全失效过程可视为攻、防双方共同作用的一个随机博弈过程,攻防双方的行动决定系统状态的转移。假定防守方行动策略固定,从攻击方角度考虑,系统状态的转移只取决于己方的行动和当前系统状态。攻击的最终结果或是攻击者获得报酬,即系统安全失效;或是攻击者付出代价,即攻击行为被检测到。无论哪种情况系统最终都将进入吸收态,即博弈有限的。因此对于不可修复网络,其失效过程是一个单方控制的、有限的随机博弈过程。

单方控制的两人零和随机博弈 $\Gamma=(\Gamma_1,\Gamma_2,\cdots,\Gamma_n)$ 是 n 个博弈元素构成的有限集合,每个元素是一个五元组$<S,A,B,q,r>$,其中 $S=O\cup T$ 表示系统状态空间,O 为瞬态,T 为吸收态;A、B 分别表示局中人 Player I 和 Player II 在每个状态的行动集合;$q:S\times A\times B\to\Delta(S)$是状态传输函数,$\Delta(S)$是集合 S 中所有状态的分布概率;$r:S\to\boldsymbol{R}$ 为有界的支付值。双方按如下规则进行博弈:给定初始状态 s,Player I 选择行动 a,整个过程 Player II 选择固定策略行动,系统以 $q(s'|s,a)$的概率转至状态 s',当系统到达状态 $s'\in T$ 时,Player I 从 Player II 获得收益 r,博弈结束;否则博弈进入下一阶段。博弈中局中人的行动历史是共同知识,即双方都有完美记忆(perfect recall)。

(1)系统状态

基金项目:湖南省 2007-2009 厅局级科技计划重点项目(No.ZJ20071008)。
作者简介:谭凌鸿(1983-),男,硕士生,主要研究方向:网络安全、博弈论;何选森(1958-),男,副教授,主要研究方向:信号与信息处理。
收稿日期:2007-12-06 **修回日期:**2008-03-12

根据“故障-异常-失效”链,将系统状态分为安全状态 s_1、脆弱性状态 s_2、异常状态 s_3、安全失效状态 s_4 和终止状态 s_5。安全状态是指采用了安全防护措施的系统在攻击发生前所处的状态;脆弱性状态指系统存在安全威胁或漏洞,当攻击者开发这些漏洞进行入侵时,系统进入异常状态;当异常行为未被检测,系统安全性失效;当异常行为被检测时,博弈终止,系统进入终止状态。

(2)行动空间

从攻击的角度看,对网络的攻击主要包括:网络机密性失效攻击,通过破译密钥和加密数据以非法接入网络获取敏感信息;网络完整性失效攻击,非法篡改或伪造数据帧并重注入使系统工作在非正常状态;网络可用性失效攻击,恶意攻击以干扰或阻止网络正常服务。针对某一类攻击定义攻、防双方的行动空间,在不同状态双方的行动空间是不同的,用 K_i 表示攻击方在状态 的行动空间。如对于无线局域网络,攻击者在每个状态的行动集合包括 K_1={社交工程以猜测、盗取密码,非法监听收集网络信息,φ}、K_2={暴力破解, 数据帧重放主动破解,}、K_3={802.1x 会话劫持,MAC 地址欺骗,φ},其中 φ 表示不攻击。

(3)报酬和代价

将正支付称为报酬,负支付称为代价。不同类型的攻击由于攻击者的目标不同,其支付包括很多方面:攻击者以机密性失效为目的,其报酬为敏感信息的获得、系统资源的占有等;以可用性失效为目的的攻击者,其报酬为对系统的破坏程度以及系统恢复需要的时间等;而攻击者的代价通常包括攻击付出的时间、攻击被检测出等。在安全失效性分析中,攻击者只关心系统进入吸收态时的支付,其阶段支付为零:$r_{s\in O}(s)=0$。

2 线性规划求解算法

对于单方控制、有限的随机博弈 Γ 可看作一类特殊的马尔可夫决策过程, 攻击方在每个状态选择行动以最大化总收益,用 $\boldsymbol{R}$ 表示这个决策过程,设系统有 n 个状态,其中 m 个为瞬态, 其余为吸收态, 若有 $i,l,h\in O,j\in T,k\in K_h$, 定义 $d_i^k\in[0,1]$为攻击方在状态 S_i 选择行动 k 的概率,$p_{ij}^k\in[0,1]$为在状态 S_i 攻击方选择行动 k 后系统转至状态 S_j 的概率。决策过程 $\boldsymbol{R}$ 的转移概率为:

$$p_{ij}(\boldsymbol{R})=\sum_{k=1}^{K_i}p_{ij}^k\cdot d_i^k \tag{1}$$

转移概率的向量为:

$$\boldsymbol{P}(\boldsymbol{R})=\begin{pmatrix}\boldsymbol{C}(\boldsymbol{R}) & \boldsymbol{N}(\boldsymbol{R})\\ \boldsymbol{0} & \boldsymbol{I}\end{pmatrix} \tag{2}$$

其中

$$\boldsymbol{C}(\boldsymbol{R})=\begin{pmatrix}p_{11}(\boldsymbol{R}) & \cdots & p_{1m}(\boldsymbol{R})\\ \vdots & & \vdots\\ p_{m1}(\boldsymbol{R}) & \cdots & p_{mm}(\boldsymbol{R})\end{pmatrix},\boldsymbol{N}(\boldsymbol{R})=\begin{pmatrix}p_{1(m+1)}(\boldsymbol{R}) & \cdots & p_{1n}(\boldsymbol{R})\\ \vdots & & \vdots\\ p_{n(m+1)}(\boldsymbol{R}) & \cdots & p_{nn}(\boldsymbol{R})\end{pmatrix},$$

$\boldsymbol{I}$ 为单位矩阵。

决策过程 $\boldsymbol{R}$ 的支付函数为:

$$r_{ij}(\boldsymbol{R})=\sum_{k=1}^{K_i}r_{ij}^k\cdot d_i^k,\text{其中 }S_i\in O,S_j\in T \tag{3}$$

系统从瞬态 S_i 到吸收态 S_j 的总支付为:

$$V_{ij}(\boldsymbol{R})=p_{ij}(\boldsymbol{R})r_{ij}(\boldsymbol{R})+\sum_{S_h\in O}p_{ih}(\boldsymbol{R})V_{hj}(\boldsymbol{R}) \tag{4}$$

式(4)右边包括两个部分,第一部分表示系统直接进入吸收态 S_j 的支付, 第二部分表示系统经过瞬态 S_h 转入吸收态 S_j 的支付。令 $h_{ij}(\boldsymbol{R})=\sum_{k=1}^{K_i}p_{ij}^k\cdot r_{ij}^k\cdot d_i^k$,对式(4)进行矩阵变换可得:

$$\boldsymbol{V}(\boldsymbol{R})=\boldsymbol{H}(\boldsymbol{R})+\boldsymbol{C}(\boldsymbol{R})\boldsymbol{V}(\boldsymbol{R})=(\boldsymbol{I}-\boldsymbol{C}(\boldsymbol{R}))^{-1}\boldsymbol{H}(\boldsymbol{R}) \tag{5}$$

令 $\boldsymbol{Q}(\boldsymbol{R})=\boldsymbol{I}-\boldsymbol{C}(\boldsymbol{R})$,$\boldsymbol{G}(\boldsymbol{R})=(\boldsymbol{I}-\boldsymbol{C}(\boldsymbol{R}))^{-1}=[g_{ih}(\boldsymbol{R})]$为 $m\times m$ 的矩阵,其中 $g_{ih}(\boldsymbol{R})$为从状态 S_i 出发在到达吸收态之前系统在状态 S_h 停留的平均次数,故有:

$$\sum_{l=1}^{m}g_{ih}(\boldsymbol{R})q_{hl}(\boldsymbol{R})=\delta_{il} \tag{6}$$

其中 δ_{il} 为 δ 函数。考虑从瞬态 S_i 到所有吸收态的总支付,有:

$$\boldsymbol{V}(\boldsymbol{R})\cdot\boldsymbol{1}=[\sum_{j\in T}V_{ij}(\boldsymbol{R})]=\boldsymbol{G}(\boldsymbol{R})\boldsymbol{H}(\boldsymbol{R})\cdot\boldsymbol{1} \tag{7}$$

其中 $\boldsymbol{1}=(1\ 1\ \cdots\ 1)^{\mathrm{T}}$。

若初始状态为非吸收态,令 $\boldsymbol{\pi}=(\pi_1,\pi_2,\cdots,\pi_m)$为系统的初始状态概率向量, 表示决策过程开始时系统状态的概率分布,其中:

$$\sum_{i=1}^{m}\pi_i=1,\pi_i\geqslant 0(i=0,1,\cdots,m) \tag{8}$$

因此,决策过程 $\boldsymbol{R}$ 从初始状态到所有吸收态的总支付期望为:

$$\begin{aligned}\boldsymbol{E}(\boldsymbol{R})&=\boldsymbol{\pi}\boldsymbol{V}(\boldsymbol{R})\cdot\boldsymbol{1}=\boldsymbol{\pi}\boldsymbol{G}(\boldsymbol{R})\boldsymbol{H}(\boldsymbol{R})\cdot\boldsymbol{1}=\\ &\sum_{i=1}^{m}\pi_i\sum_{h=1}^{m}g_{ih}(\boldsymbol{R})\sum_{j\in T}h_{hj}(\boldsymbol{R})=\\ &\sum_{h=1}^{m}(\sum_{i=1}^{m}g_{ih}(\boldsymbol{R})\pi_i d_h^k)\sum_{j=m+1}^{n}\sum_{k=1}^{K_h}p_{hj}^k r_{hj}^k\end{aligned} \tag{9}$$

若令 $X_{hk}=\sum_{i=1}^{m}g_{ih}(\boldsymbol{R})\pi_i d_h^k$,根据文献[7]有如下推导:

$$\begin{aligned}&\sum_{h=1}^{m}\sum_{k=1}^{K_h}q_{hl}^k X_{hk}=\sum_{h=1}^{m}\sum_{k=1}^{K_h}q_{hl}^k\sum_{i=1}^{m}g_{ih}(\boldsymbol{R})d_h^k\pi_i=\\ &\sum_{i=1}^{m}\sum_{h=1}^{m}(\sum_{k=1}^{K_h}q_{hl}^k d_h^k)g_{ih}(\boldsymbol{R})\pi_i=\\ &\sum_{i=1}^{m}\sum_{h=1}^{m}q_{hl}(\boldsymbol{R})g_{ih}(\boldsymbol{R})\pi_i=\sum_{i=1}^{m}\delta_{il}\pi_i=\pi_l\end{aligned} \tag{10}$$

攻击方的目标即找到最优决策过程 $\boldsymbol{R}$ 使得 $\boldsymbol{E}(\boldsymbol{R})$最大。因此根据式(9)和式(10),随机博弈的求解等价于求解以下线性规划问题:

$$\begin{cases}\max\boldsymbol{E}(\boldsymbol{R})=\max\sum_{h=1}^{m}\sum_{j=m+1}^{n}\sum_{h=1}^{K_h}p_{hj}^k r_{hj}^k X_{hk}\\ \sum_{h=1}^{m}\sum_{k=1}^{K_i}q_{hl}^k X_{hk}=\pi_l\quad(l=1,2,\cdots,m)\end{cases} \tag{11}$$

3 数值结果及分析

本章对攻击环境下 WLAN 可用性失效过程进行分析,系统状态划分为安全状态 s_1、脆弱性状态 s_2、异常状态 s_3,安全失效状态 s_4 和终止状态 s_5, 其中 s_1、s_2、s_3 为瞬态,s_4、s_5 为吸收态。不同于文献[4],假定 WLAN 可用性失效是拒绝服务攻击的结果,攻击方的行动空间包括 K_1={社交工程,非法监听收集网络信息,φ},K_2={搭建非法 AP 进行射频干扰, 伪造取消关联的管理帧或持续时间长的控制帧,φ},K_3={继续攻击,φ}。表 1 给出了博弈 Γ 的状态转移概率、支付值等数据。以状态 s_1 为例,表 1 表示在状态 s_1 进行社交工程或非法监听, 系统分别以 0.7 和 0.5 的概率转入脆弱性状态 s_2,获得阶段收益 0;或有 0.5 和 0.2 的概率行为被系统检测,攻击方分别付出代价 10 和 5。若选择

不攻击，系统则停留在 s_1 状态。

表 1　随机博弈数据表

状态 h	行动 $k\in K_h$	转移概率及支付值				
		p_{h1}^k	p_{h2}^k	p_{h3}^k	$p_{h4}^k(r_{h4}^k)$	$p_{h5}^k(r_{h5}^k)$
s_1	1	0	0.7	0	0(−)	0.5(−10)
	2	0	0.5	0	0(−)	0.2(−5)
	3	1	0	0	0(−)	0(−)
s_2	1	0	0	0.8	0.8(10)	0.8(−5)
	2	0	0	0.6	0.6(10)	0.8(−8)
	3	0	1.0	0	0(−)	0(−)
s_3	1	0	0	0	0.8(10)	0.8(−5)
	2	0	0	1.0	0(−)	0(−)

由于无线信道的开放性，攻击者很容易获得网络信息，因此大部分时候系统对于攻击者是脆弱的。假定系统初始状态向量 $\boldsymbol{\pi}$=(0.2，0.7，0.1)时，表示系统以较高的概率处于脆弱性状态，较低的概率处于其他状态。根据表 1 和式(11)可得线性规划：

$$\begin{cases}\max\ \boldsymbol{E}(\boldsymbol{R})=(-5X_{11}-1X_{12}+0X_{13}+4X_{21}-0.4X_{22}+0X_{23}+4X_{31}+0X_{32})\\ \text{s.t.}\ -0.7X_{11}-0.5X_{12}+0X_{13}+1X_{21}+0X_{22}+0X_{23}+0X_{31}+0X_{32}=0.7\\ \quad 0X_{11}+0X_{12}+0X_{13}-0.8X_{21}-0.6X_{22}+0X_{23}+1X_{31}+0X_{32}=0.1\\ \quad 1X_{11}+1X_{12}+0X_{13}+0X_{21}+0X_{22}+0X_{23}+0X_{31}+0X_{32}=0.2\\ \quad -0.7X_{11}-0.5X_{12}+0X_{13}+1X_{21}+0X_{22}+0X_{23}+0X_{31}+0X_{32}=0.7\\ \quad 0X_{11}+0X_{12}+0X_{13}-0.8X_{21}-0.6X_{22}+0X_{23}+1X_{31}+0X_{32}=0.1\\ \quad X_{11},X_{12},X_{13},X_{21},X_{22},X_{23},X_{31},X_{32}\geqslant 0\end{cases}\tag{12}$$

采用单纯性方法求解上述线性规划可得：X_{12}=0.2，X_{21}=0.8，X_{31}=0.74，X_{11}=X_{13}=X_{22}=X_{23}=X_{32}=0，博弈的值为 5.96，即对于博弈 Γ，攻击方的最优策略是在状态 s_1 选择行动 2，状态 s_2 选择行动 1，状态 s_3 选择行动 1，根据此策略行动可获得 的收益。因此，对于表 1 给定的状态转移概率和支付值，攻击者采用社交工程获取网络信息，再对指定 AP 进行射频干扰可获得最大的攻击效应。

通过对式(12)的目标函数进行灵敏度分析，可得攻击行动选择与报酬/代价关系，如表 2。

表 2　目标函数系数范围

变量	当前系数	允许增加	允许减少
X_{11}	−5.0	2.56	无穷
X_{12}	−1.0	无穷	2.56
X_{13}	0	0	无穷
X_{21}	4.0	12.80	5.20
X_{22}	−0.4	5.20	无穷
X_{23}	0	0	无穷
X_{31}	4.0	16.00	26.00
X_{32}	0	0	无穷

表 2 表明变量在允许变化范围内改变时，最优基解不变。以状态 s_1 为例，式(11)中的目标函数为：

$$\max\sum_{h=1}^{m}\sum_{k=1}^{K_h}\sum_{j=m+1}^{n}p_{hj}^k r_{hj}^k X_{hk}=\max\sum_{h=1}^{m}\sum_{k=1}^{K_h}(p_{h4}^k r_{h4}^k+p_{h5}^k r_{h5}^k)X_{hk}$$

由于状态 s_4、s_5 分别为失效态和终止态，故 r_{h4}^k、r_{h5}^k 分别表示博弈结束攻击方获得的收益和付出的代价。定义报酬代价期望：

$$h(k)=p_{h4}^k r_{h4}^k+p_{h5}^k r_{h5}^k\tag{13}$$

当 $h(1)\leqslant$−5+2.56 时，攻击者的选择不会改变，即行动 1 改变的临界支付值为−2.44。同理，行动 2 改变的临界支付值为−3.56，即当其余系数不变，$h(2)$减至−3.56 时行动 1 将会被选择。同时，当选择的攻击行动改变时，相应的收益值也会改变。图 1 描述了上述关系。

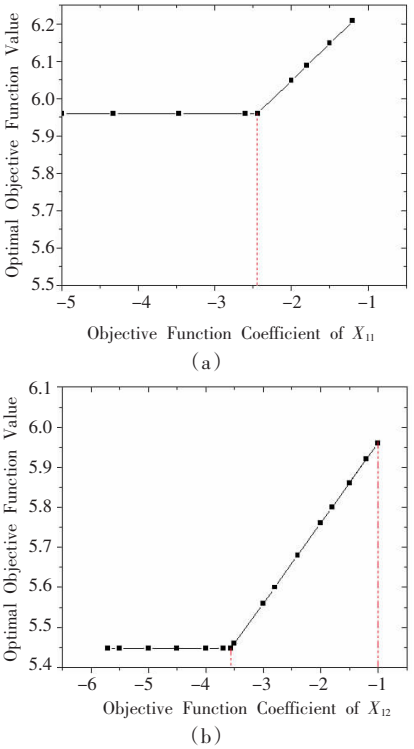

图 1　$h(k)$与最优值关系图

4　结论

提出了一种不可修复网络系统安全性失效分析的方法：将失效过程模型化为攻击方控制状态转移的随机博弈过程，采用线性规划的方法求解博弈中攻击方的最优策略和总收益。结果表明当支付期望值在一定的范围内变化时，攻击者将不改变其行动选择。在实际的网络安全评价中，这种分析方法作为攻击行为预测、安全性能评估的一种手段，将有利于指导安全措施的部署。

参考文献：

[1] Avizzienis A，Laprie J C，Randell B，et al.Basic concepts and taxonomy of dependable and secure computing[J].IEEE Transactions on Dependable and Secure Computing，2004：1(1).

[2] Griffin C，Madan B，Trivedi K S.State space approach to security quantification[C]//Proc of IEEE Int Conf Computer Software and Applications，2005.

[3] 林闯，王元卓，杨扬，等.基于随机 Petri 网的网络可信赖性分析方法研究[J].电子学报，2006，34(2).

[4] Hneiti W，Ajlouni N.Dependability analysis of wireless local area networks[C]//Proc of 2nd ICTTA'06，2006.

[5] Lye K，Wing J M.Game strategies in network security[J].International Journal of Information Security，2005，4(1/2)：71−86.

[6] Sallhammar K，Helvik B E，Knapskog S J.Towards a stochastic model for integrated security and dependability evaluation[C]//Proc of IEEE Int Conf on Availability，Reliability and Security，2006.

[7] Mine H，Yamada K，Osaki S.On terminating stochastic games[J]. Management Science，1970，16(9)：560−571.