Journal of Computer Applications
计算机应用,2013,33(5):1347-1349,1352
ISSN 1001-9081
CODEN JYIIDU
2013-05-01
http://www.joca.cn

文章编号:1001-9081(2013)05-1347-03
doi:10.3724/SP.J.1087.2013.01347

基于非零和攻防博弈模型的主动防御策略选取方法

陈永强*,付　钰,吴晓平
(海军工程大学 信息安全系,武汉 430033)
(*通信作者电子邮箱 chenyongqiang919@163.com)

摘　要:针对现实网络攻防环境中防御措施的滞后性以及攻防对抗过程中双方收益不完全相等的问题,提出一种基于非零和博弈的主动防御策略选取方法。首先依据攻击者与系统的博弈关系,结合网络安全问题实际情况提出网络安全博弈图;其次在此基础上给出一种基于非零和博弈的网络攻防博弈模型,结合主机重要度以及防御措施成功率计算单一安全属性攻防收益值,进而根据攻防意图对整体攻防收益进行量化;最后通过分析纳什均衡得到最优主动防御策略。实例验证了该方法在攻击行为预测和主动防御策略选取方面的有效性和可行性。

关键词:网络安全;攻防模型;非零和博弈;主动防御;策略选取
中图分类号:TP309　　**文献标志码**:A

Active defense strategy selection based on non-zero-sum attack-defense game model

CHEN Yongqiang*, FU Yu, WU Xiaoping
(*Department of Information Security, Naval University of Engineering, Wuhan Hubei 430033, China*)

Abstract: In order to deal with the problems that defensive measures are lagging behind the attack and that the payoffs of attacker and defender are unequal, an active strategy selection method based on non-zero-sum game was proposed. Firstly, a network security game graph was presented combined with the actual situation of network security and the relationship between the attacker and the defender. Secondly, a network attack-defense game model was proposed based on non-zero-sum game. The attack-defense cost of single security attribute was calculated combined with the host important degree and success rate of defense measures, and according to attack-defense intention, the total attack-defense cost was quantified. Finally, the best strategy for defender was obtained by analyzing the Nash equilibrium of the game model. A representative example was given to illustrate the efficacy and feasibility of the method on attack prediction and active defense strategy selection.

Key words: network security; attack-defense model; non-zero-sum game; active defense; strategy selection

0　引言

随着网络的发展,网络安全研究的理念已经从被动防御转向了积极防御。积极防御的目的是为了提前识别系统潜在的安全威胁,采用针对性的措施阻止或减少系统的损失。因此能否选择合适的防御策略显得尤为重要,而选择的防御策略是否有效,不仅取决于系统自身,同时也要考虑到攻击行为对防御策略可能产生的影响,即攻防双方策略的依存性。对于这种攻防行为交互的关系可应用博弈论进行建模分析[1]。

博弈论是一种研究利益冲突主体在理性对抗情况下寻求最优策略的理论,由于在冲突理解和建模方面的价值,被广泛应用于系统安全相关问题。文献[2]将博弈论引入复杂、异构的军事系统,描述了如何用博弈论来分析网络攻击事件。文献[3-4]提出了一种基于动态博弈论的网络安全主动防御模型,但未充分考虑博弈过程中攻防收益问题。文献[5]应用随机博弈建立了攻防博弈模型,通过计算纳什均衡得到双方最优策略,虽然其收益计算较为简单,但具有很好的借鉴意义。文献[6]通过建立贝叶斯博弈模型,使用贝叶斯法则对网络中存在的恶意主机节点概率进行修正,对攻击行为进行预测。文献[7]在贝叶斯博弈的基础上引入粗糙集理论构建了粗糙攻防博弈模型,对攻防策略进行分析。文献[8-10]通过建立非合作博弈模型,对入侵检测场景、攻击概率计算以及攻防实验整体架构进行了分析,但其多将攻防行为看成零和博弈,而在现实网络环境下,攻击防御成本的不同导致了其攻防收益并非完全相等。

针对上述问题,本文给出一种基于非零和博弈的网络防御策略分析方法。首先结合网络安全实际给出网络安全博弈图,在此基础上构建非零和攻防博弈模型,并将攻防意图和网络安全属性相结合,给出攻防成本量化方法,进而通过求解纳什均衡得到最优防御策略。

1　网络安全博弈模型构建

博弈论与网络安全存在密切的联系。博弈论是关于策略相互作用的理论,主要研究理性的团队或个人在一定的目标下,从各自存在的行为策略中进行选择并加以实施,最终取得相应结果的过程。

网络安全包括三个主体:攻击者、网络系统和合法用户。攻击者的目的是尽可能地破坏网络获取资源,而网络系统(常由多台网络设备组成)则希望阻止或减少损失的发生,双方的目标完全对立,不可能达成合作意向;合法用户不论在什

收稿日期:2012-10-12;**修回日期**:2012-12-04。
基金项目:国家自然科学基金资助项目(71171198);湖北省自然科学基金资助项目(2011CDB052)。
作者简介:陈永强(1981-),男,湖北武汉人,博士研究生,主要研究方向:网络与信息安全、系统性能评价;　付钰(1982-),女,湖北武汉人,讲师,博士,主要研究方向:信息系统安全性评估、系统建模与仿真;　吴晓平(1961-),男,山西新绛人,教授,博士,主要研究方向:系统分析与决策、密码算法。

么状态下只希望以较少付出获得尽可能多的网络服务，不会与任一方进行合作。所以网络安全问题本质上是一种多人非合作博弈，整个博弈的过程就是各参与者互相追求各自收益最大化的过程。

在追求收益最大化的过程中，我们假设参与者都是理性的，因此各方均需要选择合适的策略以最小的代价达到目的，但策略的选择并不仅仅取决于参与者的自身条件，三方之间任何一方的策略改变都可能对另外两方的收益产生影响，迫使其改变策略来应对，参与者的策略之间具有相互依存性。

在网络安全问题中，参与者行为都具有特定意图，参与者根据不同意图采取不同的行为，不同行为因其差异性导致收益不同。同时攻击者会选取较易利用、破坏性大的漏洞发动攻击，在获得高收益的同时以降低自身成本；而防御者也会首先修补重要的安全漏洞以尽量降低遭到攻击时的损失。

因此，可将网络安全问题看作是一个多人非合作博弈过程，据此可给出如图 1 的网络安全博弈图。

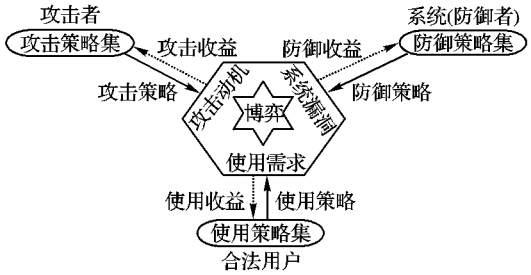

图 1 网络安全博弈图

一般情况下，合法用户对博弈的影响很小，因此在本文攻防博弈模型中其不作为参与者出现。同时考虑到网络攻防对抗过程中攻防双方收益并非完全相等，依据攻击者与系统的博弈关系，在网络安全博弈图的基础上给出如下非零和攻防博弈模型：

非零和攻防博弈模型(Non-zero-sum Attack-Defense Game model，NADG)为一个四元组 $NADG = (P,A,S,U)$，其中：

$P = (P_a,P_d)$ 为参与者集合，其中，P_a 表示攻击者，P_d 表示防御者，即网络系统。在网络攻防对抗过程中，攻防双方是策略选择的主体和制定者。

$A = (A_a,A_d)$ 为攻防动作集，其中，A_a 为攻击行为集，A_d 为防御行为集。

$S = (S_a,S_d)$ 为攻防策略集。攻击者(防御者)选择的一个实际可行的完整的行动方案称为攻击(防御)策略，攻防策略是完整的行动方案所包含动作的概率分布。攻击策略集 $S_a = (s_a^1,s_a^2,\cdots,s_a^m)$，其中 $s_a^i = (p_a^i(a_1),p_a^i(a_2),\cdots,p_a^i(a_t))$ 为攻击者第 i 个策略，$p_a^i(a_j)$ 表示攻击者选用策略 s_a^i 时采取行为 a_j 的概率；同理，防御策略集 $S_d = (s_d^1,s_d^2,\cdots,s_d^n)$，$s_d^j = (p_d^j(d_1),p_d^j(d_2),\cdots,p_d^j(d_l))$。

$\boldsymbol{U} = (\boldsymbol{U}_a,\boldsymbol{U}_d)$ 分别为攻防双方收益函数矩阵。

2 网络攻防收益的量化

2.1 攻防收益量化基础

定义 1 网络设备资产值。其由能够反映网络设备安全特性的机密性、完整性和可用性属性组成，用 $R = (r(C),r(I),r(V))$ 表示。其中 $r(C),r(I),r(V)$ 分别为网络设备在机密性、完整性和可用性方面的资产价值。

定义 2 属性影响因子。其反映了攻击成功后对网络设备安全属性的影响程度，用 $W = (w_C,w_I,w_V)$ 表示。其中 w_C，w_I,w_V 分别为攻击对网络设备机密性、完整性和可用性的影响程度。

定义 3 设备重要度。其用来表示设备在网络中的重要性程度，根据设备类型、所在网络拓扑位置等因素取值，用 η 表示。本文采用文献[11]的量化标准，如表 1 所示。

表 1 主机重要度

等级	类别	设备重要度
1	网关、防火墙	5
2	重要服务器	4
3	普通服务器	3
4	重要主机	2
5	普通主机	1

定义 4 攻防意图类型。攻防意图类型反映了攻防双方的目的和需求，用 $\Theta = (\theta_a,\theta_d)$ 表示。其中 $\theta_a = (\theta_{aC},\theta_{aI},\theta_{aV})$ 为攻击者类型，表明了攻击者对完整性、保密性以及可用性的攻击偏好；$\theta_d = (\theta_{dC},\theta_{dI},\theta_{dV})$ 为防御者类型，表明用户对网络设备完整性、保密性以及可用性的重视程度。

2.2 攻防收益的量化

假设系统对攻击行为 a_t 的检测成功率为 α_t，则攻防双方在安全属性 c_x 上期望值：

$$E_a^{tk}(c_x) = \alpha_t[(1-\lambda_{tk})v_x(W)r(c_x)] + (1-\alpha_t)[v_x(W)r(c_x)] \tag{1}$$

$$E_d^{tk}(c_x) = \alpha_t\lambda_{tk}v_x(W)r(c_x) \tag{2}$$

其中：λ_{tk} 为针对攻击行为 a_t 所采取防御行为 d_k 的防御成功率，$v_x(W)$ 为攻击成功对网络设备安全属性 c_x 的影响权重，$r(c_x)$ 表示被攻击网络设备在安全属性 c_x 上的价值。

若攻防双方采取策略对 (s_a^i,s_d^j)，攻击收益为：

$$u_a(s_a^i,s_d^j) = \sum_{t=1}^{m}s_a^i(a_t)\sum_{k=1}^{n}s_d^j(d_k)r_a(a_t,d_k);$$

$$r_a(a_t,d_k) = \sum_{x=1}^{3}\eta v_x(\theta_a)E_a^{tk}(c_x) - D_a(a_t) \tag{3}$$

其中：(c_1,c_2,c_3) 为设备属性向量，c_1,c_2,c_3 分别表示设备的机密性、完整性和可用性；$v_x(\theta_a)$ 为攻击类型在安全属性 c_x 上的偏好值；$D_a(a_t)$ 为发起攻击行为 a_t 的成本。同理，防御收益为：

$$u_d(s_a^i,s_d^j) = \sum_{k=1}^{n}s_d^k(d_k)\sum_{t=1}^{m}s_a^t(a_t)r_d(a_t,d_k);$$

$$r_d(a_t,d_k) = \sum_{y=1}^{3}\eta v_y(\theta_a)E_d^{tk}(c_y) - D_d(d_k) \tag{4}$$

当攻防双方分别采取混合策略 $S_a = (p_a^1,p_a^2,\cdots,p_a^m)$，$S_d = (p_d^1,p_d^2,\cdots,p_d^n)$ 时，攻防双方混合策略收益[12]可分别表示为：

$$U_a(S_a,S_d) = \sum_{i=1}^{m}\sum_{j=1}^{n}p_a^ip_d^ju_a(s_a^i,s_d^j) \tag{5}$$

$$U_d(S_a,S_d) = \sum_{j=1}^{n}\sum_{i=1}^{m}p_d^jp_a^iu_d(s_a^i,s_d^j) \tag{6}$$

其中：p_a^i,p_d^j 是攻防双方分别选择纯策略 s_a^i,s_d^j 的概率，且 $\sum_{i=1}^{m}p_a^i = 1$，$\sum_{j=1}^{n}p_d^j = 1$。

3 攻防均衡策略的求解

攻击者为了达到攻击目的通常需要实施多个攻击动作，不同的攻击动作组合形成了不同的攻击策略。针对攻击者的

混合策略,结合收益量化方法,给出如下攻防最优防御策略选取算法:

输入　非零和攻防博弈模型 $NADG$。

输出　攻击行为预测及主动防御策略。

1)初始化 $NADG = (P,A,S,\boldsymbol{U})$;

2)依据攻防行为构建攻防策略集 $S_a = (s_a^1, s_a^2, \cdots, s_a^m)$, $S_d = (s_d^1, s_d^2, \cdots, s_d^n)$;

3)对攻击策略集 S_a 中的每一个策略 s_a^i,利用式(1)、(3)计算攻击策略收益 $u_a(s_a^i, s_d^j)$;

4)对防御策略集 S_d 中的每一个策略 s_d^j,利用式(2)、(4)计算各防御策略收益 $u_d(s_a^i, s_d^j)$;

5)由式(5)、(6)计算攻防双方混合策略收益 $U_a(S_a, S_d)$, $U_d(S_a, S_d)$;形成攻防收益矩阵 $\boldsymbol{U}_a$, $\boldsymbol{U}_d$;

6)求解如下线性规划:

$$\max f(S_a,S_d,\boldsymbol{U}_a,\boldsymbol{U}_d) = \sum_{i=1}^{m}\sum_{j=1}^{n} u_a(s_a^i,s_d^j)p_a^i p_d^j + \sum_{i=1}^{m}\sum_{j=1}^{n} u_d(s_a^i,s_d^j)p_a^i p_d^j - v_1 - v_2$$

$$\text{s.t.} \quad \sum_{j=1}^{n} u_a(s_a^i,s_d^j)p_d^j \leqslant v_1; i = 1,2,\cdots,m$$

$$\sum_{i=1}^{m} u_d(s_a^i,s_d^j)p_a^i \leqslant v_2; j = 1,2,\cdots,n$$

$$\sum_{i=1}^{m} p_a^i = 1$$

$$\sum_{j=1}^{n} p_d^j = 1$$

得到混合策略纳什均衡 p_a^*, p_d^*。

7)对得到的纳什均衡解进行分析,预测最有可能的攻击行为,确定主动防御策略。

当攻防双方达到纳什均衡时,攻防双方所选择的策略都是对对方策略的最优反应,攻防双方单方面改变各自的策略都不可能获得更多的收益。

4　算例分析

假定有如图 2 所示拓扑结构的实验网络平台,3 台设备分别是 Web 服务器、File 服务器和 Data 服务器(分别简称为 W/F/D),重要度 η 分别用数字 3、3、4 表示。攻击者目的是获得数据库服务器的 ROOT 权限,攻击影响因子及防御成功率根据历史统计数据并结合管理员经验综合给出。实验网络防火墙规则及初始连接关系如表 2 所示,攻防行为如表 3 与表 4 所示。

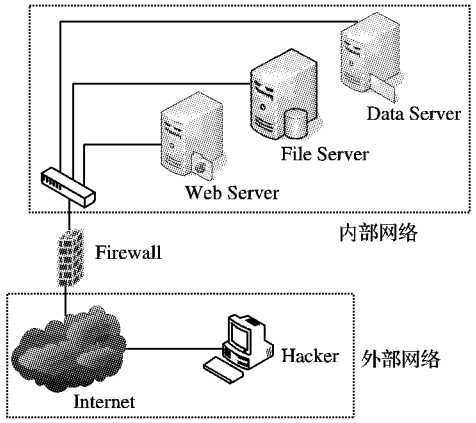

图 2　网络拓扑结构

表 2　防火墙规则及初始连接关系

源设备	目的设备	服务	漏洞
Hacker	WS	HTTP(80)	ap
Hacker	WS	FTP(21)	Wu
Hacker	F	FTP(21)	ftpb
WS	DS	Oracle(1521)	TNS
F	DS	FTP(21)	TNS

表 3　攻击行为信息

代号	攻击行为	影响因子	攻击成本
a_1	ApacheChunked-Enc	{0.6,0.4,0.6}	2
a_2	Wu-FtpdSockPrintf()	{0.5,0.6,0.6}	3
a_3	FTP Bounce	{0.4,0.8,0.5}	5
a_4	Oracle TNS Listener	{1,1,1}	1

表 4　防御行为信息

代号	防御行为	λ	防御成本
d_1	Close rsh on Smtp Sever	0.6	1
d_2	Patch Ftp. rhost on Smtp Sever	0.8	2
d_3	Patch Ftp. rhost on Ftp Sever	0.7	5
d_4	Close rsh on Ftp Sever	0.5	2
d_5	Rmove compromised account	0.9	1
d_6	restart ftpd	0.8	1

表 5　防御措施成功率

λ_{ij}	d_1	d_2	d_3	d_4	d_5	d_6	α
a_1	0.7	0.4	0.6	0.8	0.5	—	0.7
a_2	0.6	0.8	0.4	0.7	0.8	—	0.6
a_3	0.8	0.4	0.5	0.5	0.7	—	0.7
a_4	—	—	—	—	—	0.7	0.8

攻击者从外部网络主机发起多步攻击,第一步攻击者存在三种行为可选择:利用安全漏洞 ap 或 Wu 对 Web 服务器发起攻击 a_1、a_2,或者利用安全漏洞 ftpb 对 File 服务器发起攻击 a_3,取得 Web 服务器或 File 服务器的权限;第二步依靠网络连接关系由已控制的 Web 服务器或 File 服务器出发利用漏洞 TNS 对 Data 服务器发起攻击 a_4,进而实现最终攻击目标。攻防策略如表 6 所示。

表 6　攻防策略

种类	描述	种类	描述
攻击策略	s_a^1: H $\xrightarrow{a_1}$ WS $\xrightarrow{a_4}$ DS	防御策略	s_d^1: H $\xleftarrow{d_1}$ WS $\xleftarrow{d_6}$ DS
	s_a^2: H $\xrightarrow{a_2}$ WS $\xrightarrow{a_4}$ DS		s_d^2: H $\xleftarrow{d_2}$ WS $\xleftarrow{d_6}$ DS
	s_a^3: H $\xrightarrow{a_3}$ WS $\xrightarrow{a_4}$ DS		s_d^3: H $\xleftarrow{d_3}$ WS $\xleftarrow{d_6}$ DS
			s_d^4: H $\xleftarrow{d_4}$ WS $\xleftarrow{d_6}$ DS
			s_d^5: H $\xleftarrow{d_5}$ WS $\xleftarrow{d_6}$ DS

为方便计算,假设 Web 服务器和 File 服务器的安全属性值均为(20,20,20),Data 服务器的安全属性值为(30,30,30),攻击者类型均为 $\theta_a = (1,1,0)$,防御者类型均为 $\theta_d = (1,0,1)$,根据式(1)~(6)可得攻防双方收益:

$$\boldsymbol{U}_a = \begin{array}{c} \\ s_a^1 \\ s_a^2 \\ s_a^3 \end{array} \begin{array}{c} \begin{array}{ccccc} s_d^1 & s_d^2 & s_d^3 & s_d^4 & s_d^5 \end{array} \\ \begin{bmatrix} 151.20 & 168.00 & 156.80 & 145.60 & 162.40 \\ 166.72 & 156.16 & 177.28 & 161.44 & 156.16 \\ 152.64 & 179.52 & 172.80 & 172.80 & 159.36 \end{bmatrix} \end{array}$$

(下转第 1352 页)

A5:$R_e \mid \equiv \varphi(R_{ID} \parallel R)$;

A6:$T \mid \equiv \varphi(T_{ID} \parallel R)$;

A7:$S \mid \equiv \varphi(R \parallel R_{ID}), \varphi(R \parallel T_{ID})$。

2)GNY 逻辑证明。

①$S \ni R, S \ni H(R \parallel R_{ID}), S \mid \equiv \#R$(由 M3 得);

②$S \mid \equiv \#(R \parallel R_{ID} \parallel H_k), S \mid \equiv \#H(R \parallel R_{ID})$(由①新鲜性规则得);

③$S \mid \equiv \#R_e \mid \sim H(R \parallel R_{ID})$(由 A2、A3、A7、② 消息解释规则得);

④$S \mid \equiv R_e \mid \sim \#R, \#H(R \parallel R_{ID})$(由 ②、③ 得)。

至此 O1 完成。

本协议最重要的就是服务器对阅读器与标签的认证,服务器整个认证过程的中介。同理多次利用新鲜性规则与消息解释规则,结合已知条件可以得到下式:

O2:$R_e \mid \equiv S \mid \sim \#H(R_{ID} \parallel R)$

O3:$T \mid \equiv R_e \mid \sim \#H(T_{ID} \parallel R)$

至此完成协议的安全性认证,三方都得到了有效的相互认证,证明该协议符合实际应用的条件。

5 结语

针对现有 RFID 认证协议在安全性与适应环境方面的不足,本文提出了一种基于 Hash 的轻量级认证协议,该协议可以有效防止重放、位置跟踪、伪造等一系列攻击,并适应了移动射频识别系统中阅读器与后端服务器无线通信的环境,同时服务器承担了大部分相对复杂的计算,将成本转移至后端的服务器,有助于大规模应用的实现。并经 GNY 逻辑形式化的推理,证明该协议在逻辑上不存在漏洞,可以满足移动 RFID 系统中三方通信实体身份认证的需求。

参考文献:

[1] WEIS S A. Security and privacy in radio-frequency identification devices [D]. Cambridge: Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, 2003.

[2] WEIS S, SARMA S, RIVEST R, *et al*. Security and privacy aspects of low-cost radio frequency identification systems[C]// Proceedings of Security in Pervasive Computing'04. Piscataway: IEEE Computer Society Press, 2004: 201 - 212.

[3] 曾丽华, 熊璋, 张挺. Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J]. 计算机工程, 2007, 33(3): 151 - 155.

[4] OHKUBO M, SUZUKI K, KINOSHTCA S. Cryptographic approach to "Privacy-Friendly" tags[C]// Proceedings of RFID Privacy Workshop. Cambridge: Massachusetts Institute of Technology Press, 2003: 212 - 219.

[5] 陈信刚. 基于移动网的 RFID 安全接入机制研究[D]. 南京: 南京邮电大学, 2008.

[6] 王新锋, 刘建国, 蒋旭, 等. 移动型 RFID 安全协议及其 GNY 逻辑分析[J]. 计算机应用, 2008, 28(9): 2239 - 2241.

[7] 张亚玲, 张超奇, 马巧梅. 读写器可移动的 RFID 高效认证协议[J]. 计算机工程, 2012, 38(1): 264 - 267.

[8] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]// Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Washington, DC: IEEE Computer Society, 1990: 234 - 248.

[9] 米志强. 射频识别(RFID)技术与应用[M]. 北京: 电子工业出版社, 2011.

[10] 马巧梅, 王尚平. 一个超轻量级的 RFID 认证协议[J]. 计算机工程, 2012, 38(2): 151 - 153.

[11] 邓淼磊, 王玉磊. 无需后端数据库的 RFID 认证协议[J]. 北京邮电大学学报, 2009, 32(4): 59 - 62.

[12] 蔡豪. RFID 安全认证协议的研究与设计[D]. 武汉: 华中科技大学, 2010.

(上接第 1349 页)

$$U_d = \begin{array}{c} \\ s_a^1 \\ s_a^2 \\ s_a^3 \end{array} \begin{array}{c} \begin{array}{ccccc} s_d^1 & s_d^2 & s_d^3 & s_d^4 & s_d^5 \end{array} \\ \begin{bmatrix} 161.28 & 120.96 & 147.84 & 174.72 & 137.40 \\ 136.32 & 151.68 & 109.44 & 141.12 & 151.68 \\ 174.72 & 107.52 & 117.60 & 117.60 & 137.76 \end{bmatrix} \end{array}$$

根据纳什均衡的存在条件[13]:任意有限策略型博弈至少存在一个混合策略纳什均衡。由最优策略选取算法可得最优混合策略均衡解 $S_a = (0.243, 0.645, 0.111)$, $S_d = (0.217, 0, 0, 0.068, 0.715)$。由此可见,攻击者为了达到攻击目标,最可能以 0.243 的概率采取攻击策略 s_a^2,而防御者为了达到最佳防御效果则应主动采取策略 s_d^5 进行防御。

5 结语

本文针对网络安全问题具有利益对立性、策略依存性的特点结合博弈论提出了一种网络安全博弈图。在此基础上,结合实际攻防环境将网络攻防对抗理解为两人非合作、非零和博弈模型,从网络安全属性的角度给出了攻防成本量化方法。实验结果表明,本文所提出的评估模型能有效对攻击行为做出预测,并为系统做好主动防御提供最优防御策略选择。

参考文献:

[1] 林闯, 汪洋, 李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报, 2005, 28(12): 1943 - 1956.

[2] BROWNE R. C 4 I defensive infrastructure for survivability against multi-mode attack[C]// Proceedings of the 21st Century Military Communication - Architectures and Technologies for Information Superiority. Washington, DC: IEEE Computer Society, 2000, 1: 417 - 424.

[3] 林旺群, 王慧, 刘家红, 等. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展, 2011, 48(2): 306 - 316.

[4] 张少俊, 李建华, 陈秀真, 等. 基于动态博弈理论的分布式拒绝服务攻击防御方法[J]. 上海交通大学学报, 2008, 42(2): 198 - 201.

[5] LYE K, WING J M. Game strategies in network security[J]. International Journal of Information Security, 2005, 4(1): 71 - 86.

[6] 曹晖, 王青青, 马义忠, 等. 基于动态贝叶斯博弈的攻击预测模型[J]. 计算机应用, 2007, 27(6): 1545 - 1547.

[7] 王纯子, 黄光球. 基于粗糙贝叶斯博弈的网络攻防策略[J]. 计算机应用, 2011, 31(3): 784 - 789.

[8] HADI O, MONA M, CHADI A, *et al*. Game theoretic models for detecting network intrusions[J]. Computer Communications, 2008, 31(10): 1934 - 1944.

[9] SALLHAMMAR K, HELVIK B E, KNAPSKOG S J. On stochastic modeling for integrated security and dependability evaluation[J]. Journal of Networks, 2006, 1(5): 31 - 42.

[10] 王元卓, 林闯, 程学旗, 等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报, 2010, 33(9): 1748 - 1762.

[11] 司加全, 张冰, 荷大鹏, 等. 基于攻击图的网络安全性增强策略制定方法[J]. 通信学报, 2009, 30(2): 123 - 128.

[12] ROBERT G. A primer in game theory[M]. Princeton: Princeton University Press, 1992.

[13] OSBORNE M J, RUBINSTEIN A, AUMANN R, *et al*. A course in game theory [M]. 2nd ed. Cambridge: MIT Press, 1994.