基于非合作博弈攻击预测的防御策略选取方法

张恒巍 张 健 韩继红
(解放军信息工程大学 郑州 450001)

摘 要 为更好地解决信息安全防御策略的选取问题,针对攻击方和防御方具有的目标对立性、策略依存性和关系非合作性特征,建立了非合作非零和攻防博弈模型。在模型中提出一种改进的收益量化和计算方法,其包含了对防御者反击收益的考虑,能够更加准确地计算博弈均衡。通过对博弈均衡的混合策略进行分析,在理性假设下实现了对攻击动作的有效预测。在攻击预测的基础上,设计了安全防御策略选取算法,其能够针对攻击威胁实现最优防御策略的选取。实例分析验证了模型和方法的有效性。

关键词 非合作博弈,反击收益,混合策略,均衡分析,攻击预测,防御策略选取
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.044

Defense Strategies Selection Method Based on Non-cooperative Game Attack Forecast

ZHANG Heng-wei ZHANG Jian HAN Ji-hong
(PLA Information Engineering University, Zhengzhou 450001, China)

Abstract To better solve the issue of information security defense strategies selection, in view of the characters that attacker and defender's objectives are oppositional, strategies are interdependent and relationship is non-cooperative, the non-cooperative nonzero-sum attack-defense game model was built. In the model, an improved payoff calculation method was presented. The method takes the defender counterattack payoff into account, therefore the equilibrium is calculated more accurately. With analyzing the mixed strategy game equilibrium, attack action can be credibly forecasted based on rationality hypothesis. On the basis of attack action forecast, an algorithm of defense strategies selection was proposed, which can select the optimal defense strategies against the attack threat. The example analysis proves the effectiveness of the model and algorithm.

Keywords Non-cooperative game, Counterattack payoff, Mixed strategy, Equilibrium analysis, Attack forecast, Defense strategies selection

1 引言

攻击方式的复杂化和自动化对信息安全提出了严峻的挑战。目前以防火墙、入侵检测和反病毒软件为主的安全防御技术强调以攻击为中心,检测到攻击后才进行响应,属于被动防御方式,缺乏对攻击预测的能力,在防御策略生效前信息系统可能已经遭受严重的损失[1]。因此研究有效的攻击预测模型和防御策略选取方法具有迫切的现实意义,已经成为研究热点之一[2]。信息安全会受到攻击者和防御者的对抗行为以及行为所造成结果的影响[1-3]。攻防双方之间具有目标对立性、策略依存性、关系非合作性的本质特点[4],这正是博弈论的基本特征。在具有相互对抗特征的环境中,博弈论是有效的决策理论和分析工具[5],其在信息安全领域的应用已成为一个新的发展方向。姜伟等[2]把网络攻击者和防御者作为博弈的局中人,建立二人非合作零和博弈模型,进行网络安全测评和防御策略选取,但是该模型没有考虑局中人类型的不确定性。王元卓等[3]结合随机 Petry 网和博弈论,提出一种基于随机博弈模型的网络攻防量化分析方法,对目标网络进行安全评价并指导最优防御策略的选择。林旺群等[6]通过"虚拟节点"将网络攻防图转化为攻防博弈树,并设计了适用于完全信息攻防博弈的均衡求解算法。刘玉岭等[7]运用静态博弈模型对蠕虫攻防策略的绩效进行评估,帮助安全管理者选择最有效的安全防御策略。石乐义等[8]应用博弈理论对蜜罐诱骗防御机理进行了分析。Carin 等[9]提出了一种用于安全策略有效性分析的网络安全风险量化评估计算方法,其利用攻防博弈模型分析关键基础设施防护策略的效能。Gueye 等[10]以病毒攻击为例,分析了病毒设计者、数据篡改者与防御者之间的博弈关系并给出防御策略。上述研究都将信息安全视作攻击者与防御者的博弈过程,通过攻防双方的策略、收益以及博弈均衡来研究不同的问题。目前,基于攻防博弈的安全策略选取方法存在两个问题:(1)将攻防博弈中均衡局势下的混合策略定义为攻击者和防御者的最优策略。现实中具体的攻防博弈场景下,攻击者和防御者实施的都是纯策略,攻击者对目标系统在某时刻采用的攻击手段是明确的、唯一的,

到稿日期:2014-12-30 返修日期:2015-04-03 本文受国家自然科学基金项目(61303074,61309013),国家重点基础研究发展计划("973"计划)基金项目(2012CB315900),河南省科技攻关计划项目(12210231003,13210231002)资助。
张恒巍(1978—),男,博士生,讲师,主要研究方向为信息安全态势分析与预测、需求工程,E-mail:zhw11qd@126.com;张 健(1989—),男,硕士生,主要研究方向为安全风险分析;韩继红(1966—),女,博士,教授,博士生导师,主要研究方向为网络与信息安全、云资源管理。

防御者为信息系统设置的防御策略也是明确和唯一的。因此，直接采用均衡下的混合策略定义攻防双方的最优策略，实用性较差。(2)未将防御者反击收益纳入攻防双方博弈收益的计算中。在信息安全对抗中，无论防御者能否成功抵御攻击，都可以通过反击行为获得收益。例如，在攻防过程中，防御者能收集攻击的方式、序列、规模、路径等信息，通过数据分析、模式识别、逆向追踪等技术，搜索甚至识别攻击源或攻击者身份，然后利用法律手段追责或实施反制攻击，这些措施能形成威慑，降低攻击威胁和攻击收益。因此，应改进博弈收益的计算方法，在考虑防御者反击收益的基础上综合计算双方收益，准确求解博弈均衡。

本文对安全防御策略选取问题进行了形式化描述，由此提出一种二人非合作非零和攻防博弈模型 NSADG(Nonzero-Sum Attack-Defense Game)。NSADG 按攻击者类型构建博弈场景，并对其分别进行研究，综合考虑攻击者与防御者之间的利益矛盾关系，将防御者反击收益纳入攻防双方的收益考察中，计算攻击收益和防御收益，求解博弈均衡。通过分析构成均衡的混合策略，得到不同攻击动作的可能概率，实现对理性攻击者行为的可信预测。在此基础上，设计了一种安全防御策略选取算法，其能够针对攻击威胁选取最有效的防御纯策略，为安全管理人员的决策提供有效建议。

2 防御策略选取问题描述

在信息安全管理中，防御策略的实施能够减少攻击所造成的损失，但同时会增加防御成本，两者之间如何权衡，如何选取最优防御策略，是安全管理员面临的关键问题。防御策略的选取不仅要考虑防御成本，更要考虑资产关键度和可能的攻击方式。防御策略对不同攻击动作的抵御效果是不同的，一种防御策略可能对某个攻击动作抵御效果很好，而对其它攻击动作无效，所以选择防御策略要综合考虑应对攻击时的有效性、防御成本、后果影响等因素。要想充分发挥防御策略的效能，必须在对攻击动作可信预测的基础上，有针对性地选择综合效果最好的防御策略。

根据上述分析，在借鉴文献[3]的基础上，定义防御策略选取问题如下。

定义 1 称 $f_{select}:(IA,AS,DS,SC,G)\rightarrow D_{best}$ 为防御策略选取函数。各项元素的含义如下：

IA，即信息资产集合。信息资产可以是服务器、路由器等硬件类实体，也可以是敏感文件、信息服务等软件类实体，或者综合类实体，如提供文件下载服务的 FTP 服务器。

AS，即攻击策略集合(不采取攻击动作也是一种攻击策略，即 $\emptyset\in AS$)。攻击策略 $A\in AS$ 代表攻击者对信息系统的某个攻击动作，只有对攻击 A 进行可信预测，才能选择具有针对性的防御策略，提高安全防御的效能。

DS，即防御策略集合(不采取防御措施也是一种防御策略，即 $\emptyset\in DS$)。例如针对蠕虫病毒，采取主动防御策略 $D=$(吞噬蠕虫：Nullifying Worm)，$D\in DS$。

SC，即策略成本。表示攻击者和防御者使用某策略时需要付出的代价值。

G，即攻防博弈模型。可以根据具体的信息安全环境建立合适的攻防博弈模型，例如本文第 3 节建立的 NSADG 模型。

D_{best}，即选取的最优防御策略集合，且 $D_{best}\subseteq DS$。f_{select} 是从 (IA,AS,DS,SC,G) 到最优防御策略 D_{best} 的映射。对于任意 i、j，有 $(IA_i,AS_i,DS_i,SC_i,G_i)\rightarrow D^i_{best}$，$(IA_j,AS_j,DS_j,SC_j,G_j)\rightarrow D^j_{best}$，如果 $(IA_i,AS_i,DS_i,SC_i,G_i)=(IA_j,AS_j,DS_j,SC_j,G_j)$，则 $D^i_{best}=D^j_{best}$。

针对给定的 (IA,AS,DS,SC,G) 信息，研究基于攻防博弈模型 NSADG 的最优安全防御策略选取方法，简称最优防御策略选取。

3 攻防博弈模型 NSADG

在信息安全博弈中，一方面，攻击者和防御者之间具有目标对立和关系非合作的特点；另一方面，攻击动作和防御动作的实施要支付相应的代价，双方的收益之和不为零，因此根据二人非合作非零和博弈的基本理论建立攻防博弈模型——NSADG。在攻防博弈过程中，双方都倾向于选择使自己的期望收益达到最大化的策略，最终各参与者会达到一种均衡，即纳什均衡。此时，任何参与者改变其策略所获得的收益都不会大于均衡状态下的收益[5]，因此双方都无利益动机偏移均衡策略。

从上述基本理论出发，定义 NSADG 模型中纳什均衡下攻击者所采取的混合策略，来代表实际博弈中攻击者采取各种纯策略(攻击动作)的概率。如同天气预报是对未来天气变化概率的预测，在遵循基本假设的前提下，利用纳什均衡下的攻击者混合策略形成对攻击动作的预测。这一攻击预测由于符合理性假设和利益假设，具有较高的可信性。在此基础上，针对各个防御策略(纯策略)分别进行分析，能够确定最优防御策略，为安全管理人员提供决策支持。

3.1 模型基本假设

实际的信息安全攻防博弈中，攻击者往往是博弈的发起者，防御者依据现有的策略进行应对，任何一方在行动之前都无法观测到对方的行动，因此双方可以看作是同时行动。攻防博弈模型的建立满足如下 3 个基本假设。

假设 1(理性假设)　假设攻击者和防御者是完全理性的，攻击者和防御者都按照使自己收益最大的原则选取策略。

对于非理性攻击者，其追求最大收益而不考虑代价，只需要对能使其获得最大收益的策略进行研究即可。而理性攻击者行为较复杂，更加具有研究意义。

假设 2(利益假设)　假设依据信息资产的经济价值评价博弈收益。

假设 3(类型假设)　假设防御者对攻击者类型的概率分布有先验判断，而防御者类型为攻击者与防御者的共有信息。

依据防御者对攻击者的认识，可将攻击者分为冒险型攻击者 P_a^H 和保守型攻击者 P_a^L，冒险型攻击者愿意支付更多的成本，进行更大频率、更长时间的攻击，以获得更高的攻击成功率；但是被防御者收集相关信息和证据，进而实施法律追责或反制攻击的概率也较高。保守型攻击者倾向于以较少的成本来进行攻击，其攻击成功率相对较低；但被法律追责或反制攻击的概率也较低。

3.2 模型定义

一般来说，一个攻防博弈的组成要素主要包括局中人(Player)、策略集(Strategy)和收益函数(Payoff Function)。攻防双方的策略执行效果不仅仅与其自身的策略有关，还与对方的策略密切相关，这就是“策略依存”原理，是博弈过程的基本特点。

定义 2(攻防博弈模型,NSADG) 信息安全攻防博弈可以定义为一个五元组 $NSADG=(P,B,F,AS,DS)$。模型中各项元素的含义如下:

(1)$P=(P_a,P_d)$表示博弈的参与者集合。参与者是策略制定和策略选择的主体,大部分信息安全博弈可以看成是攻击者 P_a 和防御者 P_d 的二人博弈。

(2)B 表示攻击者和防御者的先验信念空间。$B(P_a^H)$和 $B(P_a^L)$是防御者对攻击者类型推断的先验信念,$B(P_d)$是攻击者对防御者类型推断的先验信念。其中,$B(P_a^H)=q$,$B(P_a^L)=1-q$,$B(P_d)=1$。

(3)$F=\{f_a,f_d\}$是参与者 P_a 和 P_d 的收益函数。反映了参与者的收益,当采用不同的策略进行博弈时,会得到不同的博弈结果,收益也会不同。

(4)AS、DS 是攻击者和防御者的行动空间。在本文中,定义攻击者行动空间为攻击策略集合 $AS=\{A_i\mid 1\leqslant i\leqslant m\}$,防御者行动空间为防御策略集合 $DS=\{D_j\mid 1\leqslant j\leqslant n\}$。

3.3 收益量化与计算方法

定义 3(攻击策略成本,Attack Cost,AC) 表示采用某一攻击策略发动攻击所耗费的代价。可以从经济、时间、软硬件资源和人工代价等方面进行量化。根据类型假设,本文将攻击策略 A_i 的成本分为冒险型攻击策略成本 AC_i^H 和保守型攻击策略成本 AC_i^L。

定义 4(防御策略成本,Defense Cost,DC) 表示采用某一防御策略进行防御所耗费的代价 DC_j,是防御策略的操作代价、负面代价和残余代价之和。

攻击策略成本和防御策略成本的详细定义及相应计算方法参见文献[2,4]。

定义 5(攻击回报,Attack Reward,AR) 攻击回报表示一次攻击成功后攻击者获得的回报,一般用信息系统的损失表示。攻击策略回报用$|A_i|$([0,100]内的整数)表示,参考 MIT 林肯实验室攻击分类[11]和美国国家漏洞数据库 NVD (National Vulnerability Database)[12]评价数据,制定攻击回报量化评价标准,如表 1 所列。

表 1 收益量化评价

攻击回报	攻击描述	防御回报	防御描述
90	有致命威胁,将造成系统巨大损失	90	完全遏制了攻击策略,最大限度地保护系统资产
70	有重大威胁,将造成系统严重损失	70	有效遏制了攻击策略,保护大部分系统资产
50	有一定威胁,将造成系统部分损失	50	发挥一定遏制作用,保护部分系统资产
30	有轻度威胁,将造成系统较少损失	30	遏制效果较弱,系统资产遭受一定损失
10	几乎没有威胁,将造成系统极少量损失	10	基本没有遏制效果,系统资产遭受严重损失

定义 6(防御回报,Defense Reward,DR) 表示针对某一攻击策略采取防御策略后防御者的回报情况。防御策略回报分为两类,分别用$|D_j|$和$|D_j'|$(均为[0,100]内的整数)表示。$|D_j|$表示在攻击成功的情况下,防御策略的实施能够降低的信息资产损失。$|D_j'|$表示在受到攻击的情况下,防御者收集相关信息和证据进而对攻击者实施法律追责或反制攻击所取得的回报。防御回报的量化评价标准如表 1 所列。

在信息安全对抗中,无论防御者能否成功抵御攻击,都可以通过反击行为获得收益。例如,防御者在采取防御动作的同时,可以收集攻击行为信息,例如攻击的方式、序列、规模、路径等,然后利用法律手段追责或实施反制攻击,这些措施不但能为防御者带来直接回报,降低攻击者的收益,而且能对攻击者形成威慑,降低未来的攻击威胁,本文将这种形式的防御回报定义为$|D_j'|$。由上述分析可知,无论攻击成功或失败,防御回报$|D_j'|$都会发生。因此,在攻击成功和攻击失败两种情况下,博弈双方的收益计算都必须考虑$|D_j'|$。现实环境中,如果一个组织重视信息安全,其对攻击者的法律追责或反制攻击也会比较严厉,因此$|D_j|$和$|D_j'|$一般具有正相关关系,但是具体的关系表述还需进一步研究。

定义 7(攻击成功率) 攻击成功率 p_{ij}($p_{ij}\in[0,1]$)指攻击者、防御者采取相应攻击、防御策略时攻击策略成功的概率,可通过对历史数据统计分析得出。p_{ij} 受双方策略的针对性影响很大,例如防御策略 D_1 对攻击策略 A_1 的抵御效果可能很好,但是对 A_2 的抵御效果就可能较差。

根据上述定义,得到攻击者的策略描述元组($|A_i|$,AC_i)和防御者的策略描述元组($|D_j|$,$|D_j'|$,DC_j),建立起攻防博弈场景。下面针对冒险型攻击者、保守型攻击者和防御者之间的博弈,研究攻防双方的收益计算方法。

当冒险型攻击者和防御者进行博弈时,双方的收益计算公式详见表 2。

表 2 冒险型攻击者和防御者博弈的收益计算公式

	攻击成功
攻击者 P_a^H 收益	$a_{ij}\mid_{win}=f_a(A_i,D_j)\mid_{win}=\lvert A_i\rvert-\lvert D_j\rvert-\lvert D_j'\rvert-AC_i^H$
防御者 P_d 收益	$d_{ij}\mid_{lose}=f_d(A_i,D_j)\mid_{lose}=-\lvert A_i\rvert+\lvert D_j\rvert+\lvert D_j'\rvert-DC_j$
	攻击失败
攻击者 P_a^H 收益	$a_{ij}\mid_{lose}=f_a(A_i,D_j)\mid_{lose}=-\lvert D_j'\rvert-AC_j^H$
防御者 P_d 收益	$d_{ij}\mid_{win}=f_d(A_i,D_j)\mid_{win}=-\lvert D_j'\rvert-DC_j$

对于冒险型攻击者,假设攻击成功率为 p_{ij}^H,可以得到攻击者和防御者的收益期望:

$$a_{ij}^H=p_{ij}^H(|A_i|-|D_j|-|D_j'|-AC_i^H)+(1-p_{ij}^H)(-|D_j'|-AC_i^H) \tag{1}$$

$$d_{ij}^H=p_{ij}^H(-|A_i|+|D_j|+|D_j'|-DC_j)+(1-p_{ij}^H)(|D_j'|-DC_j) \tag{2}$$

将式(1)、式(2)两式相加,得到该博弈场景中的收益和为

$$a_{ij}^H+d_{ij}^H=-(AC_i^H+DC_j) \tag{3}$$

当保守型攻击者和防御者进行博弈时,假设策略成功率为 p_{ij}^L,同理可以得到双方的收益期望:

$$a_{ij}^L=p_{ij}^L(|A_i|-|D_j|-|D_j'|-AC_i^L)+(1-p_{ij}^L)(-|D_j'|-AC_i^L) \tag{4}$$

$$d_{ij}^L=p_{ij}^L(-|A_i|+|D_j|+|D_j'|-DC_j)+(1-p_{ij}^L)(|D_j'|-DC_j) \tag{5}$$

此博弈场景的双方收益和为

$$a_{ij}^L+d_{ij}^L=-(AC_i^L+DC_j) \tag{6}$$

综合式(3)、式(6)可知,在信息安全博弈中攻击者和防御者的收益之和为负值,即此博弈为负和博弈。也就是说,每一轮博弈中无论双方收益如何,都必然会有成本损失,因此采用较高成本的策略在总体统计上对双方都是不利的。

根据式(1)、式(2)、式(4)、式(5)进行计算,得到冒险型攻击者和防御者之间 $m\times n$ 的纯策略收益期望矩阵,记为 M_a^H 和 M_d^H;保守型攻击者和防御者之间的收益期望矩阵为 M_a^L 和 M_d^L。攻击者和防御者之间构成双矩阵非零和博弈,收益矩阵如图 1 所示。

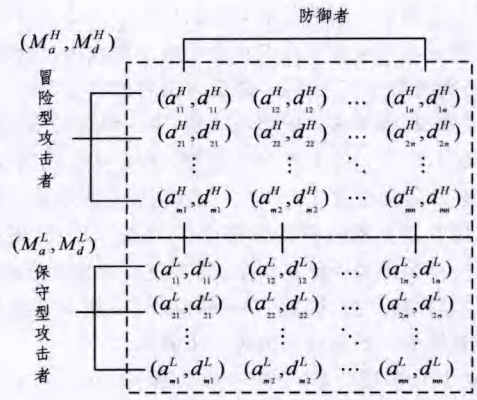

图 1　收益矩阵

综上可知，在 NSADG 模型中，无论博弈结果如何，攻防双方都要消耗成本，导致双方的收益之和为负值。这同信息安全基本理论一致，说明攻防博弈是一个利益在攻击者和防御者之间转移的过程，而该过程中双方策略的应用必然消耗成本。攻击策略成功和失败时的博弈态势如图 2 和图 3 所示。

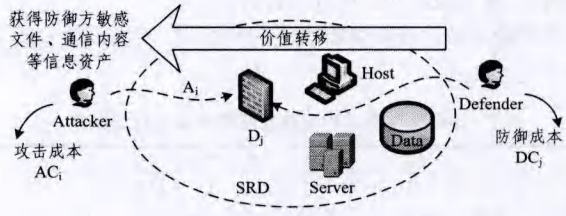

图 2　攻击成功时的博弈态势

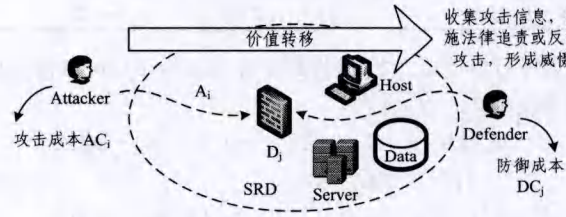

图 3　攻击失败时的博弈态势

4　基于博弈均衡的攻击预测

在信息安全博弈中，攻防双方在给定自己的类型和先验信念空间的情况下，都希望最大化自己的期望收益。依据博弈基本理论[5]，在完全纯策略的情况下，博弈均衡的存在性无法保证。同时，由于纯策略可看作对应策略的选择概率为 1、其余策略的选择概率为 0 的混合策略，因此，本文使用混合策略进行 NSADG 模型的博弈均衡分析。均衡局势下攻击者的混合策略代表了攻击方采用各种纯策略的概率，是理性假设和利益假设下对攻击者实际行为的可信预测。

设攻击者和防御者分别依据概率向量 $(x_1, x_2, \cdots, x_m)$、$(y_1, y_2, \cdots, y_n)$ 选择攻击策略 A 和防御策略 D，则攻击者和防御者的混合策略为

$$X=\{x=(x_1,x_2,\cdots,x_m)\mid \sum_{i=1}^{m}x_i=1, x_i\geqslant 0\}$$
$$Y=\{y=(y_1,y_2,\cdots,y_n)\mid \sum_{j=1}^{n}y_j=1, y_j\geqslant 0\} \tag{7}$$

由于攻击者和防御者在行动之前都无法观测到对方的行动，因此双方的策略选择可以认为是独立、同时进行的。定义攻击者的收益期望为 E_a，防御者的收益期望为 E_d。

$$E_a=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_iy_j, E_d=\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_iy_j, a_{ij}\in M_a, d_{ij}\in M_d \tag{8}$$

由博弈均衡的定义可知，均衡策略的收益期望值 E_a 和 E_d 优于其它任何策略。根据二人非合作有限博弈的基本理论，利用布鲁韦尔不动点定理[13]，可以得到 NSADG 模型的纳什均衡存在性定理。

定理 1　对于信息安全攻防博弈 NSADG，必定存在混合策略 (x^*, y^*) 构成纳什均衡，且 (x^*, y^*) 满足如下条件：

$$\begin{cases}\forall x_i, \sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_i^*y_j^*\geqslant\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_iy_j^*\\ \forall y_j, \sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_i^*y_j^*\geqslant\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_i^*y_j\\ \sum_{i=1}^{m}x_i=1 \text{ 且 } x_i\geqslant 0\\ \sum_{i=1}^{m}y_j=1 \text{ 且 } y_j\geqslant 0\end{cases} \tag{9}$$

其中，x^* 和 y^* 分别称为攻击者和防御者的最优混合策略（Optimal Mixed Strategy），当某个纯策略的选取概率为 1 时，混合策略退化为纯策略。在纳什均衡下，攻击者和防御者的收益分别是

$$E_a^*=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_i^*y_j^*, E_d^*=\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}x_i^*y_j^* \tag{10}$$

定理 1 说明当攻击者选择策略 $x^*=(x_1^*, x_2^*, \cdots, x_m^*)\in X$、防御者选择策略 $y^*=(y_1^*, y_2^*, \cdots, y_m^*)\in Y$ 时，双方的收益均达到最优。

综上，可以得出混合策略 $x^*=(x_1^*, x_2^*, \cdots, x_m^*)$ 是攻击者最优选择的结论，因此在遵循理性假设和利益假设的前提下，该混合策略 x^* 即为攻击动作的可信预测。在此基础之上，可以对各个防御策略（纯策略）的防御效果进行对抗性分析和评价，选取最优防御策略。

5　最优防御策略选取方法

5.1　最优防御策略选取方法

以基本假设和博弈模型为基础，通过第 3 节的分析实现了对攻击动作的可信预测。从信息安全防御的实际出发，防御者一般不了解攻击者的类型信息，同时防御者所采取的策略在某一时间段内是固定的、明确的，不存在按概率配置防御策略的情况，因此混合策略难以对防御方进行直接有效的指导。

针对这一实际问题，基于纯防御策略 $y_j=(0,0,\cdots,y_j=1,\cdots,0)$（即纯策略 D_j），结合对攻击行为的预测（即混合策略 x^*），可通过式(10)计算攻击者的收益期望，以此量化信息系统的损失，利用系统损失评价纯防御策略的效能，帮助安全管理人员选取最优防御策略。

假设基于前述方法，对冒险型攻击者和保守型攻击者的预测结果分别为 $x_H^*=(x_{H1}^*, x_{H2}^*, \cdots, x_{Hm}^*)$ 和 $x_L^*=(x_{L1}^*, x_{L2}^*, \cdots, x_{Lm}^*)$，如果防御者采用的纯防御策略是 $y_j=(0,0,\cdots,y_j=1,\cdots,0)$（即纯策略 D_j），则冒险型攻击者造成的系统期望损失为 L_j^H，保守型攻击者造成的系统期望损失为 L_j^L。

$$L_j^H=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_{Hi}^*y_j, L_j^L=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_{Li}^*y_j \tag{11}$$

结合攻击者类型的先验概念 $B(P_a^H)$ 和 $B(P_a^L)$，得到使用纯防御策略 y_j 时信息系统总的期望损失 L_j。

$$L_j=B(P_a^H)\cdot L_j^H+B(P_a^L)\cdot L_j^L \tag{12}$$

选取使信息系统期望损失 L_j 最小的纯防御策略 D_j 作为最优防御策略。

基于上述分析结论，提出最优防御策略选取算法，具体描述如下。

算法输入：攻防博弈模型 NSADG；攻击策略成本向量 AC^H 和 AC^L，防御策略成本向量 DC；攻击成功率向量 p^H 和 p^L；攻击者类型的先验信念 q[k]；Gambit[14] 中均衡求解算法 NE(M_a,M_d)

算法输出：最优安全防御策略 D_{best}

算法描述：

1. Begin
2. $x_H^*=(x_{H1}^*,\cdots,x_{Hm}^*)=0$；$x_L^*=(x_{L1}^*,\cdots,x_{Lm}^*)=0$；
   //初始化攻击者和防御者混合策略
3. $M_a^H[i][j]=[0]$，$M_d^H[i][j]=[0]$；
   $M_a^L[i][j]=[0]$，$M_d^L[i][j]=[0]$；
   //初始化收益矩阵
4. for (i=1;i=i+1;i<=m)
   { //计算冒险型攻击者收益矩阵 M_a^H 和 M_d^H
5. for (j=1;j=j+1;j<=n)
   {
6. $a_{ij}^H=p_{ij}^H(|A_i|-|D_j|-|D_j'|-AC_i^H)+(1-p_{ij}^H)(-|D_j'|-AC_i^H)$
7. $d_{ij}^H=p_{ij}^H(-|A_i|+|D_j|+|D_j'|-DC_j)+(1-p_{ij}^H)(|D_j'|-DC_j)$
   }
   }
8. $x_H^*=NE(M_a^H[i][j],M_d^H[i][j])$；
   //计算冒险型攻击者 Nash 均衡下的混合策略
9. for(i=1;i=i+1;i<=m)
   { //计算保守型攻击者收益矩阵 M_a^L 和 M_d^L
10. for (j=1;j=j+1;j<=n)
   {
11. $a_{ij}^L=p_{ij}^L(|A_i|-|D_j|-|D_j'|-AC_i^L)+(1-p_{ij}^L)(-|D_j'|-AC_i^L)$
    $d_{ij}^L=p_{ij}^L(-|A_i|+|D_j|+|D_j'|-DC_j)+(1-p_{ij}^L)(|D_j'|-DC_j)$
    }
   }
12. $x_L^*=NE(M_a^L[i][j],M_d^L[i][j])$；
    //计算保守型攻击者 Nash 均衡下的混合策略
13. for (j=1;j=j+1;j<=n)
    { //计算不同纯防御策略下系统的期望损失
14. $(y_1,y_2,\cdots,y_m)=0$；
15. $y_j=1$；//设定当前纯防御策略为 D_j
16. $L_j^H=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_{Hi}^*y_j$；
    //计算冒险型攻击者造成的系统期望损失
17. $L_j^L=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_{Li}^*y_j$
    //计算保守型攻击者造成的系统期望损失
18. $L_j=q[k]L_j^H+(1-q[k])L_j^L$
    //计算信息系统总的期望损失
    }
19. $D_{best}=\text{argmin}\{L_j|D_j\}$
    //选取使 L_j 最小的纯防御策略 D_j 作为最优防御策略
20. return D_{best}
21. End

算法利用 NSADG 模型，基于攻击预测方法，对使用不同纯防御策略时系统的期望损失进行了量化计算，选取使期望损失最小的策略作为最优防御策略。算法的时间复杂度主要集中在收益计算部分，为 $O(m\cdot n\cdot|P_a|)$，其中 $|P_a|$ 代表攻击者的类型数量，本文取值为 2；算法的空间消耗大部分在于收益矩阵的存储。

5.2 博弈模型和策略选取方法的比较

将本文提出的博弈模型和策略选取方法同文献[2,3,6,7]在攻击者类型、防御者类型、收益量化、可操作性、时间复杂度等方面进行分析比较，结果如表 3 所列。

表 3 博弈模型和策略选取方法的比较

文献	攻击者类型	防御者类型	收益量化	可操作性	时间复杂度
文献[2]	1	1	未考虑防御方反击收益	一般(混合策略)	O(m·n)
文献[3]	2	1	未给出回报和成本的具体计算方法	一般(混合策略)	O(m·n·|Pa|)
文献[6]	1	1	未考虑防御方反击收益	一般(混合策略)	O(m·n)
文献[10]	2	1	未考虑攻击成功率； 未考虑防御方反击收益	较差 (未给出具体的策略选择算法)	O(m·n·|Pa|)
本文	2	1	同时考虑攻击成功率和反击收益	较好(纯策略)	O(m·n·|Pa|)

与文献[2,6]相比，本文提出的模型和策略选取方法在考虑攻击者类型的基础上分别构建博弈场景，更加符合实际，适用性更好。在收益量化计算方面，其它文献大多设计简单，未将防御者反击收益纳入博弈收益的计算中，而本文的收益量化同时考虑了攻击成功率和反击收益，更加全面和准确。可操作性是指文献给出的方法为用户所选取的最佳防御策略是否具有较强的实用性和指导作用。对于防御者而言，在确定的时间只能选取一种防御策略，因此以概率形式给出的混合策略实用性较差，难以为安全管理人员的决策提供指导，而通过计算纯防御策略效能，以纯策略形式给出的策略选取方案具有更好的可操作性。策略选取算法的时间复杂度主要集中在博弈收益的计算上，各文献方法基本相同。

6 实例分析

6.1 实验系统描述

为验证提出的攻防博弈模型、攻击预测和防御策略选取方法，本文采用如图 4 所示的网络拓扑结构来模拟攻防情景进行实验。

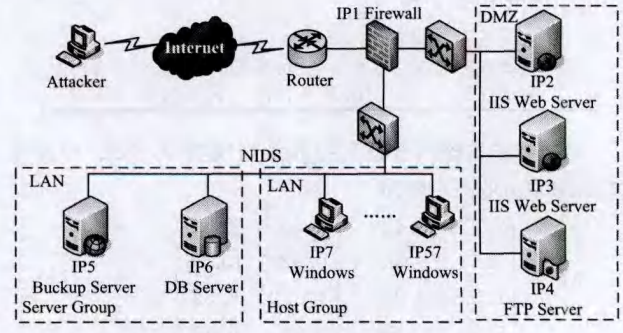

图 4 实验网络环境

攻击主机位于外部网络，目标信息系统是交换网络，包括 57 台节点机器。设置有 3 台服务器，分别用于提供数据库服务、文件服务和备份服务。IP6 信任 IP5，IP6 为数据库服务

器，存有各种敏感信息。由于防火墙的存在，非本地主机只能访问 DMZ 区的服务器，IP2 和 IP3 可以利用网络服务访问 IP6的数据，但是却被禁止访问 LAN 内其他主机。假设外网的攻击者试图获取数据库服务器中的数据。服务器和主机提供的服务以及存在的漏洞如表 4 所列。

表 4　实验网络系统的漏洞情况

Host-ID	Vulnerability ID	Vulnerability-Description	Result
IP1	12918	Telnet Overflow	Root
IP2	8668	Wu-ftpd 远程打印漏洞	Root
IP3	4855	IIS 缓冲区溢出漏洞	Root/DoS
IP4	8628	(1)OpenSSH 3.3 Buffer Overflow;(2)弱口令漏洞	Root
IP5	38115	Oracle TelCommand Execute	Root
IP7－IP57	31874	Windows Server TeleRpc Overflow	Root

防御策略是各项防御措施的结合，考虑资金限制、安全措施对业务的影响和相关专家建议，系统可供选择的防御策略如表 5 所列，其中“√”表示防御策略中所包含的安全措施。

表 5　防御策略及描述

防御措施	防御策略 D_1	防御策略 D_2	防御策略 D_3	防御策略 D_4
更新 22918 补丁		√	√	
更新 4648 补丁	√	√	√	
更新 5875 补丁	√	√	√	√
更新 2638 补丁	√	√		√
更新 71674 补丁		√		√
使用高强度口令	√		√	
禁止访问端口	√		√	
变更信任关系	√			√
网络访问控制	√		√	√
防御策略描述	(45,42,8)	(20,18,5)	(24,24,6)	(38,36,8)

6.2　攻防双方收益计算

假设防御者对攻击者类型的先验信念为：(冒险型，保守型)=$(B(P_a^H),B(P_a^L))=(0.4,0.6)$。设冒险型攻击者的策略包括缓冲区溢出攻击 A1(68,9)、木马攻击 A2(56,6)、计算机病毒攻击 A3(46,3)和拒绝服务攻击 A4(64,4) 4 种策略。策略成功率如表 6 所列。

表 6　攻击策略成功率

防御策略 \ 攻击策略	策略 A_1	策略 A_2	策略 A_3	策略 A_4
策略 D_1	0.60	0.65	0.75	0.55
策略 D_2	0.78	0.96	0.94	0.82
策略 D_3	0.58	0.88	0.72	0.83
策略 D_4	0.48	0.72	0.64	0.45

根据攻防策略的描述元组和策略成功率，由式(1)和式(2)计算双方收益矩阵为

$$M_a^H=\begin{pmatrix}7.83 & 6.42 & -8.56 & 4.60\\ 6.42 & 9.84 & 0.92 & 15.76\\ 7.52 & 3.20 & -12.72 & 7.52\\ 7.20 & 10.84 & 6.61 & 6.70\end{pmatrix}$$

$$M_d^H=\begin{pmatrix}-22.82 & -18.42 & -8.44 & -18.60\\ -18.41 & -18.84 & -13.08 & -26.76\\ -16.48 & -9.21 & 1.72 & -15.52\\ -17.22 & -17.81 & -18.61 & -15.70\end{pmatrix}$$

6.3　攻击预测和最优防御策略选取

将 M_a^H 和 M_d^H 输入博弈工具 Gambit，计算冒险型攻击者和防御者在博弈均衡下的混合策略。

$$x_H^*=\begin{pmatrix}A_1 & A_2 & A_3 & A_4\\ 0.02 & 0.16 & 0 & 0.82\end{pmatrix}$$

$$y_H^*=\begin{pmatrix}D_1 & D_2 & D_3 & D_4\\ 0.885 & 0 & 0.024 & 0.091\end{pmatrix}$$

由上文的分析可知，冒险型攻击者的混合策略 $x_H^*=(0.02,0.16,0,0.82)$是对攻击者行为的可信预测。攻击者最有可能采用的策略是“拒绝服务攻击”。虽然“拒绝服务攻击”的收益不是最大的，但凭借较低的攻击成本和较高的成功率，该策略取得的收益期望最大，成为了攻击者最有可能选择的策略。

防御者采用的策略是固定、明确的。设防御者采用的防御策略为 D_1，则根据式(11)计算冒险型攻击者可能造成的系统损失。

$$L_1^H=a_{11}\cdot x_{H1}^*+a_{21}\cdot x_{H2}^*+a_{31}\cdot x_{H3}^*+a_{41}\cdot x_{H4}^*$$
$$=0.02\times7.83+0.16\times6.42+0.82\times7.2=7.1$$

同理，设计算得到的保守型攻击者可能造成的系统损失为

$$L_1^L=a_{11}\cdot x_{L1}^*+a_{21}\cdot x_{L2}^*+a_{31}\cdot x_{L3}^*+a_{41}\cdot x_{L4}^*=4.5$$

结合对攻击者类型的先验信念，由式(12)可以得到防御者采用策略 D_1 时，信息系统总的期望损失为

$$L_1=B(P_a^H)\cdot L_j^H+B(P_a^L)\cdot L_j^L=0.4\times7.1+0.6\times4.5$$
$$=5.54$$

依据同样的流程，可以计算防御者采用策略 D_2、D_3、D_4 时信息系统总的期望损失。设计算得到的数值为 $L_2=6.71$，$L_3=10.26$，$L_4=7.98$，则信息系统的最优防御策略是 D_1。

结束语　本文在形式化描述最优防御策略选取问题的基础上，建立了二人非合作非零和攻防博弈模型，将攻击者按先验信念进行分类，分别构建博弈场景进行研究。在博弈收益的量化和计算中，将防御者反击收益纳入考查范围，综合考虑攻击者与防御者之间的利益矛盾关系，提出一种更加准确的收益计算方法。基于攻防博弈模型，通过分析均衡局势的混合策略，实现了对攻击行为的可信预测。在上述基础上，设计了一种最优防御策略选取算法，它利用攻击预测结果评价系统使用不同防御策略时的期望损失，并选取期望损失最小的策略为最优防御策略。该方法能够针对攻击威胁选取最有效的纯防御策略，为安全管理人员的决策提供直接、有效的帮助。实例分析验证了模型和方法的有效性。

下一步的研究工作将集中在两个方向：一方面，由于完全信息的类型假设限制了模型和方法的使用范围，可以考虑基于静态贝叶斯博弈模型进行分析研究。另一方面，由于攻防行为都是人在环路的控制过程，人不可能是完全理性的，采用基于有限理性假设的演化博弈模型进行研究将会更加贴近实际。

参 考 文 献

[1] Fang Bin-xing. Explain the innovation and breakthrough of information security [EB/OL]. http://www.Cert.org.crdarticles/news/common/2012051823317.html

[2] Jiang Wei, Fang Bin-xing, Tian Zhi-hong, et al. Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model [J]. Chinese Journal of Computers, 2009, 32(4): 817-827(in Chinese)

姜伟,方滨兴,田志宏,等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,2009,32(4):817-827

[3] Wang Yuan-zhuo, Lin Chuang, Cheng Xue-qi, et al. Analysis for Network Attack-Defense Based on Stochastic Game Model [J]. Chinese Journal of Computers, 2010, 33(9): 1748-1762(in Chinese)
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

[4] Jiang Wei, Fang Bin-xing, Tian Zhi-hong, et al. Research on Defense Strategies Selection Based on Attack-Defense Stochastic Game Model [J]. Journal of Computer Research and Development, 2010, 47(10): 1714-1723(in Chinese)
姜伟,方滨兴,田志宏,等. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展,2010,47(10):1714-1723

[5] 谢政. 对策论导论[M]. 北京:科学出版社,2010

[6] Lin Wang-qun, Wang Hui, Liu Jia-hong, et al. Research on Active Defense Technology in Network Security Based on Non-Cooperative Dynamic Game Theory [J]. Journal of Computer Research and Development, 2011, 48(2): 306-316(in Chinese)
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

[7] Liu Yu-ling, Feng Deng-guo, Wu Li-hui, et al. Performance Evaluation of Worm Attack and Defense Strategies Based on Static Bayesian Game [J]. Journal of Software, 2012, 23(3): 712-723 (in Chinese)
刘玉玲,冯登国,吴丽辉,等. 基于静态贝叶斯博弈的蠕虫攻防策略绩效评估[J]. 软件学报,2012,23(3):712-723

[8] Shi Le-yi, Jiang Lan-lan, Jia Chun-fu, et al. A Game Theoretic Analysis for the Honeypot Deceptive Mechanism [J]. Journal of Electronics & Information Technology, 2012, 34(6): 1420-1424 (in Chinese)
石乐义,姜蓝蓝,贾春福,等. 蜜罐诱骗防御机理的博弈理论分析[J]. 电子与信息学报,2012,34(6):1420-1424

[9] Carin L, Cybenko G, Hughes J. Quantitative evaluation of risk for investment efficient strategies in cyber security: The queries methodology [J]. IEEE Computer System, 2013, 47(7): 235-242

[10] Gueye A, Walrand J C. Security in Networks: A Game-Theoretic Approach [C]// Proceedings of the 47th IEEE Conference on Decision and Control Cancun. Mexico: Springer, 2013: 829-834

[11] Gordon L, Loeb M, Lucyshyn W. CSI/FBI computer crime and security survey [C]// Proceedings of the Computer Security Institute. San Francisco: Springer, 2012: 12-29

[12] National vulnerability database version 2. 3 [EB/OL]. http://nvd. nis. gov/2013

[13] Nash J. Non-cooperative games [J]. Annals of Mathematics, 1951, 54(2): 286-295

[14] Mckelvey T, Richard D, Mclennan K. Gambit: Software tools for game theory[EB/OL]. http://www. gambit-project. org

(上接第 180 页)

(3)签名信息的不可否认性

无人装置采用私钥对广播消息进行签名保护,具有唯一性,而且接收到消息的节点只有使用发送者的匿名公钥证书才能正确验证该消息的合法性,通信消息具有可验证性,是不可否认的。

(4)身份信息的可追溯性

由于无人装置的身份信息在 KDC 中有注册,如果在安全组网过程中采用了匿名证书进行签名,在合法条件下可以追溯签名消息对应匿名证书的真实身份。

结束语 本文分析了无人装置协同操作的安全组网的特性和需求,并针对协同操作前端动态组网的问题,提出了一种具有身份保护的认证协议。该协议采用基于匿名证书的广播认证机制,为安全域内的无人装置动态建立安全传输密钥,并为传输密钥提供机密性、不可否认性和不可伪造性等安全属性。

参 考 文 献

[1] Mark C C. A Discussion of a Modular Unmanned Demonstration Air Vehicle: A GARD CP2600[R]. 2000

[2] John A T. The Air Force is Pursuing Uninhabited Combat Air Vehicles in a Big Way[J]. Air Force Magazine, 2001, 84(8): 64

[3] Jones M C A. Unmanned Aerial Vehicles (UAVS)- an Assessment of Historical Operations and Future Possibilities: AU/ACSC/0230D/97-03[R]. 1997

[4] Siddiqui M S, Seon V C. Security Issues in Wireless Mesh Networks[C]// IEEE International Conference on Multimedia and Ubiquitous Engineering (MUEy07). 2007

[5] Zhang W, Wang Z, Das S K, et al. Security Issues in Wireless Mesh Networks[M]// Wireless Mesh Networks: Architectures and protocols. New York: Springer, 2008

[6] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems: IEEE Std 802. 16-2004[S]. 2004: 1-857

[7] Shamir A. Identity-based cryptography and signature schemes [M]// Advances in Cryptology (CRYPTO'84): Lecture Notes in Computer Science 196. Berlin: Springer-Verlag, 1985: 47-53

[8] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[M]// Advances in Cryptology (CRYPTO 2001): Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2001: 213-229

[9] Ke Zeng. Pseudonymous PKI for ubiquitous computing[M]// Public Key Infrastructure: Lecture Notes in Computer Science. Springer Berlin Heideleberg, 2006: 207-222

[10] Tu Jun-yang. Research on Synthesis Data Links of Multi-UAV Cooperative Combat[C]// China Unmanned Aircraft Systems Summit 2008. Beijing, 2008: 735-739

[11] Wang Gang, Wen Tao, Guo Quan, et al. An Efficient and Secure Group Key Management Scheme in Mobile Ad Hoc Networks [J]. Journal of Computer Research and Development, 2010, 47 (5): 911-920

[12] Hu Liang, Liu Zhe-li, Sun Tao, et al. Survey of Security on Identity-Based Cryptography[J]. Journal of Computer Research and Development, 2009, 46(9): 1537-1548

[13] Shi Rong-hua, Yuan Qian. A secure hierarchical key management scheme in mobile ad hoc networks[J]. Journal of Central South University (Science and Technology), 2010, 41(1): 201-206

[14] Lauter K. The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless Communications, 2004, 11 (1): 62-67