蜜罐诱骗防御机理的博弈理论分析

石乐义*[①] 姜蓝蓝[①] 贾春福[②] 王晓蕊[①]
[①](中国石油大学计算机与通信工程学院 青岛 266555)
[②](南开大学信息技术科学学院 天津 300071)

摘 要：论文运用博弈理论形式化描述了蜜罐诱骗中各博弈局中人的策略与收益，通过求解博弈均衡策略及均衡条件，分析推理了传统蜜罐在网络攻防博弈中的有效性和局限性，证明了蜜罐是一种“被动式主动”防御手段。讨论了符合防御者预期的理想诱骗博弈均衡策略，剖析了影响诱骗博弈有效性和主动性的要素条件，并受生物拟态现象启发，给出了提高诱骗主动性和有效性的策略建议，为构建主动有效的蜜罐诱骗防御手段提供了理论支持。

关键词：博弈论；纳什均衡；蜜罐；主动性；有效性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2012)06-1420-05
DOI: 10.3724/SP.J.1146.2011.00929

A Game Theoretic Analysis for the Honeypot Deceptive Mechanism

Shi Le-yi[①] Jiang Lan-lan[①] Jia Chun-fu[②] Wang Xiao-rui[①]
[①](*College of Computer and Communication Engineering*, *China University of Petroleum*, *Qingdao* 266555, *China*)
[②](*College of Information Technical Science*, *Nankai University*, *Tianjin* 300071, *China*)

Abstract: A game-theoretic analysis is performed to acquire the equilibrium strategies and their precondition by formalizing the strategies and payoffs of players in the honeypot game. The effectiveness and the deficiency of honeypot are inferred for network confrontation game, which demonstrate that honeypot is a passive-proactive defense mechanism. The ideal equilibrium combined strategy for defender and the factor affecting the effectiveness and activeness are discussed in detail. Inspired by the mimicry phenomena in biological competition, the propositional methods are given to enhance the deception performance for honeypot. The work is a theoretical support for the effective and proactive tactics of honeypot.

Key words: Game theory; Nash equilibrium; Honeypot; Activeness; Effectiveness

1 引言

近年来，网络攻防日益受到重视并已成为信息化战争中争夺制信息权的竞争焦点。然而，防火墙、入侵检测等防范手段本质上都是敌暗我明的被动防御，难以应对无处不在的未知敌手攻击。蜜罐则是一种主动网络防护手段，它通过模拟易受攻击的目标系统，给黑客提供一个包含漏洞并容易被攻破的系统作为他们的攻击目标，干扰和迷惑攻击者，从而诱骗敌手并研究学习其行为手段[1]。蜜罐具有数据集小、误报漏报率低、可检测未知攻击等优点。随着网络攻击事件的跳跃式增长，蜜罐已经成为在网络犯罪取证、蠕虫传播检测、拒绝服务防范等方面有效的主动防御手段。然而，蜜罐本身只是一个静态、固定不动的陷阱网络，这对于误入陷阱的鲁莽敌手十分有效，但一旦攻击者意识到陷阱的存在而离开或是完全控制，蜜罐将失去原本的价值。可见，传统蜜罐本质上是一种“被动式主动防御”手段。伴随着网络对抗的发展，攻击者意识到蜜罐的制约效用并开始着手研究如何识别、躲避和反制蜜罐，甚至出现了商业反蜜罐软件[2,3]；而防御方也推出动态蜜罐[4]、阵列蜜罐[5]、虚假蜜罐[6]等对抗手段，诱骗攻防已进入到了深层演化阶段。

国内外学者将博弈理论应用于网络安全对抗的研究已不乏见到，运用于蜜罐诱骗系统以提高蜜罐自适应性和决策优化的研究工作也已经出现，但运用博弈理论深入推理分析诱骗攻防机理的研究目前尚未见到文献提及。文献[7,8]将网络攻防过程视为一种非合作双人博弈，通过求解理性双方的占优博弈获得纳什均衡策略，证明了网络攻防是一种非合作不完全信息的动态博弈过程。文献[9,10]则对DoS

2011-09-06 收到，2012-02-15 改回
国家自然科学基金(60973141)，山东省中青年科学家科研奖励基金(2009BSA05001)和中央高校基本科研业务费专项(27R0907018A, 11CX04052A)资助课题
*通信作者：石乐义 stoneglad@hotmail.com

攻防过程进行了博弈理论分析，推证分析了DoS攻防中防御者的被动特性。文献[11]则将博弈理论运用在蜜罐诱骗博弈中，通过将诱骗双方形式化描述为简单双人博弈，对攻防博弈局中人的最优或次优策略进行了理论分析。文献[12]将博弈理论运用于自适应高交互蜜罐的决策支持中，从而提高了蜜罐的交互性和智能自适应性。文献[13]则提出了运用博弈理论实现蜜罐对入侵行为监测的信息融合方法，得到了信息融合最优的安全决策。文献[14]探讨了蜜罐诱骗中的完全但非完美信息的动态博弈模型，叙述了蜜罐诱骗情形下的动态博弈框架，进行了简单博弈分析并提到了运用基于博弈理论的蜜罐诱骗框架实施入侵检测。该文献工作仅探讨了蜜罐诱骗的博弈模型而未进行蜜罐诱骗过程中的攻防双方收益情况的全面分析，并且所采用的完全信息博弈并不符合网络诱骗攻防过程的特征。

文献[15]运用博弈理论进行了蜜罐诱骗策略分析，通过不完全信息动态博弈确定网络诱骗系统的信息获取策略。然而，该工作只研究关注诱骗系统的策略选取问题，而不是本文讨论的蜜罐诱骗机理证明。文献[16]采用了静态博弈和扩展的完美信息博弈手段对蜜罐诱骗博弈中的攻防双方收益及行为策略进行了形式化描述和推理，并对诱骗博弈中的混合策略均衡进行了讨论。文献[17]则使用信令博弈(signaling game)方法推理了采用虚拟蜜罐策略情形下的诱骗攻防博弈。然而，文献[16,17]的论文工作主要着眼于对虚假蜜罐进行动态博弈推理，这与本文所研究关注的蜜罐诱骗攻防机理的研究是不同的，并且所运用博弈推理方法也不同。本文旨在运用非合作不完全信息博弈理论，分析诱骗博弈局中人的各自收益和占优策略，推理传统蜜罐在网络攻防中的有效性和局限性，证明诱骗博弈具有“被动式主动防御”特点。在此基础上，深入剖析影响诱骗博弈主动性和有效性的要素条件，给出提高诱骗防御主动性的策略建议，为构建主动有效的诱骗防御手段提供理论支持。

2　诱骗攻防博弈分析

网络攻防博弈的局中人包括了攻击者和防御者，而从不同局中人视角来看，博弈对手又具有不同的类型。传统攻防博弈中，防御者视角中的博弈对手是一个具有两种不同类型的来访者，即合法用户和攻击者。服务方无法掌握来访者的具体类型，但可以通过防火墙、入侵检测等手段提高推测准确率，以便更好地为合法用户提供服务并阻止攻击者。而攻击者视角中的博弈对手则是一个单一固定的服务提供者，攻击者可以通过踩点、侦察等手段获取服务者类型，假冒合法用户发起恶意访问，达到破坏或阻止合法用户访问信息服务的目的。显然，这种信息的不对称对防御者十分不利。我们的前期工作对传统攻防博弈进行了不完全信息博弈推理，得出了传统攻防博弈中 $(\pi_{11},(\pi_{21},\pi_{21}))$“服务-访问-攻击”策略在 $p<2/(2+\gamma)$ 条件下达到纳什均衡，这里的攻击概率 p 和攻击破坏因子 γ 均受攻击者控制，服务方难以准确预期并且容易受到攻击者的元策略欺骗而影响博弈决策，从而导致了传统网络防御十分被动[10]。

蜜罐的出现改变了传统攻防博弈。在蜜罐诱骗博弈中，防御者视角中的博弈对手仍然是一个具有两种不同类型的来访者，而攻击者视角中的博弈对手不再只有单一服务类型，而是增加了“蜜罐”这一虚假服务类型。下面本文从攻防双方的视角给出蜜罐诱骗博弈的描述，并进行不完全信息博弈分析。描述如下：

局中人集合：$N=\{1,2\}$，1 为服务方，2 为访问者。

局中人类型：服务类型 $\Theta_1=\{\theta_{10},\theta_{11}\}=\{\text{Service, Honeypot}\}$，访问类型 $\Theta_2=\{\theta_{20},\theta_{21}\}=\{\text{User,Attacker}\}$。

局中人策略集：服务方策略集 $A_1=\{\pi_{11},\pi_{10}\}$，$\pi_{11}$ 表示提供服务，π_{10} 表示不提供服务；访问者策略集 $A_2=\{\pi_{21},\pi_{20}\}$，$\pi_{21}$ 表示访问 θ_{11} 类型的服务，π_{20} 则表示不访问。

局中人收益：首先考虑服务者提供正常服务的情况，服务方若为合法用户提供服务，双方收益均为 a $(a>0)$，否则收益为 $-a$；若为攻击者提供服务，服务性能将恶化，收益为 $-\gamma a$，攻击者收益 $\gamma a-b$（γ 为攻击破坏因子，反映不同攻击的破坏程度且 $\gamma\geq 1$，b 为攻击代价且 $a\gg b>0$）[10]，否则攻击者收益为 $-b$，服务者收益为0。再考虑服务方提供蜜罐服务的情况，无论服务者拒绝或提供给合法用户蜜罐服务，合法客户均不能获得正常所需服务，因而收益均为 $-a$，蜜罐策略得不到所需的攻击信息，收益为0；对于攻击者，如果服务者提供有效的蜜罐服务成功诱骗敌手，则收益为 ηc（$c>0$，η 为诱骗因子，反映对攻击者的诱骗程度且 $\eta\geq 1$），攻击者行为被监测，收益为 $-\eta c-b$。诱骗攻防博弈收益矩阵如表1所示。

我们在博弈分析中引入海萨尼虚拟局中人“自然”进行服务方和访问者的类型选择。服务者不知道访问者类型，但对访问类型有一个先验概率判断，假定为 $\{P(\theta_{21})=p,P(\theta_{20})=1-p\}$。同样，诱骗博弈中来访者也需要对服务者类型进行分析判断，假定

表1 诱骗攻防博弈收益矩阵

			访问者			
			θ_{20} 合法用户		θ_{21} 攻击者	
			π_{21}	π_{20}	π_{21}	π_{20}
服务方	θ_{10} 服务	π_{11}	a, a	0,0	$-\gamma a$, $\gamma a - b$	0,0
		π_{10}	$-a, -a$	0,0	$0, -b$	0,0
	θ_{11} 蜜罐	π_{11}	$0, -a$	0,0	ηc , $-\eta c - b$	0,0
		π_{10}	$0, -a$	0,0	$0, -b$	0,0

为 $\{P(\theta_{11}) = q, P(\theta_{10}) = 1 - q\}$。在局中人观测到对手行为后，运用贝叶斯法则得到博弈局中人类型后验概率，并计算使得各方期望收益极大化的策略。显然，访问者行为策略存在4种纯策略组合，分别是 $\{(\pi_{21}, \pi_{21}), (\pi_{21}, \pi_{20}), (\pi_{20}, \pi_{21}), (\pi_{20}, \pi_{20})\}$，这里 (π_{2m}, π_{2n}) 表示合法用户和攻击者的策略组合；同样服务者行为策略也存在 $\{(\pi_{11}, \pi_{11}), (\pi_{11}, \pi_{10}), (\pi_{10}, \pi_{11}), (\pi_{10}, \pi_{10})\}$ 4种纯策略组合，表示了服务和蜜罐是否提供服务。本文以访问者组合策略 (π_{21}, π_{21}) 为例，分析服务者视角下是否存在博弈均衡。

服务方包括了真实服务和蜜罐两种服务类型(实际上是真实服务和蜜罐两个参与者)。由表1的诱骗攻防博弈矩阵显然可知，对于蜜罐服务类型，π_{11} 提供服务策略是服务者的绝对占优策略。因而不论访问者是何种类型，蜜罐总是选择提供服务策略 π_{11}。而对于真实服务，当观测到来访策略 π_{21} 后推测得到来访者访问类型的后验概率 $\tilde{p}_{11} = p(\theta_{21} \mid \pi_{21}) = p$，$\tilde{p}_{10} = p(\theta_{20} \mid \pi_{21}) = 1 - p$，这样就可以计算得出真实服务器选择 π_{11} 服务策略和选择 π_{10} 不服务策略情况下的期望收益，得到真实服务的占优策略。

$$u_{\theta_{10}}(\pi_{11}) = p(\theta_{21} \mid \pi_{21}) \times (-\gamma a) + p(\theta_{20} \mid \pi_{21}) \times (a) = (1 - (1 + \gamma)p)a \tag{1}$$

$$u_{\theta_{10}}(\pi_{10}) = p(\theta_{21} \mid \pi_{21}) \times 0 + p(\theta_{20} \mid \pi_{21}) \times (-a) = (p - 1)a \tag{2}$$

类似文献[10]，不难得出对于访问者策略组合 (π_{21}, π_{21})，当 $p < 2/(2 + \gamma)$ 的来访为攻击者时，真实服务方的占优策略是 π_{11} 提供服务，反之占优策略为 π_{10} 不服务；而 $p > 2/(2 + \gamma)$ 时真实服务方占优策略为 π_{10} 不服务。考虑到蜜罐服务的绝对占优策略为 π_{11} 提供服务，这样就可以得到服务方视角下对于访问者组合策略 (π_{21}, π_{21}) 在 $p < 2/(2 + \gamma)$ 条件下占优策略为 (π_{11}, π_{11}) 二者均提供服务，而在 $p > 2/(2 + \gamma)$ 时占优策略为 (π_{10}, π_{11})，即真实服务不提供服务，蜜罐提供服务。

以上从服务方视角推理了攻防博弈中对于来访者组合策略 (π_{21}, π_{21}) 博弈行为的服务方占优策略，下面还需要从访问者视角分析组合访问策略 (π_{21}, π_{21}) 是否构成对服务方组合策略的占优对策。

首先考虑 $p < 2/(2 + \gamma)$ 情况，该情况下服务方组合策略为 (π_{11}, π_{11})，分别计算合法客户和攻击者的不同策略的期望收益如下：

$$u_{\theta_{20}}(\pi_{21}) = p(\theta_{11} \mid \pi_{11}) \times (-a) + p(\theta_{10} \mid \pi_{11}) \times a = (1 - 2q)a \tag{3}$$

$$u_{\theta_{20}}(\pi_{20}) = p(\theta_{11} \mid \pi_{11}) \times 0 + p(\theta_{10} \mid \pi_{11}) \times 0 = 0 \tag{4}$$

$$u_{\theta_{21}}(\pi_{21}) = p(\theta_{11} \mid \pi_{11}) \times (-\eta c - b) + p(\theta_{10} \mid \pi_{11}) \times (\gamma a - b) = \gamma a - b - (\eta c + \gamma a)q \tag{5}$$

$$u_{\theta_{21}}(\pi_{20}) = p(\theta_{11} \mid \pi_{11}) \times 0 + p(\theta_{10} \mid \pi_{11}) \times 0 = 0 \tag{6}$$

由式(3)，式(4)可知，若蜜罐服务类型出现概率 $q < 1/2$ 时，π_{21} 访问策略才是合法客户对于服务者 (π_{11}, π_{11}) 组合策略的占优策略。同理，由式(5)，式(6)得出，攻击者 π_{21} 访问策略为对服务者 (π_{11}, π_{11}) 占优策略的条件是 $q < (\gamma a - b)/(\gamma a + \eta c)$。联立得到：在 $p < 2/(2 + \gamma)$, $q < 1/2$，且 $\eta c \geq \gamma a - 2b$ 条件下，$((\pi_{11}, \pi_{11}), (\pi_{21}, \pi_{21}))$ 构成了贝叶斯均衡策略。

再考察 $p > 2/(2 + \gamma)$ 情况，服务者组合策略为 (π_{10}, π_{11})，即真实服务不提供服务，蜜罐提供服务，如上所述分别计算合法客户和攻击者的期望收益得知，$((\pi_{11}, \pi_{11}), (\pi_{21}, \pi_{21}))$ 不构成均衡策略。

以上分别从服务方和来访者视角分析了访问者组合策略 (π_{21}, π_{21}) 是否存在服务方均衡策略，并得出了在 $p < 2/(2 + \gamma)$，$q < 1/2$ 且 $q < (\gamma a - b)/(\gamma a + \eta c)$ 条件下，$((\pi_{11}, \pi_{11}), (\pi_{21}, \pi_{21}))$ “服务-服务-访问-攻击”组合策略构成了博弈均衡。同理，依次分析来访者其它各种组合策略，可以计算得到 $((\pi_{11}, \pi_{11}), (\pi_{21}, \pi_{20}))$ “服务-服务-访问-不攻击”策略在条件 $(\gamma a - b)/(\gamma a + \eta c) < q < 1/2$ 下构成博弈均衡；而组合策略 $((\pi_{10}, \pi_{11}), (\pi_{20}, \pi_{20}))$ “不服务-服务-不访问-不攻击”策略在条件 $q > 1/2$ 且 $q > (\gamma a - b)/(\gamma a + \eta c)$ 也存在均衡。

与传统攻防博弈相比较，诱骗攻防博弈的均衡条件已发生很大变化。传统攻防博弈中，$(\pi_{11}, (\pi_{21}, \pi_{21}))$ “服务-访问-攻击”策略在 $p < 2/(2 + \gamma)$ 条件下即可达到均衡，而与其它条件无关，因而传统攻防博弈的均衡结果只受攻击者攻击概率 p 和攻击破坏因子 γ 影响，服务者无法准确预期，并易于遭受攻击者的元策略欺骗，从而导致传统攻防博弈中防御者十分被动。诱骗博弈中，$p < 2/(2 + \gamma)$ 只是几个均衡博弈的条件之一，并且还受蜜罐出现概率 q、

攻击破坏因子 γ、诱骗程度 η 取值的影响，因而博弈均衡条件不再只受攻击者控制，而是由攻防双方的行为参数共同影响。防御者可以通过调整蜜罐部署的概率，使得诱骗攻防达到相应的博弈均衡，从而为防御机制带来了主动性。

进一步分析诱骗博弈均衡条件，在 $q<1/2$ 条件下，根据 q 与 $(\gamma a-b)/(\gamma a+\eta c)$ 关系比较结果，诱骗博弈可能进入不同的贝叶斯均衡，即 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{21}))$“服务-服务-访问-攻击”策略(还需满足条件 $p<2/(2+\gamma)$ 且 $q<(\gamma a-b)/(\gamma a+\eta c)$)和 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”策略(还需满足条件 $q>(\gamma a-b)/(\gamma a+\eta c)$)。这里，q 与 $(\gamma a-b)/(\gamma a+\eta c)$ 之间的关系本质上反映了攻击行为的博弈收益情况。而当 $q>1/2$ 且 $q>(\gamma a-b)/(\gamma a+\eta c)$ 时，$((\pi_{10},\pi_{11}),(\pi_{20},\pi_{20}))$“不服务-服务-不访问-不攻击”策略中服务器、合法客户和攻击者均停止服务或访问，这并不符合实际。显然，$((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”策略是防御者最期望的博弈结果，均衡策略中真实服务和蜜罐提供服务、合法客户访问而攻击者不攻击，此时博弈均衡条件为 $(\gamma a-b)/(\gamma a+\eta c)<q<1/2$，与蜜罐部署概率 q 有关而与攻击概率 p 无关，因此博弈过程中蜜罐防御者是积极主动的。不难推知，$\eta c>\gamma a-2b$ 是 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”博弈均衡的必要条件，也就是说，若 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”构成博弈均衡，则蜜罐诱骗给攻击者带来的损失应该大于攻击者破坏真实服务的收益。然而，传统蜜罐是静态、固定不动的陷阱系统，一旦攻击者识破或者绕过，传统蜜罐将失去任何效用，加之近来反蜜罐技术的发展使得蜜罐往往在部署后很快被攻击者识破，因此诱骗程度 η 取值受到很大制约，难以满足 $\eta c>\gamma a-2b$ 博弈均衡条件，因而致使诱骗攻防博弈难以达到 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”理想博弈均衡，而是趋于 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{21}))$“服务-服务-访问-攻击”策略均衡。而 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{21}))$“服务-服务-访问-攻击”博弈均衡条件受攻击概率 p、蜜罐部署概率 q 等攻防双方行为的共同影响，这就证明了传统蜜罐诱骗仍然只是一种“被动式”主动防御手段。

3　诱骗博弈的有效性和主动性

以上我们分析了蜜罐诱骗的有效性和局限性，推证了传统蜜罐诱骗是一种“被动式”主动防御手段。下面进一步讨论诱骗博弈的有效性条件。由前述推理得知，诱骗博弈存在3种贝叶斯纳什均衡，即 $p<2/(2+\gamma)$，$q<1/2$ 且 $q<(\gamma a-b)/(\gamma a+\eta c)$ 条件下的 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{21}))$“服务-服务-访问-攻击”策略均衡；$(\gamma a-b)/(\gamma a+\eta c)<q<1/2$ 条件下的 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”策略均衡以及 $q>1/2$ 且 $q>(\gamma a-b)/(\gamma a+\eta c)$ 条件下的 $((\pi_{10},\pi_{11}),(\pi_{20},\pi_{20}))$“不服务-服务-不访问-不攻击”均衡，而 $((\pi_{10},\pi_{11}),(\pi_{20},\pi_{20}))$“不服务-服务-不访问-不攻击”均衡博弈并不符合实际。可以得到结论：在一个有效的诱骗攻防博弈中，蜜罐服务出现的概率应满足 $q<1/2$。这表明在有效的诱骗博弈中，模拟者出现的概率应小于被模拟个体的出现概率。该结论与贝茨氏拟态现象[18](Batesian-mimicry)有效性条件完全一致，而后者是生物种群斗争中常见的伪装诱骗手段，经历了亿万年“物竞天择，适者生存”的有效性验证，是一种“即破即演化”的斗争方式。拟态者通过不断模仿其他对象的特征来诱骗敌手和保护自身，而保护色和警戒色则是拟态现象的常见手段。其中，保护色机制通过将自身特征隐蔽在周边环境之中而躲开敌手的攻击，警戒色机制则通过模仿敌手敬畏的特征而吓退敌手。显然，生物拟态现象对于诱骗攻防博弈应该具有十分重要的借鉴意义。

进一步讨论诱骗博弈的主动性。前面推理了实现 $((\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$“服务-服务-访问-不攻击”理想诱骗博弈均衡的条件，即：$(\gamma a-b)/(\gamma a+\eta c)<q<1/2$。该条件受蜜罐部署概率 q、蜜罐诱骗程度 η、攻击破坏因子 γ 的取值影响而与攻击者概率 p 无关，因而是一种积极主动的诱骗博弈。考虑到攻击破坏因子对某一种具体攻击而言是一个常数，因而提高蜜罐诱骗程度 η，合理部署蜜罐概率 q 使其可以满足条件 $(\gamma a-b)/(\gamma a+\eta c)<q<1/2$，是实现理想诱骗博弈均衡的基本方法。显然，提高蜜罐诱骗程度 η，可以通过增加蜜罐的动态性，摒弃固定不动的静态陷阱模式而获得。动态蜜罐[4]、阵列蜜罐[5]等工作均采用此方法提高了蜜罐诱骗程度，从而获得了更好的诱骗性能。而蜜罐概率设置则既可以通过合理部署蜜罐获得，也可以通过元策略欺骗而满足 $(\gamma a-b)/(\gamma a+\eta c)<q<1/2$ 均衡条件。虚假蜜罐[6]采用元策略欺骗方式，通过假冒的蜜罐系统迷惑攻击者，从而影响到攻击者对蜜罐部署概率 q 的后验概率判断，获得了更高的诱骗主动性。进一步分析不难发现，虚假蜜罐正是拟态现象中警戒色机制在网络诱骗中的运用，它通过将正常服务伪装成令攻击者躲避的蜜罐特征而吓退敌手。可见，防御者通过增加蜜罐的动态性和实施适度的元策略欺骗，可以提高蜜罐诱骗的主动性，更好地迷惑敌手而获得主动防御效果。

4 总结

本文运用博弈理论，首先给出了蜜罐诱骗博弈各局中人的策略和收益的形式化描述，然后分别从服务者视角和攻击者视角考察各种来访组合策略和服务组合策略是否构成贝叶斯博弈均衡，推理得到了诱骗攻防可能达到的3种均衡博弈及其均衡条件。通过分析3种均衡博弈及条件，指出了防御者最期望的“服务-服务-访问-不攻击”理想诱骗博弈均衡，并推理了传统蜜罐在网络攻防中的有效性和局限性，证明了诱骗博弈具有“被动式主动防御”的特点。在此基础上，本文进一步剖析了影响诱骗博弈有效性和主动性要素条件，并通过与生物拟态现象的比较，给出了诱骗攻防策略的建议，即蜜罐防御者可以通过增加蜜罐的动态性和实施适度的元策略欺骗来提高蜜罐诱骗性能。

参 考 文 献

[1] Spitzner L. Honeypots: definitions and value of honeypots. http://www.tracking-hackers.com/, 2003.

[2] Krawetz N. Anti-honeypot technology. *IEEE Security & Privacy*, 2004, 2(1): 76–79.

[3] 郭文举. 反蜜罐技术的研究与实践. [硕士论文], 重庆邮电大学, 2005: 25–55.

[4] Spitzner L. Dynamic honeypots. http://www.securityfocus.com/infocus/1731, 2003.

[5] Shi L, Li J, Han X, *et al*.. Design and implementation of distributed self-election dynamic array honeypot system. *China Communications*, 2011, 8(4): 109–115.

[6] Rowe N, Custy E, and Duong B. Defending cyberspace with fake honeypots. *Journal of Computers*, 2007, 2(2): 25–36.

[7] Lye K and Wing J. Game strategies in network security. *International Journal of Information Security*, 2005, 5(4): 71–86.

[8] Shiva S, Roy S, and Dasgupta D. Game theory for cyber security. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, New York, 2010: 1–4.

[9] Bedi H, Roy S, and Shiva S. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, 2011: 129–136.

[10] 石乐义, 贾春福, 吕述望. 服务跳变抗 DoS 机制的博弈理论分析. 电子与信息学报, 2009, 31(1): 228–232.

[11] Cai J, Yegneswaran V, and Alfeld C. Honey games: a game theoretic approach to defending network monitors. *Journal of Combinatorial Optimization*, 2011, 22(8): 305–324.

[12] Wagener G, State R, and Dulaunoy A. Self adaptive high interaction honeypots driven by game theory. Lecture Notes in Computer Science, 2009, 5873: 741–755.

[13] Wei L and Wang X. Research on honeypot information fusion based on game theory. 2010 Second International Conference on Computer Research and Development, Kuala Lumpur, 2010: 803–806.

[14] Li H, Yang X, and Qu L. On the offense and defense game in the network honeypot. Advances in Automation and Robotics, 2011, LNEE Vol.2: 239–246.

[15] 李娟利. 基于博弈论的网络诱骗系统研究. [硕士论文], 西安建筑科技大学, 2006: 20–26.

[16] Garg N and Grosu D. Deception in honeynets: a game-theoretic analysis. IEEE Workshop on Information Assurance, New York, 2007: 107–113.

[17] Carroll T and Grosu D. A game theoretic investigation of deception in network security. *Security and Communication Networks*, 2011, 4(10): 1162–1172.

[18] Duncan C and Sheppard P. Sensory discrimination and its role in the evolution of Batesian mimicry. *Behaviour*, 1965, 24(3/4): 269–282.

石乐义： 男，1975 年生，博士，副教授，硕士生导师，研究方向为网络与信息安全、博弈理论、移动计算.

姜蓝蓝： 女，1986 年生，硕士生，研究方向为网络与信息安全.

贾春福： 男，1968 年生，博士，教授，博士生导师，研究方向为信息安全、运筹优化、随机过程.

王晓蕊： 女，1987 年生，硕士生，研究方向为网络与信息安全.