拟态式蜜罐诱骗特性的博弈理论分析

石乐义*[①] 姜蓝蓝[①] 刘 昕[①] 贾春福[②]
[①](中国石油大学(华东)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：该文基于非合作不完全信息动态博弈理论，形式化描述了拟态式蜜罐诱骗博弈的各局中人策略和收益，构建了诱骗博弈收益矩阵，推理分析了拟态式蜜罐诱骗博弈中存在的贝叶斯纳什均衡策略，通过进一步讨论博弈均衡条件和影响因素并与传统蜜罐博弈相比较，给出了拟态式蜜罐模型中保护色、警戒色等机制在诱骗博弈中的适用条件，证明了拟态式蜜罐模型具有更好的主动性、有效性和迷惑性。

关键词：信息安全；博弈理论；纳什均衡；蜜罐；伪蜜罐；拟态
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2013)05-1063-06
DOI: 10.3724/SP.J.1146.2012.01213

Game Theoretic Analysis for the Feature of Mimicry Honeypot

Shi Le-yi[①] Jiang Lan-lan[①] Liu Xin[①] Jia Chun-fu[②]
[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: This paper firstly gives the formalization description of both players' strategies and payoffs in the mimicry honeypot game, and constructs the payoff matrix of the fraudulent game using non-cooperative and incomplete dynamic game theory. Then the equilibrium strategies and the equilibrium conditions are inferred. The equilibrium conditions and relative factors are discussed in detail, and the comparison to traditional honeypot is also performed. The theoretic analysis depicts the effective condition for protective coloration and warning coloration mechanism in the fraudulent game, and demonstrates that the mimicry honeypot has better activeness, efficiency and fraudulence than the traditional scheme.

Key words: Information security; Game theory; Nash equilibrium; Honeypot; Fake honeypot; Mimicry

1 引言

随着网络信息技术的不断发展，安全防范和网络对抗技术日益受到重视。传统的网络防护手段如防火墙、入侵检测系统等，已难以应对日益多元化的攻击技术。蜜罐则是一种主动防御手段，通过模拟真实系统诱骗和分析攻击者。然而，传统蜜罐本质上只是一个静态固定的陷阱系统，一旦攻击者意识到陷阱的存在并离开，蜜罐将失去价值。近年来，攻击者开始系统研究如何识别和反利用蜜罐技术，并通过黑客社区共享知识，导致诸多传统蜜罐技术纷纷失去功效。在此背景下，新型蜜罐防御技术被相继提出，出现了动态蜜罐[1]、阵列蜜罐[2]、虚假蜜罐[3]等网络诱骗防御手段。

自然界生物斗争中，为了更好地避敌、捕猎或繁衍，生物种群进行着同样的诱骗博弈，不仅出现了弱者隐藏于周边环境的保护色机制，强者威吓敌手的警戒色机制，还出现了弱者模仿强者警戒色特征从而避开攻击的贝茨氏拟态(Batesian-mimicry)机制[4]。拟态现象经历了亿万年“物竞天择，适者生存”的有效性验证，对于网络安全防护具有重要的借鉴意义。受生物拟态现象启发，文献[5]提出了拟态式蜜罐(mimicry honeypot)概念。

拟态式蜜罐是指在传统蜜罐网络基础上通过综合运用模拟服务环境的保护色机制和模拟蜜罐特征的警戒色机制进行拟态演化和对抗博弈，从而可以有效地迷惑和诱骗攻击者，实现网络对抗。拟态式蜜罐中的保护色是指蜜罐在硬件、软件、数据、服务信息等方面模仿周边服务器和网络环境的特征，使得攻击者难以识别蜜罐的存在。而警戒色则是指服务器在硬件、软件或数据等方面模仿蜜罐特征，使得攻击者将该系统认作蜜罐而躲避攻击。拟态式蜜罐系统中，不仅蜜罐可以模仿网络服务以便诱骗攻击者，网络服务也可以模拟蜜罐特征威吓和避开

2012-09-19 收到，2012-12-11 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, 11CX06085A)资助课题
*通信作者：石乐义 stoneglad@hotmail.com

敌手攻击，这些正是保护色和警戒色机制在网络对抗中的应用。

本文旨在运用博弈理论，形式化描述拟态式蜜罐诱骗博弈各局中人的策略和收益，推理分析拟态式蜜罐诱骗博弈下贝叶斯纳什均衡策略、均衡条件和影响博弈均衡条件的因素，在博弈理论上证明拟态式诱骗的主动性和有效性，为拟态式蜜罐的研究与应用提供理论支持。

作为蜜罐新技术，拟态式蜜罐的研究刚刚起步，运用博弈理论分析其诱骗机理的研究也尚未见文献提及。国内外相关工作主要有：文献[6]分析了网络攻防对抗的基本特征，指出网络攻防具有理性、非合作等特点，攻防双方无法完全掌握敌手的类型和信息价值，从而构成非合作不完全信息的攻防博弈。文献[7]则针对这种静态方式无法应对攻击者攻击意图和攻击策略动态变化的不足，基于非合作、非零和动态博弈理论提出了完全信息动态博弈主动防御模型，通过“虚拟节点”将网络攻防图转化为攻防博弈树，给出了分别适应于完全信息和非完全信息两种场景的攻防博弈算法。

文献[8]将攻防过程形式化为简单双人博弈，并对博弈最优和次优策略进行了分析。文献[9]则运用不完全信息动态博弈理论进行诱骗防御的策略选择。文献[10]基于博弈理论提出了自适应高交互蜜罐模型，它把蜜罐和攻击者看作博弈的双方，利用博弈论的思想分析各自的收益并计算纳什均衡，找到蜜罐和攻击者的最优策略，从而更好地配置蜜罐，提高其诱骗性能。文献[11]运用博弈理论建立了漫游蜜罐攻防模型，找出了攻击方与防御方之间的贝叶斯纳什均衡，并对蜜罐系统最佳漫游时刻和最优位置策略进行了研究。文献[8–11]的研究将博弈理论引入到传统蜜罐之中，推理分析最有利于诱骗防御的策略。然而，这些研究工作关注蜜罐系统在攻防博弈中的策略选择而不是诱骗机理证明，更没有进行蜜罐真伪的博弈分析和研究。

文献[12,13]研究了伪蜜罐服务下的诱骗博弈，分别运用标准静态博弈、完美信息博弈和信令博弈的方法，对伪蜜罐诱骗进行形式描述，推理讨论了伪诱骗博弈中的均衡策略。文献[12,13]基于博弈理论研究“伪蜜罐”而不是传统静态蜜罐，这与本文研究有一定的相似性。但该工作同样关注于诱骗防御的策略选择，而不是本文开展的诱骗机理证明。此外，该工作所运用的标准静态博弈、完美信息博弈以及信令博弈方法与本文所用的非完全信息动态博弈都是不同的。

文献[14]运用不完全信息动态博弈理论对传统蜜罐的诱骗机理进行了研究，形式化描述了蜜罐诱骗博弈各局中人的收益矩阵，证明了传统诱骗博弈的“被动式主动防御”特点。文献[14]着眼于传统蜜罐而开展，而本文则在此基础上针对拟态式蜜罐开展博弈分析，并通过与传统蜜罐诱骗的比较，理论上证明拟态式蜜罐系统的主动性和有效性。

2 诱骗攻防博弈分析

蜜罐防护是防御者和攻击者参与的理性、非合作的诱骗过程，攻防双方策略相互依存，都期望保护自身信息并获得对方信息以获得收益最大化，因而构成了非合作不完全信息动态博弈。从不同局中人视角来看，博弈对手却具有不同的类型：从攻击者视角中，博弈对手不再是只有“真实服务”这一单一服务类型，而是增加了“蜜罐”和“伪蜜罐”这两种欺骗服务类型；从防御者视角下，博弈对手有合法用户和攻击者两种不同类型的来访者。本文运用博弈理论作为数学分析手段，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。形式化描述如下[14]：

局中人集合：N={1,2}, 1 表示服务提供者，2 则表示访问者；

局中人类型：服务类型 $\Omega_1=\{\theta_{10},\theta_{11},\theta_{12}\}=$ {服务，蜜罐，伪蜜罐}，访问类型 $\Omega_2=\{\theta_{20},\theta_{21}\}=$ {合法用户，攻击者}；

局中人策略：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 $A_2=\{\pi_{21},\pi_{20}\}$，$\pi_{21}$ 为访问服务，π_{20} 则不访问服务；

局中人收益：需要根据服务者类型分情况考虑，具体如下：

(1)当服务类型为正常服务情况下，如果系统为合法用户提供服务，则双方收益为 $a(a>0)$，反之，系统不为合法用户提供服务，双方代价则为$-a$；而如果系统提供服务给攻击者，则系统性能降低，收益为 $-\gamma a$，攻击者收益为 $\gamma a-b$（γ 为攻击破坏因子且有 $\gamma>1$，b 为攻击代价且有 $a>>b>0$），否则系统不为攻击者提供服务，攻击者收益为$-b$，服务者收益为 0。

(2)当服务类型为蜜罐情况下，此时合法用户无论访问或不访问都不能获得正常服务，因而收益为 0，同时蜜罐也无法获得所需攻击者的信息，收益也为 0；而对于攻击者访问的情况，若服务者提供蜜罐服务且成功诱骗攻击者，则系统收益为 $\eta_1 c\ (c>0,\ \eta$ 为蜜罐诱骗因子且 $\eta\geq 1)$，同时攻击者的恶意行为被跟踪，攻击者收益为 $-\eta_1 c-b$。

(3)当服务类型为伪蜜罐情况下，对合法用户来

讲，伪蜜罐就是正常服务，其收益与正常服务相同；若为攻击者提供服务时，则访问者服务性能降低，收益为 $-\gamma a$，攻击者收益为 $\gamma a-\eta_2 c-b$（η_2 为伪蜜罐诱骗因子且 $\eta_2\geq 1$）。若伪蜜罐诱骗攻击者成功，则攻击者不攻击伪蜜罐，服务者收益为 $\eta_2 c$。

以上给出了拟态式蜜罐诱骗博弈的形式化描述，博弈分析中还需要引入海萨尼虚拟局中人“自然”以便选择服务方和访问者类型。显然，访问者存在 4 种纯策略组合，即{(π_{21},π_{21}),(π_{21},π_{20}),(π_{20},π_{21}),(π_{20},π_{20})}，服务者策略则存在着 8 种纯策略组合，即{(π_{11},π_{11},π_{11}),(π_{11},π_{10},π_{11}),(π_{11},π_{10},π_{10}),(π_{11},π_{11},π_{10}),(π_{10},π_{11},π_{11}),(π_{10},π_{11},π_{10}),(π_{10},π_{10},π_{11}),(π_{10},π_{10},π_{10})}，组合策略数与传统蜜罐博弈相比有了几何增长[14]。这里，访问者组合策略(π_{20},π_{21})“不服务-攻击”，(π_{20},π_{20})“不服务-不攻击”，以及服务策略(π_{10},π_{10},π_{10})“不服务-不服务-不服务”并不符合网络安全中的实际情况，因而本文将只考虑在(π_{21},π_{21})和(π_{21},π_{20})访问策略下服务者达到策略均衡的策略组合。

根据攻击者是否知晓伪蜜罐的存在，本文分两种情况分别推理分析诱骗博弈如下：

情况 1　攻击者不知晓存在伪蜜罐　该情景下，攻击者并不知道伪蜜罐的存在，因而服务者视角和攻击者视角的服务者类型是不同的。服务者对访问类型有个先验概率判断：$p(\theta_{21})=p$, $p(\theta_{20})=1-p$；访问者也对服务者类型有先验判断：$p(\theta_{11})=q$, $p(\theta_{10})=1-q-q'$, $p(\theta_{12})=q'$。在服务者视角下，服务者有服务、蜜罐和伪蜜罐 3 种类型。而在攻击者视角下，攻击者不知道伪蜜罐的存在，在他们看来只有服务和蜜罐存在，服务先验概率 $p(\theta_{10})=1-q-q'$，蜜罐概率则变为 $p(\theta_{11})=q+q'$。若服务者提供蜜罐服务且成功诱骗攻击者，则收益 $\eta c\left(c>0,\eta c=\dfrac{q}{q+q'}\eta_1 c+\dfrac{q'}{q+q'}\eta_2 c\right)$，而攻击者行为被记录，收益为 $-\eta c-b$。服务者和攻击者视角下的收益矩阵如表 1 和表 2 所示。

下面以访问者策略为(π_{21},π_{21})为例，分析服务者视角下是否存在博弈均衡。

根据表 1，计算真实服务和伪蜜罐选择 π_{11} 和 π_{10} 服务类型下的期望收益，分析得到其占优策略为

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

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

表 1 服务者视角下诱骗博弈收益矩阵

			访问者类型			
			θ_{20} 合法用户		θ_{21} 攻击者	
			π_{21}	π_{20}	π_{21}	π_{20}
服务者类型	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	$\eta_1 c,-\eta_1 c-b$	0,0
		π_{10}	$0,-a$	0,0	$0,-b$	0,0
	θ_{12} 伪蜜罐	π_{11}	a,a	0,0	$-\gamma a,\gamma a-\eta_2 c-b$	$\eta_2 c$,0
		π_{10}	$-a,-a$	0,0	$0,-b$	0,0

表 2 攻击者视角下诱骗博弈收益矩阵

			访问者类型			
			θ_{20} 合法用户		θ_{21} 攻击者	
			π_{21}	π_{20}	π_{21}	π_{20}
服务者类型	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	$\eta c,-\eta c-b$	0,0
		π_{10}	$0,-a$	0,0	$0,-b$	0,0

$$u_{\theta_{12}}(\pi_{11})=p(\theta_{21}\mid\pi_{21})\times(-\gamma a)+p(\theta_{20}\mid\pi_{21})\times a=-\gamma a p+(p-1)a \tag{3}$$

$$u_{\theta_{12}}(\pi_{10})=p(\theta_{21}\mid\pi_{21})\times(-\gamma a)+p(\theta_{20}\mid\pi_{21})\times a=(p-1)a \tag{4}$$

由式(1)，式(2)，式(3)和式(4)可知：当 $p<2/(2+\gamma)$ 的来访者为攻击者时，真实服务和伪蜜罐的占优策略均为 π_{11} 提供服务，反之占优策略为 π_{10} 不服务，因为蜜罐服务的绝对占优策略为 π_{11} 提供服务，因此可以得到服务者视角下对于来访者的组合策略(π_{21} π_{21})在 $p<2/(2+\gamma)$ 下占优策略为(π_{11},π_{11},π_{11})提供服务，而在 $p<2/(2+\gamma)$ 的占优策略为(π_{10},π_{11},π_{10})，即真实服务和伪蜜罐不提供服务，蜜罐提供服务。这样就要判断两种条件下访问策略(π_{21},π_{21})是否构成对服务方组合策略的占优策略。

(1) $p<2/(2+\gamma)$ 条件成立，此时服务方占优组合策略为(π_{11},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：

$$u_{\theta_{20}}(\pi_{21})=p(\theta_{11}\mid\pi_{11})\times(-a)+p(\theta_{10}\mid\pi_{11})\times a=(1-2(q+q'))\times a \tag{5}$$

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

$$u_{\theta_{21}}(\pi_{21})=p(\theta_{11}\mid\pi_{11})\times(-\eta_1 c-b)+p(\theta_{10}\mid\pi_{11})\times(\gamma a-b)=\gamma a-b-(\gamma a+\eta c)(q+q') \tag{7}$$

$$u_{\theta_{21}}(\pi_{20})=p(\theta_{11}\mid\pi_{11})\times 0+p(\theta_{10}\mid\pi_{11})\times 0=0 \tag{8}$$

由式(5)，式(6)可知，当 $q+q'<1/2$ 时，π_{21} 才是合法客户对于组合策略 $(\pi_{11},\pi_{11},\pi_{11})$ 的占优策略，由式(7)，式(8)可知，攻击者 π_{21} 访问策略对服务者 $(\pi_{11},\pi_{11},\pi_{11})$ 占优策略的条件是 $q+q'<(\gamma a-b)/(\gamma a+\eta c)$ 联立式(5)，式(6)，式(7)，式(8)可知，在 $p<2/(2+\gamma)$, $q+q'<1/2$，且 $q+q'<(\gamma a-b)/(\gamma a+\eta c)$ 条件下 $((\pi_{11},\pi_{11},\pi_{11}),(\pi_{21},\pi_{21}))$ 构成了贝叶斯纳什策略均衡。

(2) $p>2/(2+\gamma)$ 条件成立，服务者占优组合策略为 $(\pi_{10},\pi_{11},\pi_{10})$。分别计算服务者和攻击者视角下合法客户和攻击者的期望收益如下。首先计算出服务者视角下合法用户和攻击者的期望收益：

$$u_{\theta_{20}}(\pi_{21})=p(\theta_{11}\mid\pi_{11})\times(-a)+p(\theta_{10}\mid\pi_{10})\times(-a)+p(\theta_{12}\mid\pi_{10})\times(-a)=-a \tag{9}$$

$$u_{\theta_{20}}(\pi_{20})=p(\theta_{11}\mid\pi_{11})\times 0+p(\theta_{10}\mid\pi_{10})\times 0+p(\theta_{12}\mid\pi_{10})\times 0=0 \tag{10}$$

$$u_{\theta_{21}}(\pi_{21})=p(\theta_{11}\mid\pi_{11})\times(-\eta_1 c-b)+p(\theta_{10}\mid\pi_{10})\times(-b)+p(\theta_{12}\mid\pi_{10})\times(-b)=-\eta_1 cq-b \tag{11}$$

$$u_{\theta_{21}}(\pi_{20})=p(\theta_{11}\mid\pi_{11})\times 0+p(\theta_{10}\mid\pi_{10})\times 0+p(\theta_{12}\mid\pi_{10})\times 0=0 \tag{12}$$

显然，$u_{\theta_{20}}(\pi_{21})=-a<0=u_{\theta_{20}}(\pi_{20})$，且 $u_{\theta_{21}}(\pi_{21})=-\eta_1 cq-b<0=u_{\theta_{21}}(\pi_{20})$，$((\pi_{10},\pi_{11},\pi_{10}),(\pi_{21},\pi_{21}))$ 不构成均衡策略。同理，计算出攻击者视角下合法用户和攻击者的期望收益，可知在攻击者视角下组合策略 $((\pi_{10},\pi_{11},\pi_{10}),(\pi_{21},\pi_{21}))$ 也不构成贝叶斯纳什均衡。

这样，我们分析得出了服务者与来访者组合策略 $((\pi_{11},\pi_{11},\pi_{11}),(\pi_{21},\pi_{21}))$ 即“服务-服务-服务-访问-攻击”在 $p<2/(2+\gamma)$，$q+q'<1/2$ 且 $q+q'<(\gamma a-b)/(\gamma a+\eta c)$ 条件下构成了贝叶斯纳什均衡。同理不难推知，组合策略 $((\pi_{11},\pi_{11},\pi_{11}),(\pi_{21},\pi_{20}))$ 即“服务-服务-服务-访问-不攻击”在条件 $(\gamma a-b)/(\gamma a+\eta c)<q+q'<1/2$ 下达到均衡，$((\pi_{10},\pi_{11},\pi_{10}),(\pi_{20},\pi_{20}))$ 在条件 $q+q'<1/2$ 且 $q+q'>(\gamma a-b)/(\gamma a+\eta c)$ 下也构成了均衡策略。

情况 2　攻击者知晓存在伪蜜罐　该情景下，攻击者知晓伪蜜罐的存在，因而服务者和攻击者视角下服务者都有服务、蜜罐和伪蜜罐 3 种类型，此时服务概率 $p(\theta_{10})=1-q-q'$，蜜罐概率为 $p(\theta_{11})=q$，伪蜜罐的概率为 $p(\theta_{11})=q'$，诱骗博弈收益矩阵如表 3 所示。

下面仍以访问者策略 (π_{21},π_{21}) 为例，分析诱骗博弈中是否存在博弈均衡。由表 3 可知，无论访问者为何种类型，π_{11} 服务策略是蜜罐的绝对占优策略。如同情况 1，计算真实服务和伪蜜罐选择 π_{11} 和

表 3 攻防诱骗博弈的收益矩阵

			访问者类型			
			θ_{20} 合法用户		θ_{21} 攻击者	
			π_{21}	π_{20}	π_{21}	π_{20}
服务者类型	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	$\eta_1 c,-\eta_1 c-b$	0,0
		π_{10}	$0,-a$	0,0	$0,-b$	0,0
	θ_{12} 伪蜜罐	π_{11}	a,a	0,0	$-\gamma a,\gamma a-\eta_2 c-b$	$\eta_2 c$,0
		π_{10}	$-a,-a$	0,0	$0,-b$	0,0

π_{10} 服务类型下的期望收益，即可得到其占优策略：$p<2/(2+\gamma)$ 条件下，服务者对于来访组合策略 (π_{21},π_{21}) 的占优策略为 $(\pi_{11},\pi_{11},\pi_{11})$，即“服务-服务-服务”，而在 $p>2/(2+\gamma)$ 条件下的占优策略为 $(\pi_{10},\pi_{11},\pi_{10})$，即真实服务和伪蜜罐不提供服务而蜜罐提供服务。同样，我们需要进一步分析访问者策略 (π_{21},π_{21}) 是否构成不同条件下服务方策略的占优策略。类似情况 1 的推理，计算合法客户和攻击者的不同策略的期望收益，得到其占优策略，具体如下：

(1) $p<2/(2+\gamma)$ 条件下，服务方占优组合策略为 $(\pi_{11},\pi_{11},\pi_{11})$：

$$u_{\theta_{20}}(\pi_{21})=p(\theta_{11}\mid\pi_{11})\times(-a)+p(\theta_{10}\mid\pi_{11})\times a+p(\theta_{12}\mid\pi_{11})\times a=(1-2q)\times a \tag{13}$$

$$u_{\theta_{20}}(\pi_{20})=p(\theta_{11}\mid\pi_{11})\times 0+p(\theta_{10}\mid\pi_{11})\times 0+p(\theta_{12}\mid\pi_{11})\times 0=0 \tag{14}$$

$$u_{\theta_{21}}(\pi_{21})=p(\theta_{11}\mid\pi_{11})\times(-\eta_1 c-b)+p(\theta_{10}\mid\pi_{11})\times(\gamma a-b)+p(\theta_{12}\mid\pi_{11})\times(\gamma a-\eta_2 c-b)=\gamma a-b-q\gamma a-(q\eta_1 c+q'\eta_2 c) \tag{15}$$

$$u_{\theta_{21}}(\pi_{20})=p(\theta_{11}\mid\pi_{11})\times 0+p(\theta_{10}\mid\pi_{11})\times 0+p(\theta_{12}\mid\pi_{11})\times 0=0 \tag{16}$$

由式(13)和式(14)可知，当 $q<1/2$ 时，π_{21}“访问”策略才是合法客户对于组合策略 $(\pi_{11},\pi_{11},\pi_{11})$ 的占优策略；而由式(15)和式(16)可知，攻击者 π_{21}“访问”对 $(\pi_{11},\pi_{11},\pi_{11})$ 占优的条件为 $q+q'<(\gamma a-b-q\gamma a)/\eta c$，其中 $\eta c=q/(q+q')\eta_1 c+q'/(q+q')\eta_2 c$。联立式(15)和式(16)并进一步分析访问者占优策略的条件，有：

若 $q+q'<(\gamma a-b-q\gamma a)/\eta c<1/2$，即 $\gamma a-2b<\eta c$，则 $p(\theta_{10})=1-(q+q')>1/2$，由 $q+q'<1-q$，可得 $q'<1-2q$，$p(\theta_{10})>p(\theta_{11})$，$p(\theta_{10})>p(\theta_{12})$。也就是说，服务概率大于蜜罐和伪蜜罐概率，且 $q'<1-2q$。

若 $1/2 < q+q' < (\gamma a - b - q\gamma a)/\eta c$ ，即 $\gamma a - 2b > \eta c$，由 $\dfrac{\eta c - (\gamma a - b - q\gamma a)}{\eta c} < 1-(q+q') < 1/2$ 可得

$$\frac{\eta c - (\gamma a - b - q\gamma a)}{\eta c} > \frac{(q-1)\gamma a + \eta c}{\eta c} > \frac{(q-1)(\eta c + 2b) + \eta c}{\eta c} > q$$

即 $1-(q+q') > q$，此时服务概率大于蜜罐概率，且 $q' < 1-2q$, $q+q' > 1/2$ 。

由以上分析可知：在 $p < 2/(2+\gamma)$, $q < 1/2$，且 $q\eta_1 c + q'\eta_2 c < \gamma a - b - q\gamma a$ 时，组合$((\pi_{11}, \pi_{11}, \pi_{11}), (\pi_{21}, \pi_{21}))$即“服务-服务-服务-访问-攻击”，构成了贝叶斯均衡策略。在这种情况下，服务概率总是大于蜜罐概率，且服务和伪蜜罐出现的概率之和大于 $1/2$。

(2) $p > 2/(2+\gamma)$ 条件下，服务者占优组合策略为$(\pi_{10}, \pi_{11}, \pi_{10})$，计算合法客户和攻击者收益，可知$((\pi_{10}, \pi_{11}, \pi_{10}), (\pi_{21}, \pi_{21}))$并不构成均衡策略。

同理推知，当 $q\eta_1 c + q'\eta_2 c > \gamma a - b - q\gamma a$ 且 $q < 1/2$ 时，此时的服务概率小于蜜罐概率，攻击者选择不攻击，组合策略$((\pi_{11}, \pi_{11}, \pi_{11}), (\pi_{21}, \pi_{20}))$即“服务-服务-服务-访问-不攻击”可以构成贝叶斯纳什均衡策略。

3　拟态式蜜罐诱骗特性分析

以上我们运用博弈理论，形式化描述了拟态蜜罐的诱骗博弈，推理了攻击者知晓和不知晓伪蜜罐存在的两种情况下攻防双方达到贝叶斯纳什均衡博弈的条件和均衡策略。

在攻击者不知道伪蜜罐存在的情况下，拟态式蜜罐存在 3 种均衡博弈策略。其中，“服务-服务-服务-访问-攻击”均衡策略是常见的博弈结果，此时攻击者和合法用户都发起访问请求，而服务、蜜罐和伪蜜罐全部提供服务，均衡条件为 $p < 2/(2+\gamma)$, $q+q' < 1/2$ 且 $q+q' < (\gamma a - b)/(\gamma a + \eta c)$ 成立。该条件不仅与攻击概率 p 有关，还与蜜罐、伪蜜罐的概率有关。也就是说，攻击者攻击概率可以影响到博弈结果，因而具有“被动式主动防御”特点[12]。另一个博弈均衡策略“服务-服务-服务-访问-不攻击”则需满足条件 $(\gamma a - b)/(\gamma a + \eta c) < q+q' < 1/2$，该条件显然只与蜜罐和伪蜜罐出现的概率、诱骗因子等有关，而与攻击者的攻击概率 p 无关。也就是说，防御者能够完全控制博弈均衡条件，因而是防御者最理想的主动防御博弈结果。第 3 种博弈均衡策略“不服务-服务-不服务-不访问-不攻击”中，服务和伪蜜罐都停止服务，合法客户和攻击者都不访问，这显然不符合实际情况。

与传统蜜罐诱骗博弈做相比，拟态式蜜罐的博弈均衡条件更具有灵活性和迷惑性。传统蜜罐诱骗中存在博弈均衡条件是：$q < 1/2$ 成立前提下，比较 q 与 $(\gamma a - b)/(\gamma a + \eta c)$ 大小关系，进而选择不同的贝叶斯均衡策略[12]。而在拟态式蜜罐中博弈均衡条件变为：$q+q' < 1/2$ 成立前提下，比较 $q+q'$ 与 $(\gamma a - b)/(\gamma a + \eta c)$ 的结果，均衡条件与 $q+q'$，即蜜罐和伪蜜罐出现的概率和有关，不再只受单一的蜜罐概率 q 的限制，因而可以通过调节蜜罐和伪蜜罐的部署，使拟态蜜罐诱骗博弈达到不同的博弈均衡，提高防御机制的灵活性、主动性和对敌手的迷惑性。

在攻击者知晓伪蜜罐存在的情况下，拟态蜜罐同样存在 3 种博弈均衡策略，但博弈均衡条件有所变化。其中，常见均衡策略“服务-服务-服务-访问-攻击”要求满足条件 $p < 2/2+\gamma$, $q < 1/2$ 且 $q\eta_1 c + q'\eta_2 c < \gamma a - b - q\gamma a$，此时服务概率总是大于蜜罐概率并且服务和伪蜜罐出现的概率之和大于 $1/2$。另一个主动防御的均衡策略“服务-服务-服务-访问-不攻击”则要求满足条件 $q\eta_1 c + q'\eta_2 c > \gamma a - b - q\gamma a$ 且 $q < 1/2$，该情况下服务概率小于蜜罐概率，且蜜罐和伪蜜罐的概率之和大于 $1/2$；第 3 种均衡策略“不服务-服务-不服务-不访问-不攻击”同样不符合实际情况。

得到结论：在拟态蜜罐系统中，当服务出现概率总是大于蜜罐概率，服务和伪蜜罐出现概率之和大于 $1/2$，即真实服务概率大于 $1/2$ 且 $q' < 1-2q$，此时攻击者选择攻击，组合策略$((\pi_{11}, \pi_{11}, \pi_{11}), (\pi_{21}, \pi_{21}))$“服务-服务-服务-访问-攻击”达到贝叶斯纳什均衡。这与生物拟态中被模拟者出现概率大于模拟者出现概率的有效性条件相一致，体现出了拟态式系统的保护色机制。而组合策略$((\pi_{11}, \pi_{11}, \pi_{11}), (\pi_{21}, \pi_{20}))$“服务-服务-服务-访问-不攻击”均衡策略需要满足 $1-(q+q') < q$ 且 $q+q' > (\gamma a - b - q\gamma a)/\eta c > 1/2$，即蜜罐出现概率大于服务出现概率，且蜜罐和伪蜜罐出现概率之和大于 $1/2$，此时蜜罐出现概率较大，攻击者选择不攻击，体现出了拟态式系统的警戒色机制。

进一步讨论博弈均衡情况，不论攻击者已知或未知伪蜜罐的存在，诱骗博弈可以在 $(\gamma a - b)/(\gamma a + \eta c) < q+q' < 1/2$ 或 $q\eta_1 c + q'\eta_2 c > \gamma a - b - q\gamma a$ 且 $q < 1/2$ 条件下达到理想博弈均衡，即达到$((\pi_{11}, \pi_{11}, \pi_{11}), (\pi_{21}, \pi_{20}))$“服务-服务-服务-访问-不攻击”均衡策略。该均衡条件只与蜜罐出现的概率 q，伪蜜罐出现的概率 q'，以及蜜罐和伪蜜罐的诱骗因子 η_1 和 η_2 有关，而与攻击者概率 p 无关，也就是说博弈结果是由服务者完全控制的。与传统蜜罐相比较，

博弈结果不再只受单一的蜜罐概率 q 的限制，而是可以通过调节蜜罐概率 q 和伪蜜罐概率 q' 灵活部署，因而大大提高了防御机制的灵活性和迷惑性。防御者可以通过合理部署蜜罐和伪蜜罐从而改变其均衡条件来实现不同的博弈均衡，从而达到迷惑攻击者的目的。这就证明了拟态式蜜罐系统具有更好的主动性、有效性和迷惑性。

4 结束语

本文形式化描述了拟态式蜜罐诱骗博弈的局中人、博弈策略，构建了诱骗博弈收益矩阵，基于非合作不完全信息动态博弈理论，推理分析了拟态式蜜罐诱骗博弈中存在的贝叶斯纳什均衡策略和均衡条件，深入讨论了拟态式蜜罐模型中保护色、警戒色等拟态机制在诱骗博弈中的适用条件；通过对理想的诱骗博弈均衡策略、均衡条件以及影响因素的分析，证明了拟态式蜜罐诱骗博弈具有良好的主动性；通过与传统蜜罐博弈均衡条件的比较，阐述了拟态式蜜罐系统具有更好的灵活性、有效性和迷惑性。论文工作能够为拟态式蜜罐主动网络防御新策略性能及系统部署提供理论上的支持。

参 考 文 献

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

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

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

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

[5] Shi L, Jiang L, Liu D, *et al*.. Mimicry honeypots: a brief introduction[C]. WiCOM2012, IEEE Computer Society, Shanghai, 2012, 09: 1–4.

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

[7] 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.
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.

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

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

[10] Wagener G and State R. Self adaptive high interaction honeypots driven by game theory[C]. Stabilization, Safety, and Security of Distributed Systems, Lecture Notes in Computer Science, 2009, Vol.5873: 741–755.

[11] 厉章忠. 基于蜜罐技术的 DDOS 防御模型研究[D]. [硕士论文], 东华大学, 2009: 40–46.

[12] Garg N and Grosu D. Deception in honeynets: a game-theoretic analysis[C]. Proceedings of IEEE Information Assurance and Security Workshop, New York, 2007: 20–22.

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

[14] 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.
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.

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、博弈理论.

刘 昕： 女，1974 年生，博士，讲师，研究方向为网络与信息安全、社会网络.

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.