基于动态伪装网络的主动欺骗防御方法

王硕[1,2]，王建华[1]，裴庆祺[2,3]，汤光明[1]，王洋[1]，刘小虎[1]

（1. 信息工程大学密码工程学院，河南 郑州 450001；2. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
3. 西安电子科技大学陕西省区块链与安全计算重点实验室，陕西 西安 710071）

摘 要：针对现有蜜罐易被攻击者识破而导致其抵御渗透攻击时经常失效的问题，提出一种基于动态伪装网络的主动欺骗防御方法。首先，给出动态伪装网络定义并描述基于动态伪随网络的主动欺骗攻防场景；然后，在分析攻防交互过程的基础上，构建信号博弈模型来指导最优欺骗策略选取；进一步，设计基于双层威胁渗透图的攻防策略收益量化方法；最后，提出一种统一纯策略与混策略的博弈均衡求解方法。实验结果表明，基于动态伪装网络，精炼贝叶斯均衡能够为防御者实施最优防御策略提供有效指导，实现防御者收益最大化。此外，还总结了利用动态伪装网络进行主动欺骗防御的特点与规律。

关键词：蜜罐；网络欺骗防御；动态伪装网络；信号博弈；博弈均衡

中图分类号：TP393.8

文献标识码：A

doi:10.11959/j.issn.1000−436x.2020026

Active deception defense method based on dynamic camouflage network

WANG Shuo[1,2], WANG Jianhua[1], PEI Qingqi[2,3], TANG Guangming[1], WANG Yang[1], LIU Xiaohu[1]

1. Department of Cryptogram Engineering, Information Engineering University, Zhengzhou 450001, China
2. National Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China
3. Shaanxi Key Laboratory of Blockchain and Security Computing, Xidian University, Xi'an 710071, China

Abstract: In view of the problem that the existing honeypots often fail to resist the penetration attack due to the lack of confidentiality, an active deception defense method based on dynamic camouflage network (DCN) was presented. The definition of DCN was given firstly, and then the attacker-defender scenario of active deception based on DCN was described. Next, the interaction process of the attacker-defender scenario was modeled by using a signaling game, whose equilibrium can guide the selection of optimal deception strategy. Furthermore, to quantify the payoffs accurately, the two-layer threat penetration graph (TLTPG) was introduced. Finally, the solution for game equilibrium was designed, through which pure strategy and mixed strategy could be calculated simultaneously. The experimental results show that, based on the dynamic camouflage network, the perfect Bayesian equilibrium can provide effective guidance for the defender to implement the optimal defense strategy and maximize the benefits of the defender. In addition, the characteristics and rules of active deception defense DCN-based are summarized.

Key words: honeypot, network deception defense, dynamic camouflage network, signaling game, game equilibrium

1 引言

随着网络应用的广泛普及以及支撑技术的不断发展，云计算、智能设备、区块链、物联网等不断涌现的新技术正在深刻改变人们的生活，推动社会的飞速发展。然而，与此同时，伴随网络而来的

收稿日期：2019−10−31；**修回日期**：2019−12−09

基金项目：国家自然科学基金资助项目（No.U1636209）；陕西省重点研发计划基金资助项目（No.2019ZDLGY13-04, No.2019ZDLGY13-07）

Foundation Items: The National Natural Science Foundation of China (No.U1636209), The Key Research and Development Program of Shaanxi Province (No.2019ZDLGY13-04, No.2019ZDLGY13-07)

安全问题也越发严重。据国家计算机网络应急技术处理协调中心 2018 年度网络安全工作报告显示[1]，2018 年，我国境内感染计算机恶意程序的主机数量约为 1 256 万个，规模在 100 个主机以上的僵尸网络数量达 3 143 个，规模在 10 万个主机以上的僵尸网络数量达 32 个，WannaCry 蠕虫病毒事件爆发等。然而，在众多网络攻击形式中，渗透攻击威胁尤其巨大，特别是以高级持续攻击（APT, advanced persistent threat）为代表的渗透攻击，给人们带来了巨大的威胁。传统的网络防御以“筑高墙、堵漏洞、打补丁”为主，手段单一被动，不能有效应对新型攻击形式，且存在“攻防不对称”的严重劣势。

网络欺骗防御是改变“攻防不对称”劣势的创新思路，已成为当前网络安全防御的研究热点和重要研究方向之一[2-3]。它的核心思想在于：防御者在己方目标网络中布设骗局，干扰、误导攻击者对己方网络系统的认知，使攻击者采取对防御方有利的动作，从而有助于发现、延迟或阻断攻击者的活动，达到防护目标网络的目的[4]。美国提出的移动目标防御（MTD, moving target defense）[5-6]是增加攻击者的认知难度，而网络欺骗是干扰攻击者的认知，甚至使攻击者产生错误认知，显然网络欺骗相对移动目标防御层次更高，目标更远。也有学者称网络欺骗是“后移动目标防御时代”。2016 年，Springer 出版社出版了《Cyber Deception》[7]，这是第一本专门介绍网络欺骗研究的著作，汇集了最新的网络欺骗研究成果。网络欺骗不是一种具体的防御技术，而是由蜜罐演进而来的一种防御思想。

现有研究可将蜜罐分为狭义的蜜罐和广义的蜜罐。狭义的蜜罐作为传统意义的蜜罐，用来模拟服务或服务器等网络资源。根据交互水平，狭义的蜜罐可分为低交互蜜罐、中交互蜜罐和高交互蜜罐。Provos[8]提出了一种低交互蜜罐，通过模仿网络堆栈行为来欺骗 nmap 等指纹识别工具。此外，一些学者也提出了用于应用层协议的蜜罐，如 Telnet[9]和 HTTP[10]，还有一些针对特殊设备的蜜罐，如智能手机[11]、USB 设备[12]和数据采集装置[13]。广义的蜜罐则是基于蜜罐这种模拟思想，针对相对广泛的对象来模拟一些伪造的对象，从而达到欺骗攻击者的效果。Juels 等[14]提出一种 Honeywords 方法，通过构造虚假账户密码来检测用该密码尝试攻击的攻击者。Araujo 等[15]提出一种 Honey-patches 方法，通过巧妙设计虚假漏洞补丁来欺骗攻击者。Conroy 等[16]提出利用虚假新闻来欺骗攻击者。Lee 等[17]则提出在社交网络上设计蜜罐来欺骗垃圾邮件制造者。Lazarov 等[18]提出用虚假的 URL 地址欺骗攻击者。加密消息也被用来吸引并欺骗攻击者[19-20]。广义的蜜罐形式多种多样，理论上只要攻击者对网络中某一个对象有兴趣，则可依据该对象伪造一个虚假的对象，达到欺骗攻击者的目的。

此外，为了提高蜜罐的隐蔽性，避免其被攻击者识破，Clark 等[21]通过周期性地改变蜜罐节点的 IP 地址，使攻击者已识别出的蜜罐 IP 失效，从而增加蜜罐节点的安全性。Sun 等[22-23]将 IP 随机化与伪造欺骗节点巧妙结合，在目标网络中放置蜜罐节点，并通过真实节点与蜜罐节点的 IP 随机化来干扰攻击者。Venkatesan 等[24]提出利用强化学习来部署检测器和蜜罐，实现最优化地去除僵尸节点的目的。然而该方法学习周期过长，模型训练较难。石乐义等[25]提出基于动态阵列蜜罐的协同部署方法来达到干扰和防范攻击者的目的。然而上述几种方法往往不考虑防御成本，从而导致实用性较低。为了获得有限防御成本下的最优欺骗策略，一些学者[26-30]用博弈论思想描述攻防对抗过程，并用纳什均衡解作为最优欺骗策略，取得了较好的效果。然而大多研究仅考虑纳什均衡的纯策略而忽略了混策略。事实上，混策略由于其特有的随机性更能使攻击者产生不确定性，更适合于欺骗防御攻防场景。

基于以上分析可知，当前的渗透攻击往往是针对特定目标的定向攻击，持续时间长且隐蔽性强。现有蜜罐很容易被攻击者识破而失效。为了实现对渗透攻击者的最大化欺骗，本文提出一种基于动态伪装网络的主动欺骗防御方法。动态伪装网络包括真实网络和伪装网络，其中伪装网络是依据真实网络而创建的虚假网络。首先，基于动态伪装网络描述了攻防对抗场景。该场景中，借助动态伪装网络，防御者通过向攻击者发送伪装信号，从而使处于真实网络中的攻击者受到威慑而放弃攻击，并使处于伪装网络中的攻击者受到欺骗而攻击虚假目标，从而实现对真实网络的更好防护。其次，为了最大化防御收益，将攻防双方对抗过程用信号博弈模型进行描述，设计了基于双层威胁渗透图的攻防策略收益量化方法；进而提出了一种统一纯策略与混策略的精炼贝叶斯纳什均衡求解方法，利用精炼贝叶斯纳什均衡作为最优欺骗策略，实现了防御收益的最

大化。最后，实验表明了本文方法的有效性，并在分析实验结果的基础上提出了针对性的主动欺骗防御规律及建议。

2　基于动态伪装网络的主动欺骗攻防场景

一般来讲，蜜罐主要通过布置一些作为虚假的主机、网络服务或者信息，致使攻击方对其实施攻击，从而捕获攻击者信息。多个蜜罐组成的模拟网络称为蜜网，其本质仍是蜜罐，反而有时更容易被攻击者识破。然而事实上，对于真正高水平的渗透攻击者，其不仅对目标网络有一定的了解，且其攻击目标非常明确，为了不暴露自己的攻击痕迹，攻击者仅对自己的攻击目标感兴趣，如“震网”病毒没有发现攻击目标时，其一直保持“静默”，直到满足攻击条件。面对该种攻击者，传统的蜜罐或蜜网很难引起攻击者的兴趣且容易被其识别，往往不能达到欺骗攻击者的目的。基于上述考虑，为了进一步提高欺骗环境的真实性而达到欺骗攻击者的目的，本文提出一种基于动态伪装网络的主动欺骗防御方法。动态伪装网络的定义如定义 1 所示。

定义 1　动态伪装网络（DCN, dynamic camouflage net）DCN=(G,G')。对一个特定的真实网络 G，动态实时地模拟真实网络 G 中节点、拓扑、功能及数据等，创建用于欺骗攻击者入侵而获得攻击者知识的伪装网络 G'。其中 G'可以是真实的物理网络，也可以是利用软件定义网络（SDN, software defined network）及虚拟化的容器技术创建的网络。动态伪装网络的拓扑示例如图 1 所示。

由定义 1 及图 1 可知，与传统的蜜罐或蜜网不同，DCN 近似完美地“复制”真实网络 G，真实网络中的每一个节点都能在伪装网络 G'中找到它的“影子”节点，其真实性更高，对攻击者的干扰性也更强，更易实现欺骗攻击者的目的。然而，通常情况下，真实网络运行着正常的业务活动或为合法用户提供服务，其系统活跃性较高；相反，伪装网络尽管与真实网络相似，但由于伪装网络是专门为攻击者打造的，缺少正常的网络业务活动，其系统活跃性相对较低，一旦有用户访问伪装网络，则认为该用户为攻击者。该问题也导致攻击者会依据所在网络的系统活性来分辨其所处的网络类型，防止被欺骗。

鉴于此，本文深入分析该攻防场景，利用主动欺骗思想，设计了一种基于动态伪装网络的主动欺骗防御方法。该方法中，借助动态伪装网络，防御者向攻击者发送伪装信号，使处于真实网络中的攻击者受到威慑而放弃攻击，并使处于伪装网络中的攻击者受到欺骗而攻击虚假目标，从而实现对目标网络的更好防护。基于动态伪装网络的主动欺骗攻防场景如图 2 所示。

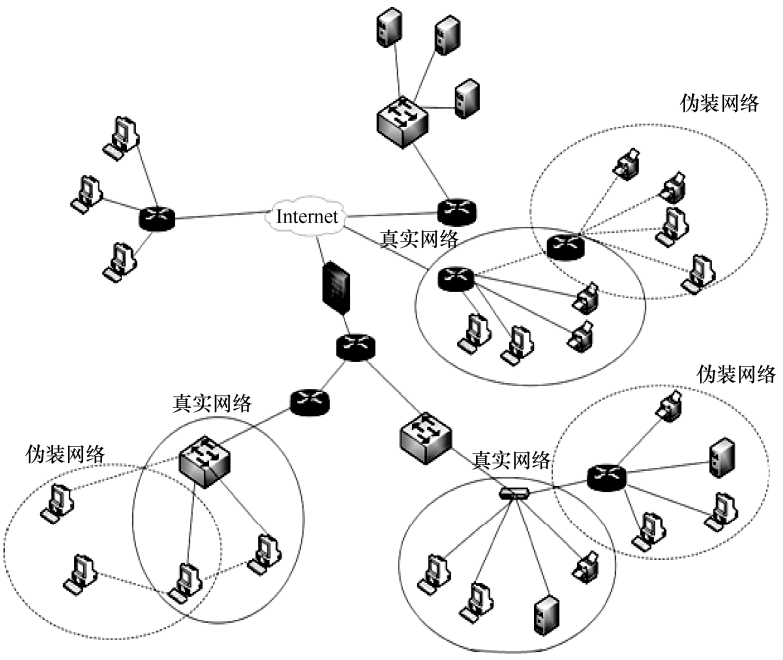


图 1　动态伪装网络的拓扑示例

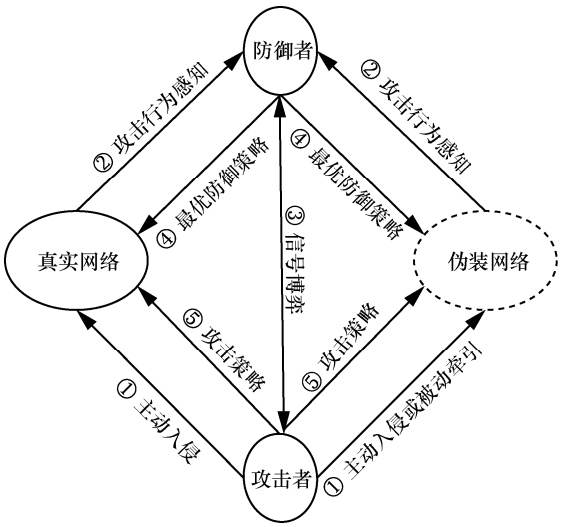


图 2 基于动态伪装网络的主动欺骗攻防场景

依据图 2，基于伪装网络的网络主动欺骗攻防场景可分为以下 5 个步骤。

Step1 攻击者为了达到攻击目标，需要对目标网络进行持续渗透，在渗透过程中，攻击者可能入侵真实网络或者伪装网络。此外，防御者可通过流量牵引的方法，将处于真实网络中某一节点的攻击者牵引到伪装网络中对应的节点，从而实现攻击者由真实网络到伪装网络的被动牵引。

Step2 防御者通过分析网络产生的告警来实现对攻击者的行为感知，进而推断攻击者当前所处的节点及攻击目标。

Step3 一方面，攻击者通过分析所在网络的系统活性来识别该网络类型，进而决策下一步的攻击；另一方面，防御者可发送伪装信号来干扰攻击者（通过减少或暂停部分网络活动来降低真实网络的系统活性，或通过伪造虚假的流量来提高伪装网络的系统活性），使攻击者无法正确识别其所处的网络类型。在此过程中，攻击者与防御者展开博弈，该博弈过程可用信号博弈模型描述。

Step4 依据博弈结果，防御者选取最优的防御策略，即是否发送伪装信号。

Step5 依据博弈结果，攻击者选取最优的攻击策略，即是否对攻击目标发动攻击。

3 信号博弈模型

任何实用的防御策略均需要考虑防御收益，博弈论是网络安全领域公认的定量分析攻防对抗收益的有力工具。在基于动态伪装网络的网络主动欺骗防御攻防场景中，网络类型对攻击策略有着重要的影响：若攻击者处于真实网络中，它将继续渗透最终实现攻击目标；若攻击者处于伪装网络中，它将放弃攻击以减少毫无意义的攻击花费。事实上，攻击者并不知道其所处网络的类型，而需通过探测所处网络的系统活性来推断网络类型；防御者可通过发送伪装信号来干扰攻击者的推断。已有研究表明，信号博弈模型可以使防御者通过主动选择及发送伪装信号，实现对攻击者的欺骗、干扰，提升主动欺骗防御能力，适用于本文提出的攻防场景，能够为防御者选取最优防御策略提供指导。

3.1 信号博弈模型定义

作为不完全信息动态博弈的一种，信号博弈能够准确描述不确定信息对攻防策略选择的影响。由第 2 节的攻防场景描述可知，攻防对抗过程是一个非合作、不完全信息、多阶段、动态博弈的过程。因此，该过程可用信号博弈模型来描述，定义如下。

定义 2 信号博弈模型（SGM, signaling game model）是一个五元组，即 SGM=(Ω,Θ,S,P,U)，各变量具体定义如下。

1) $\Omega=\{\Omega_d, \Omega_a\}$为局中人集合，$\Omega_d$为防御者，作为信号发送者；$\Omega_a$为攻击者，作为信号接收者。

2) $\Theta=\{N, H\}$为防御者类型空间，在该攻击过程中，防御者类型可认为是攻击者所处的网络类型，N表示攻击者处于真实网络G，H表示攻击者处于伪装网络G'。攻击者并不知道其所处的网络类型，其仅有对自己所处网络类型的先验概率。

3) $S=\{D,A\}$为防御者与攻击者的行动空间。其中，$D=\{d_1, d_2\}$为防御者的行动空间，d_1代表维持和真实网络相似的较高的系统活性，d_2表示维持和伪装网络相似的较低的系统活性。具体来讲：① 当防御者类型为N时，防御者一方面可不采取任何动作来实现行动d_1，另一方面可通过减少或暂停部分网络活动来降低真实网络的系统活性，使真实网络看起来与伪装网络相似，从而来实现行动d_2；② 当防御者类型为H时，防御者一方面可通过伪造虚假的流量来提高伪装网络的系统活性，使伪装网络看起来与真实网络相似，从而来实现行动d_1，另一方面可不采取任何动作来实现行动d_2。$A=\{a_1,a_2\}$为攻击者的行动空间，a_1表示攻击者选择入侵，a_2表示攻击者选择不入侵。

4) $P:\Theta\mapsto[0,1]\times[0,1]$为攻击者对防御者类型的先验概率。$P=[p,1-p]$，其中 $p=P(\Theta=N)$表示防御者类型是真实网络的概率，$1-p=P(\Theta=H)$表示防御者

类型是伪装网络的概率。

5) $U=\{u_d,u_a\}$为防御者和攻击者的收益函数。

本文所提信号博弈模型主要分为 4 个阶段。

1) 自然以概率分布$(p,1-p)$从防御者类型空间$\Theta=\{N, H\}$选择防御者类型，即 $P(\Theta=N)=p\in[0,1]$，$P(\Theta=H)=1-p\in[0,1]$。

2) 由于目标网络入侵检测系统的存在，防御者能够实时感知攻击者所处的网络类型。当防御者观察到防御者类型后，从伪装信号集 $D=\{d_1,d_2\}$中选择一个信号进行执行。

3) 攻击者不能观测到防御者类型，但能观测到防御者发送的信号，然后从攻击行动集 $A=\{a_1,a_2\}$中选择一个动作。

4) 攻防双方得到收益函数 $U=\{u_d,u_a\}$，收益函数的设定原则为回报与花费之差。

图 3 给出了本文所提信号博弈模型的一种扩展式描述。图 3 中的每一个分支表示一种博弈情况，由虚线连接的节点构成一个信息集。由于攻击者不能确定防御者的类型，因此攻击者不能区分信息集中的节点属于哪一种防御者类型。图 3 中包含了 2 个信息集，一个是 d_1 信息集，另一个是 d_2 信息集。

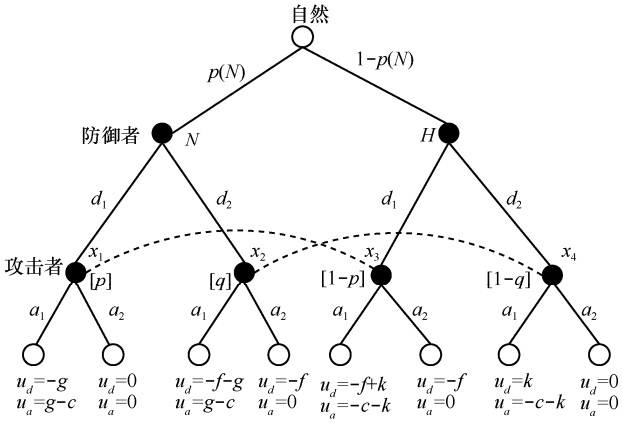


图 3　信号博弈的扩展式表述

对于防御者来讲，当防御者类型为 N，即攻击者当前所处的网络为真实网络时，若防御者执行行动 d_1，表示防御者没有采取任何动作，其花费为 0；若防御者执行行动 d_2，表示防御者减少或暂停部分网络活动来降低真实网络的系统活性，需要一定的花费。同样，当防御者类型为 H，即攻击者当前所处的网络为伪装网络时，若防御者执行行动 d_1，表示防御者伪造虚假流量来提高伪装网络的系统活性，需要一定的花费；若防御者执行行动 d_2，表示防御者没有采取任何动作，其花费为 0。为了简化，假设处于真实网络中的防御者减少或暂停部分网络活动来降低真实网络系统活性所需的花费与处于伪装网络中的防御者伪造虚假流量来提高伪装网络系统活性所需的花费相同，统一记为 f。

对于渗透攻击的攻击者来讲，攻击者入侵的最终目标往往是获得目标网络中一个攻击目标节点的 Root 权限，如入侵目标网络的数据库服务器进而获得机密数据。不妨设攻击者的攻击目标节点价值为 g，则攻击者入侵真实网络中的攻击目标节点成功时，其获得收益 g，付出的攻击代价记为 c，显然，此时防御者便失去了价值 g。相反，若攻击者入侵了伪装网络中的攻击目标节点时，由于伪装网络和真实网络的拓扑相同，其付出的攻击代价同样为 c，然而攻击者在伪装网络中获取的数据只能是虚假数据，其攻击收益为 0。此外，该种情况下，由于入侵伪装网络，攻击者的身份等信息会暴露给防御者，对攻击者造成一定的损失，记为 k，显然，此时防御者可得到收益 k。一般来说，k 的值相对较小，本文假设 $g>k$，$f>k$。

在图 3 中，当防御者类型为 N，防御者和攻击者分别采取策略(d_1,a_1)时，防御者的收益为$-g$，攻击者的收益为 $g-c$；当防御者类型为 N，防御者和攻击者分别采取策略(d_1,a_2)时，防御者的收益为 0，攻击者的收益为 0。其他情况的攻防双方收益不再赘述。

3.2　基于双层渗透威胁图的攻防策略收益量化

3.1 节给出了攻防双方的信号博弈模型，依据博弈均衡理论可知，该博弈模型的纳什均衡能够给出攻防双方的最优策略。而事实上，博弈模型的均衡结果往往取决于攻防双方的收益函数。因此，如何准确量化博弈模型中攻防双方的收益函数成为选取最优防御策略的关键。依据图 3 可知，本文信号博弈模型中，有 4 个需要量化的参数：真实网络中攻击目标节点的价值 g、攻击者入侵伪装网络产生的损失 k、防御者发送伪装信号所需的代价 f 和攻击者渗透过程花费的攻击代价 c。由于前 3 个参数的设定相对简单，可依据网络自身价值以及攻击者知识直接量化。攻击者渗透过程花费的攻击代价 c 往往与网络中的漏洞难易程度、攻击者能力及攻击者所处的网络位置等因素有关，不能直接设定。鉴于此，为了准确量化该参数，本文提出基于双层渗透威胁图（TLTPG, two-layer threat penetration graph）的攻击代价量化方法。双层渗透威胁图是一

个双层图结构，下层为主机威胁渗透图（HTPG, host threat penetration graph），描述了目标网络中任意 2 个主机间的微观渗透场景；上层为网络威胁渗透图（NTPG, network threat penetration graph），描述了目标网络中各主机之间的宏观渗透关系。

定义 3 主机威胁渗透图 $G_{\mathrm{HTPG}}=(N_{\mathrm{HTPG}}, E_{\mathrm{HTPG}})$。$N_{\mathrm{HTPG}}$ 表示节点，用<Host,Privilege>表示，描述攻击者获得的主机权限，其中 Host 表示攻击者已渗透的主机，可用该主机的 IP 地址表示，Privilege 表示攻击者获得的主机权限，分为 User 和 Root；E_{HTPG} 表示边，用于描述单步渗透攻击，用<Service, Vulnerability, Probability>表示，其中 Service 表示渗透攻击所利用的主机服务，Vulnerability 表示渗透攻击所利用主机服务上的漏洞，一般用公共漏洞和暴露（CVE, common vulnerability and exposure）编号表示，Probability 表示渗透攻击成功的概率。

定义 4 网络威胁渗透图 $G_{\mathrm{NTPG}}=(N_{\mathrm{NTPG}}, E_{\mathrm{NTPG}})$。$N_{\mathrm{NTPG}}$ 表示节点，描述主机标识，一般用主机的 IP 地址表示；E_{NTPG} 表示边，描述主机间渗透成功概率，用<U_P, R_P>表示，其中 U_P 表示从源主机渗透获得目的主机 User 权限的概率，R_P 表示从源主机渗透获得目的主机 Root 权限的概率，二者均为 0~1 之间的实数。

图 4 展示了一个简单的 TLTPG 实例。相对于传统的攻击图，TLTPG 通过分层，宏观与微观相结合，有效减少了由于生成全局攻击图造成的高计算复杂度和空间复杂度，便于量化及计算面向渗透攻击的攻击代价。

TLTPG 能够给出目标网络中任意 2 个主机的直接渗透成功概率，在此基础上，文献[31]给出了任意 2 个主机间的最优渗透路径的生成方法。由于攻击者在入侵时，总希望付出较少的攻击代价，因此可假设攻击者进行渗透攻击时，会沿着最优渗透路径传输。此外，TLTPG 给出了渗透成功概率，而事实上，攻击代价与渗透成功概率有着重要的联系。一般人们认为，渗透成功概率越高，攻击代价越低；相反则攻击代价越高。渗透成功概率是依据通用漏洞评分系统（CVSS, common vulnerability scoring system）和网络拓扑量化得来，可信度较高，也得到学者的广泛认可。然而，针对攻击代价量化评估的相关研究较少，大多

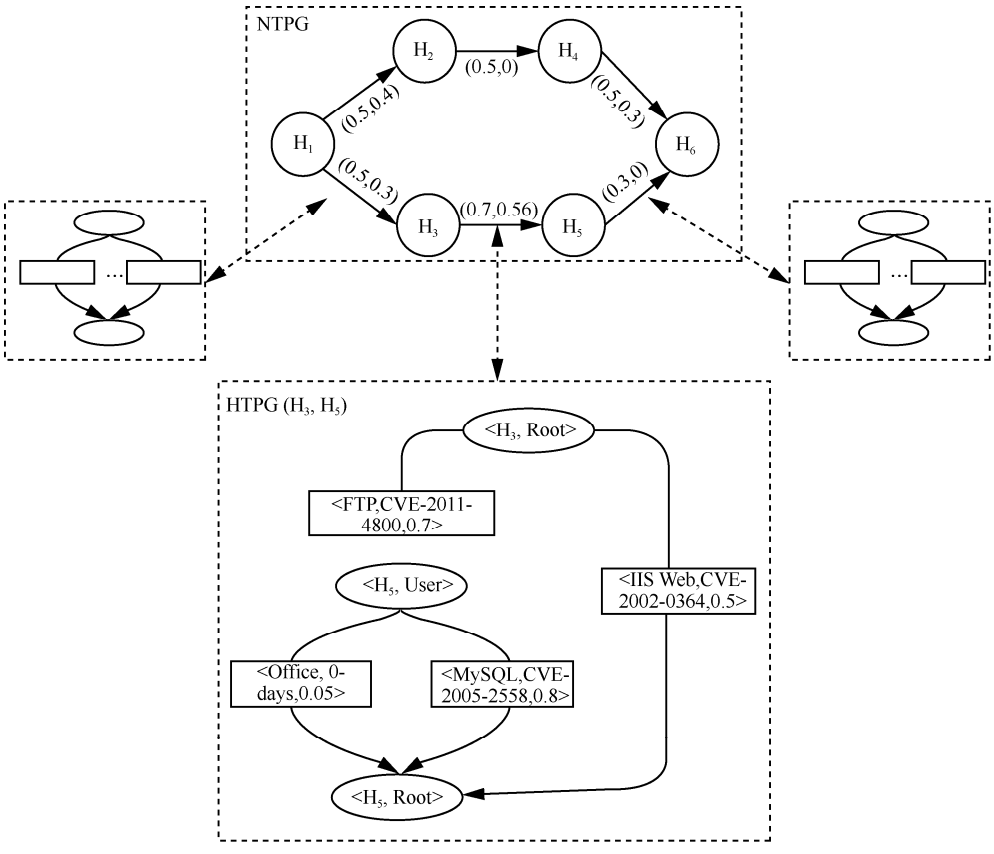


图 4 一个简单的 TLTPG 实例

依据专家经验，准确度不高。因此，通过渗透成功概率来间接量化攻击代价是一种合理的方法。鉴于此，本文研究得出一种利用渗透成功率量化攻击代价的新方法。不妨设当攻击者从节点 n_i 入侵节点 n_j 时，其攻击成功率为 s_{ij}，其需要的攻击代价记为 c_{ij}。则在同一个 TLTPG 中，c_{ij} 的量化需要满足以下 2 个条件。

1) 对于任意 2 个渗透动作 e_{ij}（攻击者从节点 n_i 入侵节点 n_j）和 e_{pq}（攻击者从节点 n_p 入侵节点 n_q），若 $s_{ij} \leqslant s_{pq}$，则 $c_{pq} \geqslant c_{ij}$。

2) 对于任意 2 条攻击路径 $\text{path}_{ij} = n_i \to n_x \to n_y \to \cdots \to n_z \to n_j$ 和 $\text{path}_{pq} = n_p \to n_{x'} \to n_{y'} \to \cdots \to n_{z'} \to n_q$，若存在 $s_{ix}s_{xy}\cdots s_{zj} \geqslant s_{px'}s_{x'y'}\cdots s_{z'q}$，则有 $c_{ix} + c_{xy} + \cdots + c_{zj} \leqslant c_{px'} + c_{x'y'} + \cdots + c_{z'q}$。

定理 1　当 $c_{ij} = \kappa \log \dfrac{1}{s_{ij}}$ 时，其中 κ 为一正值，可用 c_{ij} 来表示攻击者能力系数，其满足上述 2 个条件。

证明

针对条件 1)，当 $c_{ij} = \kappa \log \dfrac{1}{s_{ij}}$ 时，$c_{pq} - c_{ij} = \kappa\left(\log \dfrac{1}{s_{pq}} - \log \dfrac{1}{s_{ij}}\right) = \kappa \log \dfrac{s_{ij}}{s_{pq}}$，又 $\kappa > 0$，$s_{ij} \leqslant s_{pq}$，可得 $\kappa \log \dfrac{s_{ij}}{s_{pq}} \geqslant 0$，即 $c_{pq} \geqslant c_{ij}$，故条件 1)满足。

针对条件 2)，当 $c_{ij} = \kappa \log \dfrac{1}{s_{ij}}$ 时，$c_{ix} + c_{xy} + \cdots + c_{zj} = \kappa \log \dfrac{1}{s_{ix}s_{xy}\cdots s_{zj}}$，同理可知 $c_{px'} + c_{x'y'} + \cdots + c_{z'q} = \kappa \log \dfrac{1}{s_{px'}s_{x'y'}\cdots s_{z'q}}$，则 $c_{px'} + c_{x'y'} + \cdots + c_{z'q}$ 与 $c_{ix} + c_{xy} + \cdots + c_{zj}$ 的差可化简为 $\kappa \log \dfrac{s_{ix}s_{xy}\cdots s_{zj}}{s_{px'}s_{x'y'}\cdots s_{z'q}}$，由条件 2)易知，当满足 $s_{ix}s_{xy}\cdots s_{zj} \geqslant s_{px'}s_{x'y'}\cdots s_{z'q}$ 时，可得 $\kappa \log \dfrac{s_{ix}s_{xy}\cdots s_{zj}}{s_{px'}s_{x'y'}\cdots s_{z'q}} \geqslant 0$，进而可得 $c_{ix} + c_{xy} + \cdots + c_{zj} \leqslant c_{px'} + c_{x'y'} + \cdots + c_{z'q}$。

证毕。

由定理 1 可知，$c_{ij} = \kappa \log \dfrac{1}{s_{ij}}$ 能够作为定量评估攻击代价的方式，其中 κ 可依据具体的攻防场景及标准化需求确定。

4　精炼贝叶斯纳什均衡求解及最优欺骗防御策略选取

信号博弈作为一种不完全信息动态博弈，其对应的纳什均衡为精炼贝叶斯纳什均衡。纳什均衡的存在性定理表明，任何一个有限博弈都至少存在一个纳什均衡（纯策略和混策略）[32]。然而，许多学者在分析信号博弈的均衡过程中，为了简化均衡求解过程，往往通过主观限定条件，仅仅考虑纯策略（包含分离策略和混同策略），忽略混策略。这种情况往往会遗漏最优策略。除此之外，由于混策略可看成纯策略的随机组合。在混策略中，局中人在博弈前通过随机装置确定自己的策略，如上抛一枚硬币等，其他局中人便不能观测到其行为，这增加了对方的不确定性，更适合于欺骗防御攻防场景。鉴于此，本文提出一种统一简洁的精炼贝叶斯纳什均衡求解方法，该方法能将纯策略与混策略统一起来求解，且求解方式快速简洁。

定义 5　信号博弈模型（SGM, signaling game model）具有精炼贝叶斯纳什均衡 $\text{EQ} = (d^*(\theta), a^*(d), \tilde{P}(\theta \mid d))$，其中 $d^*(\theta)$ 为防御者的类型依存信号策略，表明防御者类型为 $\theta \in \Theta$ 时，其执行的伪装信号策略为 $d^*(\theta)$；$a^*(d)$ 为攻击者的依存信号策略，表明攻击者在接收到防御者发送的信号 d 时，其执行的攻击策略为 $a^*(d)$；$\tilde{P}(\theta \mid d)$ 为攻击者在接收到防御者发送的信号 d 后，判断防御者类型的后验概率。该均衡满足以下 3 个条件。

1) $a^*(d) = \arg\max_{a \in A} \sum \tilde{P}(\theta \mid d) u_a(\theta, d^*(\theta), a)$。

2) $d^*(\theta) = \arg\max_{d \in D} u_d(\theta, d, a^*(d))$。

3) $\tilde{P}(\theta \mid d)$ 为攻击者基于先验概率、观测到的信号 d 和攻击策略 $a^*(d)$ 依据贝叶斯法则计算得到。

依据定义 5，本文的精炼贝叶斯均衡的求解方法可分为 4 步。

1) 攻防双方策略形式化表示

若防御者的策略为：当节点类型为 N 时，以概率 e_1 发送信号 d_1，以概率 $1-e_1$ 发送信号 d_2；当节点类型为 H 时，以概率 e_2 发送信号 d_1，以概率 $1-e_2$ 发送信号 d_2。则该策略可形式化表示为

$\left(\left(\begin{matrix}d_1\\e_1\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_1\end{matrix}\right)\right),\left(\left(\begin{matrix}d_1\\e_2\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_2\end{matrix}\right)\right)$。

若攻击者的策略为：当接收到信号 d_1 时，以概率 τ_1 选择动作 a_1，以概率 $1-\tau_1$ 选择动作 a_2；当接收到信号 d_2 时，以概率 τ_2 选择动作 a_1，以概率 $1-\tau_2$ 选择动作 a_2。则该策略可形式化表示为 $\left(\left(\begin{matrix}a_1\\\tau_1\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_1\end{matrix}\right)\right),\left(\left(\begin{matrix}a_1\\\tau_2\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_2\end{matrix}\right)\right)$。

2) 攻击者对防御者类型的后验概率确定

攻击者对防御者类型的后验概率的确定由其先验概率与防御者策略决定，并依据贝叶斯定理推断得出。

不妨设先验概率 $p(N)=p$，则 $p(H)=1-p$。当防御者采取策略 $\left(\left(\begin{matrix}d_1\\e_1\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_1\end{matrix}\right)\right),\left(\left(\begin{matrix}d_1\\e_2\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_2\end{matrix}\right)\right)$ 时，由贝叶斯定理知

$$p(N\mid d_1)=\frac{p(N)p(d_1\mid N)}{p(N)p(d_1\mid N)+p(H)p(d_1\mid H)}=\frac{pe_1}{pe_1+(1-p)e_2} \tag{1}$$

$$p(N\mid d_2)=\frac{p(N)p(d_2\mid N)}{p(N)p(d_2\mid N)+p(H)p(d_2\mid H)}=\frac{p(1-e_1)}{p(1-e_1)+(1-p)(1-e_2)} \tag{2}$$

$$p(H\mid d_1)=1-\frac{pe_1}{pe_1+(1-p)e_2} \tag{3}$$

$$p(H\mid d_2)=1-\frac{p(1-e_1)}{p(1-e_1)+(1-p)(1-e_2)} \tag{4}$$

3) 防御者最优策略判定

当策略 $\left(\left(\begin{matrix}d_1\\e_1\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_1\end{matrix}\right)\right),\left(\left(\begin{matrix}d_1\\e_2\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_2\end{matrix}\right)\right)$ 为防御者最优策略时，需满足

$$e_1=\arg\max_{0\leqslant e_x\leqslant 1}u_d\left(N,\left(\left(\begin{matrix}d_1\\e_x\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_x\end{matrix}\right)\right),\left(\left(\begin{matrix}a_1\\\tau_1\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_1\end{matrix}\right)\right),\left(\left(\begin{matrix}a_1\\\tau_2\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_2\end{matrix}\right)\right)\right) \tag{5}$$

$$e_2=\arg\max_{0\leqslant e_y\leqslant 1}u_d\left(H,\left(\left(\begin{matrix}d_1\\e_y\end{matrix}\right),\left(\begin{matrix}d_2\\1-e_y\end{matrix}\right)\right),\left(\left(\begin{matrix}a_1\\\tau_1\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_1\end{matrix}\right)\right),\left(\left(\begin{matrix}a_1\\\tau_2\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_2\end{matrix}\right)\right)\right) \tag{6}$$

进而可化简为

$$e_1=\arg\max_{0\leqslant e_x\leqslant 1}\left(e_x[(\tau_2-\tau_1)g+f]-(\tau_2 g+f)\right) \tag{7}$$

$$e_2=\arg\max_{0\leqslant e_y\leqslant 1}\left(e_y[(\tau_1-\tau_2)k-f]+\tau_2 k\right) \tag{8}$$

4) 攻击者最优策略判定

当策略 $\left(\left(\begin{matrix}a_1\\\tau_1\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_1\end{matrix}\right)\right),\left(\left(\begin{matrix}a_1\\\tau_2\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_2\end{matrix}\right)\right)$ 为攻击者最优策略时，需满足

$$\tau_1=\arg\max_{0\leqslant\tau_x\leqslant 1}E_{u_a}\left(\left(\left(\begin{matrix}a_1\\\tau_x\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_x\end{matrix}\right)\right)\middle| d_1\right) \tag{9}$$

$$\tau_2=\arg\max_{0\leqslant\tau_y\leqslant 1}E_{u_a}\left(\left(\left(\begin{matrix}a_1\\\tau_y\end{matrix}\right),\left(\begin{matrix}a_2\\1-\tau_y\end{matrix}\right)\right)\middle| d_2\right) \tag{10}$$

进而可化简为

$$\tau_1=\arg\max_{0\leqslant\tau_x\leqslant 1}\left(\tau_x[p(N\mid d_1)(g+k)-(c+k)]\right) \tag{11}$$

$$\tau_2=\arg\max_{0\leqslant\tau_y\leqslant 1}\left(\tau_y[p(N\mid d_2)(g+k)-(c+k)]\right) \tag{12}$$

不妨令

$$F_1(\tau_1,\tau_2)=(\tau_2-\tau_1)g+f \tag{13}$$

$$F_2(\tau_1,\tau_2)=(\tau_1-\tau_2)k-f \tag{14}$$

$$H_1(e_1,e_2)=p(N\mid d_1)(g+k)-(c+k) \tag{15}$$

$$H_2(e_1,e_2)=p(N\mid d_2)(g+k)-(c+k) \tag{16}$$

由一次函数单调性可知

$$e_1=\begin{cases}1, F_1(\tau_1,\tau_2)>0\\0, F_1(\tau_1,\tau_2)<0\\\text{rand}(0,1), F_1(\tau_1,\tau_2)=0\end{cases} \tag{17}$$

$$e_2=\begin{cases}1, F_2(\tau_1,\tau_2)>0\\0, F_2(\tau_1,\tau_2)<0\\\text{rand}(0,1), F_2(\tau_1,\tau_2)=0\end{cases} \tag{18}$$

$$\tau_1=\begin{cases}1, H_1(e_1,e_2)>0\\0, H_1(e_1,e_2)<0\\\text{rand}(0,1), H_1(e_1,e_2)=0\end{cases} \tag{19}$$

$$\tau_2=\begin{cases}1, H_2(e_1,e_2)>0\\0, H_2(e_1,e_2)<0\\\text{rand}(0,1), H_2(e_1,e_2)=0\end{cases} \tag{20}$$

其中，rand(0,1) 表示 0~1 之间的任意值。显然，任意一组 (e_1,e_2,τ_1,τ_2) 解，均可构成一个纳什均衡

$$\left(\left(\left(\left\langle\begin{matrix}d_1\\e_1\end{matrix}\right\rangle,\left\langle\begin{matrix}d_2\\1-e_1\end{matrix}\right\rangle\right),\left(\left\langle\begin{matrix}d_1\\e_2\end{matrix}\right\rangle,\left\langle\begin{matrix}d_2\\1-e_2\end{matrix}\right\rangle\right)\right),\right.$$
$$\left.\left(\left(\left\langle\begin{matrix}a_1\\\tau_1\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_1\end{matrix}\right\rangle\right),\left(\left\langle\begin{matrix}a_1\\\tau_2\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_2\end{matrix}\right\rangle\right)\right)\right)$$

例如，当满足

$$\begin{cases}F_1(\tau_1,\tau_2)=(\tau_2-\tau_1)g+f<0\\F_2(\tau_1,\tau_2)=(\tau_1-\tau_2)k-f<0\\H_1(e_1,e_2)=p(N\mid d_1)(g+k)-(c+k)>0\\H_2(e_1,e_2)=p(N\mid d_2)(g+k)-(c+k)<0\end{cases}\tag{21}$$

时，可得 $(e_1,e_2,\tau_1,\tau_2)=(0,0,1,0)$，此时存在均衡 $\left((d_2,d_2),(a_1,a_2)\right)$。式(21)可化简为

$$\begin{cases}f<g\\k<f\\p(N\mid d_1)>\dfrac{c+k}{g+k}\\p(N\mid d_2)<\dfrac{c+k}{g+k}\end{cases}\tag{22}$$

于是，当满足式 (22) 时，存在均衡 $\left((d_2,d_2),(a_1,a_2)\right)$，显然，该均衡为纯策略。同理可求得该信号博弈模型中的所有纳什均衡。特别地，当 (e_1,e_2,τ_1,τ_2) 的解中不存在 rand(0,1) 时，其对应的纳什均衡为纯策略纳什均衡；反之，当 (e_1,e_2,τ_1,τ_2) 的解中存在 rand(0,1) 时，其对应的纳什均衡为混策略纳什均衡。最终计算得出，本文信号博弈模型存在的所有纳什均衡如表 1 所示。表 1 纳什均衡中 e_1、e_2、τ_1、τ_2 的解均可视为 rand(0,1)。

表 1 展示了不同网络攻防条件下的所有精炼贝叶斯纳什均衡解。由纳什均衡的存在性定理知，对于不同的网络攻防条件，必存在纳什均衡解，而该均衡解便可作为最优欺骗防御策略。此外，在本文的攻防博弈模型中，防御者先于攻击者做决策，即防御者具有“提前选择”优势[27]。若存在多重均衡问题，一方面防御者可依据最大化自己的收益来选择策略；另一方面由于混策略具有干扰攻击者的作用，适用于欺骗防御策略，在收益相同的条件下，防御者可倾向于采用混策略。当防御者采用混策略时，需要根据实际情况使用一种随机装置，而该种

表 1　　**不同网络攻防状态条件下的所有精炼贝叶斯均衡解**

编号	纳什均衡	条件	类型
EQ_1	$\left((d_1,d_2),(a_2,a_2)\right)$	$g<c$	纯策略
EQ_2	$\left((d_1,d_2),(a_1,a_2)\right)$	$g>c; f>g$	纯策略
EQ_3	$\left((d_2,d_2),(a_1,a_2)\right)$	$g>c; k<f<g;\ \ p<\dfrac{c+k}{g+k}; p(N\mid d_1)>\dfrac{c+k}{g+k}$	纯策略
EQ_4	$\left(\left(\left(\left\langle\begin{matrix}d_1\\e_1\end{matrix}\right\rangle,\left\langle\begin{matrix}d_2\\1-e_1\end{matrix}\right\rangle\right),d_2\right),\left(a_1,\left(\left\langle\begin{matrix}a_1\\\tau_2\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_2\end{matrix}\right\rangle\right)\right)\right)$	$g>c; f<g;\ \ p>\dfrac{c+k}{g+k}$	混策略
EQ_5	$\left((d_2,d_2),\left(\left\langle\begin{matrix}a_1\\\tau_1\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_1\end{matrix}\right\rangle,a_2\right)\right)$	$g>c; f<g;\ \ p<\dfrac{c+k}{g+k};\ \ p(N\mid d_1)=\dfrac{c+k}{g+k}$	混策略
EQ_6	$\left((d_2,d_2),\left(a_1,\left(\left\langle\begin{matrix}a_1\\\tau_2\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_2\end{matrix}\right\rangle\right)\right)\right)$	$g>c; f<g;\ \ p=\dfrac{c+k}{g+k};\ \ p(N\mid d_1)>\dfrac{c+k}{g+k}$	混策略
EQ_7	$\left(\left(\left(\left\langle\begin{matrix}d_1\\e_1\end{matrix}\right\rangle,\left\langle\begin{matrix}d_2\\1-e_1\end{matrix}\right\rangle\right),d_2\right),(a_1,a_2)\right)$	$g>c; f=g$	混策略
EQ_8	$\left((d_2,d_2),\left(\left\langle\begin{matrix}a_1\\\tau_1\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_1\end{matrix}\right\rangle,\left\langle\begin{matrix}a_1\\\tau_2\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_2\end{matrix}\right\rangle\right)\right)$	$g>c;\ \ p=\dfrac{c+k}{g+k};\ \ p(N\mid d_1)=\dfrac{c+k}{g+k}$	混策略
EQ_9	$\left((d_1,d_2),\left(\left\langle\begin{matrix}a_1\\\tau_1\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_1\end{matrix}\right\rangle,a_2\right)\right)$	$g=c$	混策略
EQ_{10}	$\left(\left(\left(\left\langle\begin{matrix}d_1\\e_1\end{matrix}\right\rangle,\left\langle\begin{matrix}d_2\\1-e_1\end{matrix}\right\rangle\right),d_2\right),\left(\left(\left\langle\begin{matrix}a_1\\\tau_1\end{matrix}\right\rangle,\left\langle\begin{matrix}a_2\\1-\tau_1\end{matrix}\right\rangle\right),a_2\right)\right)$	$g=c; f<g$	混策略

随机装置最好不要让攻击者知道。

5 实验与分析

5.1 实验环境描述

为了验证本文方法的有效性，搭建了一个实际网络环境来进行测试。实验网络拓扑如图 5 所示。

实验网络主要由 2 个网络构成，即真实网络和伪装网络。伪装网络是依据真实网络构造的，其拓扑与真实网络保持一致。两者之间的唯一差别在于真实网络部署着真实的数据且运行着正常的业务活动，而伪装网络部署着虚假的数据且没有运行正常的业务活动。攻击者可利用 Internet 访问真实网络。2 个网络都可分为 4 个区域，分别是 DMZ 区、子网 1、子网 2 和子网 3。DMZ 区有一台 Web 服务器。子网 1 有 2 台设备，分别是一台 Pad 和一台主机，可连接 Internet。子网 2 有 2 台主机，不能连接 Internet。子网 3 包括 3 台服务器，分别是打印服务器、文件服务器和数据服务器。网络中的服务访问规则如表 2 所示。其中，攻击者为 Internet 中的一台主机。通过 Nessus 漏洞扫描器对网络中各网络段进行扫描，得到各主机中漏洞信息，结合 CVSS，得到表 3 所示的各主机信息及其所含漏洞信息。特别地，Pad 和 $Host_1$ 并不能通过网络访问内网的 $Host_2$ 和 $Host_3$，但由于人为操作不当的因素，可通过 USB 等传输设备连接到 $Host_2$ 和 $Host_3$。

表 2 网络中的服务访问规则

源主机	目的主机	运行服务
攻击者	Web 服务器	HTTP
攻击者	Pad_1, $Host_1$	FTP, SMTP
Pad	$Host_1$	FTP, SMTP
$Host_1$	Pad_1	FTP, SMTP
Pad_1, $Host_1$	Web 服务器	HTTP
Web 服务器	文件服务器	HFS
Web 服务器	数据服务器	Oracle
$Host_2$	$Host_3$	FTPShell
$Host_3$	$Host_2$	FTPShell
$Host_2$, $Host_3$	打印服务器	Print
$Host_2$, $Host_3$	文件服务器	HFS, RDP
$Host_2$, $Host_3$	数据服务器	Oracle, RDP
文件服务器	数据服务器	Oracle

5.2 均衡求解与防御策略选取

依据渗透威胁图的生成方法[31]可知，整个目标网络的网络威胁渗透关系如图 6 所示。攻击者能够利用漏洞在网络中不断渗透，此外，防御者可利用流量牵引的方法将攻击者从真实网络中的一个节点牵引到伪装网络中对应的节点中。经过实验测试，流量牵引的过程时延为毫秒级，故本文假设其不会被攻击者发现。进一步，参考文献[26-27]的赋值方法，不妨设攻击者的攻击目标是入侵数据服务器并获取机密数据，其价值设为 100，即 g=100。攻击者入侵伪装网络产生的损失为 20，即 k=20。防御者发送伪装信号所需的代价为 30，即 f=30。依据图 6 可得目标网络中任意节点之间的最优渗透概率，进而可利用 3.2 节的方法来定量刻画攻击者从一个节点到另一个节点所需的攻击代价，不妨设攻击者能力系数 κ=30。最初，外部攻击者成功入侵数据服务器的最优渗透路径为攻击者→Pad→$Host_3$→数据服务器，故其渗透成功概率为 0.6×0.32×0.6=0.115 2，则在此过程攻击者需要花费的攻击代价为 c=28。不妨设防御者类型为真实网络的概率 p=0.7，则处于外

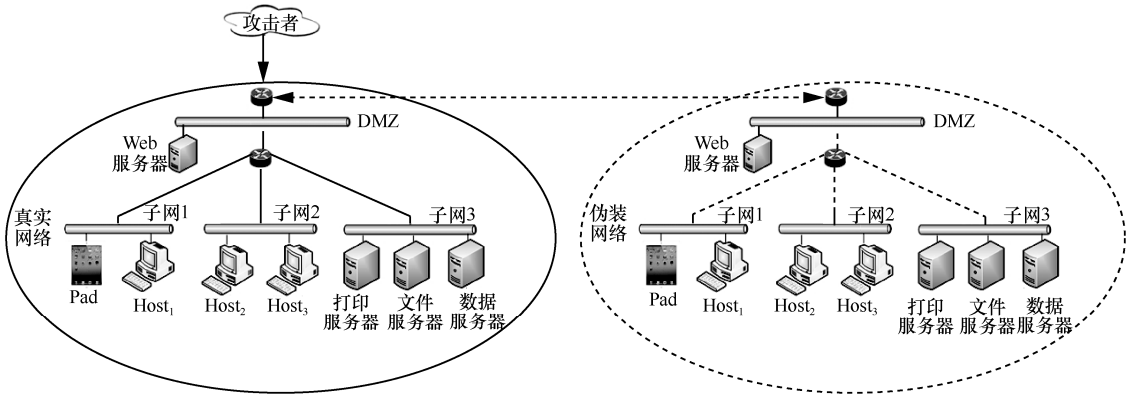


图 5 实验网络拓扑

表 3　　各主机信息及其所含漏洞信息

主机编号	主机信息	CVE 编号	攻击类型	所需源主机权限	获得目的主机权限	攻击复杂度
H_1	Web 服务器：Apache, Tomcat	CVE-2014-0226	Remote	User	Root	中
		CVE-2017-9798	Remote	User	User	低
H_2	Pad: iOS	CVE-2016-4729	Remote	User	Root	中
H_3	$Host_1$: Windows 7	CVE-2018-8174	Remote	User	Root	高
		CVE-2017-0161	Remote	User	User	中
		CVE-2018-8120	Local	User	Root	低
H_4	$Host_2$: Windows 8 FTPShell	CVE-2015-1769	Remote	User	Root	低
		CVE-2018-7573	Remote	User	Root	低
H_5	$Host_3$: Windows 8 FTPShell	CVE-2015-1769	Remote	User	Root	低
		CVE-2018-7573	Remote	User	Root	低
H_6	打印服务器：HP	CVE-2017-2741	Remote	User	Root	低
H_7	文件服务器：Windows, HFS	CVE-2014-6287	Remote	User	User	低
		CVE-2012-0002	Remote	User	Root	中
H_8	数据服务器：Windows, Oracle	CVE-2016-5555	Remote	User	User	低
		CVE-2012-0002	Remote	User	Root	低

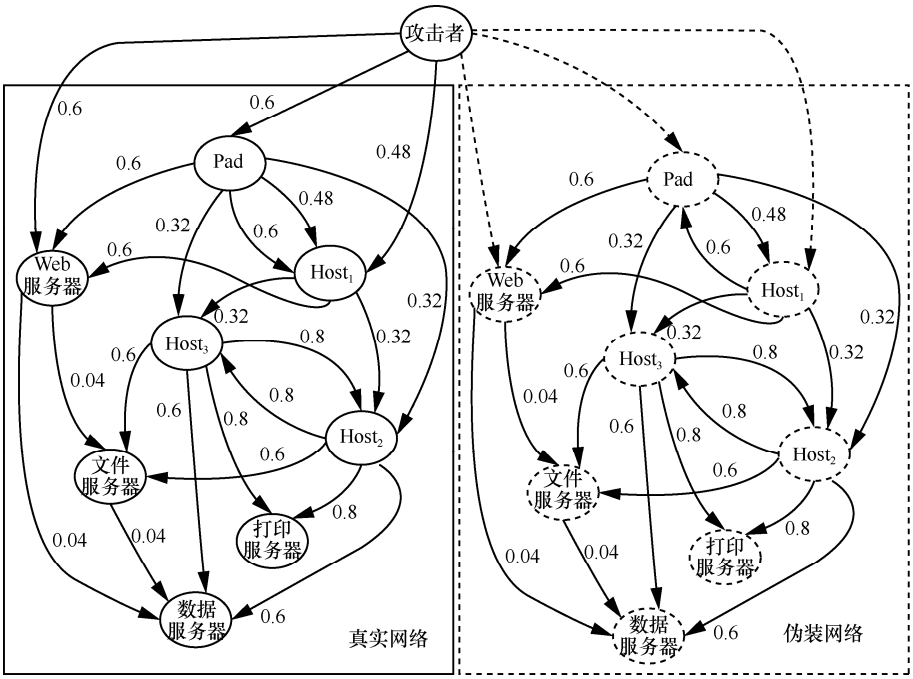


图 6　实验网络的网络威胁渗透关系

部的攻击者与防御者展开信号博弈，纳什均衡为 EQ_4，其中 $e_1 = 0.714$，$\tau_2 = 0.7$。由均衡结果可知，在此场景下，防御者的最优策略为：真实网络以 0.714 的概率发送信号 d_1，以 0.286 的概率发送信号 d_2（模拟伪装网络特征）；伪装网络则发送信号 d_2。随着攻击者的渗透过程，攻击者在网络中的位置会不断深入，本文分析了当攻击者处于不同节点时的精炼贝叶斯均衡结果，如表 4 所示。

由表 4 可知，从文件服务器及打印服务器这 2 个节点对目标数据服务器进行渗透的难度较大，攻击者很少会对这 2 个节点发起攻击。当攻击者由外部不断向网络内部渗透时，假设攻击者对防御者类型的信念 p 保持不变，攻击者需要花费的攻击代价 c 逐渐减小，存在精炼贝叶斯均衡 EQ_4。在此过程

表 4 攻击者处于网络中不同节点时的均衡分析结果

主机	攻击代价	精炼贝叶斯均衡	$p(N\|d_1)$	$p(N\|d_2)$	$U_d\|N$	$U_d\|H$	$U_a\|d_1$	$U_a\|d_2$
Web 服务器	41.9	EQ_4: $e_1=0.543,\tau_2=0.7$	1	0.516	−100	14	58.1	0
Pad	21.5	EQ_4: $e_1=0.773,\tau_2=0.7$	1	0.346	−100	14	78.5	0
$Host_1$	21.5	EQ_4: $e_1=0.773,\tau_2=0.7$	1	0.346	−100	14	78.5	0
$Host_2$	6.66	EQ_4: $e_1=0.878,\tau_2=0.7$	1	0.222	−100	14	93.34	0
$Host_3$	6.66	EQ_4: $e_1=0.878,\tau_2=0.7$	1	0.222	−100	14	93.34	0
文件服务器	41.9	EQ_4: $e_1=0.543,\tau_2=0.7$	1	0.516	−100	14	58.1	0
打印服务器	$+\infty$	EQ_1	1	1	0	0	0	0

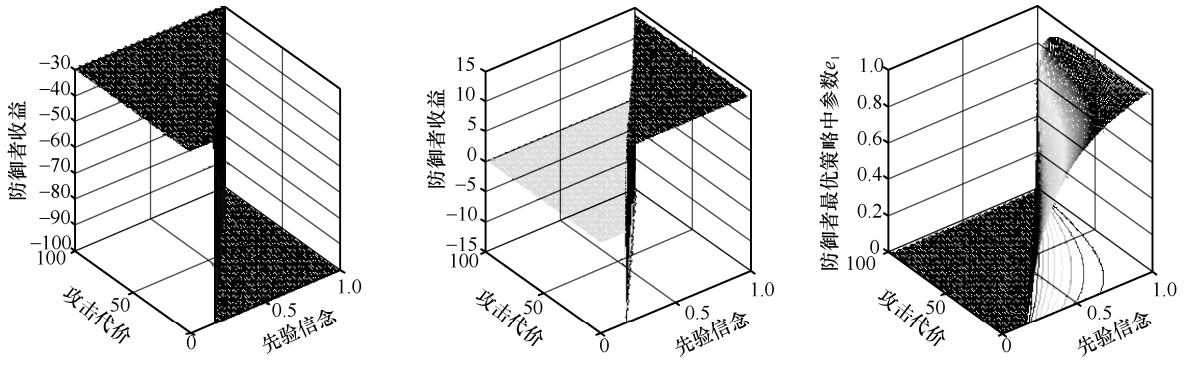
中，攻防双方均依据 EQ_4 做出最优策略，防御者最优策略中的 e_1 逐渐增大，表明随着攻击的不断深入，防御者发送真实信号的比重应该越来越大，而发送伪装信号的比重应该越来越小。

5.3 实验分析

通过分析精炼贝叶斯均衡的计算过程可知，攻击者对防御者类型的先验信念 p 和攻击代价 c 是影响策略选择和攻防双方收益的关键因素，且 p 和 c 可能会随着攻击者的渗透过程而变化。因此，本文进一步深入分析了 p 和 c 的变化对防御者最优策略的影响，其结果如图 7 所示。由于在本文的信号博弈模型中，防御者首先做决策，即防御者具有“提前选择”优势，此种情况下攻击者只能在观测到防御者发出的信号后选择最优攻击策略，攻击者收益对多重均衡选择问题并没有影响，因此本文并没有关注 p 和 c 的变化对攻击者收益的影响。

在图 7 中，当 p 和 c 同时变化时，攻防双方均依据精炼贝叶斯纳什均衡做出最优决策。图 7(a)展示了当攻击者处于真实网络中（防御者类型为 N）时，p 和 c 的变化对防御者收益的影响。当 $p<\dfrac{c+k}{g+k}$ 时，防御者的收益保持在−30；当 $p>\dfrac{c+k}{g+k}$ 时，防御者的收益保持在−100；当 $p=\dfrac{c+k}{g+k}$ 时，防御者的收益与攻击者策略有关，保持在−100～−30 之间。图 7(b)展示了当攻击者处于伪装网络中（防御者类型为 H）时，p 和 c 的变化对防御者收益的影响。当 $p<\dfrac{c+k}{g+k}$ 时，防御者的收益保持在 0；当 $p>\dfrac{c+k}{g+k}$ 时，防御者的收益保持在 20；当 $p=\dfrac{c+k}{g+k}$ 时，防御者的收益与攻击者策略有关，保持在 0~14 之间。图 7(c)展示了 p 和 c 的变化对防御者最优策略中参数 e_1 的影响。当 $p\leqslant\dfrac{c+k}{g+k}$ 时，e_1 为 0；当 $p>\dfrac{c+k}{g+k}$ 时，e_1 在 0~1 之间。此外，由图 7 可知，无论 p 和 c 如何变化，$U_d|N<U_d|H$ 恒成立，故可知流量牵引能够提高防御者的收益。为了便于分析，进一步考虑了以下 2 种攻防场景。

场景 1 攻击者对实验网络不断渗透，一方面攻击者对防御者类型的先验概率保持不变，另一方



(a) 防御者类型为N时，防御者收益变化　(b) 防御者类型为H时，防御者收益变化　(c) 防御者最优策略中参数e_1变化

图 7 先验信念 p 和攻击代价 c 的变化对防御者策略的影响

面由于攻击者位置与实验网络中漏洞情况变化会导致攻击者的攻击代价发生改变，即 c 变 p 不变。该场景中防御者策略结果如图 8 所示。

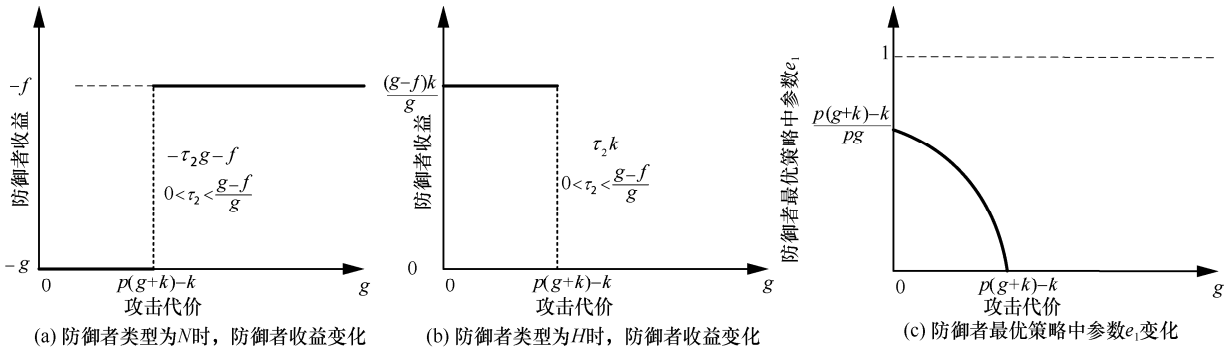
由图 8 可知，当攻击者处于真实网络中时，适当地提高 c 使其满足 $c>p(g+k)-k$，能够提高防御者的收益，本质上是提高攻击难度来震慑攻击者，使其不去攻击真实网络；当攻击者处于伪装网络中时，适当地降低 c 使其满足 $c<p(g+k)-k$，能够提高防御者的收益，本质上是降低攻击难度来诱惑攻击者，使其去攻击伪装网络以达到间接保护真实网络的目的。此外，当 $c<p(g+k)-k$ 时，若攻击者处于真实网络中，当 c 较大时，防御者策略中的 e_1 较大，表明攻击者对虚假防御信号的分辨能力较差，此时防御者发送真实信号的比重应该越来越小，而发送伪装信号的比重应该越来越大，以最大化干扰攻击者。

场景 2　攻击者一直尝试从一个固定节点对目标发起攻击且实验网络的漏洞情况不发生改变，而攻击者对防御者类型的先验信念会不断变化，即 p 变 c 不变。该场景中防御者策略结果如图 9 所示。

由图 9 可知，当攻击者处于真实网络中时，适当地减小 p 使其满足 $p<\dfrac{c+k}{g+k}$，能够提高防御者收益；当攻击者处于伪装网络中时，适当地增大 p 使其满足 $p>\dfrac{c+k}{g+k}$，能够提高防御者收益。该事实说明，防御者可利用社会工程学手段干扰并改变攻击者的先验概率来提高防御者收益。此外，当攻击者处于真实网络中时，随着其对虚假防御信号分辨能力的提高，p 会不断变大，进而防御者策略中的 e_1 变大，此时防御者发送真实信号的比重应该越来越大，而发送伪装信号的比重应该越来越小，防止防御信号被攻击者识别。

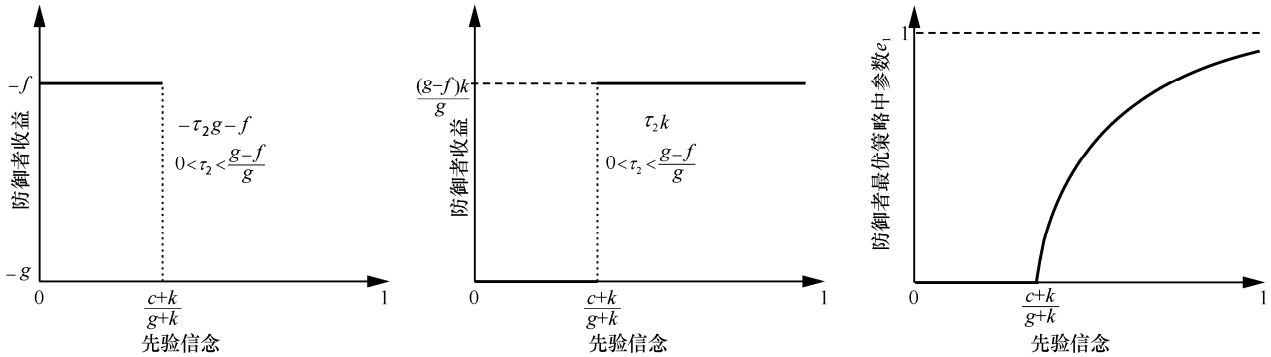
特别地，图 8 和图 9 中的垂直虚线表示均衡的一种特殊情况。在该均衡中，防御者收益受攻击者策略影响，为一变量。例如，图 8(a)中，当 $c=p(g+k)-k$ 时，均衡策略中攻击者策略参数范围为 $0<\tau_2<\dfrac{g-f}{g}$，对应的防御者收益为变量 $-\tau_2 g-f$。

信号博弈模型中，由于信号发送方能够混淆信号接收方对其类型的信念，使信号博弈模型在描述不完全信息的网络攻防中具有天然优势。当前，信



(a) 防御者类型为N时，防御者收益变化　(b) 防御者类型为H时，防御者收益变化　(c) 防御者最优策略中参数e_1变化

图 8　c 变 p 不变时对防御者策略的影响



(a) 防御者类型为N时，防御者收益变化　(b) 防御者类型为H时，防御者收益变化　(c) 防御者最优策略中参数e_1变化

图 9　p 变 c 不变时对防御者策略的影响

表 5　　本文方法与其他典型方法对比

方法	场景描述	博弈过程	方法通用性	均衡求解	混策略
文献[26]	详细	多阶段	一般	详细	不考虑
文献[27]	详细	单阶段	一般	简单	考虑
文献[28]	简单	单阶段	一般	详细	不考虑
文献[29]	简单	单阶段	较好	简单	不考虑
本文方法	详细	多阶段	较好	详细	考虑

号博弈模型已被很多学者应用于网络攻防策略选取上。鉴于此，将本文方法与其他典型方法对比，其结果如表 5 所示。

由表 5 可知，文献[26, 28-29]均不考虑混策略，仅有文献[27]和本文方法考虑了混策略，但文献[27]的博弈过程仅局限于单阶段且均衡求解方法不够详细，方法的通用性一般。本文方法适用于描述渗透攻击全过程，对场景描述详细，方法的通用性较强，且给出了一种详细的统一混策略和纯策略的均衡求解方法。均衡求解及防御策略选取也表明了混策略相比纯策略更适用于欺骗防御，能够增加策略对攻击者的干扰性，提高防御的实际效能。

综上可知，在基于伪装网络的网络主动欺骗防御攻防场景中，利用本文构建的信号博弈模型求解的精炼贝叶斯纳什均衡能够为防御者实施最优防御策略提供有效指导，实现防御者收益最大化。

6　结束语

为了抵抗目标性较强的渗透攻击，本文提出一种基于动态伪装网络的主动欺骗防御方法。借助动态伪装网络，防御者通过发送伪装信号来欺骗干扰攻击者。为了实现最大化防御者收益，将攻防过程用信号博弈模型进行刻画，进一步利用精炼贝叶斯纳什均衡解作为最优欺骗防御策略。所提方法能够同时求解出纯策略和混策略，且利用混策略更利于欺骗攻击者。实验结果表明，本文方法能有效欺骗攻击者，从而实现对真实网络的保护。未来的工作包括在动态伪装网络中利用 MTD 技术加强对攻击者的干扰，并结合欺骗防御方法实现更有效的防御。

参考文献：

[1] 国家计算机网络应急技术处理协调中心. 2018 年中国互联网络网络安全报告[M]. 北京: 人民邮电出版社, 2019.
National Internet Emergency Center. 2018 Annual report of Chinese Internet security[M]. Beijing: Posts and Telecom Press, 2019.

[2] 贾召鹏, 方滨兴, 刘潮歌, 等. 网络欺骗技术综述[J]. 通信学报, 2017, 38(12): 128-143.
JIA Z P, FANG B X, LIU C G, et al. Survey on cyber deception[J]. Journal on Communications, 2017, 38(12): 128-143.

[3] 胡永进, 马骏, 郭渊博. 基于博弈论的网络欺骗研究[J]. 通信学报, 2018, 39(Z2): 13-22.
HU Y J, MA J, GUO Y B. Research on cyber deception based on game theory[J]. Journal on Communications, 2018, 39(Z2): 13-22.

[4] WANG C, LU Z. Cyber deception: overview and the road ahead[J]. IEEE Security & Privacy, 2018, 16(2): 80-85.

[5] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats[M]. Berlin: Springer, 2011.

[6] ZHUANG R, DELOACH S A, OU X. Toward a theory of moving target defense[C]//The 2014 ACM Workshop on Moving Target Defense (MTD). ACM, 2014: 31-44.

[7] JAJODIA S, SUBRAHMANLAN V S, WANG C. Cyber deception: building the scientific foundation[M]. Berlin: Springer, 2016.

[8] PROVOS N. A virtual honeypot framework[C]//The 13th USENIX Security Symp. USENIX Association, 2004: 1-14.

[9] PA Y M P, SUZUKI S, YOSHIOKA K, et al. IoTPOT: analysing the rise of IoT compromises[C]//The 9th USENIX Conference on Offensive Technologies. USENIX Association, 2015: 9-17.

[10] FRUNHOLZ D, SCHOTTEN H D. Defending web servers with feints, distraction and obfuscation[C]//The International Conference on Computer Network and Communications(ICNC). IEEE, 2018: 21-25.

[11] AHMED H M, HASSAN N F, FAHAD A A. Designing a smartphone honeypot system using performance counters[J]. Karbala International Journal of Modern Science, 2017, 3(1): 46-52.

[12] YEHUDA R B, KEVORKIAN D, ZAMIR G L, et al. Virtual USB honeypot[C]//12th ACM International Conference on Systems and Storage. ACM, 2019: 181.

[13] JICHA A, PATTON M, CHEN H. SCADA honeypots: an in-depth analysis of Conpot[C]//IEEE International Conference on Intelligence & Security Informatics. IEEE, 2016: 196-198.

[14] JUELS A, RIVEST R L. Honeywords: making password-cracking detectable[C]//ACM Sigsac Conference on Computer & Communications Security. ACM, 2013: 145-160.

[15] ARAUJO F, HAMLEN K W, BIEDERMANN S, et al. From patches to honey-patches: lightweight attacker misdirection, deception, and disinformation[C]//ACM Sigsac Conference on Computer & Communications Security. ACM, 2014: 942-953.

[16] CONROY N J, RUBIN V L, CHEN Y. Automatic deception detection: methods for finding fake news[C]//ASIST. Wiley Online Library, 2015: 1-4.

[17] LEE K, CAVERLEE J, WEBB S. The social honeypot project: pro-

tecting online communities from spammers[C]//The 19th International Conference on World Wide Web. ACM, 2010: 1139-1140.

[18] LAZAROV M, ONAOLAPO J, STRINGHINI G. Honey sheets: what happens to leaked google spreadsheets?[C]//9th USENIX Workshop on Cyber Security Experimentation and Test. USENIX Association, 2016: 1-8.

[19] YOON J W, KIM H, JO H J, et al. Visual honey encryption: application to steganography[C]//3rd ACM Workshop on Information Hiding and Multimedia Security. ACM, 2015: 65-74.

[20] OMOLARA A E, JANTAN A, ABIODUN O S, et al. A deception model robust to eavesdropping over communication for social network systems[J]. IEEE Access, 2019, 7(8): 100881-10898.

[21] CLARK A, SUN K, POOVENDRAN R. Effectiveness of IP address randomization in decoy-based moving target defense[C]//52nd IEEE Conference on Decision and Control. IEEE, 2013: 678-685.

[22] SUN J, SUN K. DESIR: decoy-enhanced seamless IP randomization[C]//IEEE International Conference on Computer Communications(INFOCOM). IEEE, 2016: 1-9.

[23] SUN J, SUN K, LI Q. CyberMoat: camouflaging critical server infrastructures with large scale decoy farms[C]//IEEE Conference on Communincations and Network Security (CNS). IEEE, 2017: 1-9.

[24] VENKATESAN S, ALBANESE M, SHAH A, et al. Detecting stealthy botnets in a resource-constrained environment using reinforcement learning[C]//4th ACM Workshop on Moving Target Defense(MTD). ACM, 2017: 75-85.

[25] 石乐义, 李婕, 刘昕, 等. 基于动态阵列蜜罐的协同网络防御策略研究[J]. 通信学报, 2012, 33(11): 159-164.
SHI L Y, LI J, LIU X, et al. Research on dynamic array honeypot for collaborative network defense strategy[J]. Journal on Comunications, 2012, 33(11): 159-164.

[26] CHEN X Y, LIU X T, ZHANG L, et al. Optimal defense strategy selection for spear-phishing attack based on a multistate signaling game[J]. IEEE Access, 2019, 7(2): 19907-19921.

[27] CARROLL T E, GROSU D. A game theoretic investigation of deception in network security[J]. Security & Communication Networks, 2011, 4(10): 1162-1172.

[28] FENG X T, ZHENG Z Z, CANSEVER D, et al. A signaling game model for moving target defense[C]//IEEE International Conference on Computer Communications(INFOCOM). IEEE, 2017: 1-9.

[29] 蒋侣, 张恒巍, 王晋东. 基于信号博弈的移动目标防御最优策略选取方法[J]. 通信学报, 2019, 40(6): 128-137.
JIANG L, ZHANG H W, WANG J D. Optimal strategy selection method for moving target defense based on signaling game[J]. Journal on Communications, 2019, 40(6): 128-137.

[30] JAJODIA S, PARK N, SERRA, et al. SHARE: a stackelberg honey-based adversarial reasoning engine[J]. ACM Transactions on Internet Technology, 2018, 18(3): 1-41.

[31] 王硕, 王建华, 汤光明, 等. 一种智能高效的最优渗透路径生成方法[J]. 计算机研究与发展, 2019, 56(5): 929-941.
WANG S, WANG J H, TANG G M, et al. Intelligent and efficient method for optimal penetration path generation[J]. Journal of Computer Research and Development, 2019, 56(5): 929-941.

[32] NASH J F. Equilibrium points in n-person games[J]. National Academy of Sciences,1950, 36(1): 48-49.

[作者简介]

王硕（1991− ），男，河南南阳人，信息工程大学博士生，主要研究方向为网络与信息安全、机器学习。

王建华（1962− ），男，北京人，博士，信息工程大学教授、博士生导师，主要研究方向为密码学、信息安全管理、计算机网络。

裴庆祺（1975− ），男，广西玉林人，博士，西安电子科技大学教授、博士生导师，主要研究方向为无线网络安全、区块链安全技术。

汤光明（1963− ），女，湖南常德人，博士，信息工程大学教授、博士生导师，主要研究方向为网络与信息安全、信息安全管理、信息隐藏。

王洋（1985− ），女，陕西西安人，信息工程大学博士生，主要研究方向为网络与信息安全。

刘小虎（1989− ），男，河南太康人，信息工程大学讲师，主要研究方向为网络与信息安全、移动目标防御。