DOI 10.15302/J-SSCAE-2016.06.013

拟态防御基础理论研究综述

斯雪明[1]，王伟[1]，曾俊杰[1]，杨本朝[1]，李光松[1]，苑超[1]，张帆[2]

（1. 中国人民解放军信息工程大学数学工程与先进计算国家重点实验室，郑州 450001；
2. 中国人民解放军信息工程大学国家数字交换系统工程技术研究中心，郑州 450002）

摘要：随着互联网的发展，网络空间安全问题已成为关系到国家安全的大问题。本文首先介绍了一些经典的网络安全防御技术；其次介绍了拟态防御技术，包括拟态防御系统的构成、拟态防御的科学问题及其理论框架，对比传统网络防御技术，分析了拟态防御系统的有效性；最后对拟态防御基础理论还需要解决的问题做了阐述。

关键词：拟态防御；网络空间；移动目标防御；拟态变换

中图分类号：TN915　　**文献标识码：**A

A Review of the Basic Theory of Mimic Defense

Si Xueming[1], Wang Wei[1], Zeng Junjie[1], Yang Benchao[1], Li Guangsong[1], Yuan Chao[1], Zhang Fan[2]

(1. State Key Laboratory of Mathematical Engineering and Advanced Computing, The PLA Information Engineering University, Zhengzhou 450001, China; 2. National Digital Switching System Engineering & Technological R&D Center, The PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: With the development of the Internet, cyberspace security issues have become a major concern related to national security. This paper first introduces some classic network defense technology. Next, it introduces the technology of mimic defense, including mimic defense systems, related scientific problems, and the theoretical framework of mimicry defense. The effectiveness of a mimic defense system is also analyzed in comparison with a traditional network defense technology. Finally, some problems worthy of study are presented regarding the basic theory of mimic defense.

Key words: mimic defense; cyberspace; moving target defense; mimicry transformation

一、前言

近年来，世界各国高度重视网络空间这一新兴全球公共领域，并围绕网络空间发展权、主导权和控制权展开激烈角逐。随着全球网络空间重要性的日益凸显，网络空间安全问题已成为亟待解决的重要问题，网络空间安全技术已成为关系到国家利益和安全的核心技术[1]。

传统的网络安全防御思想是在现有网络基础架构的基础上建立包括防火墙和安全网关、安全路由

收稿日期：2016-10-21；**修回日期：**2016-11-01

作者简介：斯雪明，中国人民解放军信息工程大学数学工程与先进计算国家重点实验室，教授，研究方向为网络密码、拟态防御；E-mail: sxm@fudan.edu.cn

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)；国家重点研发计划 (2016YFB0800101, 2016YFB0800100)；数学与先进计算国家重点实验室开放课题 (2015A14)；国家自然科学基金创新研究群体项目 (61521003)；国家自然科学基金项目 (61572520，61602512)

本刊网址：www.enginsci.cn

器 / 交换机、入侵检测、病毒查杀、用户认证、访问控制、数据加密技术、安全评估与控制、可信计算、分级保护等多层次的防御体系，通过不同类型传统安全技术的综合应用来提升网络及其应用的安全性。但近年来不断被披露的国内外网络安全事件及由此带来的严重后果也逐渐暴露了传统的网络安全防御技术存在的问题。为此，突破依赖于对网络攻击先验知识的静态、被动式的防御技术的局限，提出网络安全动态防御的创新思路，研究新型网络安全架构的基础理论与关键技术已成为网络安全领域的重要研究方向。

二、国内外相关理论研究成果

（一）移动目标防御（MTD）技术

MTD 技术是美国近年来提出的网络空间“改变游戏规则”的革命性技术之一，其构建、评价和部署机制及策略是多样的、不断变化的 [2~5]。这种不断变化的思路可以增加攻击者的攻击难度及代价，有效限制脆弱性暴露及被攻击的机会，提高系统的弹性。在理论研究上，2014 年 Zhuang 等提出一个初步的理论来回答 MTD 的有效性问题，并讨论了 MTD 系统的关键概念和基本性质，提出了 MTD 熵假设，即系统配置的熵越大，则该系统就越有效 [6]。

（二）端信息跳变技术

端信息跳变技术是指在端到端的数据传输中通信双方或一方按协定伪随机地改变端口、地址、时隙、加密算法甚至协议等端信息，从而破坏敌方的攻击与干扰，实现主动网络防护。

基于端信息跳变的主动网络防护模型包括预警分析、协同控制、端信息管理和任务切换 4 个模块以及众多任务机群。预警分析模块负责对当前网络遭受的攻击进行信息收集分析；协同控制模块是整个系统的核心，协调各模块实现网络防御；端信息管理模块用于伪随机地产生端信息跳变图案；任务切换模块则按照协同控制模块的指令进行干扰、通信、蜜罐等任务转换，实现协同防御。研究结果表明，相比于传统的网络防护技术，端信息跳变具有抗攻击性强、主动性、抗截获性、性能增量性等优势 [7]。

（三）拟态式蜜罐动态博弈模型

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，以有效迷惑和诱骗攻击者，实现网络对抗。保护色指蜜罐在硬件、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 [8,9]。

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，博弈对手具有不同的类型。在攻击者视角中，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；从防御者视角来看，博弈对手有合法用户和攻击者两种不同类型的来访者。给定攻防双方收益矩阵，根据攻击者是否知晓伪蜜罐的存在，可分析确定出双方策略到达贝叶斯纳什均衡的条件。

（四）非相似余度计算机系统

非相似余度计算机系统是一种应用于飞控系统中的计算机系统，它使用不同的、完全独立的设计组，使用不同的开发语言、不同的开发工具，并在不同的处理器上运行，达到避免共性故障、提高关键系统的任务可靠性目的。设计者应用一种简化的马尔可夫模型对其进行了可靠性分析。试验结果表明，非相似余度计算机系统结构提高了系统可靠性，平均故障间隔时间达到了 9 000 h 以上 [10]。

三、信息系统形式化描述及其安全性

为了对网络空间中各种错综复杂的因素及其关系、影响等进行合理的数学建模，需要对信息系统进行更科学合理的描述，进而采用形式化的方法对拟态防御系统进行描述。通过对信息系统做形式化描述，进而对拟态防御系统进行形式化描述，可以为阐述如何应用拟态防御的思想对网络空间中的信息系统进行保护，介绍拟态变换的原理、方式奠定理论基础。

（一）传统信息系统的形式化描述

基于不同的关注角度和研究目的，信息系统可以由不同的核心要素来刻画。一般来说，信息系统的构成要素较多，如软件、硬件、操作、策略等，为了表述方便，可借助于多维空间中的向量（组）$(\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n)$ 进行描述（见图 1）。

信息系统通常不是一成不变的，往往需要根据外在条件或周围状况在某些时间做相应调整，从而使信息系统与时间因素相关。假定当前研究主要关注的信息系统要素除时间外还有 m 个，那么信息系统在不同的时间点可能会有多个不同的状态。当然对于这些不同的要素还可以进一步用小指标来细分表示，即可以根据所研究问题的需要，选择合适的粒度表示一个信息系统。

（二）从安全角度考虑的信息系统实例

对于网络空间中的信息系统，与安全相关的因素很多，把影响信息系统安全的某个具体因素称为基本元素，这是研究时考虑的基本单元。对于影响网络空间安全的基本元素通常可以把它们归为：网络、平台、运行环境、软件、数据等类别，它们形成了系统的不同层次。

一般来说，各要素的基本元素数量是不同的，为对这些信息系统的构成要素和元素进行统一描述，不妨假设信息系统有 m 个要素，每个要素都有 n 个元素，$n = \max\{n_1, n_2, \cdots, n_m\}$，$i = 1, 2, \cdots, m$，其中 n_i 为第 i 个要素的元素个数。对于元素个数少于 n 的要素，以空元素来进行扩充。如果用 x_i^j 表示第 i 个要素中第 j 个元素的状态，那么 t 时刻信息系统的状态我们可以用矩阵 $\boldsymbol{\Omega}(t)$ 来表示。

$$\boldsymbol{\Omega}(t) = \begin{pmatrix} x_1^1(t), x_1^2(t), \cdots, x_1^n(t) \\ x_2^1(t), x_2^2(t), \cdots, x_2^n(t) \\ \vdots \qquad\qquad \vdots \\ x_m^1(t), x_m^2(t), \cdots, x_m^n(t) \end{pmatrix}$$

为了研究方便，不妨假定当前考虑的安全相关基本要素分为网络、平台、运行环境、软件、数据 5 类。

网络要素包含网络的连接形式、通信标准、安全协议、拓扑结构、网络地址、网络端口等元素。

平台要素指的是信息系统依赖的硬件设备及支撑性软件等部件，包含多种类型的硬件设备、操作系统、处理器架构、虚拟机、存储系统等元素。

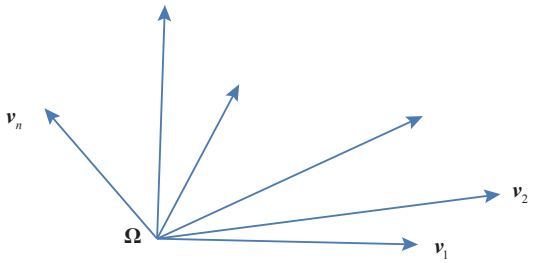

图 1　信息系统多维向量示意图

运行环境要素指的是平台与上层应用的接口，包含指令集、地址空间等元素。

软件要素是指信息系统中安装的各种应用软件，包含具有不同软件执行体、程序指令序列、指令格式、内部数据结构等元素。

数据要素指的是与信息服务相关的系统中存储的各类数据，包含格式、语法、编码等元素。上述的网络、平台、运行环境、软件、数据包含的各元素都和信息系统的安全息息相关。在这种意义下，可以把信息系统看成是网络、平台、运行环境、软件、数据的 5 层架构。

四、拟态防御系统及其形式化描述

现有网络空间的信息系统多是静态的、相似的和确定的，其安全缺陷在于体系结构层面具有持续性、稳定性和可利用性，易于被攻击或控制。基于漏洞和后门的攻击高度依赖目标系统的静态性、相似性和确定性，目标系统所暴露的时间越长，可供攻击者研究其运行规律、发现其弱点、创建和验证有效攻击方法的时间窗口就越大。如果能动态地改变信息系统的状态，阻断或扰乱攻击链所依赖的静态性、相似性和确定性，可以达成系统安全风险可控的要求。

（一）拟态防御系统

拟态防御系统一般来说由信息系统、拟态变换、异构执行体集与表决器等部件构成。拟态防御系统通过主动改变信息系统构成要素的状态，实现信息系统在不同状态间的迁移，用于改变信息系统状态的方法称为拟态变换。拟态变换可以有效地改变网络攻击所依赖的系统静态性和确定性，对于拟态变换后面将做详细描述。表决器的引入是为了进一步

迷惑攻击者，降低系统被攻击的风险，同时增加系统的可靠性，在目标对象元功能与其等价的多元实现结构或算法间导入不确定性映射关系，从而隐藏系统输入与输出的真实关系。MTD 系统可以看作是拟态防御系统的一个特例，它通过一些拟态变换使系统具有动态性特征，但是并没有应用异构冗余架构[11,12]。

（二）拟态变换

拟态变换是通过改变信息系统构成要素的基本单元来实施的。拟态变换可以仅对某一个构成要素的一个基本元素进行变换，也可以对该构成要素的多个基本元素进行变换；或是对多个要素的基本元素同时进行变换，这可以看作是多种基本拟态变化的叠加。为了达到迷惑攻击者的目的，在生存期内信息系统在不同状态间迁移所实施的拟态变换序列应该是随机的。也就是说，在不同时刻要改变信息系统的状态时，要采用什么样的拟态变换，对哪些要素及哪些基本单元进行变换，必须具有不确定性和随机性。

拟态变换应具备下列性质：

（1）功能等效性。拟态变换前后，系统的功能一致。

（2）安全性。变换后系统的安全度要高于变换前的安全度。

（3）随机性。攻击者不能预测变换后的系统状态。

（4）可叠加性。多个拟态变换共同作用到系统上其效果相当于一个更复杂的拟态变换。

（三）拟态变换的设计

拟态变换的设计主要依据异构冗余、动态化、随机化、分片化和碎片化、隐匿伪装等原理，并且需要考虑不同层次的构成要素和基本元素的特性。由于有些元素状态的改变会有相关性，改变一个元素状态可能会引起其他元素状态的变化，这会影响系统状态变化的效果，需要针对具体情况来分析。这里只是从构造不同拟态变换的角度考虑，从改变一个状态的方式来得到一个基本变换，并不关心从改变不同的元素状态得到的拟态变换之间的等价性。

1. 异构冗余原理

异构冗余原理就是为系统的基本元素产生多个功能相同的异构执行体或变体，根据某种设定的规则在这些异构体中进行随机切换。以平台层为例，在平台层，操作系统是一个基本元素，异构冗余原理就是为信息系统准备多种不同的操作系统。

2. 动态化原理

动态化原理就是使信息系统基本元素的状态动态变化。以网络层为例，系统网络之间互连的协议（IP）地址是一个基本元素，动态化就是要设计一种机制让系统的 IP 地址动态变化。

3. 随机化原理

随机化原理是使信息系统基本元素的状态变成某个范围内的随机信息。对于数据层的数据存储状态元素而言，加密是一种很容易理解的拟态变换，可以使存储的信息变成随机信息。

4. 分片化和碎片化原理

分片化和碎片化原理主要针对数据层，可以把文件分成几片按顺序存储在不同位置，甚至可以把文件分成更多的碎片，分别存储在不同的位置。假定一个文件大小是 1 M 字节，可以如下设计拟态变换：将文件分为 1 000 份，每份长度是 1 K 字节。假定计算机内现有系统文件目录 2 000 个，将这些目录编号随机选取 1 000 个，然后把文件碎片分别存储进这些目录。

5. 隐匿伪装原理

隐匿伪装原理指的是系统主动隐藏状态的真实属性，以达到迷惑攻击者的目的。如定义一个拟态变换改变文件名的后缀。M 是一个 PDF 类型的文件，通过变换把它的文件名后缀改为 word 类型，以 .doc 结尾。这样攻击者拿到这个文件后，用 word 软件无法打开，会以为这是一个错误文件而丢弃，从而起到保护文件的作用。

依据上述原则，针对不同层次的基本单元，可以设计相应的基本拟态变换，然后再由这些基本的拟态变换构造更复杂的拟态变换。表 1 中针对信息系统的 5 层架构，分别列举了主要的元素，以及可以设计的一些变换。

五、拟态防御科学问题与理论框架

（一）拟态防御科学问题

拟态安全理论研究的目标是从理论上回答拟态安全主动防御机理科学性的问题，初步建立拟态安全基础理论体系，并在此基础上对拟态安全的关键技术和现有系统向拟态安全系统的演进方法与方案

表 1　拟态防御系统中不同层次的拟态变换

信息系统主要分层（构成要素）	层中的基本元素（单元）	主要的拟态变换
网络层	地址、协议、端口等	改变目标信息系统的 IP 地址 改变目标系统的端口 改变目标系统使用的协议 上述基本变换多种形式的组合（叠加）
平台层	操作系统、异构冗余设备、虚拟机实例、存储系统等	改变操作系统 异构设备切换 改变虚拟机实例 改变存储系统 上述变换多种形式的叠加
运行环境层	指令集、地址空间等	指令集随机化 地址空间随机化 两者的叠加
软件层	软件异构变体，软件程序的指令序列、指令格式、内部数据结构布局等	软件变体切换 改变执行指令序列和形式 动态化存储资源分配方案 上述变换多种形式的叠加
数据层	数据的形式、句法、编码等	改变数据的形式 改变数据的句法 改变数据的编码 上述变换多种形式的叠加

进行研究。拟态安全基本科学问题包括网络攻击行为规律，拟态安全机制机理，拟态安全有效性，拟态安全系统量化评估等。

网络攻击行为规律研究针对信息系统的网络攻击方法，建立网络攻击链的模型，研究攻击链的建立与网络系统的静态性、确定性、相似性和持续性的依赖关系，研究漏洞利用机制的形式化描述方法。

拟态安全机制机理研究拟态安全的可重构、多态化、随机化等特征及其对系统的静态性、相似性、确定性和持续性的改变程度，阐明拟态安全破坏攻击链的形成、降低攻击成功率的机制机理，揭示拟态安全的风险控制本质。通过对相关概念的抽象，建立形式化语言刻画拟态安全的基本思想。

拟态安全有效性的科学论证是基于网络攻击行为规律和拟态安全机理所建立的拟态安全体系的形式化描述，建立合理的推理系统，对拟态安全防御的有效性进行科学论证。

拟态安全系统量化评估方法建立对拟态系统进行安全评价的量化评估模型，分析由拟态安全系统结构变化所带来的新问题，并与传统的信息安全评价方法进行对比。

（二）拟态防御安全理论框架

基于拟态防御的科学问题，拟态安全理论研究主要集中在以下 5 个方面。

1. 网络攻击行为分析与建模

现有的网络攻击建模方法有很多，主要集中于攻击语言、攻击树、攻击网、状态转移图和攻击图等。拟态防御系统将信息系统抽象为 5 层，提取各层的可变元素，进行形式化描述。信息系统的攻防对抗中攻击者需要利用 5 层及其要素以达到攻击目的，网络攻击行为的分析主要是通过对攻击流程进行分析，提取与系统相关的知识建立知识图谱，通过攻击表面和知识流统一表征网络攻击行为，建立起网络攻击链模型。

2. 拟态变换理论

根据拟态安全的思想，拟态变换可以定义如下：

$$\sigma: \boldsymbol{\Omega}(t_i) \rightarrow \boldsymbol{\Omega}(t_{i+1})$$

该变换的定义域为系统所有状态组成的集合 $\boldsymbol{\Omega}$，值域也是 $\boldsymbol{\Omega}$。

对不同要素的变换方法，对应不同的变换，因此记 $\sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$，其中 σ_1 表示第一个要素的拟态变换，其他依此类推。若 $\boldsymbol{\Omega}(t)$ 以 0,1 序列表示，则 σ 就可以看成是一个加扰序列，不同的加扰序列就对应着不同的变换。

拟态安全系统的目标可形式化为：

条件 1：$sr(\boldsymbol{\Omega}(t, \sigma)) \leqslant a$，其中 sr 表示 $\boldsymbol{\Omega}(t)$ 使用的计算存储互联等资源的函数；

条件 2：$pf(\boldsymbol{\Omega}(t, \sigma)) \leqslant b$，其中 pf 表示 $\boldsymbol{\Omega}(t)$ 的性能函数，b 为一个常数。

在约束条件 1 或约束条件 2 下，选择适当的拟态变换 σ，实现 Max($sp_i|\sigma$)。

拟态变换使得拟态安全系统具有随机性、动态性和多样性等特点，有效改善了传统系统的确定性、静态性和相似性，从而使得整个信息系统的安全性得到提升。

3. 拟态安全系统构造方法

拟态安全系统构造方法主要包括态势感知方法、拟态化方法和协同化方法。研究拟态安全网络软传感器的部署方法与应用策略，安全威胁和安全态势认知与风险评估和安全态势演化预测的方法，实现供感知、认知及决策使用的统一的描述模型、参数集合、描述语言、描述方法、推理规则、决策模型和知识库系统，以优化和决策拟态安全系统的具体拟态化方法强度、主动变迁和协同化时机。研究拟态安全系统的随机化、多样化和动态化等拟态化方法，以提供动态随机化机制、输入输出代理机制、异构冗余机制、分片化和碎片化机制、单线联系机制，以及伪装、蜜罐等“欺骗”机制的具体实现方法和组合应用方法。

4. 拟态安全有效性理论

研究拟态安全的可重构、多态化、随机化等特征的主动防御理论和机制对当前主流网络攻击的有效性；研究各种拟态防御机制有效组合方式，建立信息系统拟态安全防御的攻击表面刻画；研究拟态安全防御对攻击表面的影响，刻画其对抵抗攻击的贡献。

5. 拟态安全量化评估理论

传统网络安全量化评估模型包括故障树模型、攻击树模型、基于 Petri Net 的模型、特权图模型、攻击图模型等，这些评估模型虽然具有一定的借鉴意义，但拟态防御系统特性有别于传统系统的确定性、静态性和相似性，因此有必要根据拟态网络的定义和特点，结合网络各层次安全的属性，建立适合拟态网络安全的评估模型；细化模型中不同维度上的评价指标，构建层次化的拟态网络安全评估指标体系；根据拟态网络的评估指标体系和安全要素模型，建立拟态网络安全指标到安全要素状态的映射关系，即通过评估指标能够清晰刻画拟态网络的安全防护能力；采用聚类等方法对安全空间进行划分，建立拟态网络安全等级评定标准。

六、拟态防御系统有效性分析

一般情况下，要完成攻击任务，可将攻击过程分解为若干步骤，而不同的拟态机制可能在不同的步骤中起作用。以下基于网络攻击链模型对拟态防御机制进行有效性分析（见表 2）。

异构冗余机制下：访问和提权攻击成功的概率被降低，因为这两个步骤一般都依赖于漏洞和后门，而冗余机制可以有效防御依赖漏洞和后门的攻击。

单线联系机制：在单线联系下，由于敏感路径或关键环节权限不同，因而在不同的权限下，所收集的信息和信息的窃取会不完整，从而降低其成功概率。

分片化和碎片化机制：由于文件和系统信息分别被分片存储和多路径传输，可以有效降低攻击者获得信息的概率，因而对信息收集和信息窃取有效。

在攻击链概率模型下，对于每一个攻击链，在不同拟态机制下，其可以降低其中某几步攻击成功的概率，从而降低整个攻击链攻击成功的概率，所以拟态安全系统的攻击成功率要小于传统信息系统的攻击成功率。

七、结语

目前，针对拟态防御思想，给出了信息系统的

表 2　拟态防御机制的有效性分析

安全机制	信息收集	访问			提权		信息窃取或破坏
		密码嗅探	蛮力攻击	渗透工具	破解密码	利用漏洞	
异构冗余机制				√		√	
单线联系机制	√					√	√
分片化和碎片化机制	√					√	√
输入 / 输出代理机制	√						√
随机动态机制	√	√	√		√	√	√

注：表中 √ 表示在对应机制下可以降低对应攻击步骤攻击成功的概率。

形式化描述和拟态防御系统的形式描述，并对不同拟态防御机制进行了初步分析。下一步拟态安全基础理论研究将集中在信息系统形式化表示的细化、网络攻击行为的形式化表示、网络攻击场景的分类与描述、网络安全的度量问题、拟态安全 5 种机制的有效性详细分析以及拟态安全体系结构的数学抽象等。

参考文献

[1] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. 中国科学: 信息科学, 2016,46(2):125–164.
Zhang H G, Han W B, Lai X J, et al. Survey on cyberspace security [J]. SCIENTIA SINICA Informationis, 2016, 46(2):125–164.

[2] Jajodia S, Ghosh A K, Swarup V, et al, editors. Moving target defense—Creating asymmetric uncertainty for cyber threats [M]. New York: Springer Publishing Company, 2011.

[3] Evans D, Nguyen-Tuong A, Knight J. Effectiveness of moving target defenses [M]// Jajodia S, Ghosh A K, Swarup V, et al, editors. Moving Target Defense—Creating asymmetric uncertainty for cyber threats. New York: Springer Publishing Company, 2011:29–48.

[4] Han Y J, Lu W L, Xu S H. Characterizing the power of moving target defense via cyber epidemic dynamics [C]// HotSoS'14 proceedings of the 2014 symposium and bootcamp on the science of security. New York: Association for Computing Machinery (ACM), 2014:1–12.

[5] 张晓玉, 李振邦. 移动目标防御技术综述[J]. 通信技术, 2013,46(6):111–113.
Zhang X Y, Li Z B. Overview on moving target defense technology [J].Communications Technology, 2013, 46(6):111–113.

[6] Zhuang R, DeLoach S A, Ou X M . Towards a theory of moving target defense[C]// MTD'14 proceedings of the first ACM workshop on moving target defense. New York: ACM, 2014: 31–40.

[7] 石乐义, 贾春福, 吕述望. 基于端信息跳变的主动网络防护研究[J]. 通信学报, 2008,29(2):106–110.
Shi L Y, Jia C F, Lv S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2):106–110.

[8] 李之棠, 徐晓丹. 动态蜜罐技术分析与设计[J]. 华中科技大学学报(自然科学版), 2005,33(2):86–88.
Li Z T, Xu X D. The analysis of dynamic honeypot and its design [J]. Journal of Huazhong University of Science and Technology (Nature Science Edition), 2005,33(2):86–88.

[9] 石乐义, 姜蓝蓝, 刘昕, 等. 拟态式蜜罐诱骗特性的博弈理论分析[J]. 电子与信息学报, 2013,35(5):1063–1068.
Shi L Y, Jiang L L, Liu X, et al. Game theoretic analysis for the feature of mimicry honeypot [J]. Journal of Electronics & Information Technology, 2013, 35(5):1063–1068.

[10] 臧红伟, 韩炜, 高德远. 非相似余度计算机系统及其可靠性分析[J]. 哈尔滨工业大学学报, 2008,33(3):492–494.
Zang H W, Han W, Gao D Y. Dissimilar redundancy computer system and reliability analysis [J]. Journal of Harbin Institute of Technology, 2008,33(3):492–494.

[11] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014,30(7):2–7.
Wu J X. Meaning and vision of mimic computing and mimic security defense [J]. Telecommunications Science, 2014,30(7): 2–7.

[12] 邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014(10):4–9.
Wu J X. Mimic security defense in cyber space [J].Secrecy Science and Technology, 2014(10):4–9.