doi:10.3969/j.issn.1000-436x.2012.11.020

基于动态阵列蜜罐的协同网络防御策略研究

石乐义[1]，李婕[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，山东 青岛 266555；2. 南开大学 信息技术科学学院，天津 300071）

摘 要：从虚实结合动态变化的兵阵对抗得到启发，提出动态阵列蜜罐概念，通过多机协同、功能角色的周期或伪随机切换，形成动态变化的阵列陷阱，从而达到迷惑和防范攻击者的目的。给出了动态阵列蜜罐防御模型，通过 NS2 网络模拟器对动态阵列蜜罐进行了系统仿真和测试，基于 Java 平台设计实现了动态阵列蜜罐原型系统并进行了攻击实验。仿真测试和原型实验结果均表明动态阵列蜜罐系统具有良好的网络对抗性能。

关键词：动态阵列蜜罐；网络防御；兵阵；协同控制
中图分类号：TP393.08 **文献标识码：**A **文章编号：**1000-436X(2012)11-0159-06

Research on dynamic array honeypot for collaborative network defense strategy

SHI Le-yi[1], LI Jie[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 Un versity, Tianjin 300071, China)

Abstract: Inspired by the ancient battle diagram for military purpose, a concept of dynamic array honeypot was proposed to bewilder the attackers by coordinating and changing the role pseudo-randomly as a huge dynamic puzzle. The dynamic array honeypot model was presented, system simulation through NS2 was performed, and the prototype implementation with Java was carried out. Detailed empirical studies were launched upon both the simulation model and the prototype. The simulation results demonstrates that the dynamic array honeypot system is feasible and effective for active network confrontation.

Key words: dynamic array honeypot; network confrontation; battle diagram; collaborative control

1 引言

伴随着互联网的大众化、黑客技术的平民化以及各种病毒、木马和蠕虫的出现，黑客攻击事件频频发生，安全防范和网络对抗技术日益引起重视。然而，传统的安全防范技术如防火墙、IDS 入侵检测等，从本质上讲都属于敌暗我明的被动式防御，面对无处不在的由攻击者发起的层出不穷的恶意攻击、漏报、误报以及大规模资源消耗使得这些安全屏障十分被动，甚至崩溃，对于网络对抗十分不利。

蜜罐技术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，学习黑客攻击的目的和手段，干扰和迷惑攻击者。蜜罐技术具有数据保真度高、可检测未知攻击等优点。然而，传统的蜜罐本身只是一个静态、固定不动的陷阱网络。这种静态陷阱对于误入陷阱的鲁莽的敌手十分有效，但一旦攻击者意识到陷阱的存在并离

收稿日期：2012-05-03；修回日期：2012-09-03
基金项目：国家自然科学基金资助项目（60973141）；山东省中青年科学家科研奖励基金资助项目（2009BSA05001）；中央高校基本科研业务费专项基金资助项目（27R0907018A, 11CX04052A）
Foundation Items: The National Natural Science Foundation of China (6097 41); The Foundation of Excellent Young Scientist of Shandong Province (2009BSA05001); The Fundamental Research Funds for the Central Universities (27R0907018A, 11CX04052A)

开，蜜罐将失去任何功效。显然，这种“被动的主动防御”手段，对于网络对抗来说是不够的。

军事斗争中，虚实结合、运动变化是一种十分有效的对抗手段。《孙子兵法》第6篇《虚实篇》中论述了虚实变化的策略，指出“故兵无常势，水无常形，能因敌变化而取胜者谓之神”。而在军事战争中发挥重要作用的兵阵，则是虚实变化的对抗典范。兵阵是兵民战斗或驻守的队形，即所谓“止即为营，动即为阵”。兵阵表现的是战争中最优化的动态组合方式，通过合理部署军事力量，使整体实力得到最大发挥，置对手于巨大的阵列迷宫之中从而克敌制胜。这种运动变化、虚实结合的兵阵思想对于网络对抗来讲具有重要的借鉴意义。

本文将兵阵思想创新运用于网络对抗中，提出了动态阵列协同防御的概念。这种通过功能角色周期性切换任务主机组成的动态变化阵列陷阱不仅能提供正常服务，也能有效地应对大规模网络攻击，实现主动式网络防御。

2 相关工作

近年来，国内外学者在克服传统蜜罐静态、部署困难等缺点方面进行了有成效的工作。

Spitzner L 在文献[1]中首次提出动态蜜罐的概念，它通过被动监听其所处的网络中的流量，获得当前网络的部署状况，然后在无需人工干预的前提下自动地配置虚拟蜜罐。当网络的部署状况发生变化时，动态蜜罐技术能够实时地识别出这些变化，并动态地进行自适应。文献[2]和文献[3]采用被动扫描手段设计实现了动态蜜罐系统并应用到入侵检测中。文献[4]则将主动探测和被动探测相结合来获取网络部署状况用来配置动态蜜罐，并提出重定向技术将攻击重定向到物理蜜罐。国内学者陈启璋等进一步提出重定向器和拦截代理技术[5]，将重定向功能与蜜罐独立分开，克服了文献[4]在重定向功能与虚拟蜜罐不独立的不足，对黑客更具有迷惑性。文献[1~5]本质上是一种易于部署的动态可配置蜜罐，难以满足网络对抗的需要。

Blake K W 等描述了一种变形蜜罐系统的专利工作[6]，它通过预先收集分析各种操作系统和服务软件的漏洞信息并存储在蜜罐表征数据库中，在蜜罐工作时将会在不同的时间模拟不同的受害系统以增加蜜罐系统的甜度，吸引攻击者入侵。变形蜜罐系统借鉴了变形金刚的思想而提出，但该系统尽管蜜罐表征在变化，但蜜罐位置是静止不动，因而仍然容易为黑客所识别而失效。

Sardana A 等则提出了综合蜜罐模型[7]，由中心控制模块首先生成并部署蜜罐和 FTP 服务器群，然后运用熵检测技术识别攻击数据流，分析判断攻击行为后将攻击者引入蜜罐，而合法数据流重定向到服务区。综合蜜罐模型每隔一定时间重新生成并部署蜜罐和 FTP 服务器，蜜罐和服务器的 IP 地址不固定，因而更具迷惑性。该模型并非对蜜罐和 FTP 服务群实施功能切换，而是采用集中控制方式重新生成并部署蜜罐和服务群，并对所有输入流进行熵检测和重定向。这些耗时且必需的工作导致综合蜜罐模型存在着大规模攻击情况下的瓶颈问题。

Khattab S M 提出了一种旨在缓解 DDoS 攻击的漫游蜜罐模型[8]，由认证中心控制蜜罐和服务器的漫游，实现蜜罐和服务器的动态变化。但该模型同样基于集中控制策略，一旦控制中心遭受攻击，系统将同样出现瓶颈问题而无法正常工作。

本文基于虚实变化的兵阵思想，着眼于动态阵列蜜罐协同式防御，研究通过多机协同和功能角色的周期或伪随机切换而形成动态的陷阱阵列，从而达到迷惑和防范攻击者的目的。

3 动态阵列蜜罐框架

从协同式网络防御角度出发，给出动态阵列蜜罐（dynamic array honeypot）的概念，并简要描述模型框架如下。

定义 1 动态阵列蜜罐是指一种广义的蜜罐系统，它不是单个的固定蜜罐，而是以诸多真实环境的功能主机为基本单元，通过服务、蜜罐等任务的动态伪随机切换而形成的动态陷阱系统，从而迷惑和干扰敌手。

动态阵列蜜罐由协同控制单元 CC、同步单元 SYN、任务切换单元 TS、任务机群 TC 和可信客户端 Client 等组成，如图 1 所示。其中，协同控制单元 CC 是模型中的控制指挥单元，它按照策略协调控制任务机群中各主机任务的周期性切换，构成动态变化的陷阱阵列；同步单元 SYN 负责实现将服务器的变化信息通知可信客户端从而可以进行数据通信；任务切换单元 TS 则在协同控制模块控制下实施任务机群中任务主机状态的周期或伪随机切换，即服务功能和蜜罐功能的切换。

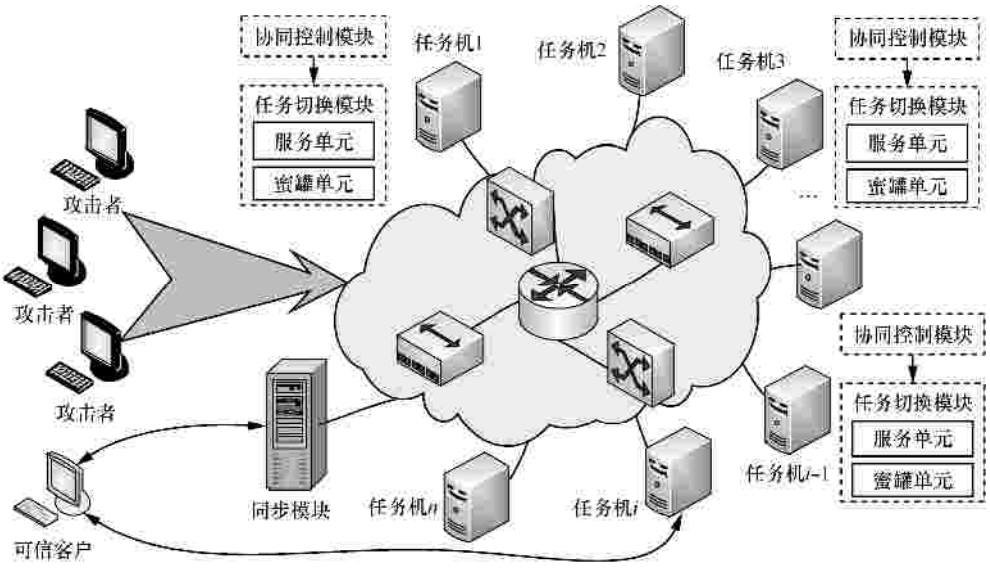

图 1　动态阵列蜜罐模型框架

可见，动态阵列蜜罐是一种多机协同、由真实系统构成的动态诱骗手段。模型中各主机任务不断切换，构成了变化的陷阱阵列，大大增加攻击者的攻击难度和攻击代价，并且有效克服了传统蜜罐存在的“即破即失效”问题，因而可以有效地防御和迷惑攻击行为，实现了积极主动的网络防范。

4　NS2 系统仿真与原型系统设计

为了对动态阵列蜜罐系统的有效性和系统性能进行分析和验证，本文采用 NS2 网络模拟平台仿真实现了动态阵列蜜罐模型，并基于 Java 平台设计实现了原型系统。

4.1　关键技术问题

4.1.1　同步机制

同步机制是动态阵列蜜罐系统的基本问题，它是通信双方在动态变化中进行数据通信时产生的。严格时钟同步[9]和报文确认异步[10]是分组网络应用中常见的同步方式，但由于网络延迟、拥塞和报文截获的存在，时钟同步和报文确认异步并不适合于大规模网络对抗应用。文献[11]对网络对抗中的同步策略进行了形式化定义和分析，给出了一种 UDP 发言人服务同步方案[12]，通过轻量级 UDP 发言人服务，将真实服务信息通过动态口令加密后提供给来访者而实现同步。该同步方案基于 UDP 协议提供轻量级任务，同步服务代价低，配合可信的动态口令分发，可以有效抵御拒绝服务和截获攻击，适于网络对抗应用。本文所设计的动态阵列蜜罐即采用了 UDP 发言人服务同步策略。

4.1.2　协同机制

协同机制则是动态阵列蜜罐的另一个关键问题，用来协同各功能主机完成预期的任务。常见的协同策略是集中式控制，但存在瓶颈问题而影响系统的可用性和顽健性，不利于网络对抗。本文借鉴 ad hoc 自组织网络中的簇头选举方法，提出了“自选举协同控制”策略，由动态阵列蜜罐各功能任务主机负荷最少的前 m 个主机执行服务器功能，而其他主机作为蜜罐。这里，负荷大小与流量、响应时间等诸多因素相关。选举操作在每一个阵列周期结束前触发执行，广播自身负荷并计算比较而得到下一周期的服务、蜜罐的配置信息。负荷小的主机将在下一周期切换为服务主机，这样可以有效利用阵列系统中的可用资源完成通信服务；而负荷大的主机则切换为蜜罐主机，从而迷惑和干扰攻击者。特殊地，在主机遭受攻击而瘫痪的情况下，由于其他结点无法接收到该主机的负荷信息，协同策略将忽略该主机而不参与选举过程，其他主机仍然可以参与协同选举，从而不影响整个系统的可用性。

4.2　NS2 系统仿真

基于 NS2 网络模拟环境对动态阵列蜜罐进行了系统仿真，修改了 TCP 代理模块，编写了 Server 服务模块、Client 客户模块、UDPServer 同步模块以及 Attacker 攻击模块，并通过编写 OTcl 脚本实现了网络拓扑仿真。系统仿真中的任务机群包含 5 个主机以进行 FTP 和蜜罐功能的切换，1 个 UDP 发言人同步服务器，2 个可信客户机，3 个攻击者，网络带宽为 1Mbit/s，如图 2 所示。仿真实验基于该

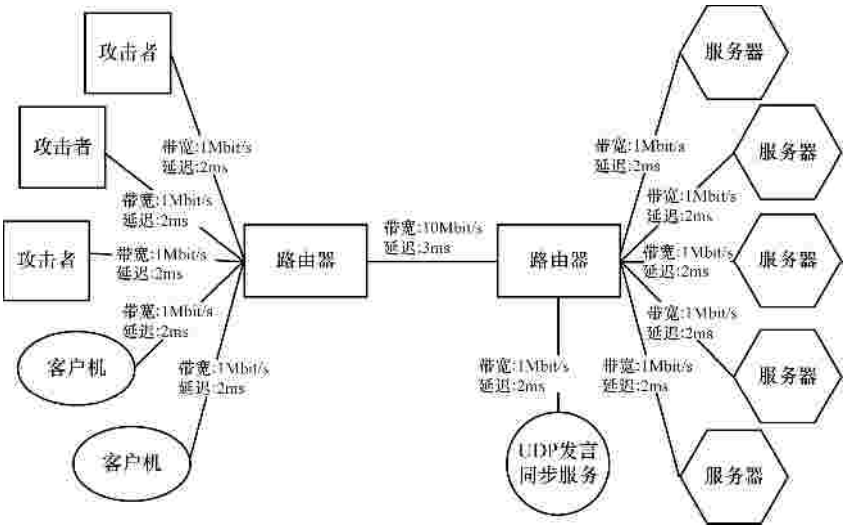

图 2 NS2 系统仿真网络拓扑

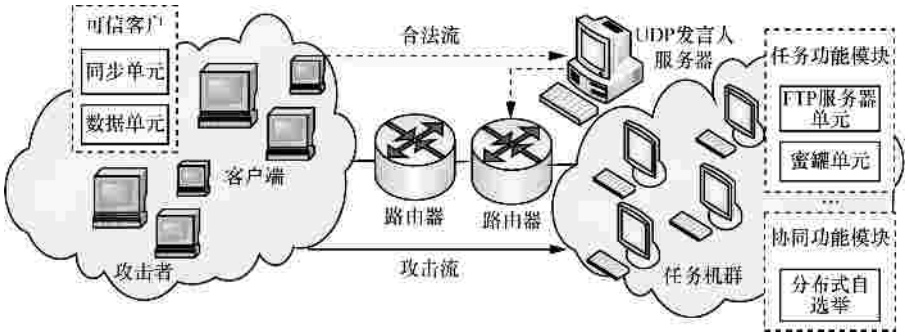

图 3 原型系统设计示意

网络拓扑模型而进行。

4.3 原型系统设计

基于 Java 平台设计实现了动态阵列蜜罐原型系统。原型系统由协同单元、任务功能模块、同步模块和客户模块组成，这几个模块协同完成 FTP 服务和蜜罐服务。协同单元是原型系统的核心，负责协调任务主机按照周期内通信量大小完成 FTP 服务器或蜜罐功能的切换；任务主机通信量统计采用 JPCAP 技术实现；同步模块负责与用户交互，提供给用户当前真实服务器的位置。原型系统功能模块示意如图 3 所示。

5 系统仿真与实验结果

在 NS2 模型仿真和原型系统的基础上，测试了 SYN-Flood 攻击情况下，不同切换周期和蜜罐/服务阵列组合对动态阵列蜜罐系统性能的影响。

5.1 不同切换周期对系统性能影响

图 4(a)给出了 NS2 仿真情况下客户请求量为 1.3Mbit/s，SYN-Flood 攻击速率为 0.8Mbit/s 和 1.3Mbit/s 时的仿真实验结果，图 4(b)给出了对应的原型系统实验在网络带宽 100Mbit/s、5 台任务主机和 1 台 UDP 同步服务器条件下的 SYN-Flood 攻击测试结果。

图 4(a)仿真实验结果显示，动态阵列蜜罐的系统性能在阵列周期为[10s, 30s]区间时较好。图 4(b)原型系统实验结果也证实了阵列周期在 20s 左右时系统抗攻击性能更优，与仿真实验结果一致。可见，动态阵列蜜罐的阵列周期对系统性能有重要影响。

如果动态阵列蜜罐系统动态变化很慢，容易因为攻击而性能恶化，不能及时缓解攻击的影响，因此客户端平均响应时间会增大。特别地，当跳变周期为无穷大时，系统进入非跳变模式，从图 4(b)实验结果明显可知，其抗拒绝服务攻击性能远远劣于阵列变化的系统。也就是说，动态阵列蜜罐系统抗攻击性能明显优于无服务切换的普通系统。然而，如果动态阵列蜜罐的阵列周期切换太快，网络拥塞和延迟将影响到服务的同步，服务器性能也会下降。

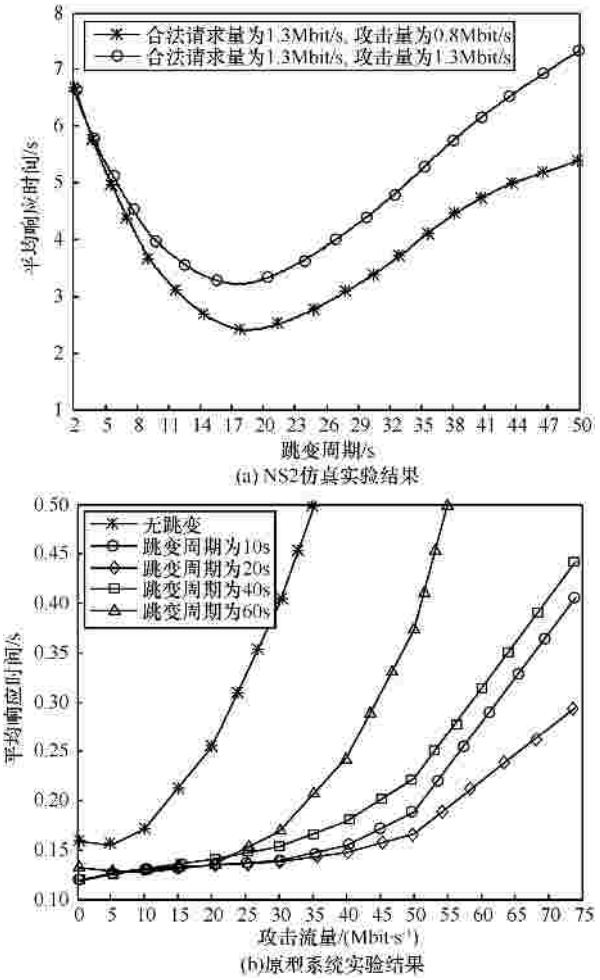

图 4　不同阵列切换周期对系统性能的影响

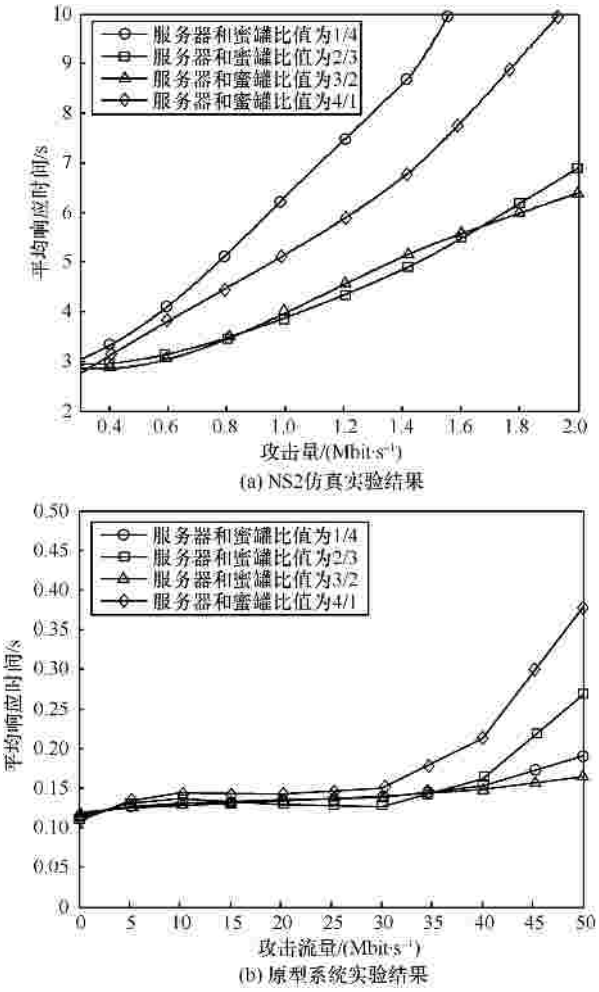

图 5　不同阵列组合对系统性能的影响

5.2　不同阵列组合对系统性能影响

测试了 5 台任务主机，阵列周期 20s，不同 SYN-Flood 攻击下服务/蜜罐主机比例对系统性能的影响。图 5(a)给出了 NS2 仿真实验结果，图 5(b)则给出了原型系统实验拟合曲线。

可见，动态阵列蜜罐中，各功能任务主机的阵列组合，即蜜罐和服务主机的比例变化，对系统性能也有重要的影响。图 5(a)和图 5(b)的结果证实了不同阵列组合可以影响到系统抗攻击性能，并具有相似的拟合趋势。尽管阵列组合实验结果并不能证明哪一种阵列组合为最优，但从另一方面表明了动态阵列蜜罐系统可以针对不同的网络对抗应用选择合适的阵列组合以获得优化的抗攻击性能。

6　结束语

针对大规模网络对抗，借鉴兵阵思想，本文提出了动态阵列蜜罐的概念，旨在通过多机协同、功能角色的周期或伪随机切换，形成动态变化的阵列陷阱，从而达到迷惑和防范攻击者的目的。在此基础上，本文给出了动态阵列蜜罐协同式网络防御的模型框架，进一步对动态阵列蜜罐进行了 NS2 仿真实现和 Java 原型系统设计，证明了动态阵列蜜罐的可行性。以仿真模型和原型系统为测试环境，分别测试了不同阵列变化周期和阵列组合情况下动态阵列蜜罐系统的抗攻击性能，仿真结果和实验结论具有良好的一致性，验证了动态阵列蜜罐系统的有效性。今后的工作将运用随机 Petri 网理论对动态阵列蜜罐系统的吞吐率、系统性能、同步代价、协同代价以及同步和协同策略的抗攻击性能进行理论分析和实验验证，为动态阵列蜜罐主动防御策略的有效应用提供支持。

参考文献：

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

[2] KUWATLY I, SRAJ M, MASRI Z. A dynamic honeypot design for

intrusion detection[A]. IEEE/ACS International Conference on Pervasive Services[C]. Beirut, Lebanon, 2004.95-104.

[3] HIEB J, GRAHAM J. Anomaly-Based Intrusion Detection for Network Monitoring Using a Dynamic Honey Pot[R]. 2004.

[4] HECKER C, NANCE K, HAY B. Dynamic honeypot construction[A]. Proceedings of the 10th Colloquium for Information Systems Securit Education[C]. Maryland, USA, 2006. 95-102.

[5] **陈启璋, 林国恩, 李建彬. 一种基于动态蜜罐和实时仿真的蜜网设计**[J]. **微计算机信息**, 2006, 22(36): 28-30.
CHEN Q Z, LIN G N, LI J B. Honeynet design based on dynamic honeypot & real-time emulation[J]. Control & Automation, 2006, 22(36): 28-30.

[6] BLAKE K, CONVERSE V, EDMARK R, *et al*. Method and System for Morphing Honey-Pot[R]. 2008.

[7] SARDANA A, JOSHI R. An integrated honeypot framework for proactive detection, characterization and redirection of attacks at ISP level[J]. Journal of Information Assurance & Security, 2008,3(1): 1-15.

[8] KHATTAB S, SANGPACHATANARUK C, MOSSE D, *et al*. Roaming honeypots for mitigating service-level denial-of-service attacks[A]. ICDCS2004[C]. Tokyo, Japan, 2004. 328-337.

[9] MILLS D. Simple Network Time Protocol[S].

[10] BADISHIY G, HERZBERG A, KEIDAR I, *et al*. Keeping denial-of-service attackers in the dark[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(3):191-204.

[11] **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.

[12] SHI L, LI J. Research on synchronization strategies for network confrontation[A]. WiCOM2010[C]. Chengdu, China, 2010.1-4.

作者简介：

石乐义（1975-），男，山东临朐人，博士，中国石油大学（华东）副教授、硕士生导师，主要研究方向为网络安全、博弈理论和移动计算。

李婕（1987-），女，山东济南人，中国石油大学（华东）硕士生，主要研究方向为网络信息安全。

刘昕（1974-），女，山东青州人，博士，中国石油大学（华东）讲师，主要研究方向为信息安全、社会网络和可信计算。

贾春福（1967-），男，河北文安人，博士，南开大学教授、博士生导师，主要研究方向为信息安全与可信计算、恶意代码发现与分析等。