doi:10.11959/j.issn.1000-436x.2017230

抵御 DoS 攻击的端信息跳变 Web 插件机制

石乐义，孙慧，崔玉文，郭宏彬，李剑蓝
（中国石油大学（华东）计算机与通信工程学院，山东 青岛 266580）

摘 要：端信息跳变技术是为了减缓网络攻击而提出的一种主动网络防御技术，它通过伪随机地改变通信中的地址、端口等端信息来达到迷惑攻击者的目的。通过浏览器插件机制，将端信息跳变技术引入到 Web 防护领域，从而在 Web 访问中迷惑和干扰攻击者。浏览器插件模型有 2 个工作模式，即非跳变模式和端信息跳变模式，插件模式根据 UDP 发言人的指令来进行切换，在通信链路安全可靠时插件不进行端信息跳变，能够降低服务代价；当网络受到攻击时切换至端信息跳变模式，保障通信链路的安全。实验结果证明，基于端信息跳变技术的 Web 插件机制在 SYN Flood 攻击和 UDP Flood 攻击下，仍具有较高的服务性能和安全性能。

关键词：网络安全；主动防御；端信息跳变；Web 插件；DoS 攻击
中图分类号：TP393 **文献标识码**：A

Web plug-in paradigm for anti-DoS attack based on end hopping

SHI Le-yi, SUN Hui, CUI Yu-wen, GUO Hong-bin, LI Jian-lan
(College of Computer & Communication Engineering, China University of Petroleum , Qingdao 266580, China)

Abstract: The end hopping technology is a proactive network defense technology proposed to mitigate the network attack. By changing the IP address, port and other information in the communication pseudo-randomly to achieve the purpose of confusing the attacker. The plug-in mechanism based on the end hopping technology was introduced, and it was applied to the field of Web protection. This plug-in was designed to confuse and interfere with attackers. The plug-in model was divided into two working modes, which are non-end-hopping mode and end hopping mode. The plug-in according to the instructions of the UDP spokesman to switch its own work mode and when the communication link is safe and reliable, it choose the fist mode which can reduce the cost of services. Another, when the network is attacked, the plug-in switches to the end hopping mode to ensure the safety of communications.The experimental results show that the plug-in mechanism based on end hopping has high service and security performance under SYN Flood attack and UDP Flood attack.

Key words: network security, active defense, end hopping, Web plug-in, DoS attack

1 引言

在 Web 技术飞速演变、电子商务蓬勃发展的今天，微信、微博、网上银行等一系列的新型 Web 应用程序层出不穷，Web 应用逐渐成为软件开发的主流之一。然而，Web 应用的普及在给人们生活带来便捷的同时，也对网络安全带来了新的挑战。许多 Web 应用程序容易受到来自服务器、应用程序和内部已开发代码等的攻击，这些攻击行为能够绕过周边防火墙措施对 Web 应用实施攻击。同时，Web 应用系统中还存在着跨站脚本攻击、缓冲区溢出攻击、拒绝服务攻击、不安全的配置管理等安全问题。

收稿日期：2017-09-20
通信作者：石乐义，shileyi@upc.edu.cn
基金项目：国家自然科学基金资助项目（No.61772551）；青岛市科技计划基金资助项目（No.15-9-1-79-jch）
Foundation Items: The National Natural Science Foundation of China (No.61772551), The Science and Technology Plan of Qingdao (No.15-9-1-79-jch)

拒绝服务攻击（DoS）是一种难以防范的攻击方式，其最终目标是破坏网络或计算机的正常服务。拒绝服务攻击是黑客最常用的攻击手段，其攻击方式有很多种。目前较为流行的DoS攻击方法包括Flood攻击、Smurf攻击、DDoS攻击等。其中，Flood攻击又包括UDP Flood和SYN Flood，它们分别针对UDP协议和TCP协议的缺陷。DoS攻击给人们带来了巨大的危害，但目前针对这种攻击的防御能力有限，无法从根本上解决这个问题。传统的网络防御技术主要包括定期扫描、配置防火墙、入侵检测、入侵防御系统等静态的、被动的防御方式，主机信息仍然处于潜在的安全威胁之中，而攻击者则可通过多种方式来隐藏自己的真实信息，如僵尸网络、多级代理、肉鸡等。为了应对传统网络防御极其被动的局面，一种新的试图改变游戏规则的主动防御技术—移动目标防御（MTD）[1]被提出，防御方通过不断的动态变化来增加攻击者的攻击难度和代价。端信息跳变（end hopping）技术[2]是一种典型的MTD机制，通过借鉴跳频通信的思想，在网络通信过程中，通信双方或一方按照约定的规律策略同时并同步地、伪随机地改变通信中使用的网络参数，这些参数包括端口、IP地址、时隙、加密算法甚至协议等端信息，从而破坏攻击者的干扰与攻击，实现主动网络防护。在这个跳变过程中可以是服务器的单方面跳变，也可以是双方面的跳变。

本文针对传统Web网络防御技术在抵抗DoS攻击上的被动与不足，引入端信息跳变技术来缓解Web应用中的DoS攻击，并且结合浏览器的插件机制，有效地提高Web访问中对DoS攻击的安全防御能力。

2 相关工作

针对日益严重的DoS攻击国内外学者也提出了各种各样的防御措施。魏春霞等[3]针对Web服务中存在的源地址伪造DoS攻击问题，提出了一种在基于安全令牌的防御Web服务DoS攻击方法。通过引入的令牌，验证Web服务请求者的源地址是否合法，从而抵御基于源地址伪造的DoS攻击。刘泽宇等[4]设计了一种基于Web行为轨迹的防御模型，把用户的行为抽象成Web行为轨迹，计算用户正常访问和攻击访问时产生的异常因素偏离值，以此来检测针对Web网站的DDoS攻击。丁彭父乐[5]提出了基于地址特征的防御框架（DFAC），通过对源IP进行分类聚合，构建其特征子集，然后基于这个特征子集对DoS攻击行为进行检测与防范。万明等[6]提出了一种基于双门限机制的DoS防范方法，结合迭代思想的谜题机制来减缓映射信息条目的增加速率，并且过滤识别此中的恶意映射信息条目，该方法能够有效地抵御映射缓存DoS攻击，防止映射缓存溢出。李星[7]提出一种基于Snort的DDoS攻击检测系统，对现有的模式匹配算法进行改进，提升了DDoS攻击检测系统的检测效率。Wang等[8]设计了一种DoS攻击缓解架构和一个基于概率图模型的DoS攻击检测系统，可以很好地处理数据集偏移问题。

Monika等[9]基于反向传播神经网络（BPNN）提出一种通过CPU性能、帧长度和流量3个参数来检测DoS攻击的方法，能够以96.2%的精度检测DoS攻击。Patel等[10]提出一种基于数据挖掘和模糊逻辑的入侵检测机制，能够识别检测新的DoS攻击是否为已知DoS攻击，有效识别入侵活动，提高入侵检测的检测率。Mousavi[11]提出一种基于目的IP地址熵变的DDoS攻击检测方案，能够在攻击流量的前500个数据分组内检测出DDoS攻击。而文献[12,13]针对SDN的DoS攻击提出了检测防御方法。综上，目前DoS攻击防御方法大多采用的是检测的方式，或是关于特定的DoS攻击而采取的防御方式，主动防御的方法研究相对较少。

而端信息跳变技术在主动防御方面受到越来越多的学者关注，它在通信过程中不断地改变通信的地址端口，只要攻击者对端信息变化的规律不知情，就难以针对通信端口和地址发起有效的攻击。目前，学术界已提出一些针对传统网络的端信息跳变技术。石乐义等[2]分析研究了端信息跳变主动网络防御模型，并且提出了一种UDP发言人服务时间戳的同步方法，验证了模型在抵抗攻击上的性能。但可能存在攻击者监听服务器端的网络或某些合法用户的网络，造成潜在的端信息网络泄漏的问题。贾春福等[14]深入分析了文献[2]中提出的基于端信息跳变的网络安全防护模型，并对其进行改进，结合浏览器插件机制，对客户端进行身份认证，以此来隐藏服务器的真实端信息。但该系统部署需要一个高性能的转发路由设备。林楷等[15]指出了端信息跳变技术在实际应用中的难点，并提出了一种基于消息篡改的端信息跳变技术，并在此基础上建立

了跳变栈模型，设计了跳变栈模型的 3 种实现方案以及分析了其工作原理。但其在用户层会带来不需要的系统开销，内核层需要严格与操作系统版本对应，网络层则需要一定的费用购置独立设备。刘江等[16]提出了基于非广延熵和 Sibson 熵融合的实时网络异常度量算法，设计了跳变周期和空间自适应策略，改善了固定跳变周期带来的防御收益下降的问题。

本文对基于端信息跳变技术的网络安全防护模型进行研究，将端信息跳变技术与插件机制结合，设计一个基于端信息跳变技术的 Web 插件机制。只有拥有该插件的客户端才可能成功访问到 Web 服务器，未安装本插件的用户则无法访问，即初步对非法客户端进行了筛选过滤，在主动防御 DoS 攻击方面有良好的效果。

3　端信息跳变 Web 插件防护模型

插件是一种根据一定规范的应用程序接口编写出来的程序，是会随着浏览器的启动自动执行的程序[8]。浏览器中的插件有无数种，安装相关的插件后，浏览器可以直接调用它来处理一些指定类型的文件。为了更好地抵抗 Web 中的网络攻击，防止端信息的泄露，本文引入了浏览器插件机制。拥有插件的合法用户能够正确得到服务器当前服务地址，而非法用户则无法获得。下面给出了该端信息跳变 Web 插件的功能模块，如图 1 所示。插件由服务模块和同步模块两大模块组成。其中，同步模块是整个系统的核心模块，包括 NTP 时间同步和 UDP 发言人。

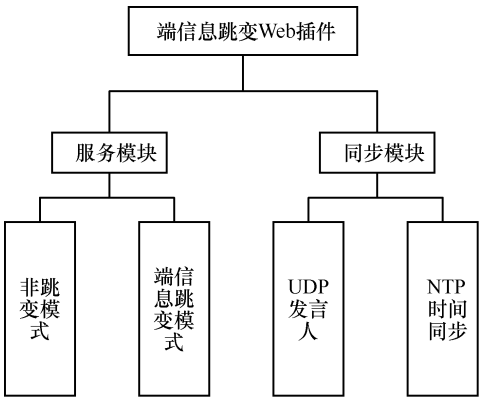

图 1　插件功能模块

网络中的时间同步通常根据各种网络时钟同步协议来实现，日期查询协议[9]和时间协议[10]虽然实现简单，但同步精度太低。而 NTP 协议可通过软件在各平台直接实现，且同步精度较高，因此，本文从实现复杂度和同步精度上分析采用 NTP 协议来实现网络时间同步。在网络中设置一台权威 NTP 时间同步服务器，为了减少每次同步带来的额外开销，插件与 Web 服务器采取定期与 NTP 服务器同步时间，减少双方的时间差，维护两端时间上的精准同步。只有在双方时间同步的情况下，才能实现客户端与服务器成功通信。

Web 服务根据人工指令切换其工作模式，UDP 发言人的功能即是将当前系统的服务状态告知客户端插件。插件通过同步模块获得当前的同步信息，计算当前服务地址和端口实现访问。服务模块提供了插件的 2 种工作模式：非跳变模式和端信息跳变模式。本文研究插件在端信息跳变模式下抵抗网络 DoS 攻击的效果。

3.1　非跳变模式

非跳变模式下即传统普通的 Web 服务，插件提供正常的 Web 访问功能，图 2 是其网络通信模型。插件通过固定的 IP 地址和端口进行通信，此时系统的开销最小，但是攻击者很容易通过网络监听获取用户的通信地址，从而针对目标发起攻击。因此，该工作模式适合网络环境是安全的状况。

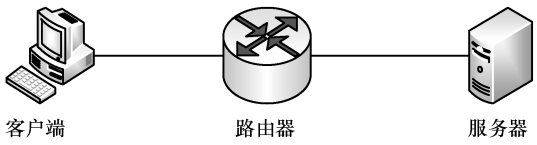

图 2　正常网络通信模型

3.2　端信息跳变模式

在端信息跳变模式中，网络通信要素不断地变化，只有合法用户才能在正确的端信息上进行信息传递并获得全部数据，非法用户或攻击者无法获得通信内容。插件在与服务器进行通信之前，首先，要知道服务器目前所使用的端信息，之后，才有可能成功向服务器发起访问请求。

首先，插件通过 UDP 发言人服务器获取当前系统服务状态。当系统处于模式 2 即端信息跳变模式时，服务器的 IP 地址和端口号信息不断地进行变换，对外其服务可看作客户端插件在和不同 IP 地址的服务器进行通信。插件每次数据传输时根据跳变策略计算 IP 地址和端口号。例如，可以将 Web 服务器看作由 N 个不同 IP 地址的虚拟服务器组成，

每个虚拟服务器设置一个 IP 地址和端口号组合，在同一时刻有且仅有一个虚拟服务器是处于服务状态。装有插件的客户端计算当前活动的端信息 IP_i+$PORT_i$ 并与服务器建立连接，端信息跳变的网络通信拓扑模型如图 3 所示。

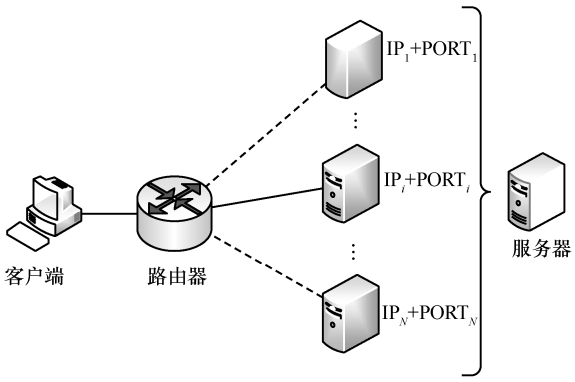

图 3 端信息跳变网络通信模型

为使攻击者无法预测用户的行为信息，下一跳变端信息的产生需具有随机性，攻击者无法分析其跳变规律，本文采用伪随机函数 R 来产生端信息的随机序列。

插件和服务器之间共享一个种子密钥 *key* 和加密算法。将服务器和客户端插件的时间分成等长的时间单元，并将它表示为 $T(i)$，i={0,1, 2,3,…}。服务器端和客户端插件的端信息每经过一个时间间隔 τ（$\tau \geqslant \delta$，δ 为最大传输时延）就进行一次端信息的跳变。假定服务器端的 IP 地址池为 IP={IP1, IP2, IP3,…, IPx}，端口号集合为 $PORT$= {$Port$1, $Port$2, $Port$3,…, $Porty$}，则服务器可用的端信息跳变组合总共有 N= xy 个。因此，根据式(1)可以确定当前应该使用的端信息组合

$$\{IP, Port\} = R\{i, key\} \tag{1}$$

其中，i 是当前时间单元号，由当前时间戳 t_{now} 除以跳变间隙 τ 然后取整计算得出。通信双方共享一个密钥 *key* 和一个处理函数 R。

客户端插件计算端信息的详细步骤如下。获取当前时间 t_{now}，计算 $INT\left(\frac{t_{\text{now}}}{\tau}\right)$ 得到时间单元号 i ；接下来将 i 和密钥 *key* 作为 R 函数的输入，得到 2 个基数，一个用于确定跳变后的 IP 地址，另一个用于确定跳变后的端口号，由于计算机系统中一般保留前 1 024 个端口，因此，若计算出的端口号小于 1 024，则在此基础上加上 1 024 即为跳变后的端口号。

当前服务 IP 和端口确定后插件建立和服务器的通信连接并传输数据，当一个服务时间周期结束后，插件重新计算端信息建立连接。

端信息跳变模式通过不断地变换通信地址和端口来迷惑攻击者，攻击者无法准确获得攻击目标，即使攻击者针对监听到的某一地址端口进行攻击，在攻击者发起攻击时，系统的服务地址和端口已然改变。本文提出的插件机制通过这种动态的、随机的变化达到主动防御的目的。

4 插件抗攻击性分析

分析本文提出的插件机制在防御 DoS 攻击方面的能力。假设攻击者知道此跳变技术的存在，并且从所有的端信息组合中任意挑选一个发起攻击。由于同一时刻有且仅有一个端信息组合处于活动状态，那么，由于端信息跳变技术的引入，攻击者能够准确攻击到目标所用的时间为

$$T' = \left(\sum_{i=1}^{N-1} i \frac{\mathrm{C}_{N-1}^{i}}{\mathrm{C}_{N}^{i}\mathrm{C}_{N-1}^{1}} + 1\right) T \tag{2}$$

其中，T 表示没有使用端信息跳变技术时攻击者击中目标所用时间。由式(3)可以看出，在插件中引入端信息跳变技术，增加了攻击者的时间代价，IP 地址和端口号的可选择范围越大 N 就越大，攻击者攻击成功所耗费的时间 T' 就越多。本文的设计中端口号的可用范围为 1 024~65 535，IP 地址由于实验环境限制设置为 10 个，地址和端口共有 645 110 种组合方式，每一时刻有且仅有一个组合被使用，攻击者成功预测该组合方式将十分困难。因此，理论上证明了基于端信息跳变技术的插件能够迷惑攻击者，并且增加了攻击代价，达到抵御攻击的目的。

5 实验与结果分析

5.1 实验环境

为测试插件策略在抵御攻击上的有效性和其自身服务性能，本文实现了插件的原型，并在实验室网内搭建了网络环境。本文从 2 个方面进行分析，一是插件在跳变状态下的服务性能；另一个是插件的安全性能，即抵御 DoS 攻击的能力。本实验设备环境如表 1 所示。插件所在客户端 IP 地址为 192.168.0.11，正常模式下服务器 IP 为 192.168.0.142，端口为 8081；跳变情况下服务器地址从 192.168.0.140 到 192.168.0.149，端口从 10000 到 65535。攻击者发起

SYN Flood 攻击和 UDP Flood 攻击。

表 1　　实验环境

对象	主机系统	内存/GB	处理器/GHz	带宽/(Mbit·s^{-1})
服务器	Ubuntu	2	3.70	1 000
客户端(插件)	Windows7	4	3.70	1 000
攻击者	Ubuntu	4	3.70	1 000
UDP/NTP 服务器	Ubuntu	2	3.70	100

5.2　服务性能测试

本文测试在无网络攻击状态下插件 2 种工作模式多次访问的响应时间，实验结果如图 4 所示。

从图 4 中可以看出端信息跳变技术的引入在一定程度上增加了系统的性能代价，但总体上来看代价在可接受范围内。在端信息跳变模式下，时间花销比正常模式增加 1~2 ms。

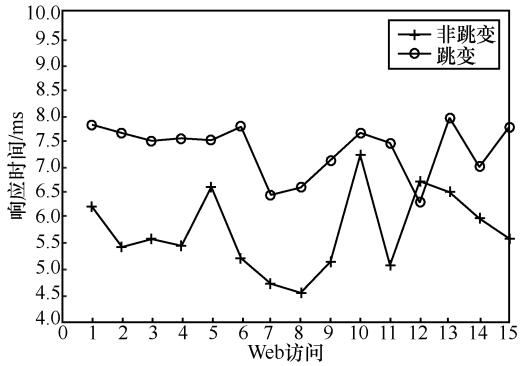

图 4　正常访问响应时间对比

5.3　安全性能测试

SYN Flood 是一种针对 TCP/IP 协议发起的攻击，其明显特征是被攻击者的主机上存在大量的 TCP 连接，它属于 DDoS 的一种，其威力比其他 DDoS 种类要强很多。UDP Flood 攻击的原理很简单，一般是利用大量的 UDP 数据分组冲击网络中的服务器。本文首先将攻击者的攻击速率设置为攻击计算机最大分组发送速度，对插件进行攻击测试。非跳变模式下遭受攻击后插件无法正常访问 Web 服务器，而在端信息跳变模式下，插件依然能够完成正常通信。图 5 分别展示了 UDP Flood 和 SYN Flood 的攻击测试结果。它展示了在固定大速率攻击时端信息跳变模式访问 Web 所消耗的时间，并与无攻击行为做对比，从图 5 中可以看到，有攻击行为时端信息跳变模式仍然能够较好地实现访问完成通信。

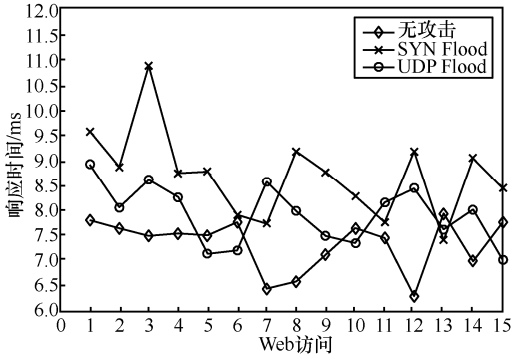

图 5　攻击测试

当网络遭受 UDP Flood 攻击时，大量的 UDP 数据分组涌入目标主机，消耗主机的网络资源，对正常的访问造成影响。但在本插件机制中，端信息跳变模式下通信地址和端口是不断变化的，攻击者无法锁定当前通信所用地址端口，避免了单一地址下因资源消耗殆尽而造成系统崩溃，能成功抵御 UDP Flood 攻击，保持正常通信。另外，其时长增加可能还有另外一个原因，就是大量的 UDP 分组阻塞了带宽，导致访问效率降低。

SYN Flood 攻击不单单是数据分组攻击，它伪造大量地址连接到服务器，发起 SYN 请求，服务器将消耗非常多的 CPU 时间和内存来处理这种请求，造成服务器无时间处理正常的连接请求，直到服务器超时后处理或耗尽服务器的处理进程。TCP 是有连接的服务，因此在耗时上较多。

图 6 和图 7 展示了不同攻击速率下非跳变模式和跳变模式的抗 DoS 攻击性能。从实验结果可以看出，随着攻击速率的增大，跳变模式下的服务响应时间无明显增大，趋于稳定。而非跳变模式下随着攻击速率的不断增大，服务响应时间也不断增大。

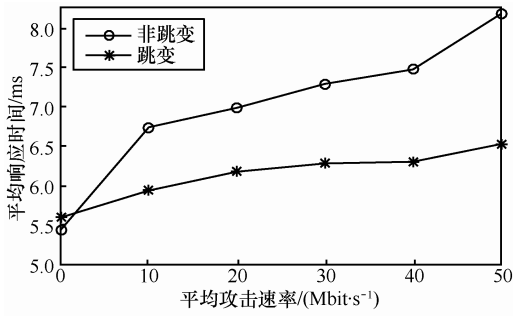

图 6　UDP Flood 攻击下服务响应时间

综上，各实验结果均证明，采用基于端信息跳变的 Web 插件机制能够很好地抵御 DoS 攻击并保持服务响应。在保持通信服务正常的同时提高了系统的安全性。

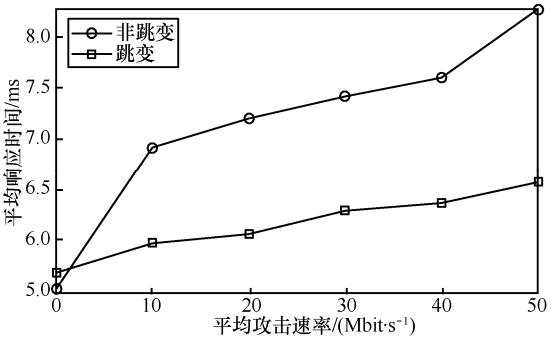

图 7　SYN Flood 攻击下服务响应时间

6　结束语

本文基于端信息跳变技术，引入浏览器插件机制，将其应用于 Web 防护领域，实现了在 Web 访问中主动防御 DoS 攻击的功能。本文插件模型包括 2 种工作模式：非跳变模式和端信息跳变模式，使用端信息跳变技术来提供系统的安全防护功能。最后分析了该插件的防御性能，利用实验验证了基于端信息跳变技术的 Web 插件机制具有较高的服务性能和安全性能。本文对基于端信息跳变的主动网络防御技术具有较高的应用价值。

参考文献：

[1] CARVALHO M, RICHARD F. Moving target defenses for computer networks [J]. IEEE Security & Privacy, 2014, 12 (2): 73-76.

[2] 石乐义, 贾春福. 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. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2): 106-110.

[3] 魏春霞, 张琳琳, 赵楷. 基于源地址伪造的 Web 服务 DoS 攻击防御方法[J]. 计算机工程与设计, 2014, 35(9): 3034-3038.
WEI C X, ZHANG L L, ZHAO K. Method research based on source address forgery defending Web service DoS attacks[J]. Computer Engineering and Design, 2014, 35(9): 3034-3038.

[4] 刘泽宇, 夏阳, 张义龙, 等. 基于 Web 行为轨迹的应用层 DDoS 攻击防御模型[J]. 计算机应用, 2017, 37 (1): 128-133.
LIU Z Y, XIA Y, ZHANG Y L, et al. Application-layer DDoS defense model based on Web behavior trajectory[J]. Journal of Computer Applications, 2017, 37 (1): 128-133.

[5] 丁彭父乐. 基于 IPv6 多地址性的 DoS 攻击与防御研究[D]. 哈尔滨: 哈尔滨工业大学, 2014.
DING P F L. Based on IPv6 Multi-addresses DoS attack and defense research[D]. Harbin: Harbin Institute of Technology, 2014.

[6] 万明, 张宏科, 尚文利, 等. 一体化标识网络映射缓存 DoS 攻击防范方法研究[J]. 电子学报, 2015, 43(10): 1941-1947.
WAN M, ZHANG H K, SHANG W L, et al. An efficient approach to defend DoS attack against mapping cache under identifier-based universal network[J]. Acta Electronica Sinica, 2015, 43(10): 1941-1947.

[7] 李星. 基于 Snort 的 DDoS 攻击检测系统研究与设计[D]. 北京邮电大学, 2015.
LI X. Research and design of DDoS attack detection system based on snort[D]. Beijing University of Posts and Telecommunications, 2015.

[8] WANG H P, XU L, GU G F. Floodguard: a DoS attack prevention extension in software-defined networks[C]//45th Annual IEEE/IFIP International Conference on Dependable Systems and Network. 2015.

[9] MONIKA K, DEEPAK K G, PRADEEP B. DoS attack detection technique using back propagation neural network[C]//International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2016.

[10] PATEL J, KATKAR V. A multi-classifiers based novel DoS/DDoS attack detection using fuzzy logic[J]. Springer, 2016: 809-815.

[11] MOUSAVI S M. Early detection of DDoS attacks in software defined networks controller[D]. Ottawa: Carleton University, 2014.

[12] 杨梦婷. 基于 OpenFlow 的 SDN 网络仿真平台设计与 DoS 攻击检测[D]. 北京: 北京邮电大学, 2015.
YANG M T. OpenFlow-based SDN network simulation platform and DoS attack detection[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[13] LIM S, HA J, KIM H, et al. A SDN-oriented DDoS blocking scheme for botnet-based attacks[C]//Sixth International Conference on Ubiquitous and Future Networks. IEEE, 2014:63-68.

[14] 贾春福, 林楷, 鲁凯. 基于端信息跳变 DoS 攻击防护机制中的插件策略[J]. 通信学报, 2009, 30(10):114-118.
JIA C F, LIN K, LU K. Plug-in policy for DoS attack defense mechanism based on end hopping[J]. Journal on Communications, 2009, 30(10):114-118.

[15] 林楷，贾春福. 基于消息篡改的端信息跳变技术[J]. 通信学报, 2013, 34(12): 142-148.
LIN K, JIA C F. End hopping based on message tampering[J]. Journal on Communications, 2013 , 34 (12) :142-148.

[16] 刘江, 张红旗, 代向东, 等. 基于端信息自适应跳变的主动网络防御模型[J]. 电子与信息学报, 2015, 37(11): 2642-2649.
LIU J, ZHANG H Q, DAI X D, et al. A proactive network defense model based on selfadaptive end hopping[J]. Journal of Electronics and Information Technology, 2015, 37(11): 2642-2649

作者简介：

石乐义（1975-），男，山东临朐人，博士，中国石油大学（华东）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。

孙慧（1991-），女，山东滕州人，中国石油大学（华东）硕士生，主要研究方向为网络安全、主动网络防御。

崔玉文（1992-），男，山东济宁人，中国石油大学（华东）硕士生，主要研究方向为网络安全、隐蔽通信。

郭宏彬（1992-），男，山东潍坊人，中国石油大学（华东）硕士生，主要研究方向为网络安全、主动网络防御。

李剑蓝（1993-），男，江西婺源人，中国石油大学（华东）硕士生，主要研究方向为网络安全、深度学习。