一种面向 C/S 模式的地址跳变主动网络防御方法

刘 江* 张红旗 杨英杰 王义功
(信息工程大学 郑州 450001)
(河南省信息安全重点实验室 郑州 450001)

摘 要：现有地址跳变方法需要设计新的地址交互协议，扩展性较差，跳变周期缺乏自适应调整，该文提出一种基于改进 DHCP 协议的地址跳变方法。利用自回归求和平均模型对网络流量进行建模和预测以计算预分配地址数目，根据地址空置周期选择预分配地址，利用基于动态时间弯曲距离的时间序列相似性度量算法检测网络异常并动态调整地址租用期，客户端和服务器基于地址映射关系进行跳变通信。该方法在无需修改现有 DHCP 协议的基础上实现了跳变地址和跳变周期的动态调整，增加了攻击者进行流量截获和拒绝服务攻击的难度，提高了攻击者代价。

关键词：地址跳变；C/S 通信模式；动态目标防御；主动防御
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2017)04-1007-05
DOI: 10.11999/JEIT160514

A Proactive Network Defense Method Based on Address Hopping for C/S Model

LIU Jiang ZHANG Hongqi YANG Yingjie WANG Yigong
(*Information Engineering University*, *Zhengzhou* 450001, *China*)
(*Henan Key Laboratory of Information Security*, *Zhengzhou* 450001, *China*)

Abstract: The existing address hopping methods need to design a new protocol of address exchanging and the scalability is usually limited. Also, its hopping cycle is difficult to make self-adaption. This paper proposes an address hopping method based on an improved Dynamic Host Configuration Protocol (DHCP). The number of hopping addresses is calculated by fitting and predicting network traffic which uses the auto regression integration moving average model. The hopping addresses are selected according to the address vacant time. The address lease time is adjusted dynamically according to the network anomaly which is detected by using the time series similarity measure algorithm based on dynamic time warping distance. Clients and application server are able to complete hopping communication based on the address mapping relationships. The proposed method can adjust hopping address and cycle dynamically without to modify the existing DHCP protocol, which not only increases attacker's difficult of intercepting traffic and launching denial of service attack but also enhances the attacker's overhead.

Key words: Address hopping; C/S communication model; Moving target defense; Proactive defense

1 引言

动态目标防御 MTD(Moving Target Defense)是指通过构建动态、异构、不确定的信息系统，增加其多样性、随机性和动态性，提升攻击难度和代价，有效限制脆弱性暴露及被攻击的机会。MTD 技术对于扭转网络安全易攻难守的局面，构建网络主动防御体系具有重要意义[1]。

地址跳变[2,3]是 MTD 在网络层的一种典型应用，指通信双方按照既定协议伪随机地改变通信地址，实现网络主动防御。传统网络的地址跳变方法有，文献[4]建立端信息跳变主动防护模型，采用移动代理技术进行端信息跳变，解决了跳变同步、数据切换等问题。文献[5]提出虚拟端信息跳变，将虚假随机端信息填充到数据报文的对应字段，达到重定向数据流的目的。文献[6]提出一种基于地址跳变的信息隐藏技术，采用多路径转发数据，提高了对等节点间数据传输的安全性。文献[7]提出一种防御 Hitlist 蠕虫攻击的网络地址空间随机化方法，运用透明地址混淆方法进行地址转换。文献[8]提出基于 IPv6 的动态目标防御架构 MT6D(Moving Target IPv6 Defense)，将当前主机 ID、会话密钥和时间戳

收稿日期：2016-05-19；改回日期：2016-12-26；网络出版：2017-02-24
*通信作者：刘江 liujiang2333@163.com
基金项目：国家 863 计划项目(2012AA012704)，郑州市科技领军人才项目(131PLJRC644)
Foundation Items: The National 863 Program of China (2012AA012704), The Scientific and Technological Leading Talent Project of Zhengzhou (131PLJRC644)

进行哈希，取前 64 位作为下一跳变地址，并采用类似 IPSec 协议的方式对数据报文进行封装。文献[9]建立了 IPv6 主动网络防御模型，给出了双重随机地址生成算法。分析上述地址跳变方案，存在以下问题：(1)现有地址跳变方法的应用依赖于新的地址交互协议，增加了网络负担，且新协议的安全性有待商榷；(2)地址跳变周期缺乏自适应调整，无法根据当前网络安全态势进行动态调整。

针对上述问题，本文利用 DHCP (Dynamic Host Configuration Protocol)协议保留字段，在不改变现有协议的基础上为同一主机同时分配多个地址，以满足地址跳变的多样性需求；基于现有 DNS(Domain Name System)协议建立客服双方的地址映射关系以及服务器固有地址与跳变地址的关联关系，在不改变服务器固有地址的情况下完成跳变通信，以满足地址跳变的随机性需求；利用基于动态时间弯曲距离 DTW(Dynamic Time Warping)的时间序列相似性度量算法检测网络异常并调整地址租用期，以满足地址跳变的动态性需求。

2 AHCSM 架构

AHCSM(Address Hopping for C/S Model)架构组成如图 1 所示，客户端部署跳变代理，应用程序服务器 AS(Application Server)配置安全网关 SG(Security Gateway)。跳变代理和 SG 保持客户端与 AS 的地址映射关系。

2.1 基于改进 DHCP 协议的动态地址分配

为减少 DHCP 协议交互次数，满足跳变通信对地址数量多样性的需求，提出以下方案流程：

(1)DHCP 服务器对地址池中的可用地址进行粒度划分，以若干地址集合作为一个地址单元，并选取一个作为主地址，其余作为辅地址。当收到 DHCP 请求报文时，将生成和分配地址单元，预分配的地址数量和地址集合将在 3.1 节中详述。(2)DHCP 服务器生成地址单元，将主地址写入 DHCP 响应报文的“yiaddr”字段，辅地址写入“option”字段。(3)跳变代理接收 DHCP 响应报文，解析出主辅地址和租用期 T_l，建立主辅地址关联关系，并将主地址转发给客户端，T_l 计算方法将在 3.2 节中详述。(4)客户端接收跳变代理转发的主地址，将其配置为本机真实地址。(5)当 T_l 到达一半时，客户端和 SG 要求更新 T_l，DHCP 服务器进行拒绝，客户端立即停止使用原有地址，并重新进行申请。

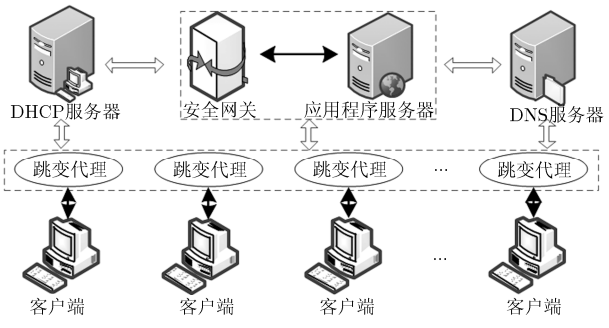

图 1 AHCSM 架构组成

为 AS 分配地址的流程与上述步骤类似，SG 建立的是 AS 自身固有地址与多个分配地址间的关联关系。该方案在一次协议交互中为同一主机分配多个互不冲突的地址，且适用于 IPv4 和 IPv6 网络。

2.2 基于地址映射关系的跳变通信

基于地址映射关系的跳变通信流程如图 2 所示，其具体流程为：

(1)DNS 域名系统除了为每个应用程序服务器 AS 保留其主机名和对应地址外，还为其关联多个相异地址。(2)客户端请求访问 AS 时，将待解析的域名写入 DNS 请求报文，以 UDP 用户数据报方式发送给本地域名服务器，此时 UDP 报文中的源地址为主 IP 地址。(3)DNS 请求报文到达跳变代理时，该代理根据主、辅地址关联关系，随机选取辅 IP 地址重写源地址，设置查询方式为递归查询，并转发至 DNS 服务器。(4)DNS 服务器每次接收到 DNS 请求报文时，从 AS 的主机与地址关联关系表中随机选取一个地址，封装为 DNS 响应报文，并赋予存活时间。(5)DNS 服务器将 DNS 请求报文中的 IP 地址和 DNS 响应报文中的 AS 地址的映射关系发送给响应请求的安全网关 SG。(6)跳变代理接收到 DNS 响应报文后，建立客户端与 AS 地址映射关系，并将客户端主 IP 地址的 DNS 响应报文推送给客户端。(7)当客户端通过域名访问 AS 时，请求报文的源地址为真实 IP 地址。(8)跳变代理利用客户端主辅地址关联关系以及客户端地址与 AS 地址映射关系，重写数据报文并进行发送。(9)SG 接收到客户端发送的数据报文，根据地址映射关系表，将报文目的地址重写为 AS 真实 IP 地址后，转发给 AS。

AS 响应请求的过程与客户端的访问过程类似。同时，SG 对接收到的数据报文进行过滤，发现报文地址为非该跳变周期内的活动地址时，立刻丢弃。

3 跳变要素计算

3.1 跳变地址

对于预分配地址数目，遵循“网络流量越大，分配地址数目越多”原则。借鉴文献[10]基于自回归求和平均模型对网络流量进行预测，依据网络流量预测值估算预分配地址数目，其概要计算方法如下：

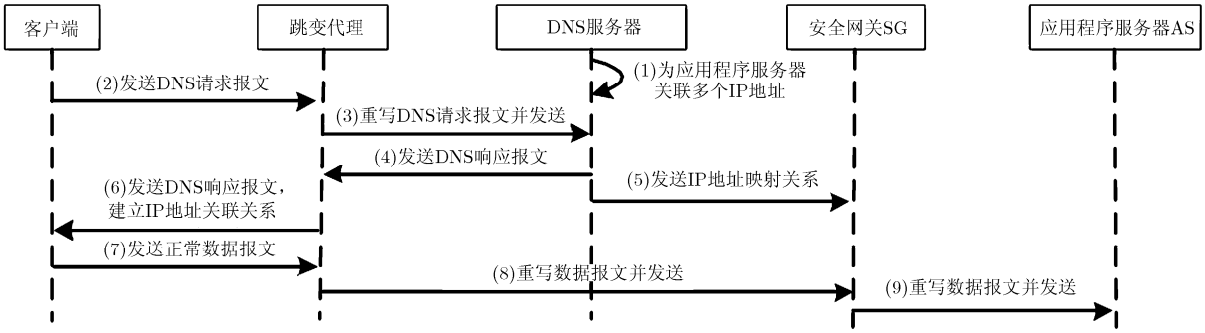

图 2 基于地址映射关系的跳变通信

$$\Phi(B)(1-B)^d X_t = \theta(B)a_t \tag{1}$$

其中，a_t 为白噪声，$\theta_i(1 \le i \le p)$ 为滑动平均系数，d 为差分次数且取正整数，B 为后向算子，$BX_t = X_{t-1}$，$\Phi(B)=(1-\varphi_1 B-\cdots-\varphi_p B^p)$ 和 $\theta(B)=(1-\theta_1 B-\cdots-\theta_q B^q)$ 分别为后向算子 B 的 p 阶和 q 阶多项式，$\varphi_i(1\le\ i \le p)$ 为自回归系数。

对于预分配地址集合，DHCP 服务器根据地址池中各个地址的闲置时间进行分配。

3.2 自适应跳变周期

AHCSM 架构的默认地址跳变周期满足参数为 λ 的泊松分布，在每一个跳变周期内对数据报文序列的源 IP 和目的 IP 进行相似性度量。度量值超出阈值说明存在网络异常，触发地址跳变并缩减跳变周期；否则，跳变周期仍服从既定的泊松分布。

3.2.1 基于 DTW[11]的地址序列相似性度量　AHCSM 架构中主机地址动态变化，攻击报文地址存在滞后性，甚至存在“过期”地址，较正常报文地址序列必然存在差异。

设客户端发送数据报文的时间序列为 $S=\left\{<t_1,s_1^k>,<t_2,s_2^k>,\cdots,<t_n,s_n^k>\right\}$，二元组 $<t_u,s_u^k>(1\le u\le n,1\le k\le 2)$ 表示时间 t_u 与 s_u^k 关联，s_u^1 和 s_u^2 表示发送报文的源、目的 IP；服务器端接收数据报文的时间序列为 $R=\left\{\left\langle t_1^{'},r_1^k\right\rangle,\left\langle t_2^{'},r_2^k\right\rangle,\cdots,\left\langle t_n^{'},r_n^k\right\rangle\right\}$，二元组 $\left\langle t_u^{'},r_u^k\right\rangle(1\le u\le n,1\le k\le 2)$ 表示时间 $t_u^{'}$ 与 r_u^k 关联，r_u^1 和 r_u^2 表示接收数据报文的源、目的 IP，点对距离为 $d\left(s_u^k,r_u^k\right)$。

$$d\left(s_u^k,r_u^k\right)=\begin{cases}0, & s_u^k=r_u^k\\ v+1, & s_u^k\ne r_u^k\cap s_{u+1}^k\\ & \quad\ne r_{u+1}^k\cap\cdots\cap s_{u+v}^k\ne r_{u+v}^k\end{cases} \tag{2}$$

其中，$s_u^k=r_u^k$ 和 $s_u^k\ne r_u^k$ 分别表示在时间节点 t_u 上，数据报文的第 k 维属性一致和不一致；$s_u^k\ne r_u^k\cap s_{u+1}^k\ne r_{u+1}^k\cap\cdots\cap s_{u+v}^k\ne r_{u+v}^k$ 表示在连续时间序列节点 t_u 到 t_{u+v} 上，数据报文的第 k 维属性都不一致。不失一般性，设 $D_i^k(S,R)$ 表示第 i 个跳变周期内第 k 维属性的时间序列相似性度量值，定义 $h_i=\max\left\{\left|D_{i+1}^k(S,R)-D_i^k(S,R)\right|\right\}$，$1\le k\le 2$，若 $h_i\ge\delta$，则表明第 i 个跳变周期的网络流量存在异常。

基于滑动时间窗口 Δt_{i+1} 生成度量时间序列，在不考虑网络时延的情况下，$D_i^k(S,R)$ 的突变值在每个 Δt_{i+1} 时刻被检测出的概率最大。定义 Δt_{i+1}：

$$\Delta t_{i+1}=T_l^i\big/Q_i \tag{3}$$

其中，$T_l^i=T_h^i$，T_h^i，T_l^i，Q_i 分别为第 i 个跳变周期的大小、地址租用期和实际分配的地址数目。

3.2.2 跳变周期自适应调整策略　若在 T_h^i 的所有滑动窗口度量值均未发生突变，增大 T_h^{i+1}；若在 T_h^i 的第 $\mu(1\le\mu\le Q_i)$ 个滑动窗口度量值发生突变，减小 T_h^{i+1}；若连续多个跳变周期的度量值均未发生突变，增加 T_h^{i+1} 的增大幅度，定义跳变周期增大因子 β：

$$\beta(h_i)=\begin{cases}0, & h_i\ge\delta\\ 1, & h_{i-1}\ge\delta,\ h_i<\delta\\ \beta(h_{i-1})+1, & h_{i-1}<\delta,\ h_i<\delta\end{cases} \tag{4}$$

跳变周期初始值 T_h^0，则跳变周期调整策略 T_h^{i+1}

$$T_h^{i+1}=\begin{cases}T_h^i+f(\beta)\cdot\Delta t_{i+1}, & h_i<\delta\\ T_h^i-g(i,\mu)\cdot\Delta t_{i+1}, & h_i\ge\delta\end{cases} \tag{5}$$

其中，$Q_i\ge 1$，$1\le\mu\le Q_i$，$1\le i\le m$。$f(\beta)$ 为跳变周期扩增函数，表示下一个跳变周期的增大幅度；$g(i,\mu)$ 为跳变周期缩减函数，表示下一个跳变周期的减小幅度。T_h^{i+1} 满足以下约束条件：(1) $h(i)<\delta$，$f(\beta)>0$；(2) $h(i)\ge\delta$，$-g(i,\mu)<0$；(3) $f(\beta)<g(i,\mu)$；(4) $\partial f(\beta)/\partial\beta>0$；(5) $\partial g(i,\mu)/\partial\mu<0$。

4 安全性分析

4.1 抗连通性 DoS 攻击

设可用跳变地址数为 m，攻击数据包中包含当前活动地址的数目为 k，r 为攻击速率，k 的期望为

$$E(k)=rT_{\text{tol}}/m \tag{6}$$

可见，m 越大，单位平均攻击强度越小；T_{tol} 越小，地址跳变越快，遭受持续攻击的概率越小。

4.2 抗流量截获攻击

设正常数据报文序列 $S=(s_1,s_2,\cdots,s_n)$，攻击者截获第 $i(1\le i\le m)$ 条链路的数据报文序列为 $V^i=(v_1^i,v_2^i,\cdots,v_{c_i}^i)$，则攻击者截获数据报文的总数为 $N_o=\sum_{i=1}^{m}c_i$。设攻击者的总开销为 C_a，则 $C_a=mC_o+A_{N_o}^nC_c$。其中，C_o 为单条链路截获数据包开销，C_c 为单个数据包分析重组开销。设攻击者在每条链路上截获的数据包数量都为 n，即 $\forall i,c_i=n$。当 AHCSM 策略增加的链路数目为 l 时，攻击者的开销增加 ΔC_a。

$$\begin{aligned}\Delta C_a&=(m+l)C_o+A_{(m+l)n}^nC_c-\left(mC_o+A_{mn}^nC_c\right)\\&=lC_o+\left(A_{(m+l)n}^n-A_{mn}^n\right)C_c\end{aligned}\tag{7}$$

由 $l>0$，得 $A_{(m+l)n}^n>A_{mn}^n$；又 $C_o>0$，$C_c>0$，得 $\Delta C_a>0$。可见，AHCSM 策略将流量进行分散，增大了攻击者开销。同时，l 越大，ΔC_a 越大，即跳变地址数目越多，攻击者开销增大的越多。

5 实验分析

5.1 实验条件

基于 NS2 对 AHCSM 架构进行仿真，利用 C++ 编写地址映射关系构建、数据报文重写等功能模块。实验环境配置如表 1 所示，设 $f(\beta)=\beta,g(i,\mu)=2^{-\mu}\cdot Q_i$，仿真实验结果如图 3–图 5 所示。

5.2 实验结果与分析

(1)抗连通性 DoS 攻击实验分析：采用 CC (Challenge Collapsar)攻击对 Web 服务器发起攻击，测试其在不同攻击强度下的平均响应时间。图 3 说明无地址跳变(no Address Hopping, nAH)、简单地址跳变(Simple Address Hopping, SAH)、文献[12]自适应地址跳变(Adaptive Ending Hopping, AEH)以及 AHCSM 跳变策略的抗攻击性能。初始跳变周期为 20 s，跳变地址数目为 10 个；AEH 策略的攻击强度阈值为 $\omega=3$ MB/s；AHCSM 策略跳变周期满足参数为 $\lambda=20$ 和 $\lambda=10$ 的泊松分布。

表 1 实验环境设置

主机角色	操作系统类型	带宽(Mbps)	数量
DHCP 服务器	Ubuntu 12.04	100	1
DNS 服务器	Ubuntu 12.04	100	1
应用程序服务器	Ubuntu 12.04	100	1
客户端	Windows 7	100	10
DoS 攻击主机	Ubuntu 12.04	100	1
Sniffer 攻击主机	Windows 7	100	1

实验结果表明：(a)自适应地址跳变策略能够通过减小跳变周期削弱攻击者发动持续 DoS 攻击的能力；(b)AHCSM 策略抗 DoS 攻击能力优于 AEH 策略，因为前者的攻击检测粒度更细，能够对攻击做出更加准确有效的反应；(c)AHCSM 策略跳变周期满足的泊松分布参数 λ 越小，抗 DoS 攻击性能越好。

(2)通信服务率实验分析：定义通信服务率为客服双方收发数据包数量的比值，可衡量跳变策略优劣。图 4 说明应用上述 4 种策略的通信服务率变化情况，CC 攻击的平均攻击速率先增大后减小。

实验结果表明：(a)攻击速率较小时，地址跳变对丢包率的影响大于 DoS 攻击对丢包率的影响；(b)随着攻击速率的增加，地址跳变对丢包率的影响逐渐小于 DoS 攻击对丢包率的影响，但是丢包率也迅速增大，通信服务率不断下降；(c)当攻击速率逐渐减小时，λ 越小，通信服务率越早开始恢复，表明 λ 越小越容易对跳变周期做出调整；但是 λ 越小，通信服务率增长得越慢，因为 λ 越小越容易丢失报文。

(3)抗流量截获实验分析：应用程序服务器 AS 的地址跳变范围为 192.168.1.1 到 192.168.1.254，客户端的地址跳变范围为 192.168.x.1 到 192.168.x.254，其中 $x\in N^*$，$2\le x\le 50$。AHCSM 策略的跳变周期满足 $\lambda=20$ 的泊松分布，每台客户机开启 5 个虚拟机终端模拟跳变客户端。使用 Sniffer 进行流量截获，记录数据报文源、目的地址分布情况，实验结果如图 5 所示。

实验结果表明：(a)AHCSM 策略将数据流量分

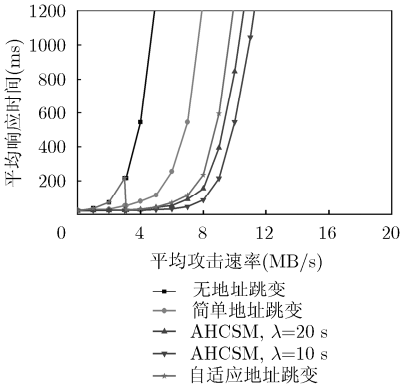

图 3 抗连通性 DoS 攻击仿真实验数据拟合

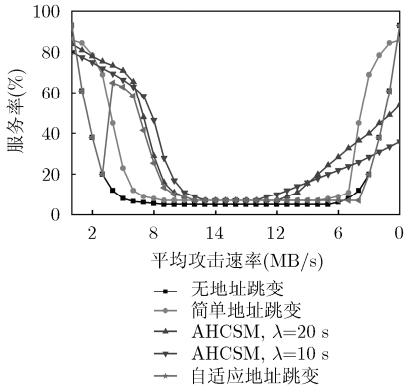

图 4 通信服务率仿真实验数据拟合

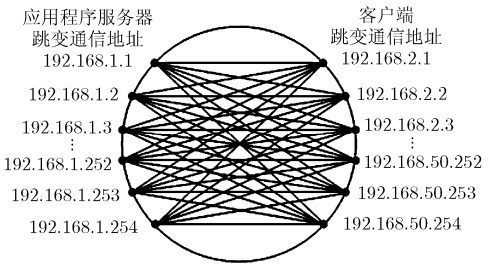

图 5 抗截获攻击分析仿真实验数据拟合

散到多条传输路径，迫使攻击者在所有可能路径进行监听，增加了攻击者进行流量截获的难度；(b)攻击者需要对所有截获到的数据包进行解析和重组，增大了攻击者成功获取有用信息的复杂度；(c) AHCSM 策略使得通信地址呈现出多样性和动态性，增加了攻击者获取网络拓扑的难度。

6　结束语

基于改进DHCP协议的地址跳变适用于传统网络的 C/S 通信模式，既避免了设计和应用新的地址交互协议，又具有良好的可扩展性。跳变周期基于网络异常自适应动态调整，增加了地址跳变的动态性和灵活性。但是，对于 DHCP 和 DNS 服务器的防护，还应结合访问控制、异常检测等安全机制进行联动防御，以期达到更好的防御效果。

参 考 文 献

[1] ZHUANG Rui, BARDAS A G, DELOACH S A, *et al*. A theory of cyber attacks: A step towards analyzing MTD systems[C]. Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, Colorado, 2015: 11–20.

[2] GREEN M, MACFARLAND D C, SMESTAD D R, *et al*. Characterizing network-based moving target defenses[C]. Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, Colorado, 2015: 31–35.

[3] JAFARIAN J H, AL-SHAER E, and QI Duan. An effective address mutation approach for disrupting reconnaissance attacks[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(12): 2562–2577. doi: 10.1109/TIFS.2015.2467358.

[4] 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 Leyi, JIA Chunfu, and LÜ Shuwang. Research on end hopping for active network confrontation[J]. *Journal on Communications*, 2008, 29(2): 106–110.

[5] ATIGHETCHI M, PAL P, WEBBER F, *et al*. Adaptive use of network-centric mechanisms in cyber-defense[C]. Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, Cambridge, MA, 2003: 183–192.

[6] SIFALAKIS M, SCHMID S, and HUTCHISON D. Network address hopping: A mechanism to enhance data protection for packet communications[C]. 2005 IEEE International Conference on Communications, London, 2005: 1518–1523.

[7] ANTONATOS S, AKRITIDIS P, MARKATOS E P, *et al*. Defending against hitlist worms using network address space randomization[J]. *Computer Networks*, 2007, 51(12): 3471–3490.

[8] DUNLOP M, GROAT S, URBANSKI W, *et al*. MT6D: A moving target IPv6 defense[C]. 2011 IEEE Military Communications Conference, Baltimore, MD, 2011: 1321–1326.

[9] 刘慧生, 王振兴, 郭毅. 一种基于多穴跳变的 IPv6 主动防御模型[J]. 电子与信息学报, 2012, 34(7): 1715–1720. doi: 10.3724/SP.J.1146.2011.01350.
LIU Huisheng, WANG Zhenxing, and GUO Yi. An IPv6 proactive network defense model based on multi-homing hopping[J]. *Journal of Electronics & Information Technology*, 2012, 34(7): 1715–1720. doi: 10.3724/SP.J.1146.2011.01350.

[10] 姜明, 吴春明, 张旻, 等. 网络流量预测中的时间序列模型比较[J]. 电子学报, 2009, 37(11): 2353–2358.
JIANG Ming, WU Chunming, ZHANG Min, *et al*. Research on the comparison of time series models for network traffic prediction[J]. *Acta Electronica Sinica*, 2009, 37(11): 2353–2358.

[11] LI Junkui and WANG Yuanzhen. EA DTW: Early abandon to accelerate exact dynamic time warping[C]. 2007 International Conference on Intelligent Systems and Knowledge Engineering, Chengdu, China, 2007: 144–152.

[12] 赵春蕾. 端信息跳变系统自适应策略研究[D]. [博士论文], 南开大学, 2012.
ZHAO Chunlei. Research on adaptive strategies for end-hopping system[D]. [Ph.D. dissertation], Nankai University, 2012.

刘　江：　男，1988 年生，博士生，研究方向为动态目标防御、网络安全管理.

张红旗：　男，1962 年生，教授，博士生导师，研究方向为网络信息安全、网络安全管理.

杨英杰：　男，1971 年生，教授，硕士生导师，研究方向为数据挖掘、态势感知.

王义功：　男，1987 年生，硕士，讲师，研究方向为网络安全管理.