端信息跳扩混合的主动网络防御技术研究

石乐义，郭宏彬，温晓，李剑蓝，崔玉文，马猛飞，孙慧
（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：受扩频通信技术启发，提出了端信息扩展的概念，利用多项端信息组成的序列来表示一条信息，使通信端信息与所传递信息无关，实现了端信息高隐蔽传输。进一步提出了端信息跳扩混合主动网络防御技术，将端信息跳变策略与同步策略分离，通过端信息扩展机制实现跳变通信双方的同步认证，解决了高隐蔽性要求下的高速跳变同步问题。详细讨论了端信息跳扩混合主动网络防御技术中扩展序列的生成、传输、同步认证方式和数据迁移策略，并对所提模型的安全性能和同步性能进行理论分析与实验验证。理论分析与实验结果表明，端信息跳扩混合主动网络防御技术提升了高速跳变下网络服务的可用性和隐蔽性，对于高强度对抗要求的主动网络防护应用具有重要意义。

关键词：端信息扩展；端信息跳扩混合；主动网络防御；数据迁移；高速跳变
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019071

Research on end hopping and spreading for active cyber defense

SHI Leyi, GUO Hongbin, WEN Xiao, LI Jianlan, CUI Yuwen, MA Mengfei, SUN Hui
College of Computer and Communication Engineering, China University of Petroleum, Qingdao 266580, China

Abstract: Inspired by the spread spectrum technology for communications, the concept of end spreading was proposed to represent a piece of information of the data transmission with a sequence of multiple end information, of which each piece of end information was irrelevant to the information it conveys. Thus the covert data transmission can be performed. Further, an active cyber defense model of end information hopping and spreading was presented, in which the hopping strategy was separated from the synchronization strategy. The synchronization was accomplished by means of end information spreading for synchronous authentication of both parties, which can solve the high-speed hopping synchronization problem with high concealment requirements. The mode of generation, transmission and authentication of the spreading sequence, and the data migration strategy in the end hopping and spreading model were described in detail, and the security performance and synchronization performance were analyzed and verified experimentally. Theoretical analysis and experimental results show that the cyber defense model of end information hopping and spreading has improved the availability and confidentiality of network services under high-speed hopping and has good anti-attack performance, which is of great significance for the proactive defense application of high intensity confrontation.

Key words: end spreading, end hopping and spreading, active network defense, data migration, high-speed hopping

1 引言

近年来，随着互联网的普及和发展，层出不穷的攻击手段使网络安全事件频发。防火墙、入侵检测技术等传统的网络防御手段由于静态、被动的特性，难以有效地应对自动的、多样的网络攻击，因此主动网络防御技术日益成为研究热点。

端信息跳变技术是一种主动网络防御技术，借鉴

收稿日期：2018−09−07；**修回日期**：2019−01−21
基金项目：国家自然科学基金资助项目（No.61772551）
Foundation Item: The National Natural Science Foundation of China (No.61772551)

了军事跳频通信对抗技术，通过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、IP 地址、时隙、协议等端信息，从而破坏敌方的攻击和干扰，达到迷惑攻击者的目的，实现主动网络防护[1]。

与跳频通信技术类似，跳变速率和跳变图案隐蔽性是影响端信息跳变抗攻击性能的 2 个重要因素。若跳变速率过低，系统易受到敌手的拒绝服务、重放攻击等；若跳变图案隐蔽性差，系统面临截获分析威胁，从而完全暴露在敌手攻击面前。然而，端信息跳变技术是一种基于分组交换的端到端的数据传输技术，与基于电路交换模式的点到点的跳频通信技术有着很大的不同，主要表现在：1) 分组交换网络本质是异步的；2) 分组数据经不同路径转发，存在乱序问题；3) 分组交换网络的网络延迟是变化的，并易受到分组转发、网络拥塞等影响，而跳频通信的网络延迟相对较小且固定。这些因素决定了端信息跳变技术在同步策略、跳变速率、抗攻击性能等方面都与跳频通信有较大差异。目前，严格时钟同步、时间戳同步等经典的端信息跳变同步方式的跟踪式同步机制最高都只能提供秒级间隙的低速率跳变，无法支持亚秒级、甚至毫秒级间隙的高速率变化。在此背景下，高速跳变、高隐蔽性成为近年来端信息跳变技术在主动网络防御部署应用中亟需解决的难题。

军事通信中，跳频系统同样存在着信号隐蔽性差、抗多频干扰、跟踪式干扰能力有限等局限性，这在通信对抗应用中通过直接序列扩频技术予以弥补，形成了高隐蔽性、高抗干扰性的军事跳扩频混合通信技术。受跳扩频混合通信技术的启发，本文摒弃传统的跟踪式同步机制，提出了端信息扩展的概念，将同步机制表述为端信息扩展认证序列的形式，着手通过认证机制解决端信息高速跳变的同步问题。通信双方通过扩展认证序列完成同步认证，不需要准确知晓对方端信息，从而实现高隐蔽性要求下的高速跳变同步。进一步提出了端信息跳扩混合主动网络防御技术，理论分析了模型抗攻击性能，并实验验证了跳扩混合模型高速率跳变下良好的隐蔽性和抗攻击性能，对于高隐蔽条件下高强度对抗要求相关场景的网络部署应用，如政府、军队、航天、保密部门等应急保密通信的开展具有重要意义。

2 相关研究

近年来，国内外学者在主动网络防御领域开展的相关研究工作主要包括移动目标防御技术、拟态安全防御技术及端信息跳变技术。

移动目标防御技术（MTD，moving target defense）[2]是由美国国家科学技术委员会于 2011 年借鉴增加射击难度的移动靶训练而提出的，主要目的是使构建、分析、评价、部署等策略多样化和伪随机化，从而增加攻击的成本及复杂度，降低攻击成功的概率。在移动目标防御技术研究方面，文献[3]将移动目标防御技术应用到电网中，以阻止对电网状态估计的隐形虚假数据注入攻击；文献[4]提出了一种移动目标防御模型来缓解 DDoS（distributed denial of service）攻击，并从理论和仿真两方面验证了该模型的可行性；文献[5]中介绍了 μMT6D（micro- moving target IPv6 defense）的设计和优化，将移动目标防御技术应用到新型物联网中来限制攻击时间。

拟态安全防御（MSD, mimic security defense）技术由邬江兴院士于 2014 年借鉴拟态章鱼通过形态多变保护自身的方式而提出，主要思想是除目标对象的服务功能和性能不能被隐匿之外，系统的硬件、软件等均可以通过动态变化的方式进行拟态伪装，由此实现系统对于防御者可控而对于攻击者未知的状态，进而达到保护系统免受攻击的主动网络防御目的。文献[6-7]对拟态防御技术的基础理论进行阐述，给出了拟态防御框架，从理论上说明了拟态防御机制的有效性。文献[8]构建了拟态防御 Web 服务器，从实践验证了拟态防御的有效性和可行性。

端信息跳变技术则由石乐义等[1]于 2008 年提出，借鉴了军事跳频通信对抗技术，在端到端的数据传输中，通信双方或一方按照协定伪随机地改变端口、IP 地址、时隙、协议等端信息，实现主动网络防御。近年来，端信息跳变技术受到关注并与 P2P（peer to peer）、SDN（software defined network）、IPv6 等相结合得到了部署应用[9-11]。

综上所述，移动目标防御技术的思想源于移动靶射击训练来增加射击难度，拟态安全防御技术受启发于拟态章鱼的形态变化以躲避天敌捕杀，而端信息跳变技术则借鉴军事跳频技术从而实现通信对抗。尽管思想来源不同，但移动目标防御技术、拟态安全防御技术和端信息跳变技术都通过主动改变自身参数来迷惑敌手，因此都属于主动网络防御技术。从攻击面动态转移层面分析[12]，端信息跳变技术关注如端口、IP 地址、协议等相关参数的伪

随机变化，而移动目标防御技术和拟态安全防御技术则关注包括芯片、指令、代码、主机、网络和协议在内的软件、硬件、网络、平台等方面，因此，端信息跳变技术可以视为移动目标防御技术和拟态安全防御技术的网络场景特例。

端信息跳变研究方面，文献[13-15]提出了一种适用于端信息跳变技术的分布式时间戳同步策略，利用轻量级的时间戳计算出当前端信息，在解决了时间漂移和网络拥塞问题的同时也解决了边界丢失问题；随后又进一步给出了一种基于消息篡改的端信息跳变技术框架，建立了包括用户层跳变、内核层跳变、网络层跳变等端信息跳变栈模型，并通过网络原始套接字对消息分组的修改而实现伪随机变化。Luo 等[16-17]则利用伪随机端址跳变技术抵御内外部攻击，提出了一种基于加密散列的端址自同步策略，将 HMAC（hashed message authentication code）算法生成的消息认证码用作端口地址编码和解码的同步信息，降低了网络时延影响。文献[10,18]将 SDN 技术应用到端信息跳变中，通过同时改变通信双方的端信息和路由路径来混淆攻击者，保证了较小的通信时延开销与计算开销。文献[19]提出了一种基于混沌序列的端信息跳变技术，并将该技术应用于网络音视频通信中，提高了端信息跳变图案的随机性。

在自适应性能方面，文献[20]研究了可变时隙的端口跳变策略，提出了动态时钟漂移同步算法，解决了可变时钟漂移对时间同步影响的问题，提高了端口跳变策略的抗攻击性能。文献[21-22]则针对简单匀速端信息跳变易遭受跟随攻击、半盲攻击的问题，提出了用于端信息跳变系统的时间自适应策略和空间自适应策略，这 2 种策略能够根据所遭受攻击状况动态改变跳变时隙和跳变空间，其中，时间自适应策略旨在增大跟随攻击的难度，空间自适应策略则用于抵御跟随攻击失效情景下有指导的盲目攻击（即半盲攻击）。文献[21-22]分析指出当攻击时间（即收集时间+实施时间）小于跳变时间（即部署时间+服务时间）时，端信息跳变系统将会遭受跟随攻击的严重威胁；当攻击时间大于跳变时间且量级相当时，跟随攻击失效，攻击者被迫转入有效的半盲攻击；当攻击时间远大于跳变时间时，端信息跳变系统的自适应策略才具有较好的防护效果。可见，端信息系统的抗跟随攻击和半盲攻击性能与跳变速率密切相关，而跳变速率与所采用同步机制密切相关。然而，文献[21]所采用的严格时钟同步和文献[22]所采用的时间戳同步都属于传统的跟踪式同步机制，两者的同步性能易受网络分组时延影响，最高都只能提高秒级间隙的低速率跳变（文献[21]的跟随攻击缺省设置为每跳 60 s，文献[22]设置为每跳 15 s），难以应对近年来性能日新月异的全自动化攻击。在抗截获攻击方面，文献[21-22]所采用的时间/空间自适应策略增加了截获分析难度，但跳变图案仍显式暴露从而面临严重的截获攻击威胁。

上述研究均是从跳变图案方面对端信息跳变技术进行改进，所采用的同步策略都是传统的跟踪式同步机制，受限于分组网络异步、乱序和时延的特点，无法支持亚秒、毫秒级间隙的高速率跳变，导致跳变图案易遭受全自动高速攻击而失去隐蔽性，从而造成端信息跳变技术主动防护的失效。本文工作正是为解决端信息技术高速跳变和高隐蔽性的难题而开展，受军事跳扩混合通信启发，摒弃了传统的跟踪式同步机制，将同步机制表述为端信息扩展认证序列的形式，创新性地提出了端信息扩展认证同步机制，并进一步建立了端信息跳扩混合主动网络防御技术，实现了高隐蔽的端信息高速率跳变（本文实验环境中缺省设置为每秒 100 跳），这对于高隐蔽高强度对抗要求的网络防护应用具有重要意义。

3　端信息跳扩混合主动网络防御技术

端信息跳变技术同步策略是可信客户端在攻击者无法准确探查跳变服务器真实端信息的情况下，能够有效进行服务访问的基础。基于端信息跳扩混合的主动网络防御技术采用端信息扩展的方式进行端信息跳变的同步认证，旨在建立一种不需要服务器真实端信息的跳变同步方式，提高服务器的隐蔽性，减小跳变时隙、跳变算法对端信息同步的影响，以应对高速跳变下的通信协同问题。

3.1　端信息扩展定义及其描述

扩频通信是扩展信号的频谱，发送端用扩频码序列进行扩频调制，使发送频谱与所传信息无关，从而达到良好的抗干扰性、抗截获性，以及较高的传输速率。受扩频通信思想的启发，本文提出了端信息扩展的概念，将与数据本身无关的端信息进行组合以表示数据，并用于同步认证。在网络通信中，通信双方可以利用端信息扩展序列的方式传递文字信息、认证信息等数据，通过端信息扩展算法进行数据的扩展序列生成及认证。

定义 1 端信息扩展（end spreading）：利用端信息扩展算法计算得出端信息扩展序列，将由多项端信息组成的扩展序列表示为一条数据信息，使各项端信息与所表示的数据本身无关，达到隐藏真实信息的目的，实现高隐蔽性。

端信息扩展可形式化描述为

$$L(Info)=\{endInfo_1, endInfo_2,\cdots,endInfo_m\} \quad (1)$$

其中，L(Info)为端信息扩展算法，是将数据与端信息扩展序列进行转换的方法。原始数据利用端信息扩展生成算法转化生成端信息扩展序列，与之对应，端信息扩展序列利用端信息扩展解析算法来还原数据。在一次端信息扩展过程中，端信息扩展算法与端信息扩展序列解析算法配对使用。

$endInfo_m$ 为单条端信息，由 IP 地址、端口及协议中的一项或多项组成。两项及以上的单条端信息组成端信息扩展序列，该序列是具有一定特殊含义的序列组合。

端信息扩展序列选取地址与端口组成单项端信息，由目的地址、目的端口、源地址和源端口组成。其中，采用目的地址 dIP_m 识别端信息扩展序列，目的端口 $dPort_m$ 校验序列的正确性，源地址 sIP_m 与源端口号 $sPort_m$ 用于识别来自同一个客户端的同步请求。端信息跳变的扩展序列为

$$EndSeq=\{(dIP_1,dPort_1,sIP_1,sPort_1),(dIP_2,dPort_2,sIP_2,sPort_2),\cdots,(dIP_m, dPort_m, sIP_m, sPort_m)\} \quad (2)$$

如图 1 所示，端信息扩展通过客户端的编码发送及服务器端的解码验证来实现，将传统的单一身份验证信息扩展为多条信息的组合序列。攻击者对扩展序列中某一条信息的捕获与解析无法确定用户的真实意图，同时可信客户端在端信息扩展认证过程中，不需要准确知晓服务器的真实信息，有效地保障了服务器的隐蔽性。

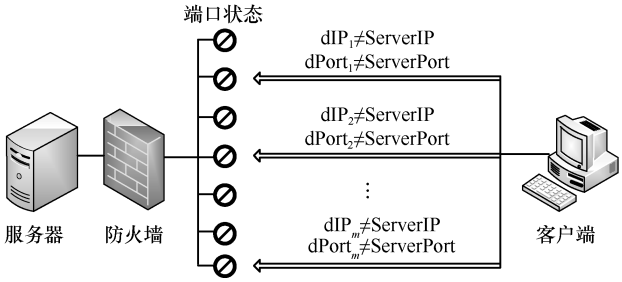


图 1 端信息扩展示意

3.2 端信息跳扩混合主动网络防御技术模型

端信息跳变技术旨在通过一定的跳变策略不断地改变服务的端信息，以动态的、未知的变化迷惑攻击者，使其无法准确地发起攻击，保障跳变服务的安全性，达到主动网络防御的目的。本文为了提高端信息跳变速率，使端信息跳变技术适应于高隐蔽性和保密性的应用场景中，从系统安全的角度出发，建立了端信息跳扩混合主动网络防御技术模型。该模型如图 2 所示，分为客户端与跳变服务器两部分，包括客户端的扩展序列生成模块、扩展序列发送模块、服务获取模块和服务器端的端信息跳变模块、扩展序列认证模块及服务提供模块。

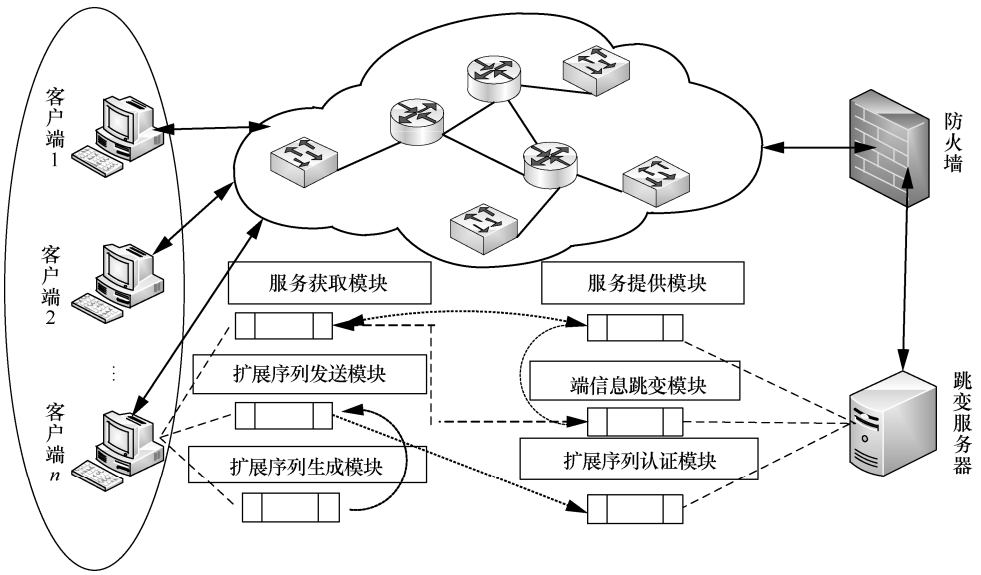


图 2 端信息跳扩混合主动网络防御技术模型

在端信息跳扩混合主动网络防御技术模型中，客户端首先生成端信息扩展序列，然后将扩展序列发送给服务器；服务器通过规则来检测扩展序列的合法性，如果合法，则通过认证并提供服务，否则不提供服务。例如客户端要选取地址 IP_1、IP_2 和 IP_3 做扩展序列的认证（扩展序列只包含目的地址和目的端口号），IP 地址与通过通信双方共同的算法分别求出 3 个地址所对应的端口号 $port_1$，$port_2$，$port_3$，这样就可以组成端信息扩展序列 $(IP_1,port_1)$、$(IP_2,port_2)$和$(IP_3,port_3)$，然后传递认证信息，由于服务器端有相同的扩展序列生成算法，服务器端接收到扩展序列之后就可以检测其合法性。

服务获取模块在端信息扩展序列发送完成后启动，等待服务器将各项信息认证通过后提供服务。端信息跳扩混合主动网络防御技术模型中的客户端不再如传统方式中那样主动向已知地址和端口的服务器发出服务请求，而是通过向未知端信息的跳变服务器发送端信息扩展认证序列，在通过认证后服务器向客户端提供特定的服务。由于客户端不需要知晓跳变服务器的真实地址便可发送同步认证信息，且跳变服务器的端信息具有动态性、未知性的特点，攻击者难以针对服务器的特定端口与服务发起攻击，因此模型具有良好的隐蔽性与抗攻击性，能够达到主动网络防御的效果。

为保证跳变系统的动态性及未知性，端信息跳变服务器采用随机跳变的跳变策略，该策略由跳变服务 S、跳变算法 HM 和跳变时隙 TS 三部分构成，如式(3)所示。

$$S\times \mathrm{HM}\times \mathrm{TS}\rightarrow \mathrm{HS} \tag{3}$$

其中，跳变服务 S 可采用 HTTP、FTP 等多项网络服务。

随机跳变算法 HM 在跳变地址池 IP_{hop} 与端口 $port_{hop}$ 范围内随机选择跳变端信息，跳变算法与地址池表示如式(4)和式(5)所示。

$$\mathrm{HM}=\mathrm{random}(IP_{hop}, port_{hop}) \tag{4}$$

$$IP_{hop}=\{IP_1,IP_2,\cdots,IP_n\} \tag{5}$$

跳变时隙 TS 是端信息跳变的一个重要参数，跳变时隙越短表示跳变速度越快，高速的跳变能够降低攻击者发起有效攻击的概率。当发起有效攻击时间一定时，若当前端信息被攻击者破获，高速跳变的情况下可在攻击者发起攻击之前改变端信息，使攻击无效。

通信双方基于端信息扩展同步策略实现跳变服务的同步过程。在端信息随机跳变的跳变策略下，客户端无法准确探查跳变服务器真实的端信息。结合端信息扩展方法能够在不需要真实服务器端信息的情况下建立连接的优势，通过客户端的端信息扩展序列生成发送及服务器的解析验证实现跳变服务的同步认证，将传统的单一身份验证信息扩展为多条信息的组合序列。

由于组成端信息扩展序列的单项端信息本身与所传数据无关，仅当满足条件的端信息组合成序列时才能从中解析出所传递的信息。传输过程中各扩展端信息是分散的，攻击者难以通过序列中的单项端信息获取有效信息，因此基于端信息跳扩混合的主动防护模型具有良好的隐蔽性与抗攻击性。

3.3　关键策略

本文中基于端信息跳扩混合的主动网络防御技术的关键策略主要指端信息扩展同步策略和数据迁移策略两大策略，前者为解决端信息高速跳变过程中通信双方同步问题而提出，后者为解决模型无法提供可持续性服务问题而提出。

3.3.1　端信息扩展同步策略

端信息扩展同步策略即采用端信息扩展算法进行端信息扩展序列的生成与认证，其中端信息扩展算法包括目的地址序列与端口序列的生成算法。通信双方在共享地址池中通过地址选取算法选取目的地址，表示为

$$dIP_m=G(\text{IP-pool},m) \tag{6}$$

在端信息扩展过程中从地址池 IP-pool 中逐个选取 m 个目的地址组成目的地址序列，利用生成的目的地址序列通过端口号生成算法计算端口号，如式(7)所示。

$$port_m=F(\mathrm{DIP},\mathrm{key},m) \tag{7}$$

其中，$F(\cdot)$为端口号生成算法；key 为共享密钥，可用于通信双方身份校验。逐一计算端口号组成本次端信息扩展的目的端口号序列，如式(8)所示。

$$\mathrm{DPort}=\{dPort_1,dPort_2,\cdots,dPort_m\} \tag{8}$$

发送方通过数据分组封装的方式将端信息扩展序列中的端信息逐个发送。

接收方利用监听进程捕获端信息扩展数据分组。通过解析数据分组获得目的地址与目的端口、源地址与源端口，采用与端信息扩展序列生成算法相对的地址验证算法识别端信息扩展目的地址，并

通过共享密钥 key 计算出相对应的端口号以校验目的地址，进行客户端身份识别。

单个端信息扩展数据分组认证成功后，对通过认证的合法数据分组是否能够组成端信息扩展序列进行判断，如式(9)所示。

$$\mathrm{IS}=\mathrm{check}(\mathrm{DIP},\mathrm{DPort},m_i,\tau) \tag{9}$$

其中，IS 为端信息扩展序列的判断，check 为地址验证算法，DIP 为目的地址，DPort 为目的端口号序列，m_i 为客户端所发送端信息中目的地址所在的地址池位置，τ 为序列容错率。允许端信息扩展序列中一定数量的端信息未通过验证，即满足数量为 $m(1-\tau)$的端信息认证通过即认证成功。

最后服务器为通过认证的可信客户端提供服务。由此实现无需服务器真实端信息的通信认证。

3.3.2 数据迁移策略

端信息跳扩混合主动网络防御技术虽然解决了端信息跳变过程中跳变时隙较小的高速跳变问题，但是同时也带来了在较小跳变时隙中服务提供无法完成的问题。这时需要一个任务调度器将未完成的服务在下一跳变时隙中继续完成，使系统能够正常地对外提供服务。TCP 迁移技术[23]是为解决负载均衡而出现的技术，主要思想是将一条 TCP 连接的一个端点迁移到另一个端点，而这个迁移对于连接的另一端点来说是透明的，并且迁移以后的连接可完全正常地运行下去。以 TCP 迁移技术为原型，将 TCP 迁移技术的特性应用到端信息跳扩混合主动网络防御技术中，形成服务迁移技术，在此称之为数据迁移策略。

数据迁移策略简化了原有 TCP 迁移模型，具体如图 3 所示。图 3 中客户端与 IP_2 建立三次握手成功，向目的 IP_2 请求服务 1，调度器 FE 作为代理将请求分组发送给地址 IP_2。当服务 1 未完全提交给客户端时，服务 1 迁移到地址 IP_1。由于是同一台服务器上的同一服务，服务器端可以利用地址 IP_1 继续为客户端提供服务 1，但在服务器端需要一个调度器 FE 装置将源地址 IP_1 修改为源地址 IP_2，这样在 IP_1 上发送给客户端的应答分组与在 IP_2 上发送的应答分组就是一样的，实现了数据的迁移。

数据迁移策略应用到端信息跳扩混合主动网络防御过程中，如图 3 所示，对于客户端来说一直是与 IP_2 进行通信、是透明的，避免了攻击者通过抓取分组分析得出跳变规律，提高了安全性；对于服务器端来说，消除了 TCP 重连三次握手的时间，提高了效率。

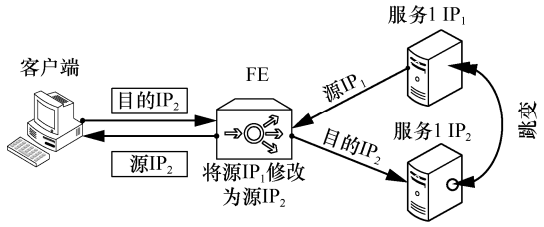


图 3 数据迁移策略示意

4 性能分析

性能分析涉及安全性能分析、同步认证性能分析和时间性能分析，本节主要讨论端信息跳扩混合主动网络防御技术能否保证服务的安全性，应对高速跳变下同步认证。

4.1 安全性能分析

基于端信息跳扩混合的主动网络防御技术的安全性能分析包括跟随攻击分析、半盲攻击分析和窃听攻击分析。

4.1.1 跟随攻击分析

跟随攻击是攻击者根据端信息跳变规律，不断地定位当前服务节点采取精确攻击。假设一个跳变周期时间为 t_s，攻击者获取当前端信息并发起攻击的总时间为 μ。由文献[22]可知，当 $t_s<\mu$ 时，攻击成功概率为 0，即在攻击者发起攻击之时端信息已经跳变；当 $t_s\geqslant\mu$ 时，t_s 越小，攻击成功的概率越低。为降低跟随攻击概率，可以选择减小 t_s 或者增大 μ。

基于端信息跳扩混合的主动网络防御技术中端信息跳变算法采用随机高速跳变策略，不需要按照跳变图案或时间戳等计算方式获取下一次跳变端信息。攻击者采取数据分组截获的方式难以获得当前端信息，从而增加攻击时间 μ，实现跳变端信息的隐蔽性和随机性。

高速跳变即采用较小的跳变时隙以减小 t_s，在同步认证分析中证明了端信息扩展同步策略与端信息跳变策略无关，能够解决高速跳变下导致的同步失败问题。

因此保证跳变服务性能的前提下，本文策略能够从理论上减小 t_s 增大 μ 以抵抗跟随攻击。

4.1.2 半盲攻击分析

半盲攻击是指攻击者虽然无法确定当前服务

节点端信息，但知道端信息跳变空间集合，从而实施有指导的盲目攻击。假设端信息跳变地址集合为 N，跳变端口空间为 P，随机选取 k 个端信息发起等量大小的攻击，则当前服务受到攻击的概率为 $\frac{k}{|N||P|}$。基于端信息跳扩混合主动网络防御技术中由于生成扩展序列的地址集合 M 的存在，此时攻击者探测到的总地址集合为 $M \cup N$，当 $M \cap N = 0$ 时，当前服务受到攻击的概率最小，为 $\frac{k}{(|N|+|M|)|P|}$，从而有效地降低当前服务节点受到攻击的概率，增强了跳变服务的隐蔽性。

4.1.3　窃听攻击分析

端信息跳扩混合方式中采用扩展序列进行同步认证。客户端将扩展序列中的端信息逐个发送，服务器在端信息扩展序列认证成功后，与可信客户端建立连接并提供跳变服务。在攻击者不知道当前采取端信息跳扩混合方式的情况下，无法通过窃听解析单个数据分组内容获取完整扩展序列，攻击成功概率 Q=0；当攻击已知当前服务器采取端信息跳扩混合方式的情况下，进行窃听攻击收集数据分组发起攻击时，假设当前网络环境下有 e 个数据分组，攻击者截获 k 个数据分组，端信息扩展认证的数据分组个数为 m，序列验证容错率 τ，则攻击者成功概率为

$$Q=\begin{cases} 0 & ,k<m(1-\tau) \\ \dfrac{\sum_{i=0}^{m\tau} C_m^{m(1-\tau)+i} C_{e-m}^{k-m(1-\tau)-i}}{C_e^k} & ,k \geqslant m(1-\tau) \end{cases} \tag{10}$$

其中，e、k 与当前网络环境和攻击者攻击强度有关，在 e 与 k 一定的条件下，分析 $k \geqslant m(1-\tau)$时攻击成功概率的影响因素 τ 与 m。

显而易见，当 m 一定且 $\tau = 0$ 时，攻击概率最小为 $Q=\frac{C_{e-m}^{k-m}}{C_e^k}$，$Q$ 随 τ 的增大而增大。针对 m 分析，取 $\tau = 0$，$Q=\frac{C_{e-m}^{k-m}}{C_e^k}=\prod_{i=1}^{m}\frac{k-i+1}{e-i+1}$，当 $m+\Delta m > m$ 时，$Q_{m+\Delta m}-Q_m=\frac{k-e}{e-(m+\Delta m)+1}\prod_{i=1}^{m}\frac{k-i+1}{e-i+1}<0$，因此 Q 与 m 呈负相关。

综上所述，当网络环境一定时，增加序列长度或减小序列验证容错率均可以使窃听攻击的成功率大大降低，针对窃听攻击有良好的防御能力。同时，合理的序列长度与容错率是保证安全性能的重要因素。

4.2　同步认证性能分析

同步过程中，客户端通过发送扩展序列进行同步请求，跳变服务器监听并捕获数据分组以解析认证。端信息扩展跳变同步成功率为

$$Q_s = p^{m(1-\tau)} \tag{11}$$

其中，p=$q_c q_v$ 为单个数据分组成功率，τ 为序列认证的容错率，m 为序列长度，q_c 为数据分组成功捕获的概率，q_v 为扩展序列中单个端信息认证成功率。

q_c 为数据分组成功捕获的概率，指客户端将端信息封装在数据分组中发送，经过网络传输被服务器监听进程成功捕获的概率。受网络传输过程中分组丢失率的影响，数据分组捕获过程存在不确定性，分组丢失率越低，成功捕获的概率越高。

q_v 为扩展序列中单个端信息认证成功率，包括数据分组中目的地址与目的端口的认证。根据地址认证算法及端口校验算法可知，认证成功率与地址池、密钥及算法效率有关。因此，算法效率是影响数据分组认证的关键因素，时间效率的提高可降低序列认证超时导致的同步失败率。

针对跳变同步成功率分析，当 $m(1-\tau)$一定时，Q_s 与单个数据分组认证成功率 p 呈正相关。在单个数据分组认证成功率 $p(0<p\leqslant 1)$一定的情况下，序列长度 m 越小，Q_s 越高；容错率 τ 越大，Q_s 越高。但 m 的减小与 τ 的增大会造成安全性能的降低，因此提高同步认证性能的关键是提高单个数据分组认证的成功率。

综上所述，端信息扩展跳变同步策略与数据分组认证、扩展序列验证等相关，与跳变时隙、跳变算法等无关，跳扩混合服务器能够有效地避免跳变性能对同步认证的影响，实现跳变策略与同步策略的分离，解决跳变时隙较小的高速跳变同步问题。

4.3　时间性能分析

在端信息跳变技术中没有使用数据迁移策略的时候，假设用户与服务器一次握手的时间为 T_1，一次长久的服务需要握手 n 次，跳变周期为 T_s，那么在没有数据迁移策略的前提下所需要的时间 T_n 为

$$T_n = (T_1 + T_s)n \tag{12}$$

数据迁移策略是为解决 TCP 三次握手时间损耗问题而提出的，使同一个合法用户在一次长时间的服务请求中仅与服务器端握手一次，但需要 IP 地址

的转换，假设中间转换器的时间损耗为 T_2，那么在使用数据迁移策略的前提下所需要的时间 T_y 为

$$T_y = (T_2 + T_s)n + T_1 \tag{13}$$

由于 IP 地址的转换操作是在服务器的内核之中操作的，所以 IP 地址的转换时间远远小于 TCP 三次握手的时间，可以忽略不计，这样其实真正的 T_y 为

$$T_y = T_s n + T_1 \tag{14}$$

由式(12)和式(14)比较可知，当服务在一次跳变周期内完成时，T_y=T_n，当一次服务在一个跳变周期内未完成时，$T_y < T_n$。因此，在引入数据迁移策略的时候可大大提高端信息跳扩混合主动网络防御技术的效率，减少长久服务的时间损耗。

综上所述，基于端信息跳扩混合的主动网络防御技术在引入数据迁移策略之后，可以很好地解决时间损耗问题，提高长久服务的服务效率。

5 实验测试与分析

本文设计实现了端信息跳扩混合主动网络防御技术原型系统，并进行同步性能、安全性能及服务性能的实验验证，客户端与服务器配置如表 1 所示。

表 1 实验系统配置

主机	内存/GB	操作系统	内核版本	工作方式
客户机	4	Ubuntu14.04	Intel Core i5	端信息扩展客户端
服务器	8	Ubuntu16.04	Intel Core i7	跳扩混合服务器

5.1 安全性能测试

针对 TCP 跳变服务特性，设计最有利于攻击者的攻击情景，在内网环境下进行拒绝服务及窃听攻击实验，测试系统的抗攻击性能。

5.1.1 可用性能测试

实验过程中，假设攻击者已知全部服务的跳变地址池，因此 SYN-flood 攻击的目标地址和端口是在跳变地址池中选取服务器的跳变地址及随机选取端口号，设定服务器为不同的跳变速率，在不同的跳变速率下发起速率为 10 Mbit/s、20 Mbit/s、30 Mbit/s、40 Mbit/s 和 50 Mbit/s 的攻击，在相应攻击速率下静态服务测得平均响应时间分别为 1 667 μs、1 791 μs、1 906 μs、2 353 μs 和 3 081 μs。在攻击的同时客户端向服务器发起 100 次同步认证请求，分别记录未受攻击与不同攻击速率下 TCP 跳变服务的响应时间，计算不同跳变速率不同攻击速率下的服务平均响应时间。

实验数据拟合结果如图 4 所示，图中 HOP-1、HOP-10、HOP-100 分别表示 1 hop/s、10 hop/s、100 hop/s，拟合曲线分别用实线、虚线和点划线表示，其中 HOP-1 和 HOP-10 属于低速跳变范围，HOP-100 属于高速跳变范围。由实验结果可以看出，随着攻击速率的增大，3 种跳变速度下的服务响应时间均无明显增大，总体平均响应时间稳定在 1 800 μs 左右，而静态服务响应时间浮动明显，均值约为 2 150 μs。由此证明了端信息跳扩混合主动网络防御技术能够有效地抵抗 SYN-Flood 攻击，保证 TCP 服务的安全性。同时在高速跳变下仍能够抵抗攻击并保持服务响应。

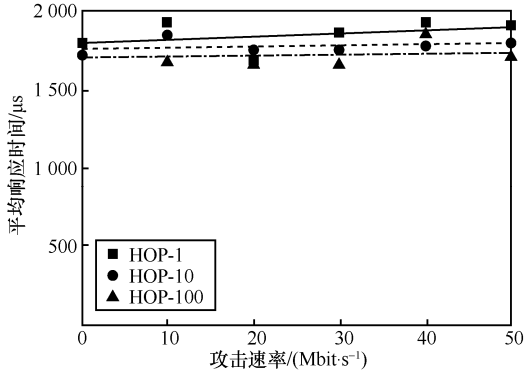


图 4 SYN-Flood 攻击下服务响应时间

本文进一步测试了 ACK Flood 攻击、NTP DoS 攻击下系统性能。表 2 给出了端信息跳扩混合模型在 SYN Flood、ACK Flood、NTP DoS 这 3 种拒绝服务攻击（攻击速率为 50 Mbit/s，跳变速度为 100 hop/s，传输数据为 20 KB 电子表格文档）下，客户端从发起请求到接受服务所需的平均服务响应时间。从表 2 可以看出，在不同的拒绝服务攻击类型下，端信息跳扩混合主动网络防御技术也可以正常提供对外服务，能很好地抵御拒绝服务攻击。

表 2 不同攻击方式下的服务完成时间

拒绝服务攻击类型	服务完成时间/ms
SYN Flood	1.803
ACK Flood	1.750
NTP DoS	1.739

综上所述，基于端信息跳扩混合的主动网络防御技术在实现高速跳变的同时，保证了良好的抗攻

击性能。

5.1.2　隐蔽性能测试

隐蔽性实验同样遵循了最有利于攻击者的设置，服务器、客户机和攻击者均在同一个共享式局域网中，端信息跳变或跳扩混合只在服务端进行，客户端与服务端进行一对一通信，攻击者使用 SnifferV4.7.5 进行截获分析。

实验首先测试比较了在 T=60 s 时间周期内传统服务与端信息跳变服务的数据传输截获分析结果，如图 5(a)和图 5(b)所示；随后进一步截获分析了 T=1 s时间周期内的跳变服务与跳扩混合服务如图 5(c)和图 5(d)所示。其中，实线为真实通信数据，虚线则是扩展序列的虚假数据。

图 5 中明显可以看出，当截获分析攻击时间为 60 s 时，端信息跳变服务与传统服务相比有明显的隐蔽性优势，数据传输流量有明显发散，增大了攻击者分析的难度；但当攻击时间降低为 1 s 时，低速跳变的跳变服务的跳变图案完全显式暴露在敌手面前，因此失去了隐蔽性增益，而高速跳变的跳扩混合服务的跳变图案杂乱无章且包括虚假的端信息扩展序列，仍然能够保持高隐蔽性。可见，端信息低速跳变难以有效地应对性能日益提升的截获攻击。端信息跳扩混合策略由于采用了每秒上百跳的高速跳变和扩展序列同步，因而具有更好的隐蔽性能。

5.2　同步性能测试

系统同步性能主要涉及跳变速度对同步认证的影响。为证明对高速跳变的适用性，选取不同跳变速度，根据跳变算法进行随机跳变，分别记录不同跳变速度下 200 次同步请求的平均服务响应时间与平均序列认证时间，实验结果如图 6 所示。

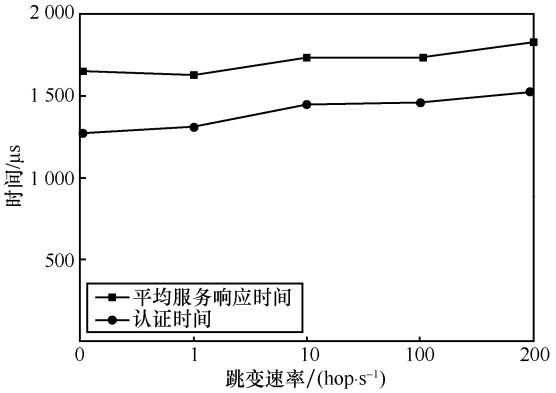
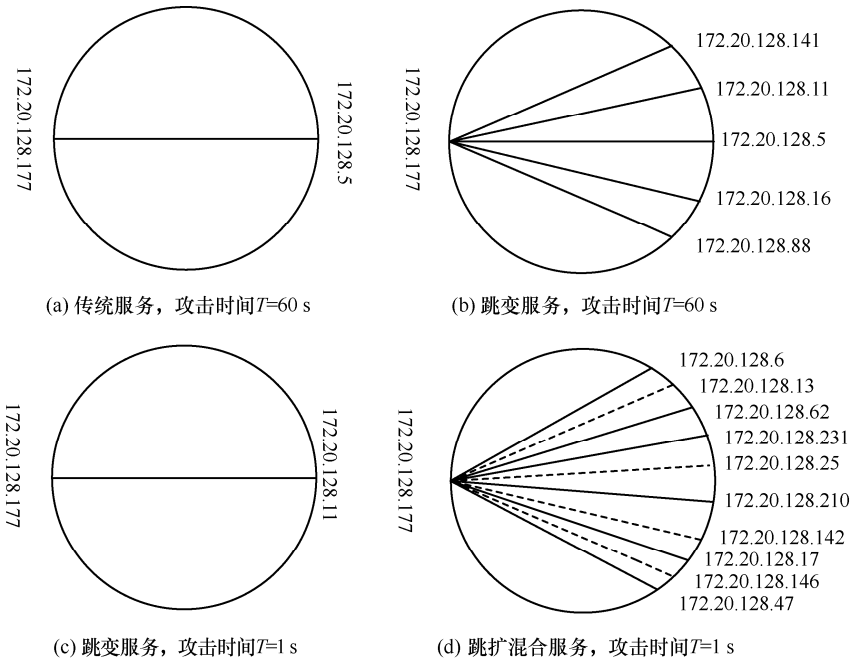


图 6　同步性能实验结果

实验结果表明，随着跳变速率的增加，平均响应时间整体呈现缓慢的上升趋势，并没有因跳变速率的增加而显著提高。在 200 hop/s 的高速跳变下，服务器仍能进行服务响应，验证了端信息扩展同步策略和数据迁移策略可以保证端信息跳扩混合主动网络防御技术的高速跳变和正常运行。



(a) 传统服务，攻击时间T=60 s　　(b) 跳变服务，攻击时间T=60 s

(c) 跳变服务，攻击时间T=1 s　　(d) 跳扩混合服务，攻击时间T=1 s

图 5　不同攻击时间下截获攻击结果

5.3 服务性能测试

端信息跳变技术的服务性能主要涉及跳变速率，与跳频通信技术类似，跳变速率是影响端信息跳变服务性能的重要因素，但该模型解决了跳变速率对服务性能的影响，表 3 为端信息跳变模型与端信息跳扩混合模型在不同跳变速率下的服务提供率对比，其中服务提供率反映客户端能够获取服务器端所提供服务的成功率。

表 3 服务提供率对比

跳变速率/(hop·s^{-1})	端信息跳变模型	端信息跳扩混合模型
1	95%	78%
2	78%	77%
10	16%	69%
100	0	75%
200	0	73%

从表 3 可以得出端信息跳变模型会随着跳变速率的提高降低服务提供率，在达到高速跳变速率 200 hop/s 时，服务提供率为 0；端信息跳扩混合模型随着跳变速率的提高基本没有变化，即使是在高速跳变速率 200 hop/s 的情况下也能提供对外服务，解决了端信息跳变防护中的跳变速率受限问题，具有较好的服务性能。

6 结束语

主动网络防护技术近年来引起了产业界和学术界的关注，其核心思想是依据任务需求，动态、随机地进行服务、IP 地址、端口等端信息的变化，从而提高网络攻击的难度。

针对端信息跳变防护中的跳变速率受限的问题，受扩频通信技术和跳扩混合通信技术的启发，提出了端信息扩展的概念，进而提出一种基于端信息跳扩混合的主动网络防御技术，将跳变策略和同步认证机制有效分离，避免了同步机制对于高速跳变性能的限制。在此基础上，建立了端信息跳扩混合主动网络防御模型，解决了端信息高速跳变下的难题，实现了不需要真实目标端信息的跳变服务请求。理论分析和实验结果均表明，端信息跳扩混合主动网络防御模型能够在高速端信息跳变下有效地完成可信客户端的同步认证，支持端信息跳变图案的高度隐蔽性，具有很好的抗攻击效果，对于高强度对抗要求的主动网络防护应用具有重要意义。

参考文献：

[1] 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, LU S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2): 106-110.

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

[3] LAKSHMINARAYANA S, YAU D K Y. Cost-benefit analysis of moving-target defense in power grids[C]//Annual IEEE/IFIP International Conference on Dependable Systems and Networks. IEEE, 2018: 139-150.

[4] VENKATESAN S, ALBANESE M, AMIN K, et al. A moving target defense approach to mitigate DDoS attacks against proxy-based architectures[C]// Communications and Network Security. IEEE, 2017:198-206.

[5] ZEITZ K, CANTRELL M, MARCHANY R, et al. Designing a micro-moving target IPV6 defense for the Internet of things[C]// IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation. IEEE/ACM, 2017:179-184.

[6] HU H, WU J, WANG Z, et al. Mimic defense: a designed-in cybersecurity defense framework[J]. IET Information Security, 2017, 12(3): 226-237.

[7] 斯雪明, 王伟, 曾俊杰,等. 拟态防御基础理论研究综述[J]. 中国工程科学, 2016, 18(6):62-68.
SI X M, WANG W, ZENG J J. A review of the basic theory of mimic defense[J]. Engineering Sciences, 2016, 18(6):62-68.

[8] 仝青,张铮,张为华,等.拟态防御 Web 服务器设计与实现[J].软件学报, 2017, 28(4): 883-897.
TONG Q, ZHANG Z, ZHANG W H, et al. Design and implementation of mimic defense web server[J]. Journal of Software, 2017, 28(4): 883-897.

[9] 谢慧, 张志刚, 聂峰. 跳端口在安全 P2P 即时通信系统中的应用[J]. 武汉理工大学学报(信息与管理工程版), 2011, 33(1):18-21.
XIE H, ZHANG Z G, NIE F. Application and implementation of port hopping in secure P2P Msystem[J]. Journal of WUT(Information & Management Engineering), 2011, 33(1):18-21.

[10] 张连成, 魏强, 唐秀存,等. 基于路径与端址跳变的 SDN 网络主动防御技术[J]. 计算机研究与发展, 2017, 54(12):2748-2758.
ZHANG L C, WEI Q, TANG X C. Path and port address hopping based sdn proactive defense technology[J]. Journal of Computer Research and Development, 2017, 54(12):2748-2758.

[11] 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.
LIU H S, WANG Z X, GUO Y. An IPV6 proactive network defense model based on multi-homing hopping[J]. Journal of Electronics & Information Technology, 2012, 34(7):1715-1720.

[12] 周余阳,程光,郭春生,等.移动目标防御的攻击面动态转移技术研究综述[J].软件学报,2018,29(9):2799-2820.
ZHOU Y Y, CHENG G, GUO C S, et al. Survey on attack surface dynamic transfer technology based on moving target defense[J]. Journal on Software, 2018, 29(9): 2799-2820.

[13] LIN K, JIA C. Distributed timestamp synchronization for end hopping[J]. China Communications, 2011, 8(4):164-169.

[14] 林楷, 贾春福, 石乐义. 分布式时间戳同步技术的改进[J]. 通信学

报, 2012 33(10):110-116.
LIN K, JIA C F, SHI L Y. Improvement of distributed timestamp synchronization[J]. Journal on Communications, 2012, 33(10):110-116.

[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] LUO Y, WANG B, WANG X, et al. RPAH: random port and address hopping for thwarting internal and external adversaries[C]// IEEE Trustcom/Bigdatase/Ispa. IEEE, 2015.

[17] LUO Y, WANG B, WANG X. A keyed-hashing based self- synchronization mechanism for port address hopping communication[J]. Frontiers of Information Technology & Electronic Engineering, 2017, 18(5): 719-728.

[18] ZHAO Z , GONG D , LU B , et al. SDN-based double hopping communication against sniffer attack[J]. Mathematical Problems in Engineering, 2016(2):1-13.

[19] 孙慧. 基于端信息跳变的网络音视频通信系统研究与设计[D]. 青岛: 中国石油大学（华东）, 2018.
SUN H. Research and design of network audio and video communication system based on end hopping[D]. Qingdao: China University of Petroleum (East China), 2018.

[20] 范晓诗, 李成海, 王昊. 基于可变时隙与动态同步的端口跳变技术研究[J]. 计算机工程与设计, 2013, 34(10):3465-3469.
FAN X S, LI C H, WANG H. Research port hopping technology on variable slot and dynamic time synchronization[J]. Computer Engineering and Design, 2013, 34(10):3465-3469.

[21] 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 & Information Technology, 2015, 37(11):2642-2649

[22] 赵春蕾. 端信息跳变系统自适应策略研究[D]. 天津: 南开大学, 2012.
ZHAO C L. Research on adaptive strategies for end-hopping system[D]. Tianjin: Nankai University, 2012.

[23] KUMAR D, DHYANI P, SHARMA A K. Migration of data from one cloud server to another cloud server using the TCP-IP protocol[J]. International Journal of Computer Applications, 2017, 157(4): 27-31.

[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。

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、网络对抗。

温晓（1992– ），女，山东聊城人，中国石油大学（华东）硕士生，主要研究方向为网络安全、网络对抗。

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。

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。

马猛飞（1993– ），男，河南禹州人，中国石油大学（华东）硕士生，主要研究方向为网络安全、网络对抗。

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。