计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200420
57(11): 2283-2293, 2020

基于端信息跳扩混合的文件隐蔽传输策略

侯博文　郭宏彬　石乐义
(中国石油大学(华东)计算机科学与技术学院　山东青岛　266580)
(78149170@qq.com)

File Covert Transfer Strategy Based on End Hopping and Spreading

Hou Bowen, Guo Hongbin, and Shi Leyi
(*College of Computer Science and Technology, China University of Petroleum, Qingdao, Shandong* 266580)

Abstract　The end hopping and spreading technology is an active defense technology that pseudorandom changes the end information in the end to end data transmission and uses the end spreading sequence to realize high-speed synchronous authentication. In this paper, the end hopping and spreading technology is introduced into file covert transfer, the file covert transmission strategy under the end hopping and spreading network is studied, the multicast time correction scheme is proposed, and the synchronization problem in communication process is solved. Two kinds of file transfer schemes based on time transfer and transmission size transfer are proposed for the end hopping and spreading network, and the data migration is added into the file transfer process to realize the covert transmission and integrity transmission of files. A prototype system is designed and implemented for the file covert transfer of end hopping and spreading, and the usability and security are tested. The experimental results show that the file covert transfer strategy can effectively meet the requirements for the integrity and concealment of file transfer.

Key words　covert communication; end hopping and spreading; file transfer; multicast time correction; data migration

摘　要　端信息跳扩混合技术是一种在端到端的网络数据传输中伪随机改变端信息,并利用端信息扩展序列实现高速同步认证的主动防御技术.将端信息跳扩混合技术引入文件隐蔽传输,研究了端信息跳扩混合网络环境下的文件隐蔽传输策略,提出组播时间校正方案,解决了通信过程中的同步问题;提出基于时间传输和基于传输大小传输的2种适用于端信息跳扩混合网络环境文件传输方案,并在文件传输过程中增加数据迁移技术,实现文件的隐蔽传输和完整性传输;设计实现端信息跳扩混合文件隐蔽传输原型系统并进行了有效性、安全性测试,实验结果表明:该文件隐蔽传输策略能够有效满足文件传输完整性和隐蔽性要求.

关键词　隐蔽通信;端信息跳扩混合;文件传输;组播时间校正;数据迁移

中图法分类号　TP393

收稿日期:2020-06-09;**修回日期**:2020-07-28

基金项目:国家自然科学基金项目(61772551);山东省自然科学基金项目(ZR2019MF034)
This work was supported by the National Natural Science Foundation of China (61772551) and the Natural Science Foundation of Shandong Province of China (ZR2019MF034).

通信作者:石乐义(shileyi@upc.edu.cn)

当今互联网已经与我们的生活紧紧联系在一起,任意形式的网络攻击都会使我们的生活受到影响,网络安全形势十分严峻.传统的网络防御技术包括防火墙技术、入侵检测、信息加密等,虽然可以提供一定程度的安全性,但是由于其静态和被动的特性,无法很好地应对自动化和多样化的网络攻击[1].

受军事跳频扩频通信启发,课题团队在2008年提出了端信息跳变[2](end hopping)概念,随后提出了端信息扩展[3](end spreading)概念,进而在端信息跳变和扩展技术的基础上了提出了端信息跳扩混合(end hopping end spreading)技术[4].

端信息跳变技术的灵感源于军事通信对抗中的跳频通信,通过动态地、随机地改变通信过程中的网络参数,如端口、IP地址、跳变算法等,来干扰迷惑外来攻击者,实现主动网络防护.端信息扩展技术则是受扩频通信思想启发而提出,客户端发送的数据信息是与真实信息含义无关的端信息序列组合,只有当所有的端信息扩展序列按照一定的规则组合在一起,才能表达客户端所发数据的真实含义.端信息跳扩混合技术是在端信息跳变技术基础上,利用端信息扩展序列进行同步认证的技术,实现跳变与同步的分离,该技术在保证安全性的同时又兼顾了跳变速率的高速性,具有更好的网络防御效果.

传统的文件传输策略大多利用数据加密方式进行隐蔽传输,如MD5加密、同态加密等,此类传输方式虽然便捷、简单、传输效率高,但均属于静态、被动的防护手段,安全性低、隐蔽性差.本文针对传统文件传输方式的问题,结合端信息跳扩混合技术,提出一种基于端信息跳扩混合的文件隐蔽传输策略,文件数据的传输依赖动态可变的端信息,实现文件的隐蔽性传输.

1 相关工作

2011年美国国家技术委员会提出了一种积极的网络防御技术——移动目标防御[5]技术,该技术主要目的是通过增加系统的随机性或降低系统的可预测性来防御攻击[6],使用不断变化的系统配置来扰乱攻击者的扫描探测,呈现给攻击者错误的系统信息,做到主动性的防御[7].在移动目标防御方面,谭晶磊等人[8]提出了一种基于Markov时间博弈的移动目标防御最优策略选取方法,利用时间博弈隐蔽对抗的特性构建MTD攻防模型,设计了最优策略选取算法.文献[9]通过MTD方法的实验研究,探讨了实证评价,利用网络杀戮链来表述攻击行为,识别出MTD方法成功阻止的攻击类型和无法阻止的攻击类型.

拟态安全防御(cyber mimic defense, CMD)由邬江兴院士在2014年提出,系统可以根据流量分析进行软硬件的自主切换,从而实现动态化、异构化的主动网络防御[10].文献[11]针对以太网交换机面临的未知漏洞和未知后门安全威胁,提出了一种基于拟态防御理论的交换机内生安全体系结构.设计实现了拟态交换机原型样机并进行了白盒插桩及攻击链安全性测试.文献[12]将拟态安全防御运用到云计算方面,提出了一种模拟云计算任务执行的科学工作流系统,有效增强云工作流执行的安全性.

端信息跳变技术[3]与移动目标防御技术、拟态安全防御技术均属于主动网络防御技术.文献[13]中从攻击面动态转移角度剖析了移动目标防御,并将端信息跳变技术划分为移动目标防御网络攻击面的动态转移技术.

在端信息跳变研究方面,文献[14]提出了基于消息篡改的端信息跳变技术,分别在用户空间、内核空间和网络空间对消息进行篡改,并建立跳变栈模型对其进行实验分析.林楷等人针对时间戳同步引起的大量时间戳请求的资源耗尽问题和边界丢失问题,提出了分布式时间戳同步(DTS)[15-16]策略,对时间戳同步进行了优化.文献[17]提出了一种基于Hash值的自同步方案,利用Hash算法生成的散列消息身份验证码作为端信息生成的关键字来进行同步认证,降低了网络延迟对同步的影响.文献[18]提出了端信息跳变技术中的时间自适应策略和空间自适应策略,根据网络状况动态地改变跳变间隙或跳变项范围的大小,增强端信息跳变技术的防御性.

在端信息跳变技术的应用场景方面,文献[19]提出一种基于SDN的双跳通信方法,通过同时改变通信双方端信息和路由路径来迷惑攻击者,通过增加攻击的开销和难度来防御攻击.张连成等人[20]提出基于路径与端址跳变的SDN网络主动防御技术,以较小的通信时延开销与计算开销实现通信双方端口与地址的随机跳变.

文件传输作为网络环境中重要的组成部分,文件传输的隐蔽性是个人信息保护的重要环节.将文件传输与端信息跳扩混合的主动网络防御技术相结合,可以实现文件的隐蔽传输,以动态、变化的思想推动现代主流业务的发展,保护网络通信中的个人隐私,具有重要的研究意义.

2 端信息跳扩混合的文件隐蔽传输策略

2.1 端信息跳扩混合的文件隐蔽传输系统

端信息跳扩混合的文件隐蔽传输系统是指在端信息跳扩混合的主动网络防御系统中实现文件的可靠性、完整性传输,来达到文件的隐蔽传输.图 1 为端信息跳扩混合的文件传输功能模块图.包括时间校正模块、扩展认证同步模块、数据迁移模块、端信息跳变模块以及文件传输模块.

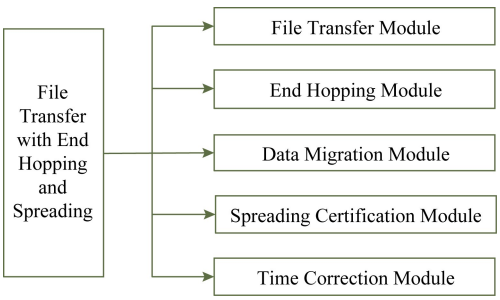


Fig. 1 End hopping and spreading file transfer function module

图 1 端信息跳扩混合的文件传输功能模块

时间校正模块主要是对时间进行校正,时间是系统之中实现同步的关键;在扩展认证同步模块中,利用端信息、时间等公共属性生成端信息认证序列实现身份认证;数据迁移模块主要实现文件数据的完整性传输,减少时间开销,提高服务效率;端信息跳变模块尽量保证端信息跳变的随机性、不可预测性;文件传输模块包括文件分片、文件重传、文件重组和文件传输策略等关键性技术.

根据端信息跳扩混合的文件传输功能模块,本文设计了基于端信息跳扩混合的文件隐蔽传输系统,如图 2 所示为该系统模型图.系统模型包括客户端和端信息跳扩混合的文件传输服务器,客户端主要包括扩展序列生成模块、文件传输服务获取模块、扩展序列发送模块;跳扩混合服务器端主要包括端信息跳变模块、扩展序列认证模块、文件传输服务提供模块.

客户端在请求文件传输服务之前,首先向 NTP 服务器发送时间校验请求以校正时间,随后生成端信息扩展序列,并发送给跳扩混合服务器,同时开启服务获取模块;跳扩混合服务器检测客户端发送的扩展序列.如果认证通过,跳扩混合服务器开启服务提供模块,与客户端建立连接并进行文件传输,否则,不提供服务.客户端在发送完端信息扩展序列后,文件传输服务获取模块启动,等待服务器认证通过后为其提供服务.

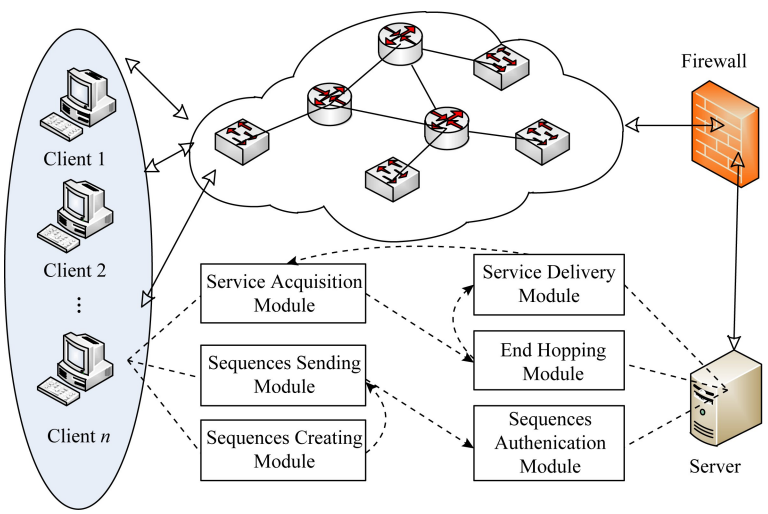


Fig. 2 File covert transfer model diagram based on end hopping and spreading

图 2 基于端信息跳扩混合的文件隐蔽传输模型图

2.2 关键技术

在基于端信息跳扩混合的文件隐蔽传输策略中,时间校正问题、文件传输方案、重组数据迁移问题和文件分片、重传与重组问题是需要重点解决的问题.时间校正问题是合法用户能够同步成功的基础,数据迁移问题关系到文件传输的可持续性,文件分片、重传和重组技术以及文件传输方案的选取可以保证文件内容的传输完整性和高效性.

2.2.1 时间校正方案

时间的准确性关系到通信双方能否完成同步,

本文提出一种组播时间校正方法进行时间校正.如图 3 所示为端信息跳扩混合的组播时间校正方案,可信客户端建立组播群,每隔一段时间通信客户端运行自身带有的组播服务器程序,将组播请求报文以组播服务器的身份发送给组播网络中的组播客户端,之后组播客户端向组播服务器(端信息跳扩混合网络中的客户端)发送时间信息应答报文,组播服务器获得网络延迟,并接收组播应答报文,通过筛选过滤和时间校正算法对时间进行校正.该方法的应用降低了时间漂移对端信息扩展同步认证和端信息跳变的影响,且无需第三方参与.

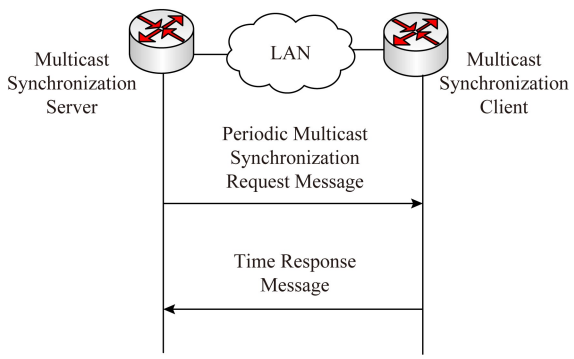


Fig. 3 Multicast time correction scheme for end hopping and spreading

图 3 端信息跳扩混合的组播时间校正方案

2.2.2 文件分片、重传与重组技术

如果以传统的文件传输策略传输文件,那么端信息的高速跳变就会为文件传输系统带来大量的 TCP 三次握手,对时间的损耗过大.因此发送方需要利用分片技术对大文件进行分片处理,生成小的文件片段,文件分片技术需要记录文件的断点位置、文件标识符、文件分片总数和文件片段 ID 号.记录断点位置是方便发送方在接收方端信息跳变之后可以更加便捷地找到所需传输的文件片段;文件标识符代表文件的唯一标识,以便之后进行文件的重组;文件分片总数用于检查文件的完整性传输;文件片段 ID 号可用于文件重传和文件重组.

发送方如果无法在一次跳变间隙内完成文件的所有片段传输,接收方进行了端信息跳变,在改变端信息之后记录断点位置,利用数据迁移技术将文件片段进行连接迁移,继续完成数据片段的传输工作,文件片段完全传输后,接收方要执行文件重组操作,重组完成即完成文件传输.图 4 为端信息跳扩混合的文件分片传输、重组示意图.文件重传、重组技术能够保证传输文件内容的完整性,这对于文件传输系统是至关重要的;文件分片技术能够有效减少时间的损耗,提高文件传输的效率.

2.2.3 文件传输方案

利用文件分片技术得到的文件片段需要通过特定的文件传输方案进行文件片段的传输,结合端信息跳扩混合技术,本文提出 2 种文件传输方案:基于时间的文件传输方案和基于传输大小的文件传输方案.

基于时间的文件传输方案流程为:

1) 客户端与服务器建立 TCP 连接,由于不能确定该建立连接的跳变间隙还剩多少,规定该跳变间隙之内不进行文件片段的传输,避免出现文件片段传输未完成的情况.

2) 跳扩混合服务器从下一跳端信息开始进行文件片段的传输,通过跳变算法、文件大小、网络流量等情况计算一跳固定传输片段数,在一个跳变间隙内始终传输该固定片段数.

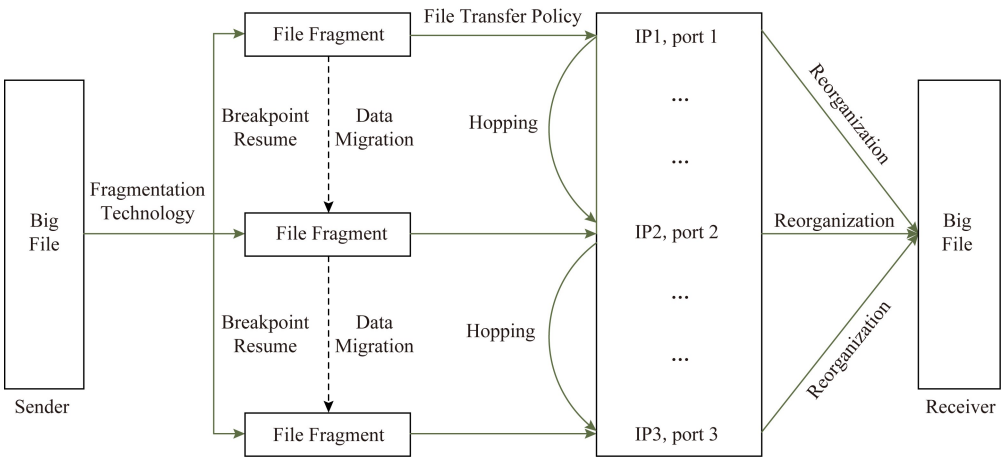


Fig. 4 End hopping and spreading file sharding transfer and reorganization

图 4 端信息跳扩混合文件分片传输、重组

3) 在完成规定的固定文件片段数传输之后,记录断点位置,在下一跳端信息的时候从断点位置继续进行文件片段的传输,循环该步骤,直到文件全部传输完成.

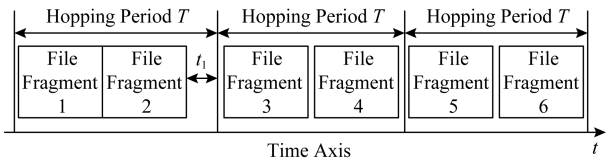


Fig. 5 Time-based file transfer scheme

图 5 基于时间的文件传输方案

如图 5 所示为基于时间的文件传输方案图,服务器每次的跳变周期均为 T,在该固定跳变周期内传输了固定大小的文件片段,即使在文件数据全部传输完成时也不会继续进行文件片段的传输,而是等到下一跳变周期时再开始文件片段的传输.考虑到网络延迟等情况的出现,必须在一个跳变周期内留出空余的时间,保证在网络不畅通的情况下也能完成数据量的全部传输,图 5 中所示的时间 t_1 为服务器留下的空余时间.该方案从跳变间隙出发考虑,将时间作为文件传输的标准,同步时的跳变策略与文件传输时的跳变策略相同,不需要额外的算法开销.但是该方案也存在缺陷:由于网络状况无法完全预测,网络延迟随时可能出现,网络阻塞可能导致大量文件片段的丢失.

针对上述方案的缺陷,提出了基于传输大小的文件传输方案,流程为:

1) 客户端与服务器建立 TCP 连接.

2) 跳变算法由基于时间的跳变算法转换为基于传输大小的跳度算法,每次传输到一定大小的数据量,即端信息的跳变不再依赖时间的变化,以传输数据量为标准来判断是否进入下一跳.

3) 在完成所传输的文件片段之后,记录断点位置,进行端信息的跳变,跳变后从断点位置继续进行文件片段的传输,循环该步骤,直到文件全部传输完成.

如图 6 所示为基于传输大小的文件传输方案图,端信息的跳变周期分别为 T_1,T_2,T_3,且 $T_1 \neq T_2 \neq T_3$,跳变周期是不固定的,而每次跳变间隙内的时间片段大小和数量都是固定的,即每次跳变周期内传输的数据量是固定的,传输完规定的数据量之后服务器进行端信息跳变.因此,该方案的跳变间隙不再依赖于时间,是以数据传输大小作为跳变标准,进行端信息跳扩混合的文件传输.将同步时的跳变策略与文件传输时的跳变策略分割开来,提高了文件传输效率.

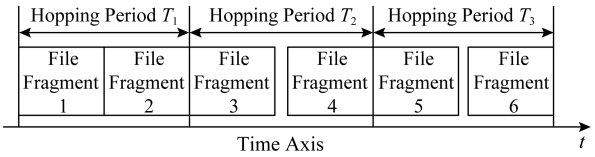


Fig. 6 Size-based file transfer scheme

图 6 基于传输大小的文件传输方案

2.2.4 数据迁移技术

为了使端信息跳扩混合的文件传输服务器能够进行文件的持续传输,本文将数据迁移技术[21]应用到端信息跳扩混合的主动网络环境中.如图 7 所示为数据迁移模型图.

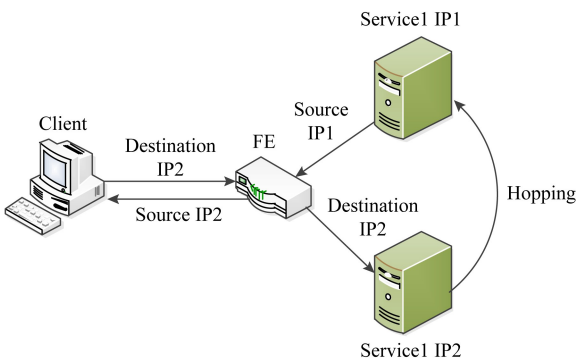


Fig. 7 Data migration model

图 7 数据迁移模型

数据迁移模型中包括客户端和端信息跳扩混合的文件传输服务器,端信息跳扩混合的文件传输服务器又包含调度器 FE 和其中的相关服务(如图 7 中的服务 1),其具体流程为:

1) 假如时刻 T_1 的文件传输服务在 IP2 上提供,那么客户端在通过端信息扩展认证后会与 IP2 进行 TCP 三次握手建立连接,此时传输的数据包中目的地址是 IP2.

2) 在时刻 T_2 端信息跳扩混合的文件传输服务器进行了端信息跳变,服务地址变成 IP1,这时在客户端不知道的情况下,客户端依然会向 IP2 请求文件服务,请求数据包的目的地址为 IP2.

3) 请求数据包到达服务器端后,服务器将请求数据包经由调度器 FE 修改目的地址为 IP1,然后将该数据包交给端信息跳扩混合的文件传输服务.

4) 端信息跳扩混合的文件传输服务接收到修改后的请求数据包后继续为客户端提供服务,首先

将应答包发送给前置 FE,此时发送的应答包源地址为 IP1.

5) 前置 FE 收到服务器应答包后,修改源地址 IP1 成为 IP2,然后将应答包以 IP2 的身份发送给客户端.

6) 之后周期性地重复第 2 步到第 5 步直到文件传输完成.

将数据迁移技术应用到端信息跳扩混合的文件隐蔽传输策略中,可以消除跳扩混合服务器在文件传输过程中的 3 次握手时间消耗,提高文件传输效率.

2.3 传输流程

图 8 为基于端信息跳扩混合的文件隐蔽传输流程图,具体流程为:

① 控制台向 NTP 服务器发送时间请求信息,对自身时间信息进行校正,保证时间准确.

② 控制台利用校准过的时间信息计算服务器端信息,将该端信息作为对外服务的主机信息,开启对外服务.

③ 控制台在开启新的服务器之后,通知旧的服务器关闭对外服务.

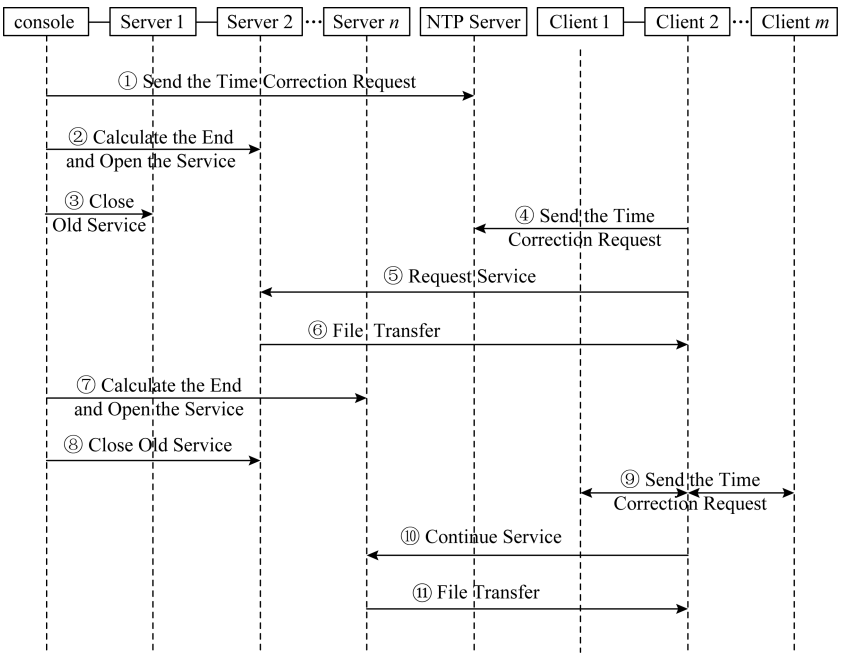


Fig. 8 File covert transfer strategy flow based on end hopping and spreading

图 8 基于端信息跳扩混合的文件隐蔽传输策略流程

④ 客户端在请求服务前,首先向 NTP 服务器发送时间请求信息进行时间校正,此时利用的是 NTP 时钟同步.

⑤ 客户端使用自身校正过的时间信息计算此刻对外提供服务的服务器端信息,进行端信息扩展认证并向该服务器请求文件传输服务.

⑥ 在通信双方建立连接之后,服务器向客户端发送文件片段进行文件传输.

⑦ 在将规定数量的文件片段传输完成之后,控制台控制服务器进行跳变,利用自身时间信息重新计算服务器端信息,并开启相应服务器.

⑧ 控制台关闭旧的服务.

⑨ 客户端在服务器跳变之后也需要重新计算服务器端信息,此时进行时间判断,如果距离上次时间校正时间超过 t,该客户端会向组播网络中发送组播请求信息进行时间校正,否则,直接转步骤⑩.此步骤中利用的是组播时间校正.

⑩ 客户端利用自身端信息重新计算服务器端信息.

⑪ 继续进行文件传输,之后重复步骤⑦~⑪,直到文件传输完成.

在整个基于端信息跳扩混合的文件隐蔽传输过程中,用到了 NTP 时间校正和组播时间校正 2 种方法,这样既保证了时间的高准确性,又减少了对 NTP 服务器的访问量.

3 性能分析

3.1 安全性分析

1) 抵抗拒绝服务攻击.假设攻击者已经掌握了

服务器端信息跳变地址池和端口跳变范围,然后对跳扩混合服务器进行拒绝服务攻击.在某一时刻,服务器端仅有一对地址、端口组合处于活动状态,那么此种情况下攻击者攻击成功所需要的时间 T' 为

$$T'=\left(\sum_{i=1}^{N-1} i\ \frac{C_{N-1}^{i}}{C_{N}^{i}C_{N-1}^{1}}+1\right)T, \tag{1}$$

其中的 $N=mn$,m 代表 IP 地址池中的 IP 地址个数,n 代表端口变化范围,T 代表的是传统网络环境下攻击者从发起攻击到击中目标所耗费的时间.可以看出,在端信息跳扩混合的网络环境下,攻击者击中目标的时间明显增大,而且随着 N 的增大,T' 也会随之增大.因此,证明了本文设计的模型可以增加攻击者的攻击代价,达到网络防御的效果.

2) 抵抗重放攻击和中间人攻击.首先,在端信息扩展认证模块中,端信息扩展认证序列的生成不仅与时间有关,而且是随时间变化的、动态的,攻击者对数据包的任意修改都将导致身份认证的失败.另外,由于端信息跳扩混合技术实现了端信息的高速跳变,攻击者在截获到合法用户的认证信息时,必然损耗一定的时间,该时间的损耗也会导致攻击者身份认证的失败.所以,攻击者无法利用重放攻击或中间人攻击对端信息跳扩混合的文件传输系统进行攻击.

3.2 时间性能分析

假如端信息跳扩混合服务器在每次跳变后需要重新建立连接,那么该情况下所需要的文件传输时间 T_{f} 为

$$T_{\mathrm{f}}=T_{1}\times d+T_{\mathrm{s}}+T_{\mathrm{h}}, \tag{2}$$

其中,T_1 表示客户端与跳扩混合服务器建立连接所需要的时间,d 表示文件传输过程中经历的跳变周期数,T_{s} 表示传统网络环境下文件传输时间,T_{h} 表示跳扩混合服务器端信息跳变过程中损耗的时间,该参数仅与 d 大小有关.

假如端信息跳扩混合服务器中应用数据迁移技术,所需要的文件传输时间 T_{y} 为

$$T_{\mathrm{y}}=T_{1}+T_{\mathrm{s}}+T_{\mathrm{h}}+T_{2}\times d, \tag{3}$$

其中,T_2 表示调度器 FE 对报文进行修改所耗费的时间.引入数据迁移技术后,跳扩混合服务器与客户端进行文件传输时只进行一次 TCP 连接,减少了 TCP 连接次数.

T_1 是在网络通信中的操作时间,T_2 是在系统内核中的操作时间,系统内核的运行速度要快得多,所以 T_2 几乎可以忽略不计.因此,在文件大小和每次跳变传输数据量相同的情况下,T_{y} 又可表示为

$$T_{\mathrm{y}}=T_{1}+T_{\mathrm{s}}+T_{\mathrm{h}}. \tag{4}$$

将式(2)、式(4)比较可知,在文件传输周期数较多时,即传输较大文件时,应用数据迁移技术的端信息跳扩混合文件传输系统传输效率要高于无数据迁移技术的跳扩混合文件传输系统.

4 系统测试

本节对端信息跳扩混合的文件传输系统原型进行了实现和相关测试.文件传输要求系统安全、高效、完整,数据不可缺失.UDP 是基于无连接的传输协议,是不可靠的,虽然效率高,但存在丢包现象,适应于对数据完整性要求不高的传输.TCP 是面向连接的传输协议,虽然过程比较复杂,但是可以保证数据的完整性传输,适用于大文件传输.综合考虑,本文采用 TCP 实现端信息跳扩混合的文件传输系统的构建.

4.1 系统功能测试

本节内容主要包括 2 部分:1)通过时间偏移的测试证明组播时间校正方法的有效性;2)通过文件传输时间的测试证明本文提出的 2 种基于端信息跳扩混合的文件传输方案的可行性.如表 1 所示为实验所需的系统参数配置表.

Table 1 System Parameter Configuration

表 1 系统参数配置

Host	RAM/GB	OS	CPU	BW/Mbps
Host A	4	Ubuntu	Intel® Core™ i5-4170	1 000
Host B_1	4	Ubuntu	Intel® Core™ i5-4170	1 000
Host B_2	4	Ubuntu	Intel® Core™ i5-4170	1 000
Host B_3	4	Ubuntu	Intel® Core™ i5-4170	1 000
Host B_4	4	Ubuntu	Intel® Core™ i7-6700	1 000

在本实验中,主机 A 作为端信息跳扩混合文件传输服务器,进行端信息高速跳变,跳变速率为 100 跳/秒.主机 B_1 作为客户端,向主机 A 请求文件下载服务.主机 B_2,B_3,B_4 和主机 B_1 组成组播网络,对主机 B_1 的时间信息进行组播时间校正.

图 9 为端信息跳扩混合的文件传输组播时间校正模型图.NTP 服务器与组播网络中的客户端和文件传输服务器进行精准时钟同步,NTP 服务器与端信息跳扩混合的文件传输服务器每隔一段时间进行一次校正,而与组播网络中的客户端在与端信息跳扩混合的文件传输服务器进行交互之前进行一次 NTP 时间同步.这样既能保证端信息跳扩混合的文件传输

服务器在时间上随时保持高度精准,又能保证组播网络中的各个客户端在加入组播网络时时间差距不大.组播网络中的各个客户端之间会进行组播时间校正.

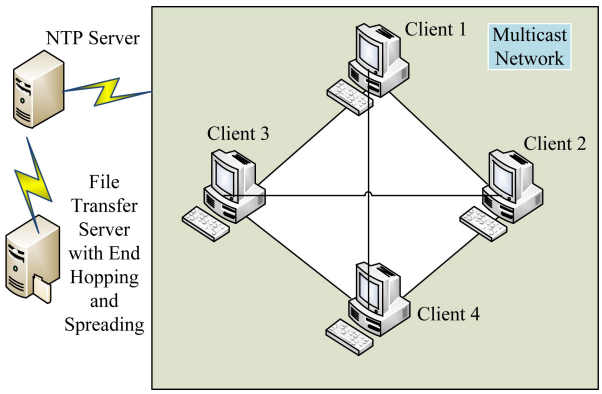


Fig. 9 File transfer time correction for end hopping and spreading

图 9 端信息跳扩混合的文件传输时间校正模型

4.1.1 时间偏移

本实验对无时间校正和组播时间校正 2 种方案做了比较,组播网络每 5 min 校正一次,无时间校正方案不进行时间校正.实验中,无时间校正方案和组播校正方案均每 15 min 记录一次,总时间为 1 h,时间偏移单位为 ms,图 10 为 2 种方案下的时间偏移量.

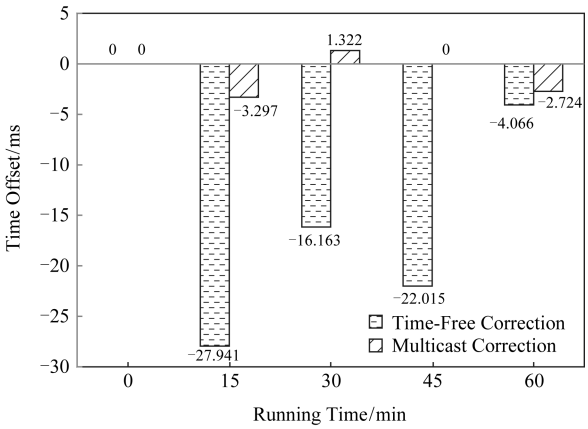


Fig. 10 Time offset

图 10 时间偏移量

通过图 10 可以看出,在第 1 次(0 时刻)时间校验的时候,2 种方案时间偏移近似为零,这是客户端与 NTP 服务器进行了时间校正,所以该时刻的时间偏移量可近似为 0.之后,无时间校正方案的时间开始上下漂移,漂移量较大,但时间偏移量却不是稳定上升的.相比于无时间校正方案,组播时间校正方案时间偏移量普遍较小.因此,证明了组播时间校正方案能较好地降低时间漂移的影响.

4.1.2 文件传输功能

端信息扩展中,系统会选择第一跳变策略,关闭所有端口.服务器对流经本地的数据包进行抓包分析,利用端信息扩展认证算法对端信息序列进行消息认证,对符合端信息扩展认证的合法用户根据算法打开相应端口,该端口作为通信双方建立连接的端口,客户端通过该端口请求文件传输服务;文件传输中,系统会自主选择第 2 跳变策略,如果在一次跳变间隙中无法完成文件传输,系统进行端信息跳变,改变端信息,这时通信双方不会断开连接,服务器端利用数据迁移策略将服务迁移,客户端在透明的情况之下继续文件的下载直到结束.

本实验对普通网络环境之下基于 TCP 协议的传统文件传输、端信息跳扩混合环境之下基于 TCP 协议的传统文件传输、基于时间的文件传输方案、基于传输大小的文件传输方案 4 种方案做了比较.如图 11 所示为实验所得的不同方案下的文件传输时间比较,其中,文件传输格式是 zip 压缩包格式,分片的文件片段大小选择了 0.5 KB.另外,在基于传输大小的文件传输方案中,文件片段数选择 200 片/跳.端信息跳扩混合网络环境中基于 TCP 的传统文件传输方案在文件大小选择 0.02 MB 时,可以完成文件的传输,剩余的 5 种文件由于文件无法重组,未能完成文件的完整性传输.因此,传统的文件传输方案无法实现端信息跳扩混合网络环境下的文件传输.

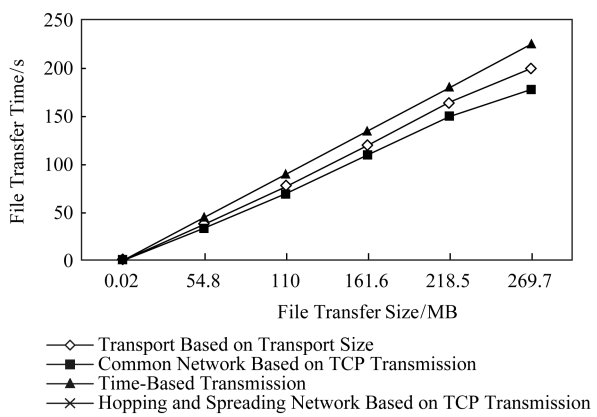


Fig. 11 Time comparison of different file transfer strategies

图 11 不同文件传输方案的时间比较

从图 11 可以看出:普通网络环境下基于 TCP 的传统文件传输方案在时间上要小于基于传输大小

的文件传输方案和基于时间的文件传输方案,但是时间差距不大,这是因为端信息跳扩混合的主动网络防御在进行端信息扩展认证和端信息跳变时损耗了时间,但时间损耗在可容忍范围内;基于传输大小的文件传输方案在时间上要小于基于时间的文件传输方案,更适合端信息跳扩混合的网络环境.

本文不仅对不同的文件传输方案做了对比实验,而且对不同的文件类型也做了对比实验.如表 2 所示为 2 种不同的文件传输方案对不同类型的文件传输所需要的时间对比.其中传输文件分别选择 160 KB 的 jpg 文件、1.1 MB 的 exe 文件、8.3 MB 的 ppt 文件、29.9 MB 的 mp4 文件和 54.8 MB 的 zip 文件 5 种类型,文件传输方案选择传统网络环境下基于 TCP 的文件传输方案和端信息跳扩混合网络环境下的基于传输大小的文件传输方案.

Table 2 Different Types of File Transfer Time Comparison

表 2 不同类型的文件传输时间对比 s

File Type	TCP Transmission Time	Size Based Transmission Time
.jpg	0.114	0.122
.exe	0.744	0.835
.ppt	6.127	6.714
.mp4	20.890	22.862
.zip	38.353	41.568

从表 2 分析可得,基于传输大小的文件传输方案可以完成不同类型的文件传输,而且任意类型的传输在时间上与传统网络环境下基于 TCP 的文件传输方案相差不大.这表明本文提出的基于传输大小的文件传输方案可适用于不同类型的文件传输,具有通用性.

4.2 系统性能测试

本节测试的主要内容包括:端信息跳扩混合文件传输系统抵抗拒绝服务攻击的抗攻击性测试和跳变伪随机的隐蔽性测试.本节的实验配置环境如表 3 所示,主机 A 代表端信息跳扩混合文件传输服务器,主机 B 代表客户端,主机 C 代表攻击者.

Table 3 Environment Configuration of System Attack Experiment

表 3 系统攻击实验环境配置

Host	Job Descripyion	OS	CPU/GHz	BW/Mbps
Host A	Server	Ubuntu	Intel® Core™ i5-4170	100
Host B	Client	Ubuntu	Intel® Core™ i5-4170	100
Host C	Attacker	Ubuntu	Intel® Core™ i5-4170	100

4.2.1 抗攻击性测试

本节对端信息跳扩混合的文件隐蔽传输系统做拒绝服务攻击实验,通过对跳扩混合服务器和普通服务器在 SYN Flood 攻击下的文件传输时间对比,验证端信息跳扩混合文件传输系统的抗攻击性.如图 12 所示为不同攻击速率下的文件传输时间.其中,文件类型为.exe 格式,文件大小为 23 KB,端信息扩展跳变速率为 100 跳/秒.

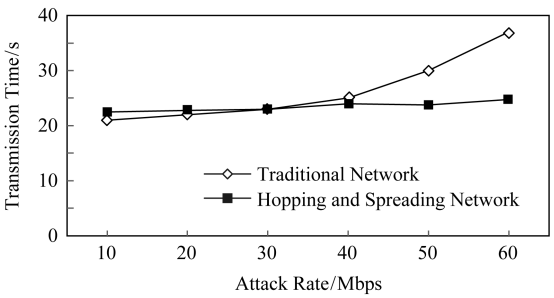


Fig. 12 Transfer time comparison at different attack rates

图 12 不同攻击速率下传输时间比较

通过图 12 可以看出:传统网络中,系统随着攻击速率的增大,文件传输完成所需的时间明显提升,而端信息跳扩混合网络中,随着攻击速率的增大,文件传输完成所需的时间没有明显的变化.由此可见,端信息跳扩混合的文件传输系统可以有效抵御 SYN Flood 攻击.

本文还对拒绝服务攻击的攻击类型做了实验分析比较.攻击机以 50 Mbps 的攻击速度,对端信息跳扩混合的文件传输服务器分别进行 SYN Flood,ACK Flood,UDP Flood 三种类型的拒绝服务攻击和无攻击行为测试,端信息跳扩混合的文件传输服务器选择 100 跳/秒的跳变速率,客户端将对文件大小为 19 KB 的 xls 文件进行下载.表 4 为不同攻击类型下客户端的文件传输时间表.

Table 4 File Transfer Schedule Under Different Attacks

表 4 不同攻击下的文件传输时间表

Type of DoS Attack	File Transfer Completion Time/ms
SYN Flood	19.33
ACK Flood	18.45
UDP Flood	18.83
No Attack	18.17

从表 4 可以看出,端信息跳扩混合的文件传输系统在不同类型的拒绝服务攻击下均可以实现文件的完整性传输,能有效抵御拒绝服务攻击.

4.2.2 隐蔽性测试

本文对通信过程中的数据包进行抓包分析,通过地址的跳变随机性证明端信息跳扩混合文件传输模型的隐蔽性.

在验证端信息跳扩混合的文件传输系统在跳变图案上的随机性实验中,本文利用 SnifferV4.7.5 抓包工具对系统进行了连续 1 000 次的抓包统计,表 5 为系统所使用的 10 个 IP 地址,图 13 为服务器 IP 地址使用统计图.

Table 5 IP Address Pool List Table

表 5 IP 地址池列表

Code	IP Address	Code	IP Address
A	172.18.213.141	*F*	172.18.213.146
B	172.18.213.142	*G*	172.18.213.147
C	172.18.213.143	*H*	172.18.213.148
D	172.18.213.144	*I*	172.18.213.149
E	172.18.213.145	*J*	172.18.213.150

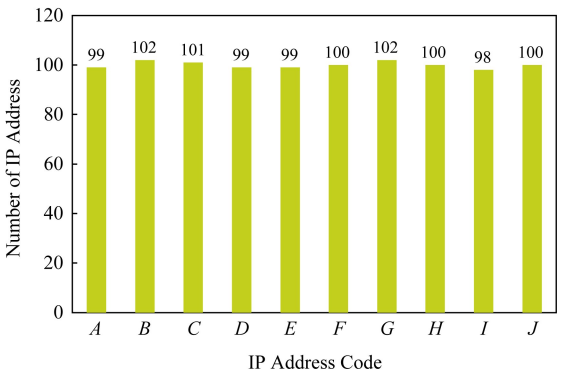


Fig. 13 IP Address Usage

图 13 IP 地址使用情况

从图 13 可以看出,10 个 IP 地址使用情况基本平均,从而证明了本文设计的模型系统跳变图案具有随机性.综上所述,基于端信息跳扩混合的文件传输系统能够实现文件的高隐蔽性传输,保证数据安全.

5 总 结

本文将端信息跳扩混合技术应用到文件传输领域,提出一种基于端信息跳扩混合的文件隐蔽传输策略,对端信息跳扩混合的文件传输关键技术进行分析研究.提出了适应端信息跳扩混合网络环境的组播时间校正方案,对文件分片、重组等关键技术进行了分析,同时提出了基于时间传输和基于大小传输 2 种适用于端信息跳扩混合网络环境的文件传输方案,并将数据迁移技术应用到基于端信息跳扩混合的文件传输策略中,实现了文件的可持续性传输,保证了文件传输的完整性.

对基于端信息跳扩混合的文件隐蔽传输系统模型进行理论分析和实验验证.理论分析结果表明:本系统的安全性较高、时间性能好.通过实验证明了本文设计的系统具有有效性和抗攻击性,可实现文件的隐蔽性传输.

参 考 文 献

[1] Fan Linna, Ma Yufeng, Huang He, et al. The research summary of moving target defense technology [J]. Journal of CAEIT, 2017, 12(2): 209-214 (in Chinese)
(樊琳娜, 马宇峰, 黄河, 等. 移动目标防御技术研究综述[J]. 中国电子科学研究院学报, 2017, 12(2): 209-214)

[2] Shi Leyi, Jia Chunfu, Lü Shuwang. Research on end hopping for active network confrontation [J]. Journal on Communications, 2008, 29(2): 106-110 (in Chinese)
(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)

[3] Wen Xiao. Research on hybrid of end hopping and spreading for active cyber defense [D]. Qingdao: China University of Petroleum, 2018 (in Chinese)
(温晓. 基于端信息跳扩混合的主动网络防御研究[D]. 青岛: 中国石油大学(华东), 2018)

[4] Shi Leyi, Guo Hongbin, Wen Xiao, et al. Research on end hopping and spreading for active cyber defense [J]. Journal on Communications, 2019, 40(5): 125-135 (in Chinese)
(石乐义, 郭宏彬, 温晓, 等. 端信息跳扩混合的主动网络防御技术研究[J]. 通信学报, 2019, 40(5): 125-135)

[5] Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats [M]. New York: Springer, 2011

[6] Lei Cheng, Ma Duohe, Zhang Hongqi. Optimal strategy selection for moving target defense based on Markov game [J]. IEEE Access, 2017, 5(99): 156-169

[7] Cai Guilin, Wang Baosheng, Wang Tianzuo, et al. Research and development of moving target defense technology [J]. Journal of Computer Research and Development, 2016, 53(5): 968-987 (in Chinese)
(蔡桂林, 王宝生, 王天佐, 等. 移动目标防御技术研究进展[J]. 计算机研究与发展, 2016, 53(5):968-987)

[8] Tan Jinglei, Zhang Hengwei, Zhang Hongqi, et al. Optimal strategy selection approach of moving target defense based on Markov time game [J]. Journal on Communications, 2020, 41(1): 42-52 (in Chinese)
(谭晶磊, 张恒巍, 张红旗, 等. 基于 Markov 时间博弈的移动目标防御最优策略选取方法[J]. 通信学报, 2020, 41(1): 42-52)

[9] Leeuwen B V, Stout W, Urias V. MTD assessment framework with cyber attack modeling [C/OL] //Proc of IEEE Int Carnahan Conf on Security Technology. Piscataway, NJ: IEEE, 2016 [2020-07-26]. https://ieeexplore.ieee.org/document/7815722

[10] Hu Hongchao, Wu Jiangxing, Wang Zhenpeng, et al. Mimic defense: A designed-in cybersecurity defense framework [J]. IET Information Security, 2017, 12(3): 226-237

[11] Song Ke, Liu Qinrang, Wei Shuai, et al. Endogenous security architecture of Ethernet switch based on mimic defense [J]. Journal on Communications, 2020, 41(5): 18-26 (in Chinese)
(宋克, 刘勤让, 魏帅, 等. 基于拟态防御的以太网交换机内生安全体系结构[J]. 通信学报, 2020, 41(5): 18-26)

[12] Wang Yawen, Wu Jiangxing, Guo Yunfei, et al. Scientific workflow execution system based on mimic defense in the cloud environment [J]. Frontiers of Information Technology & Electronic Engineering, 2018, 19(12): 1522-1536

[13] Zhou Yuyang, Cheng Guang, Guo Chunsheng, et al. Survey on attack surface dynamic transfer technology based on moving target defense [J]. Journal of Software, 2018, 29(9): 2799-2820 (in Chinese)
(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)

[14] Lin Kai, Jia Chunfu. End hopping based on message tampering [J]. Journal on Communications, 2013, 34(12): 142-148 (in Chinese)
(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)

[15] Lin Kai, Jia Chunfu. Distributed timestamp synchronization for end hopping [J]. China Communications, 2011, 8(4): 164-169

[16] Lin Kai, Jia Chunfu, Shi Leyi. Improvement of distributed timestamp synchronization [J]. Journal on Communications, 2012, 33(10): 110-116 (in Chinese)
(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)

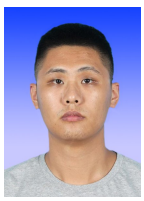
[17] Luo Yuebin, Wang Baosheng, Wang Xiaofeng. A keyed-hashing based self-synchronization mechanism for port address hopping communication [J]. Frontiers of Information Technology & Electronic Engineering, 2017, 18(5): 719-728

[18] Liu Jiang, Zhang Hongqi, Dai Xiangdong, et al. A proactive network defense model based on self adaptive end hopping [J]. Journal of Electronics & Information Technology, 2015, 37(11): 2642-2649 (in Chinese)
(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)

[19] Zhao Zheng, Gong Daofu, Lu Bin, et al. SDN-based double hopping communication against sniffer attack [J]. Mathematical Problems in Engineering, 2016, 2016(2): 1-13

[20] Zhang Liancheng, Wei Qiang, Tang Xiucun, et al. Path and port address hopping based SDN proactive defense technology [J]. Journal of Computer Research and Development, 2017, 54(12): 2748-2758 (in Chinese)
(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)

[21] Bernaschi M, Casadei F, Tassotti P. SockMi: A solution for migrating TCP/IP connections [C/OL] //Proc of the 15th Euromicro Int Conf on Parallel, Distributed and Network-Based Processing. Piscataway, NJ: IEEE, 2007 [2020-07-26]. https://ieeexplore.ieee.org/document/4135281



Hou Bowen, born in 1997. Master candidate in China University of Petroleum. Senior member of CCF. His main research interests include cyber security, covert communication.

Guo Hongbin, born in 1992. Master candidate in China University of Petroleum. His main research interests include cyber security, cyber confrontation.

Shi Leyi, born in 1975. PhD, professor in China University of Petroleum. Senior member of CCF. His main research interests include cyber security, game theory, and mobile computing.