基于端信息跳变的视频通信系统防护研究

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:端信息跳变技术目前已成为主动网络防御方向的研究热点,合理的跳变策略和同步机制是它的两个研究重点。文中主要研究了端信息跳变技术的跳变策略问题,分析了端信息跳变序列的随机性和均匀分布性问题,提出了一种基于混沌序列的端信息跳变方案。采用 NTP 协议实现同步,构建了一个端信息跳变系统模型,介绍了跳变算法的理论依据和实现步骤。最后,设计实现了端信息跳变系统原型,并进行了两组抗攻击实验,分别是截获攻击实验和 DoS 攻击实验。实验结果表明,设计的端信息跳变系统能够有效抵抗网络中的截获攻击,加大攻击者对捕获到的数据包的分析难度,增加攻击者的攻击代价;此外,在抗 DoS 攻击性能上,当 DoS 攻击速率达到 100 Mbps 时,系统仍能保持通信,具有较好的安全性能和服务性能。

关键词:主动防御;端信息跳变;混沌序列;截获攻击;DoS 攻击
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2018)11-0142-04
doi:10.3969/j.issn.1673-629X.2018.11.031

Research on Video Communication System Protection Based on End Hopping

SUN Hui
(School of Computer & Communication Engineering, China University of Petroleum, Qingdao 266580, China)

Abstract: The end hopping technology has become a research hotspot in the active network defense. The reasonable hopping strategy and synchronization mechanism are two focuses of its research. In this paper, we study the problem of end hopping strategy, analyze randomness and uniform distribution of end hopping sequence, and propose a end hopping scheme based on chaotic sequence. We use NTP protocol to achieve synchronization, construct a end hopping system model, and introduce the theoretical basis and implementation steps of hopping algorithm. Finally, we design and implement a prototype of the end hopping system, and carry on two groups of anti-attack experiments about eavesdrop attack and DoS attack. The experiment shows that the end hopping system can effectively resist the eavesdrop attacks, increase the attacker's analysis difficulty of the packets and the cost of the attacker. In addition, in the anti-DoS attack performance, when the DoS attack rate reaches 100 Mbps, the system can still communicate with better security and service.

Key words: active defense; end hopping; chaotic sequence; eavesdrop attack; DoS attack

0 引 言

随着互联网在社会各领域的深入发展,网络安全态势也面临着更加严峻的挑战。当今互联网与整个社会密切相关,任何形式的网络攻击都有可能直接影响到人们的现实生活。网络安全事件造成的影响力和破坏性正在逐步加大。2017 年上半年,全球大规模爆发“永恒之蓝”勒索病毒,不仅破坏了全球范围内的许多高价值数据,而且直接导致一大部分服务、设施无法正常运行。在当今这个万物互联的社会背景下,很多行为操作的背后其实都有着网络信息安全的影子,例如消费时使用的支付宝和微信支付,网络信息安全已经与人民的财产息息相关。而随着互联网的进一步深化与发展,可以预见,网络信息安全将越来越多地影响着人们的日常生活。

网络安全问题日益加剧,但传统的网络安全防御技术却已无法高效应对。目前应对网络安全问题普遍采取防火墙、入侵检测、防病毒网关、漏洞扫描、灾难恢复等手段,但这些手段的防护能力大多是静态的、被动的,无法应对新的网络攻击。这就使得网络防御始终落后于网络攻击,无法从根本上解决网络安全问题,因

收稿日期:2017-12-18 **修回日期**:2018-04-24 **网络出版时间**:2018-06-29
基金项目:山东省重点研发计划项目(2015GGX101045)
作者简介:孙 慧(1991-),女,硕士,研究方向为网络安全。

网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20180629.1704.032.html

此主动防御技术应运而生。在主动防御研究进程中,中国和美国分别提出了移动目标防御(moving target defense,MTD)[1]与拟态安全防御[2],均期望从根本上改变目前网络“易攻难守”的局面。端信息跳变(end hopping)技术作为一种典型的主动网络防御技术,已经得到越来越多的关注和研究,并将其应用到传统的网络通信中。它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,这些参数主要包括端口、IP 地址、时隙、加密算法和协议等端信息,从而扰乱攻击者的攻击,实现主动网络防护[3]。端信息跳变可以是服务器单方面的跳变,也可以是服务器和客户端双方面的跳变。在端信息跳变中,跳变策略和同步机制是其两种关键技术。文中主要研究端信息跳变技术中的跳变策略问题,并提出一种基于混沌算法的端信息跳变策略。

1　相关工作

端信息跳变技术是基于通信参数变换的机制,网络通信过程中所涉及的参数较多,这里主要是指 IP 地址和通信端口。目前,端信息跳变技术在国内外都取得了很大的研究进展。

在国外研究方面,文献[4]将 IP 地址随机化技术与诱骗技术相结合,设计实现了一个基于虚拟机的系统原型,解决了两个挑战,一是对合法用户的服务可用性和对未授权用户的服务安全性,二是可以确保无缝连接迁移。文献[5]提出面向 IPv6 的动态目标防御架构,利用 IPv6 巨大的地址空间,不断改变发送方和接收方的 IP 地址,以防止攻击者获得通信主机的身份,但网络时延将会造成丢包现象,进而影响通信。文献[6]通过在各种数据加密或操作协议之间动态跳跃来保护数据集的方法,获得比单一固定加密协议更高的安全性和更好的扩展性。文献[7]设计实现了 DTMC 模型,并通过控制用于通信的端口,改进了现有的随机端口跳变算法,克服了现有基于 ACK 的随机端口跳变算法的弱点,改善了现有协议的通信成功率。文献[8]提出了一种自适应算法—HOPERAA,解决了时钟漂移对同步的影响,且每个客户端与服务器的交互独立于其他的客户端,不需要第三方参与或时间服务器。

在国内研究方面,文献[3]研究了端信息跳变主动网络防御模型,并且提出了一种基于 UDP 发言人服务的时间戳同步方法,但可能存在潜在的端信息网络泄漏的问题。文献[9]融合了端信息跳变技术与自适应技术,提出自适应的端信息跳变策略,通过对各跳变节点上网络流量情况进行实时评估来决定下一跳方案,自动调整跳变相关参数,在保持较好的服务性的同时,又能保证较高的安全性。文献[10]对文献[3]提出的模型加以改进,设计了一种浏览器插件策略,对客户端身份进行认证,以此来隐藏服务器的真实信息。文献[11]构建了基于非广延熵和 Sibson 熵融合的实时网络异常测量算法,设计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。文献[12]中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,构建了跳变栈模型,设计了跳变栈模型的 3 种实现方案并分析了其工作原理。但存在在用户层会带来不必要的开销,内核层需要严格与操作系统版本对应的问题。文献[13]提出了一种基于滑动窗口的分布式时间戳同步策略,引入分布式时间服务机制,能有效克服网络中的传输时延和拥塞的影响。

在上述研究的基础上,文中主要对端信息跳变技术中的跳变策略问题进行研究,提出一种基于混沌序列的端信息跳变方案,结合视频通信系统,设计一个端信息跳变系统模型,解决通信过程中的系统和数据安全问题,实现主动网络防御。

2　端信息跳变关键技术研究

2.1　同步方案

同步机制是端信息跳变技术研究的一个重点内容,NTP 协议是服务器和客户端之间通过二次报文交换,计算两者之间的时间差,客户端校正本地系统时间,实现二者的时间同步。由于 NTP 协议的同步精度较高,且在各平台易实现,因此从同步精度和实现复杂度上考虑,文中的端信息跳变模型采用 NTP 协议来实现同步。

2.2　跳变策略

合理的跳变策略是端信息跳变技术的另一个关键,也是文中的研究重点。良好的跳变策略能够在更大程度上迷惑攻击者,使攻击者无法分析得到有用数据,从而增加攻击者的攻击代价,提高系统的安全性。在端信息跳变系统中跳变方案多采用随机序列的方法,即从端信息跳变序列集中随机选取下一跳端信息。因此,在端信息跳变系统中应使随机序列具有良好的随机性,使攻击者无法从已截获的数据包信息中分析预测当前和下一跳的端信息。而混沌序列具有结构复杂,对初始值敏感的特性,使其难以被分析和预测。混沌序列[14]理论上具有类随机性,破坏了相关分析的适用性,保密性得以加强,因而将其应用到端信息跳变系统中能够很好地满足随机序列的要求。

混沌序列的产生有多种方式,文中采用 logistic 映射,其表达式为:

$$x_{n+1} = x_n(1 - x_n), 0 < x_n < 1 \quad (1)$$

其中,$1 \leqslant r \leqslant 4$。研究证明,当 $3.569\ 9 < r \leqslant 4$ 时,产生的序列 $\{x_i, i = 0,1,2\cdots\}$ 是非周期的、不收敛的,且对初值非常敏感。当 r 无限趋近 4 时,x 在 0 到 1 区域内越接近平均分布,因此将 r 的值设定为 4。

文中建立了一个端信息跳变模型,并将其应用于视频通信中。在该模型中设置部署一个 NTP 时间服务器和两台平等的主机 A 和 B,主机 A 和主机 B 构造参数相同的 logistic 映射,时间值作为初始值。两台主机之间进行通信时,首先与 NTP 时间服务器进行时间同步,将时间值作为输入,利用 logistic 产生的混沌序列计算主机双方当前所用的端信息,计算得到端信息后即可进行通信连接。其中主机 A 和主机 B 的 IP 地址和端口均是不确定的,不断改变的。端信息跳变模型如图 1 所示。

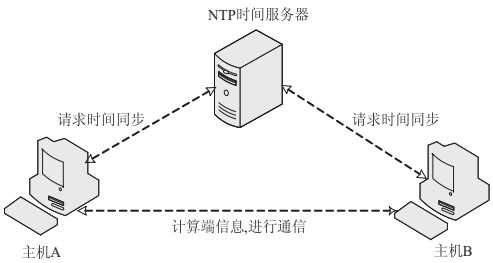


图 1 端信息跳变系统模型

主机 A 和主机 B 前期先与 NTP 时间服务器进行时间同步,同步成功后,获取当前系统时间 T,将获取的时间 T 进行预处理,预处理函数为:

$$T_0 = F(T,\text{key}), T_0 \in (0,1) \tag{2}$$

其中,key 是主机 A 和主机 B 的共享密钥。

将 T_0 作为 logistic 映射[15]的初始值 x_0,然后按照映射方程不断迭代,产生混沌序列;再对产生的序列进行 0,1 判定,得到比特混沌序列;根据地址和端口的计算需要,再将此比特序列转换成实数序列。在这个过程中,它们都是混沌序列,均保持着混沌序列的特性。端信息产生的具体过程为:

第一步:根据 logistic 映射方程式:

$$x_{n+1} = 4x_n(1 - x_n), 0 < x_n < 1 \tag{3}$$

令 $x_0 = T_0$,按式 3 迭代计算,产生一个长度为 m 的序列 $X = \{x_0, x_1, \cdots, x_n\}, 0 < x_n < 1, n = 1,2,3\cdots$。

第二步:将产生的序列 $X = \{x_0, x_1, \cdots, x_n\}$ 按式 4 进行 0,1 判定,得到一个比特混沌序列 $Y = \{y_0, y_1, \cdots, y_n\}$。

$$y_n = \begin{cases} 0, 0 < x_n \leqslant 0.5 \\ 1, 0.5 < x_n < 1 \end{cases} \tag{4}$$

文中研究的端信息跳变是指主机 IP 地址和端口号的跳变,所以进一步将比特混沌序列转换成实数混沌序列。在网络通信过程中端口号的范围为 0 ~ 65 535,其中前 1 024 个端口留用,可选取 16 位作为端口号;主机双方各配置 10 个 IP 地址用于跳变,所以取 4 位来计算所选用的 IP 地址号。综上,转换实数序列时,采取每 20 位进行转换,在这 20 位中的前 16 位计算端口,后 4 位计算 IP 地址号,即得到一个二维实数混沌序列。系统从序列初始位置起,依次选取跳变所需端信息,当一组序列遍历完成时,系统更新混沌序列,重复以上步骤计算端信息。

根据混沌序列的特性,任意两组端信息都不具有相关性,且任意一段序列不循环,因此保证了端信息跳变过程中的随机性,增大了攻击者的分析难度。同时,对函数初始值进行了加密处理,攻击者无法获得初始值,就很难预测混沌序列,也就很难知道主机端信息的跳变规律,就不可能预测下一跳端信息,从而保证了主机间的通信安全。

3 抗攻击实验及结果分析

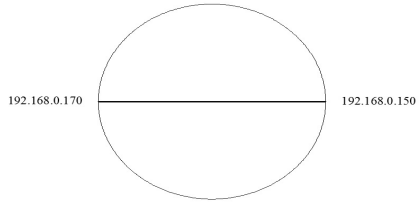
按照端信息跳变系统模型,采用 Java 语言对原型系统进行实现,并在原型系统上分别进行截获攻击实验和 DoS 攻击实验,一组是传统的不跳变系统,另一组是端信息跳变系统。对实验环境的配置见表 1。

表 1 系统攻击实验环境配置

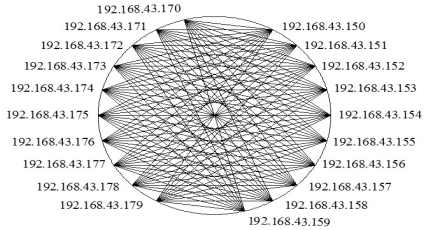
主机	主机系统	内存/G	处理器/GHz	带宽/(Mbit · s^{-1})
主机 A	Linux	4	3.70	100
主机 B	Linux	4	3.70	100
攻击机	Windows7	4	3.70	1 000

3.1 截获攻击实验

在截获攻击实验中,截获攻击机位于 Hub 构成的局域网中,保证最有利于攻击机的环境。截获攻击机使用 Sniffer 软件对局域网内的流量和数据进行抓包分析,在传统非跳变的情况下,其网络中的流量图如图 2(a)所示;在文中端信息跳变系统环境下,截获攻击机截获到的流量图如图 2(b)所示。



(a) 传统非跳变网络流量图



(b) 端信息跳变网络流量图

图 2 截获攻击实验结果

从实验结果可以看到,在传统不跳变系统中,通信双方的地址和端口是固定的,一对一的,流量是集中的,抗截获能力差,攻击者很容易从截获的流量包中分析得到有用信息,无法保证通信双方的信息安全。而在文中的端信息跳变策略下,通信双方的 IP 地址和端口都是随机组合的,攻击者截获到的流量是分散的,无规则的,大大干扰了攻击者,攻击者想要从分散的流量中完整分析出数据报文的难度十分大,这将有效抵抗网络中的截获攻击。

3.2　DoS 攻击实验

在 DoS 攻击实验中,鉴于文中原型系统中的视频通信采用的是 UDP 协议,因此在攻击机上配置 UDP-Flood 攻击。攻击机向通信主机发送大量 UDP 攻击包,其攻击速率 V 分别为 20 Mbps,40 Mbps,80 Mbps,100 Mbps,分别测试传统非跳变系统下的通信情况和文中端信息跳变系统下的通信情况,得到的实验结果如图 3 和图 4 所示。

图 3　传统非跳变的视频通信情况

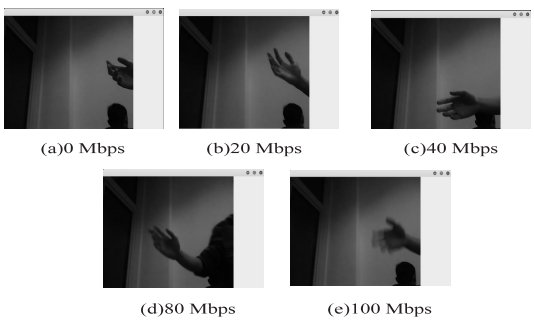


图 4　端信息跳变系统的视频通信情况

观察 DoS 攻击测试结果可以看到,传统不跳变系统在攻击速率为 20 Mbps 的情况下已经无法进行正常通信了。而在文中设计的端信息跳变系统下,一般的攻击速率对系统没有太大影响,系统仍能够正常进行通信。当攻击速率达到 100 Mbps 时,从图中可以看出,画面会稍有卡顿,但通信仍然能够进行。上述实验结果的对比证明了端信息跳变技术在抵抗 DoS 攻击上有良好的效果。

4　结束语

针对当前越来越不安全的网络大环境,提出一种基于混沌序列的端信息跳变方案,将其应用到视频通信系统中,用来防御视频通信中遭受的网络攻击。文中介绍了该端信息跳变模型和跳变算法的具体实现过程,最后设计实现了端信息跳变视频系统的原型,并对原型系统进行了截获攻击和 DoS 攻击实验。实验结果证明了该方案在网络防御中的有效性和较好的服务性。

参考文献:

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

[2] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学,2014,30(7):1-7.

[3] 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.

[4] SUN Jianhua,SUN Kun. DESIR:decoy-enhanced seamless IP randomization[C]//IEEE international conference on computer communications. San Francisco,CA,USA:IEEE,2016:1-9.

[5] DUNLOP M,GROAT S,URBANSKI W,et al. Mt6d:a moving target IPv6 defense[C]//The 2011 military communications conference. Baltimore,Maryland:[s. n.],2011:1321-1326.

[6] ELLIS J W. Method and system for securing data utilizing reconfigurable logic:US,8127130[P]. 2012-02-28.

[7] HARI K,DOHI T. Dependability modeling and analysis of random port hopping[C]//9th international conference on ubiquitous intelligence & computing and 9th international conference on autonomic & trusted computing. Fukuoka,Janan:IEEE,2012:586-593.

[8] FU Z,PAPATRIANTAFILOU M,TSIGAS P. Mitigating distributed denial of service attacks in multipartyapplications in the presence of clock drifts[J]. IEEE Transactions on Dependable and Secure Computing,2012,9(3):401-413.

[9] 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.

[10] 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(10A):114-118.

[11] 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.

[12] 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.

[13] 丰　伟. 网络通信中地址端口动态跳变技术的研究与实现[D]. 武汉:华中科技大学,2013.

[14] 金海荣. 混沌序列密码分析及应用研究[D]. 哈尔滨:黑龙江大学,2009.

[15] 施伟锋. Logistic 映射及其混沌特性研究[J]. 光电技术应用,2004,19(2):53-56.