DOI: 10.16452/j.cnki.sdkjzk.2022.01.004 文章编号:1672-3767(2022)01-0034-10

基于端址敲门的隐蔽通信系统研究

马 荣[1,4],卢 熠[2],许翰林[1],段鹏飞[3],石乐义[1]
(1. 中国石油大学(华东)计算机科学与技术学院,山东 青岛 266580;
2. 蚂蚁金服,浙江 杭州 310000;
3. 中国石油大学(华东)海洋与空间信息学院,山东 青岛 266580;
4. 宁夏长庆初级中学,宁夏 银川 750006)

摘 要:端口敲门技术是一种在端口关闭的情况下实现主机之间连接通信的方法,通过端口敲门序列对合法用户进行认证通信并阻断敌手攻击,在保密传输、隐蔽通信等领域得到了良好应用。然而,端口敲门技术使用固定 IP 地址,容易暴露真实通信地址导致隐蔽传输失效。针对该问题,提出一种基于端址敲门技术的隐蔽通信系统,通过对端口与 IP 地址的组合序列进行敲门来传递机密信息,使得通信端信息与所传输信息无关,进而实现信息的高隐蔽性传输。并详细讨论了端址敲门技术中的扩展序列生成和信息传输,针对端口选择的多样性问题,提出基于象限和正弦函数的两种端口控制策略,在保证端口选择随机性的基础上进一步提升系统的隐蔽性。最后通过搭建测试环境对该系统的隐蔽性和抗攻击性进行验证,实验结果表明该系统具有良好的实用性和隐蔽性。

关键词:网络安全;隐蔽通信;端口控制;信息隐藏;端址敲门
中图分类号:TP393.08 **文献标志码**:A

Research on covert communication system based on ports and addresses knocking

MA Rong[1,4], LU Yi[2], XU Hanlin[1], DUAN Pengfei[3], SHI Leyi[1]
(1. College of Computer Science and Technology, China University of Petroleum, Qingdao, Shandong 266580, China;
2. Ant Financial, Hangzhou, Zhejiang 310000, China;
3. College of Oceanography and Space Informatics, China University of Petroleum, Qingdao, Shandong 266580, China;
4. Ningxia Changqing Junior High School, Yinchuan, Ningxia 750006, China)

Abstract: As a method to realize the connection and communication between hosts when the port is closed, port knocking technology can authenticate the legitimate users and block the adversary attack through port knocking sequence and has been widely used in the fields of secure transmission and covert communication. However, due to the fixed IP address used in port knocking technology, the real communication address is easy to be exposed, thus leading to the failure of covert transmission. To realize the high covert transmission of information, this paper proposed a covert communication system based on ports and addresses knocking technology to transfer confidential information by knocking on the combination sequence of port and IP address, thus making the communication end information irrelevant to the transmitted information. Next, it discussed in detail the issue of the generation of extended sequence and the transmission of information based on the ports and addresses knocking technology. In view of the diversity of port selection, two port control strategies, quadrant strategy and sinusoidal function strategy, were proposed to further enhance the concealment of the system on the basis of ensuring the randomness

收稿日期:2020-08-09
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)
作者简介:马 荣(1994—),女,宁夏银川人,硕士研究生,研究方向为计算机网络与应用.
石乐义(1975—),男,山东临朐人,教授,博士生导师,主要从事计算机网络、信息安全、军事通信对抗等方面的研究,本文通信作者.E-mail:shileyi@upc.edu.cn

of port selection. Finally, the concealment and anti-attack of the model were verified by building the test environment. The experimental results show that the system has good usability and concealment.

Key words: network security; covert communication; port control; information hiding; ports and addresses knocking

隐蔽通信技术通过利用载体信息的冗余性将机密信息以伪装的方式隐藏在公共信道中进行传输,达到在网络环境中隐蔽通信和隐蔽标识的目的,为使用者提供有效且安全的信息传输服务。当前,无处不在的网络监视、流量审查等功能对用户的隐私构成越来越严重的威胁,网络安全防护形势日益严峻。

作为信息隐藏的研究分支[1],隐蔽信道的概念最初是由 Lampson[2]在 1973 年提出,比传统的信息加密技术具有更强的隐蔽性,已成为网络安全领域的研究热点。端口敲门技术作为信息隐藏的一种具体实现,允许访问预先配置好"敲门序列"的防火墙服务,通过有序访问对方端口进行机密信息的传输,使得信息安全传输从对信息加密转向信息内容扩展,以信息扩展后生成的端口访问序列作为信息传输的载体来传递机密信息,更易于机密信息的隐藏。端口敲门技术仅对端口进行安全防护,使得攻击者不能利用端口发起攻击,但对于服务器的地址并没有进行相应防护。由于端口敲门技术对固定 IP 进行多次重复访问,极易引起攻击者注意,可能会暴露通信地址,引起信息泄露或者通信中断,研究如何对端口敲门技术进行改进以增强其抗攻击能力和隐蔽传输能力十分重要。

本研究提出基于端址敲门的隐蔽通信系统,该系统在单一端口敲门认证的基础上引入 IP 地址,采用地址与端口组合作为敲门序列的端址敲门方法实现隐蔽信息的传递。这样不仅能够隐藏服务器的真实地址,而且能够实现信息的隐蔽性传输。本研究首先详细分析扩展序列的生成并针对不同信息类型进行相应的信息传输服务,然后针对端口选择随机性的问题提出基于象限的端口选择策略和基于正弦函数的端口选择策略,最后通过实验分析得到满足不同信息传输要求的端口控制策略,以达到更好的传输效果。

1　相关工作

网络隐蔽通信中的隐蔽信道分为存储型隐蔽信道(storage covert channel, SCC)和时间型隐蔽信道(timing covert channel, TCC)两种类型。存储型隐蔽信道是指通过协议数据单元(protocol data units, PDU)传输隐藏信息,如数据分组、数据帧、数据段的未使用或保留的协议头字段[3-4]。Anagnostopoulos 等[5]通过将信息嵌入到 DNSKEY 中来进行隐蔽通信。Mavani 等[6]增加新的 IPv6 目的地址选项用于传递隐蔽信息。Zander 等[7]提出一种将秘密消息映射到 IP 生存时间的新隐蔽方案,用 Live Field 取代 IP 数据包,证明了该方案的可行性及安全性。王永杰等[8]提出一种基于 DNS 协议的隐蔽通道技术,并对其基本方法及其实用化的数据编码、躲避检测、可靠通信和速率控制等关键技术进行了研究,分析结果表明该技术具有可靠性好、隐蔽性强、通信效率高等特点。谭庆丰等[9]设计实现了基于 P2P 网络的 StegoP2P,让 P2P 网络中的节点合谋隐蔽握手,达到传递隐蔽信息的目的。存储型隐蔽信道在初期被利用到了极致,但是后期网络防火墙使用了流量正规化技术,强制改写了 IP 数据包的冗余位,一定程度上打击了这种隐蔽通信模式[10-12]。时间型隐蔽信道是指将秘密信息调制进网络数据包的发包间隔、发包速率、发包次序等特征中进行传递。早期 Moskowitz 等[13]提出一种简单的时间隐蔽信道(simple timing channel, STC),是一种无噪声隐蔽信道。Cabuk 等[14]最早提出 IP 时间隐蔽信道,根据划分的若干个固定的时间窗口内是否有 IP 数据包到达进行解码。这种方法高度依赖网络情况,因此初期并未引起太多关注。李彦峰等[15]提出区块链网络隐蔽信道模型,用形式化方法建模并证明了抗干扰性和抗篡改性;然后构建基于业务操作时间间隔的区块链网络隐蔽信道的场景;最后提出包含抗检测性、顽健性和传输效率的区块链网络隐蔽信道评估向量,为基于区块链环境的新型网络隐蔽信道的实用化奠定了理论基础。王昌达等[16-17]考虑到虽然 IP 数据包传输时间间隔变化通信与基于数据包标识号传输顺序变化通信的 IP 时间隐通道具有较好的隐蔽性,但易受到网络延迟与时延抖动影响出现错序的问题,提出二维时间隐通道的构建方法,但是由于网络时间型隐蔽通信受网络数据流量、路由转发等状况的影响比较大,会造成隐蔽信道传输信息的错误,对此类型隐蔽通信的研究需要极其复杂严格的条件。

端口敲门(port knocking,PK)技术首先由 Krzywinsk[18] 提出。Shiraz 等[19] 针对移动云计算(mobile cloud computing,MCC)的安全问题提出一种动态长度端口敲门认证框架,该框架不仅提升了敲门认证的安全性,而且在时间和缓冲区管理方面优化了性能。实验结果表明,动态长度端口敲门身份验证技术可通过减少施加的负载将时间方面性能提高 23%,将缓冲区管理性能提高 28%。Major 等[20] 提出一种名为 Crucible 的新型端口断开解决方案,是一种安全的身份验证方法,具有很高的可用性和隐身性,可以使服务器和服务保持隐藏和受保护。Ali 等[21] 提出一种将源端口序列加入到敲门序列中的技术,能够有效应对重复攻击和端口监听。Mehran 等[22] 提出一种安全端口敲门隧道方法,能够应对 DoS 敲门序列攻击和 NAT 敲门序列攻击。由以上分析可知现阶段端口敲门技术大都应用于安全认证方面,未涉及隐蔽通信。

综上,存储型隐蔽信道是通过将数据包中的某些次要字段进行填充达到隐蔽通信的目的,可靠性好、隐蔽性强、通信效率高,但后期的流量正规化技术很大程度上限制了这种隐蔽通信方式的发展。时间型隐蔽信道是以时间为载体实现隐蔽通信,隐蔽性高,但传输效率较低,受网络和时延的影响极大,需要极为严苛的传输环境。因此,本研究提出一种基于端口的敲门技术,使用 IP 地址和端口作为端址敲门序列,在提高信息传输隐蔽性的同时保障系统的安全性和稳定性。相较于端口敲门技术,端址敲门中 IP 地址的加入使得端址敲门技术中扩展序列的复杂度更高,且随着配有 IP 地址的主机数量增加,序列复杂度显著提升。复杂的序列既可以防范攻击者,又可以达到很好的隐蔽传输效果。

2 基于端址敲门的隐蔽通信技术

基于端址敲门的隐蔽通信技术通过对端口加 IP 地址的复杂组合序列进行敲门,旨在建立一种高隐蔽、抗攻击的通信机制,在保护通信双方的基础上利用网络层和传输层协议的特点,构建自定义报头的数据包,并使用这些数据包组合序列作为载体隐藏机密信息,以达到隐蔽通信的目的。

2.1 基于端址敲门的隐蔽通信模型

为了使隐蔽信息能够分散且传输内容与所发送内容无关,实现高隐蔽通信,提出端址敲门技术,并将此技术应用于隐蔽通信。从信息隐蔽的角度出发,建立了基于端址敲门技术的隐蔽通信模型,如图 1 所示。该模型用一个二元组(Sender,Receiver)描述,Sender 表示发送端,包括扩展序列生成模块和扩展序列发送模块;Receiver 表示接收端,包括扩展序列接收模块,接收到的扩展序列用于对发送端身份的认证和秘密消息的传输。

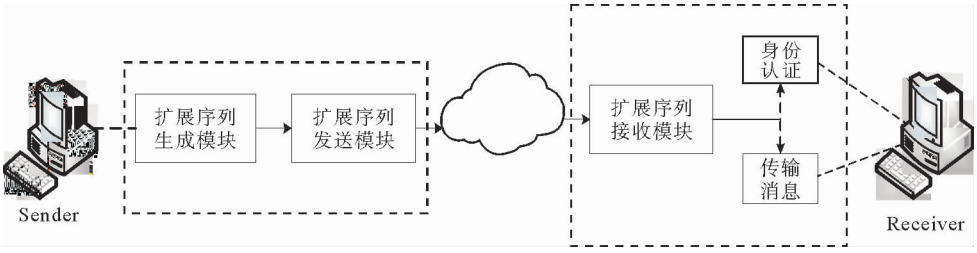

图 1 端址敲门隐蔽通信模型

Fig. 1 Covert communication model of ports and addresses knocking

在基于端址敲门技术的隐蔽通信模型中,发送端首先生成信息扩展序列,然后将扩展序列发送给接收端;接收端对接收到的扩展序列进行检测,判断用户身份的合法性。如果合法则通过认证,然后进行机密信息的传输,否则拒绝服务。

在本研究的隐蔽通信系统中,首先通信双方要分别在各自的网络部署若干个 IP 地址,然后进行隐蔽通信。发送端将所要传输的隐蔽信息进行逐个编码,选取 IP 和端口组成套接字选项,通过一系列不同的套接字生成一串扩展序列,然后将其发送到接收端。接收端始终运行着监听程序,监听并记录来访数据包中的套接字信息,根据源 IP 地址范围过滤掉无用数据包,再以源端口为过滤规则进行身份验证(校验内容为源 IP

地址、源端口、目的 IP 地址、目的端口),以免攻击者伪装合法 IP 发送恶意数据包。接收端进行身份验证是通信双方进行信息传输前必不可少的步骤之一,只有通过身份验证后才能进行机密信息的传输。一旦发送端身份得到确认,表明通信双方已经建立互信的信道,并进入信息传输模块。接收端接收到所有信息并将其存储起来,然后一并进行解码,还原出原始信息。

2.2　扩展序列的生成与认证模块

端址敲门序列是基于端址敲门技术的隐蔽通信系统的核心。其中,接收端网卡配置有 IP 地址池中的所有地址,无论数据包发往哪个 IP 地址,都可通过路由到达接收端网卡。因此接收端的端址敲门序列可以形式化描述为:

Server-Sequence=$\{(IP_1,C),(IP_2,C),(IP_3,C),\cdots,(IP_n,C)\}$,其中 IP$\in(IP_1,IP_2,IP_3,\cdots,IP_n)$的 IP 地址池,C 为常数,代表服务端口。

发送端端址敲门序列在文字模块下既作为源 IP 地址发送数据包,又用于编码文字字符。系统对所发送的字符串逐个取字符,并按规则转换为整数,再转换为二进制数,根据二进制数中"1"的位置选择 IP,最终确定发送序列。例如发送端选取了 IP_1、IP_3、IP_5 作为扩展编码(扩展序列只包含目的 IP 和目的端口号),然后通过提出的端口控制策略选择合适的端口,组成端址敲门序列$\{(IP_1,port_1),(IP_3,port_3),(IP_5,port_5)\}$。

接收端对于接收到的扩展序列首先要进行身份认证,确定是否为合法用户。接收端对序列进行解码获取相应的身份信息,当组合序列满足预设的条件时信息才能被解析出来,即接收方通过将分散的敲门包进行组合完成信息的还原,否则不予响应。身份认证是信息传输的一种特殊形式,信息传输将在下节中进行详细论述。由于传输过程中各个信息是分散的,攻击者难以通过序列中的单个敲门包获取有效信息,因此采用端址敲门的方式进行信息传递具有良好的隐蔽性及抗攻击性。

2.3　信息传输模块

信息传输模块是基于端址敲门技术的隐蔽通信系统中最为核心的部分,在身份信息验证成功后,接收端进入等待接收信息状态,发送端进入传输模块,进行机密信息的传输。针对垂直部门间的实际应用场景,提出下列两种传输模块,分别用于文字传输和文件传输。

1) 文字传输模块

文字信息隐蔽传输模块的发送和接收形式与即时通信软件类似,客户端输入信息并发送,接收端接收并呈现信息。发送端获取用户输入的文字信息,逐个字符进行转码,将单个字符转换成用若干 IP 地址组合的形式表示,配置套接字信息前需要选择所选用的序列确认方式,选择使用基于象限规则的方案或者基于正弦函数规则的方案,最后将 IP 地址和端口号配置到套接字中并发送给接收端。接收端根据同样的规则进行解码,还原出原始文字信息。

系统首先将用户编辑的文字(以英文为例)按字符分割,并将其按约定扩展为一串由不同的源/目的 IP 地址和源/目的端口套接字组成的序列。为达到隐蔽通信的目的,文字信息通过编码后进行转换发送。其中编码方案综合考虑了字符的日常使用频率和字符转码特性后,为方便字符编码,将字符集中的字符以整型数字作为标记代号,构建对照表如表 1 所示。详细转码生成 IP_Sequence 的步骤如算法 1 所示。

表 1　字符与其扩展代码对照表

Tab.1　Character and extended code comparison

字符	扩展代码	字符	扩展代码	字符	扩展代码
e	2	a	4	r	8
i	16	o	32	t	64
n	128	s	6	l	10
c	18	u	34	d	66
p	130	m	12	h	20
g	36	b	68	f	132
y	24	w	40	k	72
v	136	x	48	z	80
j	144	q	96	.	3
,	5	space	1	:	33
!	17	?	9		

接收端在接收到这些序列后,按照约定的协议解码恢复出原始信息。而文字本身并没有存放在套接字的缓存区中,在网络中传输的只是一系列缓存区为空的数据包,而且源/目的 IP 地址和源/目的端口都不同,使得网络中流量分散,让攻击者意识不到有特殊的机密信息传输,即使被截获,在不知道通信双方约定的扩展规则的情况下,机密信息仍然无法被破译,从而达到隐蔽通信的目的。

2) 文件传输模块

文件的隐蔽传输与文字有较大差异,由于不同类型的文件大小差别巨大,若像文字信息一样,在应用层进行二进制编码,会产生长度不可估计的二进制数,在后续转码传输过程中,难以保证其传输的完整性。因此,发送端采用将文件分片后再进行扩展隐蔽传输的方式传输文件。接收端将接收到的数据包以 IP 地址和源端口号为规则进行过滤,将符合套接字序列规则的数据包中的数据信息即子文件片存储在服务器本地。当接收并储存的子文件总数与客户端告知的文件总数相同时,结束本次文件接收任务。最后将所有子文件按照文件名重组,还原出原始文件内容。

由于多媒体文件的类型繁多,且包含的信息量巨大,因此采用分割后分片传输,将所需传输的文件按照固定的大小在本地进行分片处理并将每一片文件的子文件名存入一个数组,再导入 IP 地址编码方案,然后按顺序逐一读取子文件,存入套接字的发送缓存区,并从源 IP 地址池和目的 IP 地址池中随机选取 IP 地址,接着选择所用的端口序列确认方式。服务器端接收到分片传输来的文件后进行重组得到原始多媒体文件。文件传输模块工作流程如图 2 所示。

文件分片处理是文件传输模块至关重要的一步,也是唯一区别于文字

算法 1.IP_Sequence 生成算法

输入:编码字典 chr_dic,消息 message[],地址池 IP_pool

输出:地址序列 IP_Sequence[]

步骤:

```
1:读取消息 m[]
2:while i>=0 do
3:  if m[i]←chr_dic[key]  then value←dic.get(key)
4:    将 value 转换为十位二进制数
5:    对该二进制数从左到右依次编号为 0-9
6:    for j←0 to 9 do
7:      if j ←1 then 在 IP_pool 中选取 j 所对应的 ip 地址
8:        add ip[j] to IP_Sequence[]
9:                else j++
10:      end if
11:   end for
12:  else if m[] == '\0'  then add ipEnd to IP_Sequence[]//添加 ipEnd 作为结束标志
13:      else i++
14:      end if
15:  end if
16:end
```

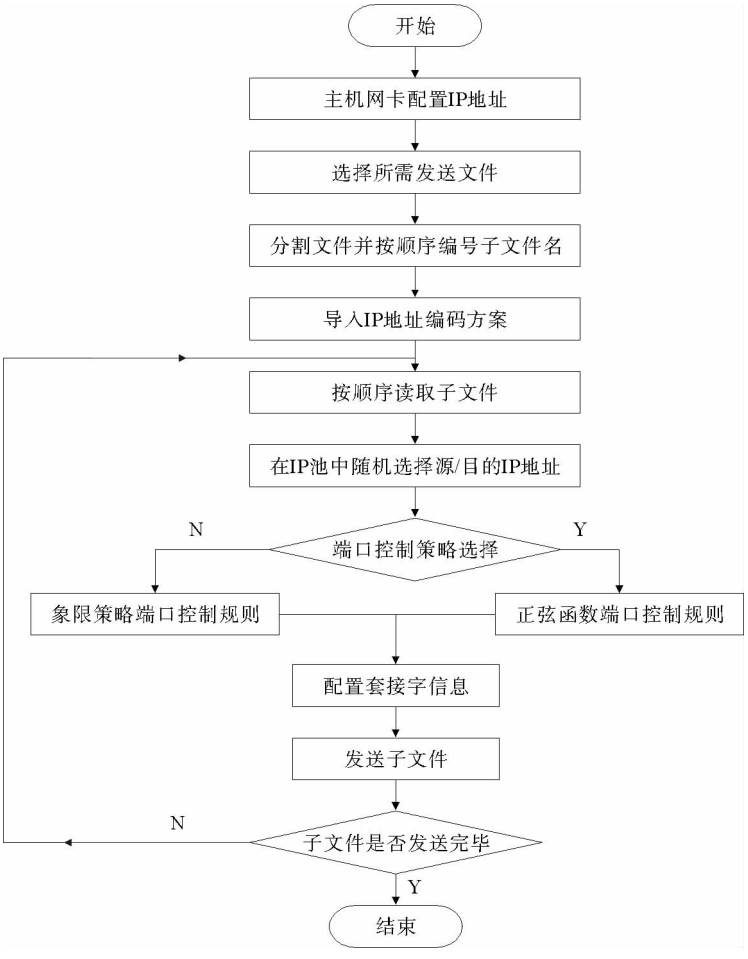

图 2 文件传输流程图

Fig. 2 Flow chart of file transfer

信息的传输。系统中设定小片文件的大小为 2 048 字节,然后按照规定子文件的大小取文件中的内容存入新文件中,并按序号给文件命名,方便后续选择子文件进行发送。当所有文件分片结束后,统计子文件总个数,告知接收端,检查接收到的文件是否齐全。

2.4　基于端址敲门的隐蔽通信技术端口控制策略

主要包括基于象限的和基于正弦函数的端口控制策略。

1) 基于象限的端口控制策略

为了保证端口选取的随机性,源端口号范围限定在 10 000～20 000,当前套接字使用的端口号所在范围决定了下一个套接字的端口号。为防止方案有规律可循,每重复 8 次后重新进行端口选择。象限端口策略相关形式化描述如下:

Port-Quadrant={Port I, Port II, Port III, Port IV},代表端口根据范围划分为 4 个象限。

Port={FirstPort, CurrentPort, NextPort},其中:FirstPort 表示第一个套接字所用的端口号,CurrentPort 表示当前套接字所用的端口号,NextPort 表示下一个套接字所用的端口号。

基于象限的端口控制策略如下:

a) 随机生成 FirstPort 端口号,范围在 10 000～20 000。

b) 若 FirstPort 端口号属于第一象限,则 NextPort 端口号为 NextPort=30 000－FirstPort。若 FirstPort 端口号属于第二、三、四象限,则 NextPort=FirstPort－2 500。

c) 配置下一个套接字信息时,使得 CurrentPort=NextPort,接着判断 CurrentPort 的范围。若 CurrentPort 端口号属于第一象限,则 NextPort 端口号为 NextPort=30 000－CurrentPort。若 CurrentPort 端口号属于第二、三、四象限,则 NextPort=CurrentPort－2 500。

d) 以此类推,直到操作执行 8 次为止。重新选定 FirstPort,继续循环,直至数据发送完毕。

由上可见,端口范围在象限中的变换规律是 I→IV→III→II→I,且一个循环内每个象限之间的端口差值为 2 500。该方法算法简单,系统开销较低,但是当数据量十分庞大时,即使每 8 次重新选定首端口号,源端口之间的规则仍容易被攻击者发现。为了应对大规模数据量的传输,进一步提出基于正弦函数策略的端口控制方案进行机密信息的传输。

2) 基于正弦函数的端口控制策略

本策略使用正弦函数作为序列验证的检验标准。构造正弦函数

$$f(k)=\sin\frac{1}{2}x \ 。 \tag{1}$$

周期为 4π 的无穷函数,推导可得:

$$f(k)=\sin\frac{\pi}{2}(4k)=0 \ , \tag{2}$$

$$f(k)=\sin\frac{\pi}{2}(4k+1)=1 \ , \tag{3}$$

$$f(k)=\sin\frac{\pi}{2}(4k+2)=0 \ , \tag{4}$$

$$f(k)=\sin\frac{\pi}{2}(4k+3)=-1 \ 。 \tag{5}$$

发送端正弦函数的端口控制策略中,随机选择范围在 2 500～14 999 的整数,转换成符合正弦函数取值为“0”、“1”和“－1”的整数作为源端口号。当所传输的信息为端址敲门序列正常信息时,使用使函数结果为 0 的端口号 $4k$ 和 $4k+2$;当所传输信息为标志分隔的端址敲门序列时,使用能使函数结果为 1 的端口号 $4k+1$;当信息传输完毕,需要传输结束端址敲门序列时,使用能使函数结果为－1 的端口号 $4k+3$。为保证源端口的可用范围在 10 000～60 000,k 的取值范围为 2 500～14 999。服务器通过数据包提取出源端口号,代入正弦函数式(1),若所得结果为 0、－1 或 1,则认为数据包合法并按规则把相关信息放入解码序列,否则认为是非法数据包并丢弃。另外,正弦函数控制策略下源端口号的选择范围更大,比象限规则中可使用的端

口范围多 2.5 倍,因此正弦函数策略比象限策略具有更明显的优势。

3 实验与结果

设计实现基于端址敲门技术的隐蔽通信系统,并对其隐蔽性、抗攻击性等各项性能进行实验验证。测试时客户端和服务器都使用 ThinkPad T420 笔记本电脑,系统为 Ubuntu14,内核版本为 Core i5,内存为 2 G,编程语言为 Java。

3.1 隐蔽性能测试结果分析

为了验证系统在传输机密信息时具有隐蔽性,以文字信息为例,分别在普通数据包传输模式、基于正弦函数的扩展传输模式以及基于象限的扩展传输模式下测试网络流量截获的情况,如图 3 所示。

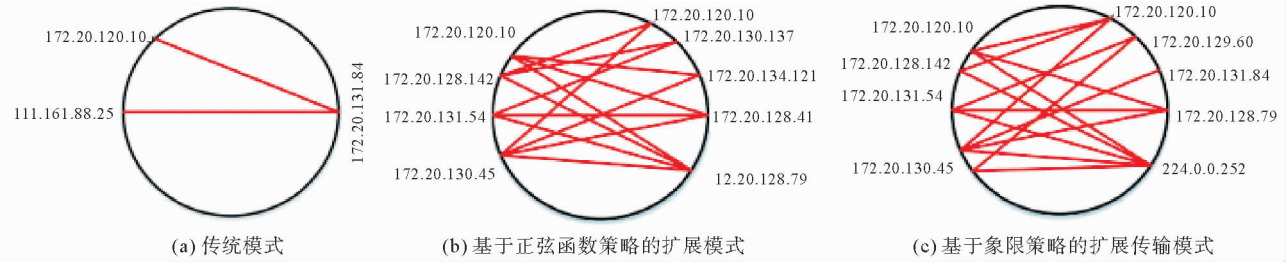

图 3 传输模式的流量情况图

Fig. 3 Flow chart of transmission mode

由图 3 可以看出,传统的端口敲门技术将大量的访问请求发送到单一 IP 地址的若干个端口上,流量目的地集中,攻击者容易察觉到数据通信并确定通信双方主机的地址。采用基于正弦函数以及基于象限的传输模式后,对于每一个数据包而言,都采用单一 IP 地址上的单一端口发送请求到服务器端的某一个 IP 地址上的一个端口。从流量图来看,网络中流量分散,符合正常网络环境,不易引起攻击者注意,能达到传递隐蔽信息的目的。文件传输与文字传输情况类似,不做过多赘述。

3.2 系统性能测试

系统性能主要涉及系统复杂度提高带来的时间损耗、IP 池中每个 IP 地址的使用率以及系统占用端口的分布律对系统安全性的影响。

本部分对基于端址敲门技术的隐蔽通信系统的时间进行测试。由于端址敲门技术在通信过程中需要消耗主机的部分资源,故需要比较 IP 时间型隐蔽通信与本方法在时间消耗上的差异,其中 IP 时间型隐蔽信道设定时间间隔为 10 ms,如表 2 所示。

从表 2 可以看出,与时间型隐蔽通信相比,本系统采用的方法在时间损耗方面具有较明显优势。

表 2 系统时间对比

Tab. 2 System time performance comparison

文件大小	端址敲门隐蔽通信时间/ms	IP 时间型隐蔽通信时间/ms
100 kB	200	1 073
1 MB	998	10 997
5 MB	1 803	55 275
10 MB	4 412	110 343

由于文件模块与文字模块的传输方式大体一致,而基于象限的扩展传输模式与基于正弦函数的传输模式亦基本相同,故仅对基于正弦函数的端口控制策略下发送不同大小文件时各个 IP 地址的使用率进行测试。发送大小为 100 kB、1 MB、5 MB 和 10 MB 的文件,得到 IP 地址的使用率分布如图 4 所示。普通传输模式下,客户端跟服务器端都使用固定 IP 和端口来进行数据的传输,因此 IP 地址和端口使用率都为 100%。

由图 4 可见,由于客户端文件扩展方式的限制,若分片太小,会导致大文件片数过多,导致每个 IP 访问多达 50 多次,影响程序的运行,最终严重影响系统的使用。发送不同大小的文件所占用的源 IP 地址的使用率曲线接近,且分布较为均匀,使得攻击者不易发现流量集中的点。

基于正弦函数和基于象限的两种传输模式的本质区别在于源端口控制策略,下面重点分析端口的使用次数分布和源端口的使用率,分别如图 5～6 所示。

由图 5～6 可得,两种策略的源端口使用分布率十分均衡。与基于正弦函数的扩展传输模式相比,基于象限的控制策略具有明显的缺点:①端口范围小,比正弦函数规则选取端口范围少 40 000 个;②象限规则的端口在 8 个连续数据包之间,容易发现端口之间的关系(相邻两端号相差 2 500),而正弦规则采用随机选取端口的方式,无规律可循。

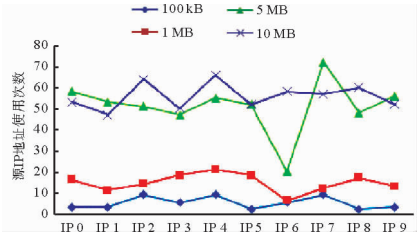

图 4　IP 地址使用次数分布图

Fig. 4　Distribution law of IP address usage

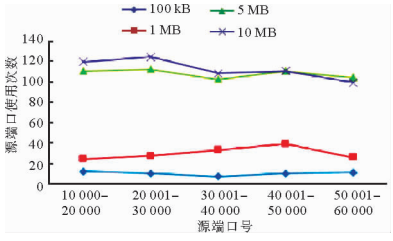

图 5　基于正弦函数控制策略的源端口使用次数分布图

Fig. 5　Distribution law of source port usage based on sine function strategy

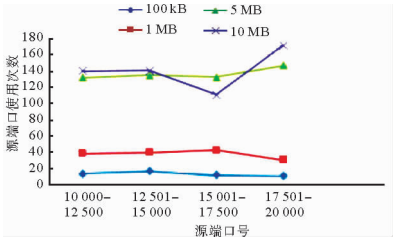

图 6　基于象限控制策略的源端口使用次数分布图

Fig. 6　Distribution of source port usage based on quadrant strategy

3.3　抗攻击性测试

本测试的目的在于提供局域网内机密信息的隐蔽传输,因此攻击者是防范的重要目标。通过抗攻击性测试,判断系统的隐蔽传输被攻击者识破后,是否仍能够继续提供通信服务且机密信息不被攻击者截获。

1) 伪装攻击结果分析

攻击者试图通过用合法 IP 池中的 IP 地址构造数据包,伪装成合法的扩展信息数据包发往服务器,以扰乱服务器的正常接收,使服务器无法正确还原原始信息。实验测试了基于正弦函数的控制策略下发起伪装攻击,WireShark 抓取的数据包结果如图 7 所示。

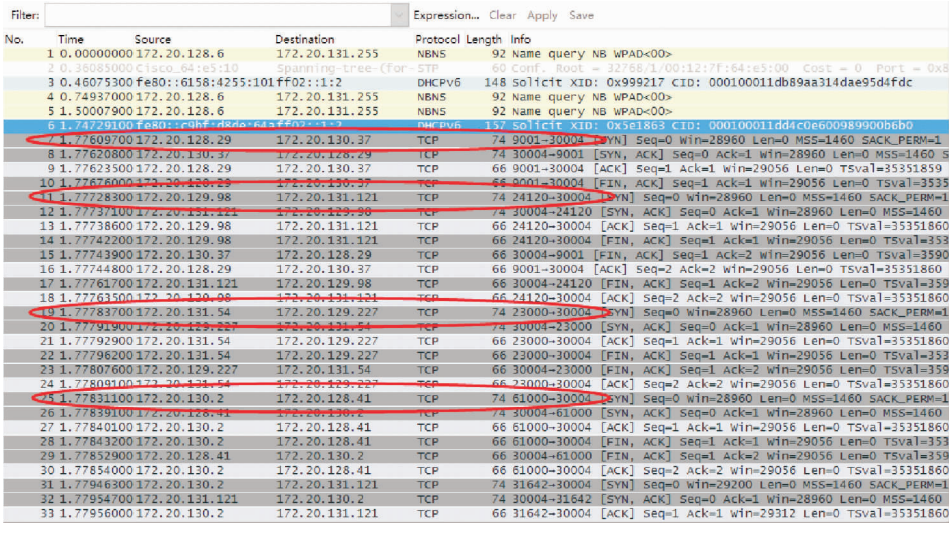

图 7　伪装攻击下信息数据包抓取结果

Fig. 7　Information packet capture result under masquerading attack

由图 7 可见,在正常端址敲门序列中夹杂着攻击者发送的恶意伪装数据包,但这些伪装数据包源端口不符合系统中的正弦函数规则,服务器端不受影响,依然可以还原出原始的文字信息。象限策略与正弦函数策略实验结果相同。

另外,根据式(6)和本测试实际环境可得,发送信息“hello world”时,客户端 IP 地址池中 IP 地址个数为 12 个,可用端口数为 50 000 个,服务端 IP 地址池个数为 10 个,可用端口数为 1 个,端址敲门序列长度为 28。因此伪装攻击完全破译该信息的概率为:

$$p=\left(\frac{1}{12}\times\frac{1}{50\ 000}\times\frac{1}{10}\times 1\right)^{28}=\left(\frac{1}{6\ 000\ 000}\right)^{28}\approx 0\ 。\tag{6}$$

说明本系统具有良好的抗伪装和抗破译性。

2) DoS 攻击结果分析

使用 Syn-Flood 攻击作为 DoS 攻击,攻击速率为 10 240 包/s。由于系统服务器配有 10 个 IP 地址,每个 IP 地址都可以接收数据包,故测试时启动两个 DoS 攻击进程分别发送攻击包到服务器的两个 IP 地址上。DoS 攻击参数如表 3 所示。

表 3 DoS 攻击参数

Tab.3 DoS attack parameters

	伪 IP 地址	攻击目标 IP 地址	攻击目标端口
1	172.20.128.150	172.20.131.121	30 010
2	172.20.128.150	172.20.128.41	30 010

测试时发送字符长度为 150 B 的字符串,在基于正弦函数的扩展传输模式下,攻击者发起 DoS 攻击时,WireShark 抓取数据包结果如图 8 所示。

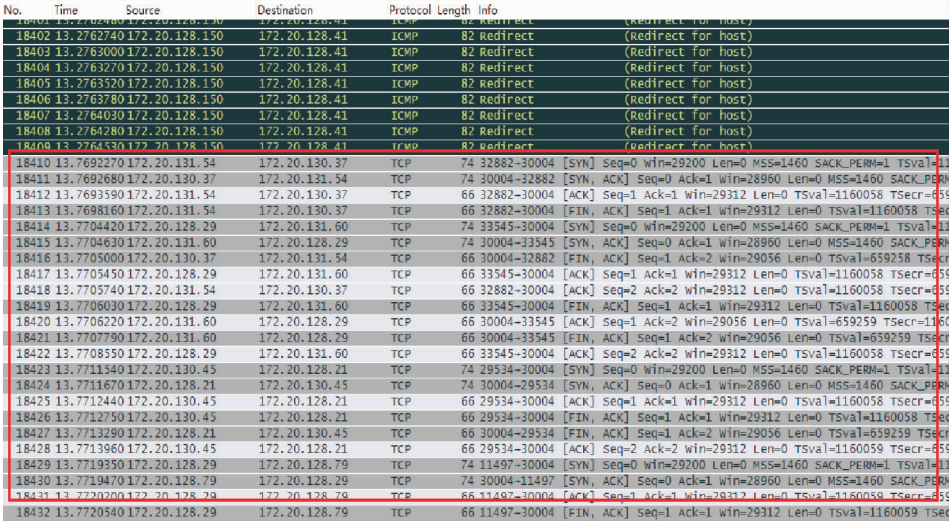

图 8 DoS 攻击下文字信息数据包抓取结果

Fig. 8 Result of text information packet capture under DoS attack

综上,尽管 DoS 攻击的数据包数量十分巨大,通过 WireShark 对 IP 地址的过滤功能,依旧能找到发送机密文字信息所用的数据包,恢复出传输的机密信息。但是当 DoS 攻击的持续时间增长或者单位时间内的攻击包增加时,系统资源将被耗尽,系统失去响应,直至主机死机自动重启。

4 结束语

针对现有的隐蔽通信方式,受端口敲门技术的启发,提出基于端址敲门的隐蔽通信系统,在端口敲门技术的基础上加入 IP 地址,构造一种 IP 加端口的复杂序列实现信息的高隐蔽性传输,提出基于正弦函数的扩展策略与基于象限的扩展策略端口确认规则。实验结果表明,该系统能够高效隐蔽的进行各种类型机密信息的传输,并具有很好的抗攻击效果,能够在一定程度上保护通信双方系统的安全,为随后的信息隐蔽通信提供了新的解决方案。下一步将考虑在信息扩展传输方面与网络跳变服务相结合,通过不断改变通信双方的端址信息,在保证系统隐蔽性的基础上进一步提高其抗 DoS 攻击能力,构建一种基于主动网络防御的隐蔽通信系统。

参考文献:

[1]MAZURCZYK W,CAVIGLIONE L.Information hiding as a challenge for malware detection[J].IEEE Security & Privacy,2015,13(2):89-93.

[2]LAMPSON B W.A note on the confinement problem[J].Communications of the ACM,1973,16(10):613-615.

[3]WENDZEL S,ZANDER S,FECHNER B,et al.Pattern-based survey and categorization of network covert channel techniques[J].ACM Computing Surveys,2015,47(3):502-525.

[4]ZANDER S,ARMITAGE G,BRANCH P,et al.A survey of covert channels and countermeasures in computer network protocols[J].IEEE Communications Surveys and Tutorials,2007,9(3):44-57.

[5]ANAGNOSTOPOULOS M,SEEM J A.Another step in the ladder of DNS-based covert channels:Hiding ill-disposed information in DNSKEY RRs[J].Information (Switzerland),2019,10(9):284.

[6]MAVANI M,RAGHA L.Covert channel in IPv6 destination option extension header[C]// International Conference on Circuits.IEEE,2014,12(5):219-223.

[7]ZANDER S,ARMITAGE G,Brach P.Covert channels in the IP time to live field[J].Network Security Technology & Application,2010,16(6):19-21.

[8]王永杰,刘京菊.基于DNS协议的隐蔽通道原理及性能分析[J].计算机工程,2014,40(7):102-105.
WANG Yongjie,LIU Jingju.Principle and performance analysis of covert tunnel based on DNS protocol[J].Computer Engineering,2014,40(7):102-105.

[9]谭庆丰,方滨兴,时金桥,等.StegoP2P:一种基于P2P网络的隐蔽通信方法[J].计算机研究与发展,2014,51(8):1695-1703.
TAN Qingfeng,FANG Binxing,SHI Jinqiao,et al.StegoP2P:A hidden communication approach in P2P networks[J].Journal of Computer Research and Development,2014,51(8):1695-1703.

[10]王永吉,吴敬征,曾海涛,等.隐蔽信道研究[J].软件学报,2010,21(9):2262-2288.
WANG Yongji,WU Jingzheng,ZENG Haitao,et al.Covert channel research[J].Journal of Software,2010,21(9):2262-2288.

[11]TOMAR N,GAUR M S.Information theft through covert channel by exploiting HTTP post method[J].IEEE on Wireless and Optical Communications,2013,10(2):1-5.

[12]ZHANG L,LIU G,DAI Y.Network packet length covert channel based on empirical distribution function[J].Journal of Networks,2014,9(6):98-105.

[13]MOSKOWITZ I S,MILLER A R.Simple timing channels[C]// IEEE Symposium on Security & Privacy.1994,78(8):56-64.

[14]CABUK S,BRODLEY C E,SHIELDS C.IP covert timing channels:Design and detection[C]// International Conference on Dependable Systems & Networks with Ftcs & Dcc.IEEE Computer Society,2008,145(8):178-187.

[15]李彦峰,丁丽萍,吴敬征,等.区块链环境下的新型网络隐蔽信道模型研究[J].通信学报,2019,40(5):67-78.
LI Yanfeng,DING Liping,WU Jingzheng,et al.Research on a new network covert channel model in blockchain environment [J].Journal on Communications,2019,40(5):67-78.

[16]王昌达,章乐,周从华.二维IP时间隐通道的构建方法研究[J].系统仿真学报,2013,25(10):2285-2293.
WANG Changda,ZHANG Le,ZHOU Conghua.Research on construction method of two-dimensional IP covert timing channels[J].Journal of System Simulation,2013,25(10):2285-2293.

[17]王昌达,黄磊,刘志锋.IP时间隐通道的信息隐藏算法及其性能分析[J].计算机研究与发展,2016,16(5):988-999.
WANG Changda,HUANG Lei,Liu Zhifeng.Information hiding algorithm of IP covert timing channels and its performance analysis[J].Journal of Computer Research and Development,2016,16(5):988-999.

[18]KRZYWINSKI M.Portknocking:Network authentication across closed ports[J].Sysadmin Magazine,2003,1(12):12-17.

[19]SHIRAZ M,BOROUMAND L,GANI A,et al.An improved port knocking authentication framework for mobile cloud computing[J].Malaysian Journal of Computer Science,2019,32(4):269-283.

[20]MAJOR W,BUCHANAN W J,AHMAD J,et al.An authentication protocol based on chaos and zero knowledge proof[J].Nonlinear Dynamics,2020,18(29):1-23.

[21]ALI F,YUNOS R,ALIAS M.Simple port knocking method:Against TCP replay attack and port scanning[C]// International Conference on Cyber Security,Cyber Warfare and Digital Forensic,2012,28(46):247-252.

[22]MEHRAN P,REZA E A,LALEH B.SPKT:Secure port knock-tunneling,an enhanced port security authentication mechanism[C].IEEE Symposium on Computers and Informatics,2012,19(38):156-160.

(责任编辑:傅　游)