一种基于闭源流媒体的隐蔽通讯方法

郭 崎 崔竞松

(武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)

(武汉大学国家网络安全学院 武汉 430072)

摘 要 隐蔽信道代表无法预见的通信方法,其利用授权的公开通信作为隐蔽消息的载体介质。隐蔽通道可以是一种安全有效的传输隐藏在明显流量中的机密信息的方式。已有的基于流媒体的隐蔽信道往往由于建立起了新的通讯链接而容易被监测到。鉴于此,文中对经过流媒体服务器的数据包进行了针对性的测试和研究,研究发现已有的闭源流媒体不对经过服务器的数据包进行严格检查,并发现数据包在修改部分数据后依然可达终端。基于以上事实,文中通过探究经过服务器修改后的数据包的数据位分布规律,建立了一个基于闭源流媒体的隐蔽通道。为了提高数据包的熵值,使用高效且小巧的 speck 算法对数据包的内容进行加密。为了实时监测现有链接和实时流量,文中将防火墙串联在网络结构中,并借助防火墙对网络连接和通讯质量进行监测。实验数据表明,所提方法不会增加网络连接的数目,也不会影响通讯质量,而且能够兼容多种流媒体设备,并且表明了所提方法实用且不容易被检测到。不仅如此,由于此隐蔽信道搭载在闭源流媒体上,隐蔽信息的传输效率较高。上述结果表明,基于现有的闭源流媒体软件的通讯流而建立起隐蔽信道的方法是可行的,且该方法在对数据包的内容进行加密后,具有较强的隐蔽性。

关键词 多媒体流,VoIP,即时通讯,隐蔽通道,流量分析

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.09.021

Covert Communication Method Based on Closed Source Streaming Media

GUO Qi CUI Jing-song

(Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China)

(School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China)

Abstract A covert channel represents an unforeseen method of communication that utilizes authorized public communication as a carrier medium for covert messages. A covert channel can be a safe and efficient way to transmit confidential information hidden in explicit traffic. Existing streaming-based covert channels are often easily detected due to the establishment of new communication links. For this reason, this paper conducted targeted tests and research on data packets passing through the streaming media server. It is found that the existing closed source streaming media does not strictly check the data packets passing through the server, and the data packets can still reach the termina lafter modifying some data. Based on the above facts, this paper established a hidden channel based on closed source streaming media by exploring the data bit distribution rules of the modified data packets through the server. In order to improve the entropy value of the data packet, this paper used an efficient and compact speck algorithm to encrypt the packet content. In order to monitor existing links and real-time traffic in real time, the firewalls were connected in series in the network structure, and the network connection and communication quality were monitored by a firewall. Experimental data show that this method does not increase the number of network connections and does not affect the communication quality, and it is compatible with a variety of streaming media devices, showing that this method is practical and not easily detected. Moreover, since the hidden channel is mounted on the closed source streaming medium, the transmission efficiency of the covert information is high. The above results show that the method of establishing a covert channel based on the communication flow of the existing closed source streaming media software is feasible, and has strong concealment after encrypting the content of the data packet.

Keywords Multimedia stream, VoIP, Instant messaging, Covert channels, Traffic analysis

到稿日期:2018-08-28 返修日期:2018-11-19

郭 崎(1995—),男,硕士生,主要研究方向为网络空间安全,E-mail:1367060166@qq.com;**崔竞松**(1975—),男,博士,副教授,主要研究方向为信息安全、云安全、芯片安全,E-mail:cuijs@qq.com(通信作者)。

1　引言

互联网协议语音（VoIP）是一种允许用户通过互联网连接而不是普通电话线进行语音呼叫的技术。通过 VoIP，可以提供诸如视频呼叫、多部分通信之类的附加服务，这些服务难以通过传统电话提供[1]。随着网络和多媒体编码技术的发展，出现了越来越多的 VoIP 应用。在众多的对 VoIP 的研究中，有对 VoIP 应用的流量进行研究的，如 Dang 等[2]提出了一种 VoIP 流量的分形分析研究，该研究表明呼叫保持时间遵循重尾分布而不是指数分布；Azfar 等[3]研究了 Skype 一类的即时通讯软件的 VoIP 流量是否进行了加密处理。现有对 VoIP 的研究中也有对 VoIP 流量进行识别的，如 Li 等[4]和吕世超[5]分别用不同的方法对 VoIP 流量进行了识别。

与上述的研究思路不同，本文以数据包内容分析为主，以微信和 QQ（包含 TIM）为切入点，用自动化的工具对网络电话多媒体流进行特征分析，根据不同的特征将同一多媒体流的数据包进行分类，从而构建出此多媒体流的特征模型。

由于多媒体应用已成为通过互联网传输的主要流量，大量数据则使其成为隐蔽通信的理想高带宽载体[6-8]，因此在成功建立了多媒体流的特征模型后，作为对此模型的应用之一，本文尝试根据此模型建立一个隐蔽信道。隐蔽信道是一种在用户的正常数据传输中隐藏秘密数据的方法，理想情况下，第三方无法检测到它[9-10]。因此，这种通信方式不是系统原始设计的一部分，但可用于将信息传递给一个进程或用户。传统上，隐蔽信道分为存储和定时信道[11]。存储隐蔽信道涉及隐藏信道发送方写入的存储位置以及接收方通常间接读取的存储位置[12]。当发送方能够以可提供信息的方式调制接收方观察到的响应时间时，可建立定时隐藏信道[13]。

在现有的方案中，有几种较为巧妙且不易被发现的方案：一种是通过延迟的音频数据包提供混合存储定时隐藏信道[14]的方法，该方法也称为 LACK（Lost Audio PaCKets Steganography）方法，如果较为合理地使用 LACK 方法来丢失数据包，则很难被发现。还有研究通过网络传输多媒体中正常或延迟的 B 帧数据包秘密传输数据[15]。此外，Swanson 等[16]对音频、图像和视频的透明数据嵌入和水印技术进行了综述，并探讨了这些技术的可适用性。Zhang 等[17]针对 VoLTE 流量提出了一种分组重排的时序式隐蔽信道，通过秘密信息调制成 VoLTE 流量的 RTCP 分组之间的分组数量来传输消息。而 Mazurczyk 等[18-19]则对 voip 流中的隐写术做了较为全面而详细的阐述。

本文介绍的这种新的隐蔽通道的建立方案属于存储隐蔽信道。在建立好隐蔽信道后，本文对其进行了性能评估。隐蔽信道的性能评估主要基于带宽、可靠性和不可检测性这 3 个特性。带宽或容量由可在媒体中插入的数据量来定义。可靠性即是通过引入公共信道来讨论隐蔽通道对正常通信的影响。不可检测性涉及隐写分析，即识别可疑信息流，确定他们是否隐藏了隐秘数据，并在可能的情况下看是否能恢复隐秘数据。

Mazurczyk 和 Zhao 等的方案设计得精细而复杂，相比较而言，本文基于自主设计的模型而设计的隐蔽信道简单且好用。实验证明，在控制隐蔽信道流量和控制发送数据包频率的基础上，本文所构建的隐蔽信道同样具有可靠性较强、不易被检测的特点。

本文第 2 节介绍如何测量各个多媒体流的特征，并根据不同的特征将同一多媒体流的数据包进行分类，进而构建出多媒体流的特征模型；第 3 节对所构建出的特征模型进行了模型分析；第 4 节根据已建立好的特征模型构建出一个隐蔽通道，并对建立好的通道进行评估；最后总结全文并展望未来工作。

2　隐蔽通道的设计

2.1　可行性探讨

一般情况下，流媒体数据包会经过服务器进行中转，在数据包经过服务器时，服务器又会对数据包进行检测。由于流媒体的数据包流量较大，因此服务器不会对其做耗时较多的完整性校验，只会做一些简单的检测。因此，如果只是改变了数据包中的部分内容，被篡改后的数据包有可能成功经过服务器，从而被接收方接收。

在此假设前提下，为了建立稳定、高效的隐蔽通道，首先需要针对每种闭源流媒体的每个数据包进行内容更改测试，测得这些数据包中能被更改的数据位和不可被更改的数据位，接着针对可被更改的数据位进行截取和添加数据的操作，看其是否依然能被接收到，从而得知隐蔽信息插入数据包的方式。如果可以进行截取和添加数据的操作，则说明只须保持不可被更改的数据位，其他地方可随意填充隐蔽信息，反之，则只能将可被更改的数据位的内容替换为隐蔽信息。通过这样的方式，可以知道怎样在数据包中插入隐蔽信息。

2.2　系统模型

完成内容更改测试后的数据包可进行归类，并生成可用于插入隐蔽信息的模板包。系统模型由通过隐蔽的方式使用这种模板包的发送方和接收方组成。系统的隐蔽信道搭载在正常的语音通话流中，即隐蔽信道的建立并没有产生新的通讯连接，这也是这种隐蔽信道的优势之一。图 1 详细地显示了整个隐蔽信道的系统模型，并显示了从发送端到接收端的数据流。发送方首先将隐蔽消息加密，然后将信息附加在模板包上，最后将其以数据包为单位混杂在正常的通讯流中并发送到接收方。接收方接收到伪造的数据包后将其解密，从而得到秘密传输的信息。为了准确地截获伪造的数据包，需要在伪造的数据包上加上水印，并假设传输双方共享了与水印有关的自定义参数。

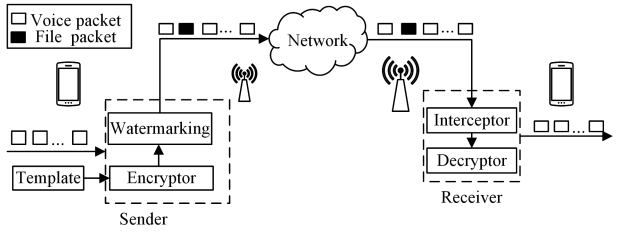

图 1　系统模型图

Fig. 1　System model diagram

2.3　设计准则

1）不可检测性

不可检测性意味着没有有效的算法可以区分合法流量和

隐蔽流量，从定义上讲，如果存在可忽略的函数 $f(\delta)$，对于某些概率多项式时间统计检验 T，测得 $|T(n)-T(n_0)|\leqslant f(\delta)$，则此隐含通道相对于安全参数 δ 是多项式不可检测的[20]。常用的多项式时间统计测试包括 KS 测试、KLD 测试等。本文利用防火墙对实时链接进行检测来评估所提出的隐蔽通道的不可检测性。而根据美国国防部的规定[21]，任何带宽大于 100 bps 的隐蔽通道必须被视为不安全的平均安全要求。此外，为了满足高安全性要求，隐蔽流量应超过 1 bps，故对隐蔽信道的测试会控制其流量在 1～30 bps 之间。

2）鲁棒性

由于本实验针对 VoIP 流建立隐蔽信道，可以用解码误码率（Bit Error Rate，BER）来测定隐蔽信道的鲁棒性，即给定鲁棒性实验参数 ε，使得解码误码率 $P_e\leqslant\varepsilon$。根据实验环境的要求可以选择不同的参数[22]。由于本实验并未涉及编码和解码，因此用数据包流失率（Packet Loss Rate，PLR）来替代解码误码率。

3）音频质量

对于一个借助多媒体流的隐蔽信道而言，保持视音频质量对于不揭示隐蔽信道的存在是重要的。其他指标的检测也需要在保持音频质量的前提下进行分析。因此，为了评估隐蔽信道对正常多媒体流的影响，需要对视音频质量进行测试。

2.4 性能评估准则

隐蔽信道的信道容量如式（1）所示：

$$C=\frac{N_cL_c}{T_c} \tag{1}$$

其中，C 表示隐蔽信道的信道容量，N_c 表示接收到的构造包个数；L_c 表示每个构造包里隐蔽信息的长度；T_c 表示隐蔽通道通讯的时间。因为 L_c 的值相对固定，所以在相同的通讯时间 T_c 下，信道容量主要取决于收到的构造包的个数。

隐蔽信道的丢包率如式（2）所示：

$$PLR=\frac{N_t-N_c}{N_t} \tag{2}$$

其中，PLR 表示丢包的概率，N_t 表示传输的构造包的数量或者发送方发送的构造包的数目。丢包率主要取决于两个因素，即隐蔽通道传输过程中的传输效率和接收方接收数据包的效率。

由上述公式可得出发包速率的公式：

$$S_t=\frac{N_t}{T_c} \tag{3}$$

3 实现方案

要使接收方能够接收到发送方发送的构造包，发送方和接受方必须在通讯上达成一致，以便接收方在正常接收语音包的同时能区分出隐蔽信息。为了达到这个目的，需要给发送的构造包添加水印，此时接受方需要对每一个数据包进行水印检测，以识别出构造包。在发送方和接受方达成一致后，首先需要进行多媒体数据流的特征分析，然后将隐蔽信息写入分析出的数据包模板中，以搭建基于闭源多媒体流的隐蔽信道。

3.1 多媒体数据流的特征分析

识别多媒体流的特征的主要步骤如下：

1）随机截取 500 个数据包，并根据数据包内容的第一个字节将同一个通讯流的数据包分成多个类别。第一字节一样的数据包为同一类数据包。

2）识别出各类数据包中可更改的部分和不可更改的部分。用 k 来表示数据包的种类，用 x_i 来记录数据包中不能被更改的数据位的下标，用 l_k 表示第 k 类数据包中下标最大的不可被更改的数据位的下标值，用 m_k 表示第 k 类数据包中下标最小的不可被更改的数据位的下标值。发送方从通讯的多媒体流中截取样本，并将样本的数据包内容修改后发送给接收方，接收方通过判断是否接收到了相应的修改包来确定数据包的相应部分能否被修改。由此可见：

$$l_k=\max_i x_i,\ i=0,1,2,\cdots,N \tag{4}$$

$$m_k=\min_i x_i,\ i=0,1,2,\cdots,N \tag{5}$$

通常情况下，l 可以作为可更改部分和不可更改部分的分割点。

3）分别对每个类别进行添加数据和截取数据的操作。此处用 C_j 来表示第 j 个包是否能被修改，初始化 C_j 为 0，测得此属性需要进行如下几个步骤：①在两端建立水印添加和识别机制；②发送方往接收方发送指令包，该指令包中包含了要更改的数据位 i、水印添加位置偏移 s 以及进行的操作 c（1 为截取，2 为添加，3 为截取和添加，用二进制表示）；③发送方发送修改后的数据包；④接收方在接收到指令包后，根据 s 值对数据包做水印识别，以检验修改后的数据包是否能被接收到。如果成功接收到，则：

$$c_j=c_j\oplus c \tag{6}$$

3.2 隐蔽通道的建立

3.2.1 模板的使用和应用的适配

通过多媒体流数据包的特征分析可以得到数据包模板，数据包的模板类似于图 2，模板的第 1 位是标识位，$1-l$ 为有意义的数据位，l 以后的数据位为隐蔽信息填充位。隐蔽信息的填充方式有两种：填充在所有可以被更改的数据位中；填充在隐蔽信息填充位中。由于不清楚在有意义的数据位中填充隐蔽信息将对通讯产生怎样的影响，因此在隐蔽信息填充位中填充隐蔽信息是一个比较理想的选择。

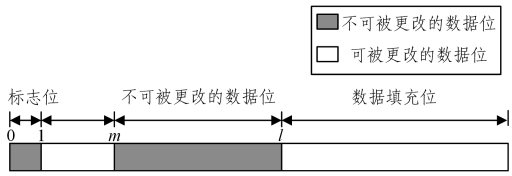

图 2 数据包模板示意图

Fig. 2 Schematic diagram of packet template

需要注意的是，不同的应用会有不同的数据包模板，因此在实现隐蔽通道时需要对不同的应用做适配操作。

3.2.2 加密

基于效率和安全性的考虑，本文用 32 位的 speck 算法对加了隐蔽消息的数据包进行加密，而对正常通讯的数据包不做任何处理。由于无法保证信息在隐蔽信道中传输的可靠性，因此采取预置密钥的办法。成功建立隐蔽信道后，用密钥协商的方式更新密钥。

3.2.3 加水印

用循环冗余校验的方式来对数据包进行水印添加，循环冗余校验主要用于检测或校验数据传输或者保存后可能出现

的错误。32 位的循环冗余校验具有低碰撞概率，因此借助这种方式，接收方能够轻易识别出构造包。首先将整个数据包进行循环冗余校验，然后将所得的 4 位校验码和数据包最后 4 位进行异或，并将所得值存放在数据包的尾部。因为部分通讯软件会改变数据包的内容，所以循环冗余校验的数据位部分在不同的流媒体中会有差别，为了使接收方能够准确接收数据包，需要先发送类似协议包的数据包去通知接收方此次校验需要校验的位数 $bitn$ 以及初始校验值 IV。

3.2.4　识别水印和解密

接收方首先需要通过接收到的协议包识别出 $bitn$ 和 IV 值，然后根据这两个值用循环冗余检验的算法对数据包进行校验值计算，若校验值为 0，则此数据包为构造包，若校验值不为 0，则将此数据包当作正常通讯包，不对其进行处理。采取先识别水印、后解密的方式对数据包进行处理，当识别出此数据包是构造包之后，再用密钥进行解密。

4　实验结果和分析

4.1　环境的搭建与配置

本文所提的隐蔽信道适用于多种流媒体软件和不同的手机，由于本文所提方案中隐蔽信道是搭载在流媒体上的，因此设备间只要能进行流媒体通讯，再用合适的方式搭建隐蔽通道，此方案就能成功实现。实验中，使用了 1 部 iphone5 手机和 1 部 iphone6 手机作为两个终端，分别对微信语音和 qq 语音进行了隐蔽信道的搭建和性能测试。

为了成功截取到通讯的数据包并对其内容进行分析，实验采用了自主开发的流量分析程序，此程序用 C 语言开发，在 linux 环境下运行，可以搭载在网络设备上，可以截取数据包和主动向多媒体流发送数据包，并且可以对数据包进行基本操作。

4.2　多媒体数据流的特征

实验中，分别对 QQ 和微信做了 4 次通话测试，记录了语音通话中各种类型的数据包的数量，结果如表 1 所列。由表 1 可知，qq 有 3 种标志位（即数据包内容的第一位），分别为 0x5b，0x28 和 0x02，其中大部分数据包的标识位为 0x5b，约占 QQ 语音通讯流量的 97.5%。WeChat 有两种标志位，即 0x75 和 0xd5，标志位为 0x75 的数据包约占 WeChat 语音通讯流量的 99.1%。一共有 5 类数据包。

表 1　4 次实验的数据统计表

Table 1　Data statistics table of four experiments

通讯软件	QQ			WeChat	
标识位种类	0x5b	0x28	0x02	0x75	0xd5
第一次实验	12817	403	0	12636	114
第二次实验	11782	31	194	12454	113
第三次实验	12714	412	0	12641	114
第四次实验	11768	43	184	12621	112

接下来根据 3.1 描述的方法对流媒体的数据包进行特征分析，结果如表 2 所列。从表 2 可知，标识位为 0x5b 的数据包的第 9 位到第 12 位不可更改，标志位为 0x75 的数据包的 0－12 位不可被更改，其他类型的数据包则是所有数据位不可被更改，或者说更改后接收方接收不到。在具体的实验中，标志位为 0x28 的数据包被更改后，有时所有的更改后的测试包都可收到数据包，有时则都收不到，具体原因不明。例如，对于标识位为 0x28 的数据包，根据算法可知，$l=+\infty$，$m=0$，即将其归为所有数据位均不可被更改一类，可保证根据表 2 的结论修改数据包的某数据位内容后，接收方依然能接收到被更改的数据包。为了验证当数据位 $x>1$ 或 $x<m$ 时所有数据位均可被更改，可以保持 $m\leqslant x\leqslant l$ 的数据位不变，用随机数填充除了标识位的其他数据位的内容，再根据接收方是否接收到更改后的数据包进行验证。

表 2　不同数据包的特点

Table 2　Characteristics of different data packets

流标识	数据包特点	其他特征
0x5b	$l=12, m=9, c_j=3$	包长 72
0x28	$l=+\infty, m=0, c_j=0$	
0x02	$l=+\infty, m=0, c_j=0$	
0x75	$l=12, m=0, c_j=3$	包长 82
0xd5	$l=+\infty, m=0, c_j=0$	

同样地，可以从表 2 中得到标识位为 0x5b 和 0x75 的数据包并对其进行添加数据和截取数据的操作，其他类别的数据包则不能进行此类操作。在截取数据包内容的实验中，设定 l_k 为截取位，即只发送数据位 0-l_k 的数据，以接收方是否能收到数据来判定此类数据包能否被截取。在添加数据包的实验中，将长度随机、有随机内容的数组添加到上述被截取的数据包中，在添加完实验用的水印后，依据接收方是否能收到更改后的数据包来判断此类数据包是否能进行添加数据操作。

在构造数据包时，QQ 选择标志位为 0x5b 的数据包作为模板数据包，WeChat 则选择标志位为 0x75 的数据包作为模板数据包（模板数据包如图 2 所示），然后在数据填充位上填充隐蔽信息。由于这两种模板包是可以截取且可以添加数据的，因此数据填充位的长度是可变的。在添加完隐蔽信息后，加密信息并为其添加上水印，最后将此数据包插入到正常通讯流中。接收方则根据水印判断数据包是否为隐蔽数据包，将此数据包识别出来后再解密，即可得到隐蔽信息。

4.3　不可检测性

通过在软路由上搭载防火墙，并监测实时的流量，可分析此隐蔽通道是否可测。

为了说明此方案并未增加新的连接，在实验中分别对 QQ 和微信测试了在同一语音连接下加入隐蔽通道前后的流量，单位是 bps，并设置 S_t 为 20 000 bps。流量时序图如图 3 和图 4 所示，经过粗略的统计分析后得到表 3，在 56 个时间段内，加入隐蔽信道后的 QQ 语音流量显著大于正常通信的 QQ 语音流量，由于方差值几乎相同，可以认为这是同一个连接。微信的流量分布情况也大致如此，只是分布更加集中，方差更小，同时也说明了微信的通讯连接情况更加稳定。这足以说明此方案并未增加新的通讯连接，当 S_t 控制在 100 bps 以下时，难以被防火墙识别。

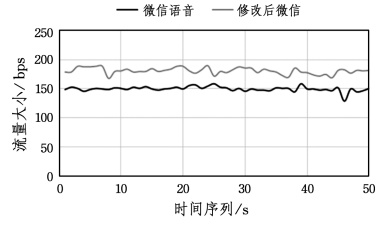

图 3　QQ 语音流量图

Fig. 3　QQ voice traffic diagram

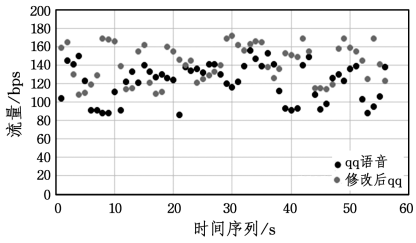

图 4 微信语音流量图

Fig. 4 WeChat voice flow graph

表 3 各次实验的均值和方差值

Table 3 Mean and variance of each experiment

实验次数	正常 qq	修改后 qq	正常微信	修改后微信
均值/bps	121600	142500	150120	181020
方差值	20.38	20.14	4.31	5.49

4.4 鲁棒性

数据包的丢失率 PLR 主要与两个因素有关：网络状况和接收方的数据处理能力。实验中采用了不同的发包速率来测试数据包的传输质量，共发送 10000 个数据包，每个数据包的内容大小为 100 B，在 5 种情况下测量 6 次数据，然后对这些数据取均值（如图 5 中黑色部分所示）。为了使数据更具说服力，需要去除每次测验最小的数据值，并重新取其均值（如图 5 中灰色部分所示）。结果显示，当 S_t 小于 80000 bps 时，由于网络偶尔有阻塞，依然会有漏包的情况发生，网络正常时都能收到；当 S_t 大于 80000 bps 时，PLR 显著增大，说明接收方的数据处理能力达到了上限。经计算可知，接收方的数据处理能力为 82400 bps。即当 S_t 小于 82400 bps 时，PLR 值较小；当 S_t 大于 82400 bps 时，PLR 值随着 S_t 的增大而增大。由于每个数据包的内容大小为 100 B，因此隐蔽信道的传输容量为 10 MB/s，高于 100 bps 的安全隐蔽信道的带宽要求。

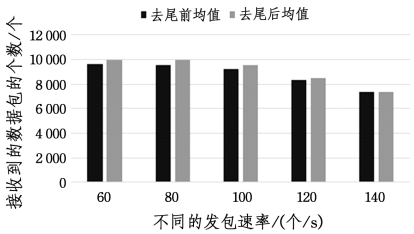

图 5 不同发包速率下的数据包接收数量统计图

Fig. 5 Statistics of number of packets received at different packet transmission rates

4.5 声音质量

实验用平均意见得分（Mean Opinion Score，MOS）来评定对话中声音的质量，实验结果如表 4 所列。每个数据包的内容的大小为 100 B，由实验结果可知，当 S_t 为 800 bps 时，声音的质量与正常通话时的几乎相同，说明此时隐蔽信道对通话质量并无显著影响，而当 S_t 大于 12000 bps 后，声音质量显著开始下降，这是因为本文所提出的隐蔽信道并未篡改语音包，只是增加了信道的拥塞程度而已，故当隐蔽信道容量较小时对通话质量的影响并不大。

由于隐蔽道存在于已有的语音连接中，因此隐蔽信道容量较大会影响正常语音通道的拥塞程度，进而影响通话质量。

表 4 mos 值和方差值

Table 4 Mos value and variance value

实验次数	正常通信	$S_t=1$	$S_t=5$	$S_t=10$	$S_t=15$	$S_t=20$
MOS 值	4.4	4.3	4.1	3.9	3.5	2.7
方差值	0.39	0.47	0.51	0.44	0.37	0.42

结束语 本文为了在建立隐蔽通道时不产生新的通讯连接，首先探究了通过服务器修改后的数据包的数据位分布规律，然后在此基础上建立了一个基于闭源流媒体的隐蔽通道。通过对此隐蔽通道的不可测性、鲁棒性和声音质量的研究，可以发现，所建立的隐蔽信道在发送构造包速率较小的情况下不易被发现。在以上研究的基础上，未来可以从以下几个方面继续进行研究。首先，可探究此方法的通用性，即可以对更多的流媒体软件进行数据分析，建立数据包模型，看是否能建立稳定且不易被识别的隐蔽信道。其次，就此隐蔽信道本身而言，可以通过提高伪造包的识别速率的方法进一步增强此隐蔽信道系统的稳定程度和通信效率。

参 考 文 献

[1] MAZURCZYK W. VoIP Steganography and Its Detection-A Survey[J]. ACM Computing Surveys, 2012, 46(2): 1-21.

[2] DANG T D, SONKOLY B, MOLNÁR S. Fractal analysis and modeling of VoIP traffic[C]// 11th International Telecommunications Network Strategy and Planning Symposium. Vienna: IEEE, 2004: 123-130.

[3] AZFAR A, CHOO K K R, LIU L. A study of ten popular Android mobile VoIP applications: Are the communications encrypted? [C]// 2014 47th Hawaii International Conference on System Sciences. Waikoloa: IEEE, 2014: 4858-4867.

[4] LI B, MA M, JIN Z. A VoIP traffic identification scheme based on host and flow behavior analysis[J]. Journal of Network and Systems Management, 2011, 19(1): 111-129.

[5] LV S C. Content filtering and analysis of instant messaging systems [D]. Chengdu: University of Electronic Science and Technology of China, 2012. (in Chinese)
吕世超. 即时通信系统内容过滤和分析研究[D]. 成都：电子科技大学，2012.

[6] WANG H T, FU Y. Instant Communication—Principles, Technologies and Applications[J]. Information and Communication-Technology, 2010, 4(3): 34-40. (in Chinese)
王海涛，付鹰. 即时通信——原理、技术和应用[J]. 信息通信技术，2010，4(3)：34-40.

[7] ZHENG L F, XIN Y. Analysis and Implementation of Instant Messaging Software Protocol Based on DPI[J]. Information Network Security, 2016(1): 51-58. (in Chinese)
郑丽芬，辛阳. 基于 DPI 的即时通信软件协议分析与实现[J]. 信息网络安全，2016(1)：51-58.

[8] JIA Z X. Design and implementation of real-time chat tool based

on IOS system [D]. Beijing: University of Chinese Academy of Sciences, 2015. (in Chinese)
贾侦修. 基于 IOS 系统的即时聊天工具的设计与实现[D]. 北京：中国科学院大学，2015.

[9] LI L P, WANG J H. Secret Communication Using Covert Channels in Network Transmission [J]. Computer Science, 2009, 36(5): 115-117. (in Chinese)
李丽萍，王建华. 网络传输中采用隐蔽通道实现秘密通信[J]. 计算机科学，2009，36(5)：115-117.

[10] YAN Y X. Research on an instant messaging system based on UDP protocol [D]. Dalian: Dalian Maritime University, 2008. (in Chinese)
燕永新. 一种基于 UDP 协议的即时通信系统的研究[D]. 大连：大连海事大学，2008.

[11] WANG Y G, WU J Z, ZENG H T, et al. Research on Covert Channel [J]. Journal of Software, 2010, 21(9): 2262-2288. (in Chinese)
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.

[12] DONG L P, CHEN X Y, YANG Y J, et al. Implementation and Dection of Network Covert Channel [J]. Computer Science, 2015, 42(7): 216-221. (in Chinese)
董丽鹏，陈性元，杨英杰，等. 网络隐蔽信道实现机制及检测技术研究[J]. 计算机科学，2015，42(7)：216-221.

[13] CABUK S, BRODLEY C E, SHIELDS C. IP covert timing channels: design and detection[C]// Proceedings of the 11th ACM conference on Computer and communications security. New York: ACM, 2004: 178-187.

[14] MAZURCZYK W, LUBACZ J. LACK－a VoIP steganographic method[J]. Telecommunication Systems, 2010, 45(2/3): 153-163.

[15] ZHAO H, SHI Y Q, ANSARI N. Hiding Data in Multimedia Streaming over Networks[C]// 2010 8th Annual Communication Networks and Services Research Conference. Canada: IEEE, 2010: 50-55.

[16] SWANSON M D, KOBAYASHI M, TEWFIK A H. Multimedia data-embedding and watermarking technologies[J]. Proceedings of the IEEE, 1998, 86(6): 1064-1087.

[17] ZHANG X, LIANG C, ZHANG Q, et al. Building covert timing channels by packet rearrangement over mobile networks[J]. Information Sciences, 2018, 445-446: 66-78.

[18] MAZURCZYK W, SZCZYPIORSKI K. Steganography of VoIP streams[C]// OTM Confederated International Conferences On the Move to Meaningful Internet Systems. Berlin: Springer Heidelberg, 2008: 1001-1018.

[19] MAZURCZYK W. Lost audio packets steganography: the first practical evaluation[J]. Security and Communication Networks, 2012, 5(12): 1394-1403.

[20] ZHANG X, TAN Y A, LIANG C, et al. A Covert Channel Over VoLTE via Adjusting Silence Periods[J]. IEEE Access, 2018, 6: 9292-9302.

[21] LATHAM D C. Department of defense trusted computer system evaluation criteria: DoD 5200. 28-STD [S]. Department of Defense, 1985.

[22] REZAEI F, HEMPEL M, SHARIF H. Towards a reliable detection of covert timing channels over real-time network traffic[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(3): 249-264.