第 35 卷 第 1 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.1 Computer Engineering January 2009
·网络与通信· 文章编号：1000—3428(2009)01—0105—03 文献标识码：A 中图分类号：TP393.0

基于平滑估计算法的网络隐蔽时间信道同步

郭 强，潘 理，李建华
(上海交通大学电子政务工程中心，上海 200240)

摘 要：研究网络隐蔽时间信道，针对已有隐蔽时间信道同步方法的不足提出一种基于平滑估计算法的同步方法，使发送方以块为单位发送数据，接收方通过平滑估计算法估计接收下一个报文需要的时间间隔。实验结果证明，在一定环境下，与原有方法相比，该方法使无差错传输所需报文间的时间间隔较短，在相同的无差错情况下，其数据传输速率提高了 33%。

关键词：网络隐蔽时间信道；同步；平滑估计算法

Synchronization of Network Covert Time Channel Based on Smoothing Estimation Algorithm

GUO Qiang, PAN Li, LI Jian-hua
(E-government Research Center, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 This paper studies the network covert timing channel, aiming at the defect of existing synchronization method of covert timing channel and presents a new synchronization method based on smoothing algorithm. The sender sends data in blocks and the receiver estimates the time interval for receiving the next packet by synchronization method. Experimental results demonstrate that under certain circumstance, compared with previous methods, this method needs shorter inter-packet interval to receive data with no error and increases the speed for data transmission by 33%.

【Key words】 network covert time channel; synchronization; smoothing estimation algorithm

1 概述

在网络隐蔽时间信道中，信息的传递通过每个时间间隔内发送与接收的报文个数来表示。报文在网络上传输时，必须经过一定数量的转发设备，如路由器、交换机、防火墙等。上述设备会增加报文延时，导致其无法在预定时间间隔内到达。利用隐蔽时间信道进行信息传送的双方需要某种机制对报文的收发时间间隔进行同步。

文献[1]提出适当增大收发时间间隔以减小报文延时变化造成的影响。文献[2]提出起始帧、时间间隔调整和沉默间隙等方法，并在此基础上实现网络隐蔽时间信道。但网络情况的复杂性导致上述方法不能处理所有情况下收发双方的同步问题。平滑估计算法最早出现在TCP协议中，被用于RTT测量[3]。该算法可以去除RTT样本的随机抖动。本文将该算法用于网络隐蔽时间信道，实现对接收时间间隔的动态调整，完成收发双方的同步。

2 网络隐蔽时间信道的分析

2.1 网络隐蔽时间信道的原理

网络隐蔽信道利用网络泄漏信息，违反了系统安全策略但很难被检测到[2]。按其实现原理，文献[4]将网络隐蔽信道分为 18 种，其中包括隐蔽时间信道。

网络隐蔽时间信道模型如图 1 所示。发送方将隐蔽信息C传送到接收方的过程如下：先对隐蔽信息进行编码，然后将编码后的信息调制到需要发送的报文 P_k 上，并将报文发送出去。调制是指控制单位时间间隔内发送的报文数。接收方检查每个时间间隔内收到的报文数，并对报文进行解码以获得隐蔽信息[1,5]。报文在网络上传递时，其延时受网络状况的影响。因为接收方在某个时间间隔内接收到的报文数与发送方发送的报文数不相同，所以接收方提取出来的隐蔽信息 C^* 与发送的隐蔽信息C也不相同。可见，隐蔽信息的传递是通过某个时间间隔内报文发送与到达的个数来表示的，这种报文的收发方式构成了网络隐蔽时间信道，如图 1 虚线部分所示。

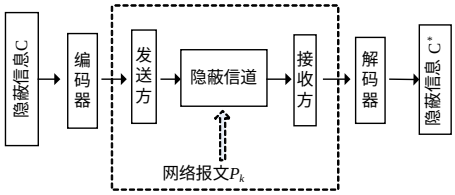


图 1 网络隐蔽时间信道模型

当信息被编码成二进制比特流时，网络隐蔽时间信道成为一个二进制信道，如图 2 所示。利用隐蔽时间信道进行通信的双方预先约定一个收发时间间隔和通信的开始方式(例如确定第 1 个发送的报文)。在每个时间间隔内，发送方发送一个报文表示为发送了比特 1，没有发送报文表示为发送了比特 0。接收方在每个时间间隔内检测是否有报文到达，如果接收到一个报文就认为收到了比特 1，若没有收到报文则认为收到了比特 0。本文研究上述二进制信道中的同步问题。

基金项目：国家“863”计划基金资助项目(2007AA01Z457)；上海市科学技术委员会基金资助项目(07QA14033)
作者简介：郭 强(1982－)，男，硕士，主研方向：网络通信，网络安全；潘 理，副教授；李建华，教授、博士生导师
收稿日期：2008-04-12 **E-mail：**guo.qiang.joe@gmail.com

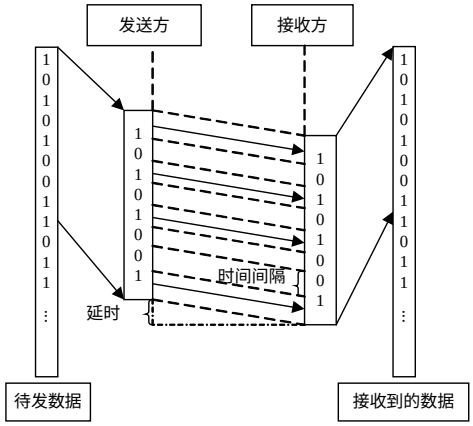


图 2　网络隐蔽时间信道的基本原理

2.2　网络状况对网络隐蔽时间信道的影响

由于网络负载以及报文在网络上所经转发设备的工作状况是不断变化的，因此报文到达接收方的延时存在变化，可能造成报文丢失。在某个时间间隔内，接收方应该收到一个报文并认为收到了比特 1，报文丢失将导致接收方认为收到了比特 0。隐蔽信息的发送方和接收方之间的网络状况可能发生突然的变化，比如某个路由器重新启动，此时某个报文会重新选择路由，它会晚于预定时间到达接收方。本文称上述情况为突变。在某段时间内，可能整个网络的业务逐渐变繁忙，在网络重新到达一个稳定状态之前，报文的延时逐渐增大。这会使接收方的同步误差逐渐积累，最终导致同步完全出错。本文称上述情况为渐变，如图 3 所示。

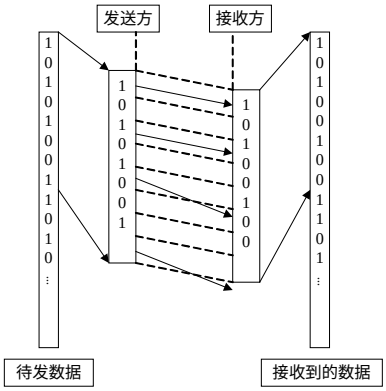


图 3　渐变引起的错误

由报文丢失和突变引起的错误并不影响后续信息的接收，位与位之间仍然是同步的。这种错误可以通过对发送的数据进行差错编码得到纠正。由渐变引起的错误发生后，位与位之间的同步已经发生了错误，接收方无论以何种方式都不能完全还原接收到的数据。本文主要讨论由渐变引起的错误，研究如何防止失步的发生。

3　平滑估计算法

3.1　网络隐蔽时间信道中平滑估计算法的依据

网络状况的变化导致报文到达接收方延时的变化，而该延时的变化则反映了网络状况的变化。平滑估计算法利用相继到达报文的时间间隔反映了网络状况变化这一特点，实现对接收时间间隔的动态调整。

网络隐蔽时间信道中的信息传输是单向的[5]，收发双方没有一致的系统时钟，且其数据传输具有突发性。因此，在网络隐蔽时间信道中，信息的传输属于异步传输，其同步属于异步传输中的同步。本文在实现隐蔽时间信道时采用块模式传输方式对数据进行发送和接收，具有如下优点：

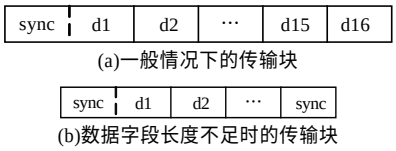
(1)传输块中包含同步字段，有利于收发双发的同步。

(2)传送完每个块后，收发双方利用同步字段进行重新同步，可以避免同步误差的积累。

3.2　隐蔽时间信道中的传输块

在设计中，传输块包含同步字段和数据字段。同步字段的引入主要是为了让接收方能确定其基本接收时间间隔，它的每个比特都设为 1。这是因为在一定时间内，如果发送方连续发送若干个比特 1，那么接收方连续接收到若干个报文。这些报文相继到达的时间间隔是发送时间间隔与报文延时变化之和。可以先计算这些时间间隔的平均值，然后根据后续到达报文的时间间隔对该平均值进行调整，并利用调整后的值来检测报文是否到达。本文进行了相关实验以确定同步字段的长度。通过实验发现，在本文所讨论的环境下，当接收方收到第 6 个报文后，报文之间时间间隔平均值的变化已经接近稳定。为了在字节上对齐，本文将同步字段定为 8 bit。数据字段长度为 16 Byte。

在图 4(a)所示的传输块中，sync 字段占一个字节，其每个比特都固定为 1。d1, d2,…, d16 表示需要传输的数据，长度为 1 Byte。在一次数据传输中，需要传输的数据总长度可能小于 16 Byte，此时在数据字段末尾增加一个 sync 字段，以标志传输块的结束，如图 4(b)所示。



(a)一般情况下的传输块

(b)数据字段长度不足时的传输块

图 4　隐蔽时间信道中传输块的格式

3.3　平滑估计算法的描述

平滑估计算法以传输块的格式为基础。在算法描述中，报文指隐蔽时间信道中作为隐蔽信息载体的 UDP 报文。平滑估计算法步骤如下：

(1)接收方确定接收时间间隔。收发双方以传输块为单位收发数据。接收方观测前 9 个报文的到达时间(第 1 个报文表示传输块的到来，并不是第 1 个比特)，并记录每个报文之间的时间间隔，分别记为 $T_1, T_2, \cdots, T_8$。对记录的时间间隔进行算术平均，记为 $T_{\exp}$，即

$$T_{\exp} = \frac{T_1 + T_2 + \cdots + T_N}{N}, N = 8 \tag{1}$$

$T_{\exp}$ 反映了发送方的发送时间间隔和当前网络状况下报文的平均延时，接收方将在这个时间间隔内检测下一个报文是否到来。

(2)接收时间间隔的更新。接收方在接收数据字段时，每接收到一个报文就计算该报文到达时间与上一个接收时间的差值，记为 T_{new}，并进行如下运算：

$$T_{\exp} = (1-a)T_{\exp}^{'} + aT_{\text{new}} \tag{2}$$

其中，a 是平滑因子；$T_{\exp}^{'}$ 为当前接收时间间隔，接收方将在 $T_{\exp}$ 内检测下一个报文是否到达；T_{new} 反映了网络的变化情况。a 越大，接收方对网络变化的反应越灵敏。a 值应根据网络状况进行调节。

如果接收方在当前接收时间间隔内没有收到报文，则 $T_{\exp}$ 保持不变，即

$$T_{\exp} = T_{\exp}^{'} \tag{3}$$

(3)接收数据的检查。接收方每收到一个字节的数据，就检测该字节是否与 sync 字段相同。若相同则结束该传输块的接收，若不同则继续接收数据。

由上述算法步骤可以看出，接收方每收到一个报文后，就对下一个接收时间间隔进行动态调整。该调整反映了网络状况的变化，减小了数据传送过程中的同步积累误差。在接收下一个传输块时，接收方利用传输块的同步字段进行重新同步，彻底消除了同步累积误差。

4 隐蔽时间信道实验

在本文实验中，发送方发出的报文在到达接收方前须经过 6 个路由器，实验的收发程序运行在 Fedora6 上。

4.1 传输块的格式中同步字段长度的选择

在传输块中，同步字段的长度会影响通信质量和速度。如果同步字段太短，计算出来的基本时间间隔将不能很好地反映发送时间间隔和网络上报文延时的变化。若同步字段过长，通信中的数据冗余就会增加。因此，必须根据实际网络状况来确定同步字段的长度。实验步骤如下：

(1)发送方连续发送 1 000 个报文，每个报文之间的发送时间间隔相同。在每个报文到达后，接收方计算前面所有报文之间时间间隔的平均值。

(2)发送方改变报文的发送时间间隔，并重复第(1)步。

(3)将接收到报文后计算出来的平均值减去发送时间间隔，以进行比较。

实验结果如图 5 所示，可以看出，接收方从收到第 6 个报文(第 5 个时间间隔)开始，报文之间时间间隔平均值的变化限制在-40 μs~30 μs 之间。即使继续增加时间间隔数量，该范围也不会明显变窄，且此时计算出来的结果已足够理想，误差在 2%之内。因此，在设计传输块格式时，同步字段长度定为 8 bit 即可。

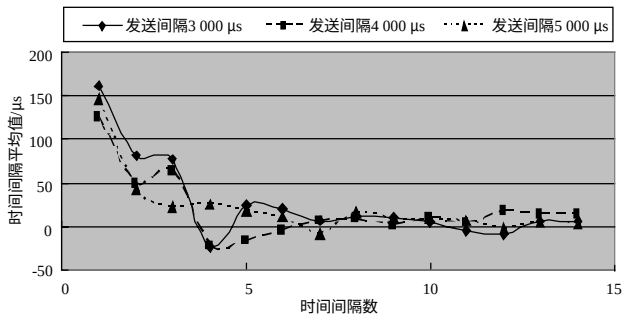


图 5 连续到达报文时间间隔平均值的变化

4.2 平滑估计算法的性能

为了更好地了解平滑估计算法性能，本文对平滑估计算法与沉默间隙法进行比较。

实验 1：基于平滑估计算法的网络隐蔽时间信道实验。设发送时间间隔为 t_s。起始时，设定 a=0.1，发送方以 t_s=100 μs 为发送时间间隔发送数据，接收方接收数据并记录接收正确率。每次数据传送结束后，发送方逐渐增加 t_s 的值，直到接收方接收正确率为 100%。改变平滑因子 a 的值，并重新进行实验。

实验 2：基于沉默间隙和接收时间间隔调整相结合方式的隐蔽时间信道实验。本文简称上述方法为沉默间隙法。为方便与实验 1 进行比较，发送方每发送 16 Byte 后沉默 8 个时间间隔。在实验中，发送方逐渐增加发送时间间隔，直到接收方的正确率为 100%。

衡量信道正确率时，以正确接收的字符数与总发送的字符数的百分比为依据。发送的字符为 ASCII 表中从 0x33(字符“！”)到 0x126(字符“～”)之间共 244 个可显示字符，每个字符发送一次。实验结果如图 6 所示。

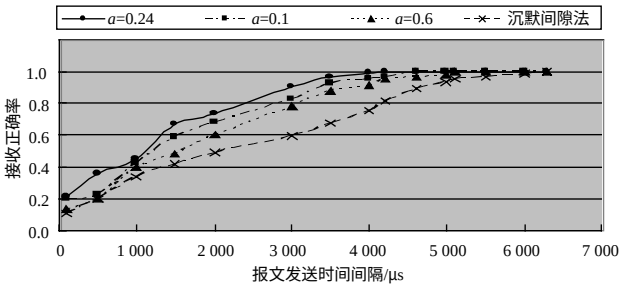


图 6 平滑估计算法与沉默间隙法的比较

由图 6 可以得到以下结论：

(1)随着发送时间间隔的不断增加，2 种方法的接收正确率不断提高。

(2)当平滑因子 a 不相同时，网络隐蔽时间信道中接收方的接收正确率不同。

(3)当平滑因子 a=0.24 时，利用平滑估计算法的隐蔽时间信道性能最佳。当 t_s = 4 200 μs 时，接收正确率达 100%。此时利用沉默间隙法的隐蔽时间信道的接收正确率只有 78.6%。当 t_s = 6 300 μs 时，沉默间隙法的正确率达 100%。

(4)在无差错的情况下，平滑估计算法的信息速率为 238.1 bit/s(a=0.24, t_s = 4 200 μs 处)，沉默间隙法的信息速率为 158.7 bit/s(t_s = 6 300 μs 处)。

经比较发现，在本文实验环境下，与沉默间隙法相比，平滑估计算法提高了网络隐蔽时间信道的同步精度。在无差错传播的情况下，利用平滑估计算法的隐蔽时间信道速度远大于沉默间隙法下的隐蔽时间信道速度。

5 结束语

本文探讨网络隐蔽时间信道的基本原理，分析隐蔽时间信道中导致信息传递出错的原因，提出平滑估计算法。对平滑估计算法和沉默间隙法进行实验比较，结果证明平滑估计算法可以提高网络隐蔽时间信道的通信质量。

参考文献

[1] Girling C G. Covert Channels in LAN's[J]. IEEE Trans. on Software Engineering, 1987, 13(2): 292-296.

[2] Cabuk S, Brodley C, Shields C. IP Covert Timing Channels: An Initial Exploration[C]//Proc. of CCS'04. Washington D. C., USA: [s. n.], 2004.

[3] Stevens W R. TCP/IP 详解卷 1: 协议[M]. 范建华, 胥光辉, 张 涛, 译. 北京: 机械工业出版社, 2000.

[4] Zander S, Armitage G, Branch P. A Survey of Covert Channels and Countermeasures in Computer Network Protocols[J]. IEEE Communications Surveys & Tutorials, 2007, 9(3): 44-57.

[5] Cabuk S, Brodley C E, Shields C. IP Covert Timing Channels: Design and Detection[C]//Proc. of the 11th ACM Conf. on Computer and Communications Security. New York, USA: ACM Press, 2004.