一种新型可靠网络隐蔽信道的研究*

王昌达，管星星，李志国，薄兆军
（江苏大学 计算机科学与通信工程学院，江苏 镇江 212013）

摘　要： 针对传统 IP 时间隐蔽信道传输速率低，在广域网中缺少一种稳定的时间同步机制，难以实现收发双方间可靠、稳定传输隐蔽信息的问题，提出了一种可靠网络隐蔽信道的模型。这种信道利用在固定时间窗口内发送的 IP 数据包数量作为载体传输隐蔽信息。通过引入一种新的信息编码机制，显著提高了网络隐蔽信道的传输带宽。进一步提出了一种比特块定界方法，解决了传统 IP 时间隐蔽信道的时间同步问题。实验结果表明，提出的可靠网络隐蔽信道的传输速率和稳定性均好于传统的 IP 时间隐蔽信道。

关键词： IP 时间隐蔽信道；网络时延抖动；编码机制；同步机制；发送算法；接收算法
中图分类号： TP393.08　　**文献标志码：** A　　**文章编号：** 1001-3695(2012)07-2650-04
doi:10.3969/j.issn.1001-3695.2012.07.068

New robust network covert channel

WANG Chang-da, GUAN Xing-xing, LI Zhi-guo, BO Zhao-jun
(*School of Computer Science & Telecommunication Engineering, Jiangsu University, Zhenjiang Jiangsu* 212013, *China*)

Abstract: To solve the problem that the transmission rate of the traditional IP covert timing channel was low, lacked a stable time synchronization mechanism in the WAN, and was difficulte to achieve transmit hidden message reliably and stably between sender and receiver, this paper proposed a robust network covert channel(RNCC). This channel used the number of IP packets sending in a fixed time window to transmit hidden message. To improve the bandwidth of RNCC, analyzed a new information encoding mechanism. Furthermore, proposed a new synchronization method, which was to solve the problem of time synchronization of the traditional IP covert timing channel, and to ensure the reliability of RNCC. The experimental results show that the capacity and robustness of RNCC is better than the traditional IP covert timing channel.

Key words: IP covert timing channel; network delay jitter; encoding mechanism; synchronization mechanism; sending algorithm; receiving algorithm

0　引言

随着计算机网络的飞速发展，网络安全问题越来越受到人们的关注，隐蔽信道作为一种重要的隐蔽通信工具，已成为传输密钥、网络身份认证和版权保护信息的重要工具。隐蔽信道是指可信系统中的高安全级用户，通过违反系统安全策略的方式将信息泄露给未授权用户的一种机制[1]。初期隐蔽信道的研究仅限于单机多安全级可信系统，但随着计算机网络的发展与普及，包交换网络中的 IP 隐蔽信道逐渐成为近期的研究热点。根据进程对资源的访问方式，可将 IP 隐蔽信道分为 IP 存储隐蔽信道(IP covert storage channel，IPCSC)和 IP 时间隐蔽信道(IP covert timing channel，IPCTC)。IPCSC 利用数据包报头中未被通信协议使用的冗余位隐藏信息[2]；IPCTC 则利用网络中相邻 IP 数据包间的时间间隔变化隐藏信息。IPCSC 容易受到防火墙交通正规化技术的拦阻而失效，即网络防火墙将进出的 IP 数据包报头冗余位强制使用相同的格式改写，能够彻底清除 IPCSC。而 IPCTC 利用 IP 数据包发送的时间间隔隐藏信息，可以有效规避大多数防火墙安全规则的检查，且隐蔽性强。因而，IPCTC 已成为近期 IP 隐蔽信道的主要研究对象。

文献[3]提出了简单时间隐蔽信道(simple timing channel，STC)，这是一种无噪声隐蔽信道，仅适用于无噪声或噪声很小的通信网络，且同步机制非常脆弱。随后，Cabuk 等人[4]提出了一种新型的时间隐蔽信道 IPOTC(IP on/off covert timing channel)，这种信道通过将待传比特序列划分成帧(等长)比特块，并在帧数据开始发送前发送同步 IP 包 SOF(start of frame)标志当前帧，解决了收发双方的同步问题。IPOTC 在局域网中可以很好地工作，但在分布式网络环境中由于网络时延的不确定性，有可能使该隐蔽信道瘫痪[5]。为了在分布式网络中建立稳定的隐蔽信道，钱玉文等人[6]提出了一种基于 Web 的可靠网络隐蔽时间信道(robust covert timing channel，RCTC)，这种隐蔽信道中接收方返回回应信息标志是否正确收到隐蔽信息，发送方根据是否接收到回应信息来判断是否重发该信息，从而建立了可靠的隐蔽信道。这种信息同步的方法会产生大量的回应信息，容易暴露隐蔽信道，并且不能保证回应信息的可靠传输。文献[7]提出了一种基于数据包长度变化特征的

收稿日期： 2011-12-22；**修回日期：** 2012-02-09　　**基金项目：** 国家自然科学基金资助项目(61003288)；江苏省自然科学基金资助项目(BK2010192)；教育部博士点基金资助项目(20093227110005)；江苏省六大人才高峰资助项目(1631170006)；江苏省高校自然科学研究计划资助项目(07KJB520016)；江苏大学高级人才资助项目(07JDG053)

作者简介： 王昌达(1971-)，男，上海人，副教授，博士，主要研究方向为信息安全技术(changda@ujs.edu.cn)；管星星(1986-)，男，硕士研究生，主要研究方向为信息安全技术；李志国(1984-)，男，硕士研究生，主要研究方向为信息安全技术；薄兆军(1986-)，男，硕士研究生，主要研究方向为信息安全技术.

网络隐蔽信道,该信道需要控制发送数据包的长度,只适用于载体信道(overt channel)与隐蔽信道(covert channel)的发送方为同一个进程的情况,且数据包长度具有明显的规律性,容易被检测系统识别。

在保证信道隐蔽性的同时,为了获得较好的通信带宽和鲁棒性,本文提出了一种新型可靠网络隐蔽信道(robust network covert channel,RNCC),该隐蔽信道利用在固定时间窗口内发送不同数量的 IP 数据包时传送不同的比特序列。进一步提出了一种比特序列块定界方法,解决了收发双方的同步问题。为了验证 RNCC 的可靠性,本文实现了这种可靠网络隐蔽信道。实验结果表明,本文提出的 RNCC 在广域网中能够实现隐蔽信息的可靠传输。

1　RNCC 的信道模型

1.1　RNCC 的系统结构

一般地,IP 时间隐通道的系统结构如图 1 所示,由发送端和接收端组成。

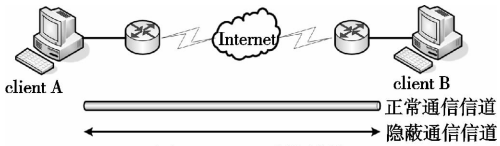

图1　RNCC系统结构

假设正常通信信道与隐蔽通信信道的发送方均在主机 client A 上,接收方均在主机 client B 上。如图 1 所示,隐蔽信息的发送方和接收方分别负责载体信息与隐蔽信息的发送和接收。RNCC 是一种基于固定时间窗口内 IP 数据包数量传输隐蔽信息的通信信道,在数据传输过程中需要大量的 IP 数据包作为信息载体,也因为大量的数据包发送可以有效隐藏隐蔽信道的存在,因此本文选择传输层中的 TCP 协议传送大文件产生的 IP 数据包作为载体传输隐蔽信息。另外,为了快速有效地接收发送方传输的隐蔽信息,接收端采用了 Sniffer 技术实时抓取、分析流经的网络数据包,并根据收发双方事先约定的通信规则提取和解码隐蔽信息。

收发双方具体的隐蔽信息传输结构如图 2 所示。发送方首先缓冲好 IP 载体数据包;待数据包缓冲完毕后,将待传隐蔽信息按字节序转换为比特序列,并根据编码表(比特块与待传 IP 数据包数量之间的映射关系表)转换为一系列待传 IP 包数;最后,发送方读取当前待传包数并据此发送 IP 数据包,实现隐蔽信息的传送。

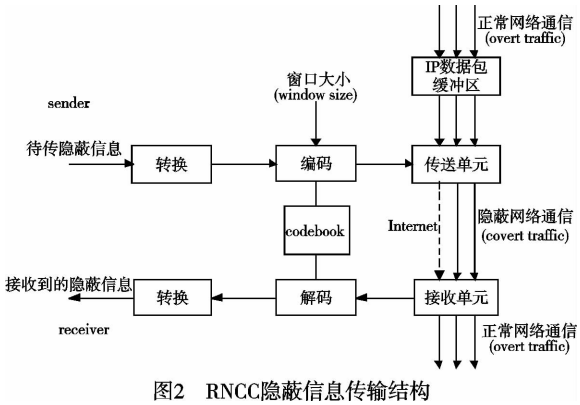

图2　RNCC隐蔽信息传输结构

接收方首先侦听当前网络,过滤指定源 IP 地址、源端口、目的 IP 地址和目的端口的网络连接,捕获并提取比特序列定界包内的 IP 数据包数;再根据解码表(同编码表)将获取的 IP 数据包数解码为比特序列块;最后按序拼接解码后的比特序列块,并将其转换为发送方传输的隐蔽信息。

1.2　RNCC 的编码机制

IPOTC 通过判断在固定长度的时间窗口内是否收到 IP 数据包来隐藏信息。即接收方以时间间隔 Δt 为长度单位将时间线划分成若干个相邻的窗口,从第 1 个窗口开始,若有发送方传来的 IP 数据包到达则接收信息 1,否则接收信息 0,然后逐次转向其后的窗口接收信息。这样,在一个时间窗口内只能传输一个比特位,传输速率低,限制了发送方数据的发送。

为了在一个时间窗口内传送更多的比特信息,本文提出了一种比特块与固定窗口内发送 IP 数据包数量之间的映射模型,即将长度为 L 的比特块 $(b_1,b_2,\cdots,b_L)$ 映射为固定窗口内发送的一系列 IP 数据包数 $(n_1,n_2,\cdots,n_k)$,其中 $n_i=0,1,\cdots,2^L-1$。

以传送长度为 2 的比特块为例,表 1 展示了待传比特块与固定窗口内发送的 IP 数据包数量的映射关系。

表 1　比特序列映射关系

比特序列	IP 数据包数量/个
00	0
01	1
10	2
11	3

当 $L=1$ 时,该模型将 1 个比特位映射为发送 0/1 个 IP 数据包,即 IPOTC 是本隐蔽信道的一个特例。

1.3　RNCC 的性能影响因素

收发双方间的网络状况、系统处理能力、发送与接收算法的时间复杂度等直接影响着 RNCC 的性能。为了便于区分,将影响因素分为两类:a)与通信网络相关;b)与收发双方相关。

与通信网络相关的影响因素主要包括平均传输时延 $\overline{T}_d$ 和时延抖动 j。平均传输时延是 IP 数据包在收发双方间传输平均消耗的时间,它与双方间的交换设备的硬件性能与传输距离有关。时延抖动则是具体 IP 数据包传输时间 T 与平均时延 $\overline{T}_d$ 的差值,即 $j=\overline{T}_d-T$。另外,IP 数据包在传输过程中的错序甚至丢失也会对 RNCC 的性能产生一定的影响。

与收发双方相关的因素主要包括发送与接收算法的时间复杂度、收发双方主机硬件性能以及编程语言的性能。用于隐蔽通信的算法必须是高效的,因此在隐蔽信道的实现过程中,采用了信息缓冲方法提高算法的执行效率。例如发送算法提前将隐蔽信息转换、编码为一系列 IP 数据包数并缓存,再根据缓存好的 IP 数据包数控制包缓冲区中 IP 数据包的发送。收发双方的主机硬件性能又包括进程间的调度耗时和系统时钟的精准度。编程语言的性能主要是语言中函数执行效率。例如 Java 语言中的 sleep( )函数,因为高级语言对系统的库函数进行了更高层次的封装,增加了函数的执行时间。

值得注意的是,在广域网中,网络环境复杂多变,伴随着网络通信状况的变化,时延抖动也不断变化着。而与收发双方相关的因素随着收发算法、主机性能以及编程语言的确定而确定,是一个恒定量,因而对 RNCC 的性能影响较小。根据上述分析,RNCC 的性能主要取决于网络时延抖动 j。

1.4　RNCC 的同步机制

在 RNCC 中,隐蔽信息的传输完全依赖于 IP 载体数据包

在接收方的到达时刻。根据 1.3 节的分析,RNCC 的性能主要取决于网络时延抖动 j,而 j 随着网络状况的变化而变化。特别地,当网络状况不断恶化时,j 抖动越剧烈。另外,收发双方所在主机的系统时钟不可能完全相同。这些都为网络隐蔽信道的时间同步带来了挑战。

在传统的网络时间隐蔽信道中,典型的时间同步方式为,在隐蔽信息开始传送前,发送方首先发送一个标志隐蔽信息开始传送的 IP 数据包——SOT(start of transmit),且忽略 SOT 包的网络时延抖动(即假设 SOT 包的时延抖动 $j=0$),接着根据当前待传比特选择是否在时间窗口 TW 内发送 IP 数据包。接收方在接收到 SOT 包后开始计时后,按事先约定好的 TW 接收比特数据,即当前时间窗口内是否有 IP 数据包到来接收比特位 1/0。收发双方的时间同步过程如图 3 所示。

图 3 中,TW 表示发送方发送时间窗口的长度。由于网络时延抖动 j 会导致 IP 数据包提前或延迟到达,为了提高隐蔽信息传输的正确率,选择在时间窗口的中点发送 IP 数据包。只要当前传送 IP 数据包的时延抖动 $j\in[-\frac{1}{2}TW,\frac{1}{2}TW)$,接收方就能够正确解析发送方传送的比特信息。然而,当时延抖动 $|j|\geq\frac{1}{2}TW$ 时,隐蔽时间信道将无法正常工作。因而,这种同步方式只适用于局域网或 j 很小的情况下($j\in[-5\ \text{ms},5\ \text{ms}]$)。

针对 IPCTC 在广域网上的时间同步问题,提出了一种比特序列块定界方法。首先将待传比特序列$(b_1,b_2,\cdots,b_n)$划分成一系列长度为 L 的比特序列块$(b_1,b_2,\cdots,b_L)$,然后根据映射表将 $(b_1,b_2,\cdots,b_L)$映射为时间窗口 TW 内需要传送的 IP 数据包数$(n_1,n_2,\cdots,n_k)$,其中 $n_i=0,1,\cdots,2^L-1$;最后用块起始包(start of block,SOB)与块结束包(end of block,EOB)分别标志发送窗口的开始时刻和结束时刻,并在时间窗口的中间点传送相应数量的 IP 数据包。具体的传输过程如图 4 所示。

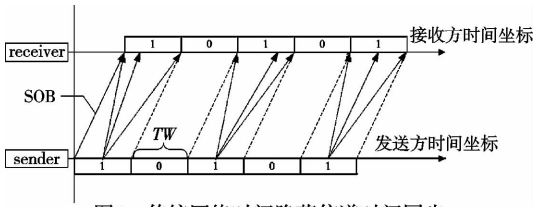

图3 传统网络时间隐蔽信道时间同步

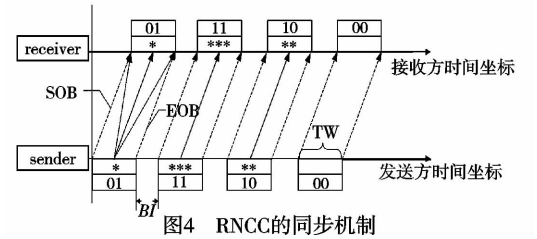

图4 RNCC的同步机制

更进一步,为了使各个比特块之间相互独立,本文引入了块间隔(block of interval,BI)。因为时延抖动 j 的存在可能会使 EOB 包与 SOB 包发生错序,这使相邻比特块之间产生了块间串扰,降低了隐蔽信息的传输正确率。因而,需要确定一个合理的 BI 使得 EOB 包与 SOB 包顺序到达。令 EOB 包的时延抖动为 j_{EOB},SOB 包的时延抖动为 j_{SOB}。只需令 $BI>|j_{\text{EOB}}|+|J_{\text{SOB}}|$,即可保证 EOB 包与 SOB 包的按序到达。

1.5 RNCC 中 TW 和 BI 的确定

根据目前的认识,时延抖动$\{j_i\}$是一组满足均值 $E(\xi)=0$,方差 $D(\xi)=\sigma^2$ 的正态分布[8],其中 $\xi\in\{j_i\}$。由正态分布函数表可知,当 j 落在$(-\sigma,\sigma)$内时,概率为 68.26%;当 j 落在$(-2\sigma,2\sigma)$内时,概率为 95.44%;当 j 落在$(-3\sigma,3\sigma)$内时,概率为 99.74%。为了确保隐蔽信息传输的正确率,令 $TW=6\sigma$。因为 IP 数据包的发送时刻为 TW 的中点,只要 IP 数据包的时延抖动 j 落在区间$(-\frac{1}{2}TW,\frac{1}{2}TW)$,即$(-3\sigma,3\sigma)$内时,接收方就能够以低于 0.26% 的误码率接收发送方传送的比特数据。

根据 1.4 节的分析知,当 $BI>|j_{\text{EOB}}|+|J_{\text{SOB}}|$时,传送的各个比特块相互独立,不会发生块间串扰。因为时延抖动落在区间$(-3\sigma,3\sigma)$外的概率很小,而且 IP 数据包在传输过程中有最大时间延迟(MTD)限制,一旦接收者等待的时间超过了 MTD,则认为该包已经丢失。基于此,本文假设 $j_{\max}=3\sigma$,则有 $|j_{\text{EOB}}|+|j_{\text{SOB}}|<2j_{\max}$。因而,只要 $BI>2j_{\max}$,即 $BI>6\sigma$,就能保证不会发生块间串扰。这里取 $BI=7\sigma$。

1.6 RNCC 的信道容量分析

根据以上分析,RNCC 的信道容量取决于比特块的长度 L、时间窗口 TW 的大小以及块间隔 BI。信道容量式为

$$C(n,L,\sigma)=\frac{nL}{nTW+(n-1)BI}=\frac{nL}{13n\sigma-7\sigma}\tag{1}$$

其中:n 表示发送比特块的数量;σ 表示当前网络环境的网络时延抖动均方差;L 表示比特块的长度。当 $n\to+\infty$ 时,有

$$\lim_{n\to+\infty}C(n,L,\sigma)=\lim_{n\to+\infty}\frac{nL}{13n\sigma-7\sigma}=\frac{L}{13\sigma}\tag{2}$$

即表示当传送的比特块数量 n 很大时,RNCC 的隐蔽信道容量 $C_{\text{RNCC}}=L/13\sigma$,是一个关于 L 和 σ 的函数,且信道容量 C_{RNCC} 与比特块长度 L 呈正相关,与网络时延抖动均方差 σ 呈反相关。

以 $L=4,\sigma=5$ 为例,RNCC 的信道容量 $C_{\text{RNCC}}=61.54$ bit/s。而在时间窗口 TW 相同的情况下,传统 IPOTC 的信道容量 C_{IPOTC}仅为 33.3 bit/s。因此本文提出的 RNCC 能够有效地提高隐蔽信道的传输带宽。

2 RNCC 的算法实现

RNCC 算法的复杂度,特别是时间复杂度,直接影响着 RNCC 的传输速率与正确率。为了降低 RNCC 算法的时间复杂度,采用了对隐蔽信息预处理并缓冲的的方法,有效地降低了 RNCC 算法的时间复杂度。具体算法处理步骤描述如下。

2.1 发送算法

输入:隐蔽信息、TW、BI 和编码表(比特块与 IP 数据包数的映射表)

输出:一系列待传 IP 数据包

a)测试当前网络时延抖动情况,获取时延抖动均方差 σ。

b)根据获取的时延抖动均方差 σ 求出时间窗口 TW 和块间隔 BI 的大小。

c)根据收发双方的事先约定确定比特块与 IP 数据包数量之间的映射关系,并根据映射关系建立编码表。

d)按字节序读取隐蔽信息文件,并将载入内存的隐蔽信息以字节为单位转换为八位二进制字符串。最后,将转换后的二进制字符串存入比特字符串缓冲区。

e)从比特字符串缓冲区中依次读取 l bit,根据读取的 l bit 查找编码表,获取对应的待传 IP 数据包的数量 $n(n\geq0)$,发送块起始包 SOB,$TW/2$ 时刻发送 n 个 IP 数据包(即在时间窗口中点处发送 IP 数据包),TW 时刻发送块结束包 EOB。

f)判断比特字符串缓冲区是否为空。若不为空,发送线程挂起 *BI* ms,重复执行步骤 e);若为空,则结束发送线程。

2.2　接收算法

输入:IP 数据包序列

输出:隐蔽信息

a)根据收发双方的事先约定确定比特块与 IP 数据包数量之间的映射关系,并根据映射关系建立解码表。

b)以阻塞模式启动 IP 数据包侦听线程,阻塞等待 SOB 包。

c)若接收到 SOB 包,则侦听线程进入非阻塞模式,开始接收隐蔽信息载体数据包,接收到 EOB 包后,记录 SOB 包与 EOB 包之间到达的 IP 数据包数,启动计时器线程并使侦听线程再次进入阻塞模式等待 SOB 包。

d)若在 3 s 内接收到 SOB 包,则重复执行 c);反之,则认为隐蔽信息已接收完毕,结束接收线程。

e)依次读取记录的 IP 数据包数,查找解码表,获取 IP 数据包数对应的比特块并存入比特字符串缓冲区。

f)转换比特字符串缓冲区内的比特序列,获取发送方传送的隐蔽信息。

3　实验结果与分析

为了验证 RNCC 的性能,本文实现了这种可靠网络隐蔽信道,并在 TCP/IP 网络环境下进行了性能测试。实验程序采用 Java 程序设计语言编写,由发送方和接收方组成。发送方通过控制固定窗口内发送的 IP 数据包数传送隐蔽信息,并通过 sleep(T)来控制 IP 数据包的发送时刻,其中 T 为 $TW/2$ 或 TW(若时间窗口 TW 内待发送的 IP 数据包数为 0,T = TW;反之,$T = TW/2$)。接收方被动侦听并捕获指定连接的 IP 数据包,获取块定界包 SOB 与 EOB 间的隐蔽信息载体数据包数,根据解码表解码为比特块,并最终转换为发送方传送的隐蔽信息。发送方与接收方所处主机的性能如下,Intel® Core 2 Duo E7500 @ 2.93 GHz/ 2.00 G/ Windows 7。

实验中,选取了长度为 4 的比特块映射模型建立收发双方的映射表。发送方传输的隐蔽信息为一个文本文件,按字节序读取、转换为比特序列,共传输了 5 016 bit 二进制比特信息。

实验测试了 RNCC 在不同网络时延抖动均方差 σ 下的误码率(P_e),结果如表 2 所示。

表 2　不同 σ 下的 RNCC 误码率

σ/%	3	5	7	10	15
Pe/%	0.917	0.877	0.977	0.937	0.957

由表 2 可知,在不同的网络时延抖动均方差 σ 下,RNCC 的误码率均小于 1%。这表明,本文提出的可靠网络隐蔽信道能够在广域网中可靠、稳定地工作。为了更好地说明 RNCC 的可靠性,实现了传统的网络时间隐蔽信道 IPOTC,并在局域网和广域网上分别测试了两种网络隐蔽信道的误码率。由于传统的时间同步方式无法让 IPOTC 在广域网上正常工作,因此,在 IPOTC 的实现过程中,同样采用了 RNCC 的同步机制。为了便于区别,选择了每传输 8 个比特位进行一次时间同步的方式。

在对比过程中,分别测试了两种网络隐蔽信道在不同情况下的误码率。一种是令 TW 固定不变(取 TW = 30 ms),分别测试在不同时延抖动均方差 σ 下的误码率,其中 σ = 0 表示测试环境为局域网。测试结果如表 3 所示。另一种是令 σ 固定不变(取 σ = 5),分别测试在不同时间窗口 TW 下的误码率。测试结果如表 4 所示。

表 3　不同 σ 相同 TW 下的误码率

σ	LAN	WAN			
	0	3	5	10	15
IPOTC P_e/%	0	4.765	4.844	28.489	44.876
RNCC P_e/%	0	0	0.877	23.6	34.549

表 4　相同 σ 不同 TW 下的误码率

TW	10ms	15ms	20ms	25ms	30ms
IPOTC P_e/%	44.677	32.695	17.245	6.24	4.844
RNCC P_e/%	33.872	25.897	12.62	5.0	0.877

为了更直观地看出两种隐蔽信道的误码率比较结果,分别给出了表 3 和 4 对应的误码率比较图,如图 4、5 所示。从图中可以看出,在这两种情况下,RNCC 的传输误码率均小于 IPOTC。可见,本文提出的网络隐蔽信道具有更好的可靠性。

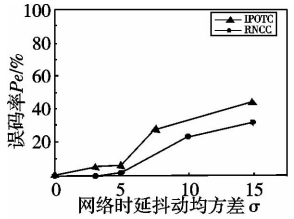

图5　不同 σ 相同 TW 下的误码率比较

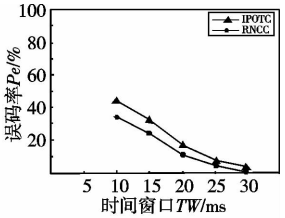

图6　相同 σ 不同 TW 下的误码率比较

4　结束语

本文提出了一种可靠网络隐蔽信道模型,根据该模型设计了一种新的隐蔽信息编码机制,提高了隐蔽信道的传输带宽,同时设计了一种时间同步机制,解决了收发双方间的时间同步问题。进一步地分析了 RNCC 的信道容量。最后,给出了 RNCC 中发送算法与接收算法的具体处理步骤。为了验证 RNCC 的性能,实现了这种可靠网络隐蔽信道。实验结果表明,在广域网环境下,RNCC 能够可靠地传输隐蔽信息,且传输速率比传统的 IP 时间隐蔽信道有显著提高。

参考文献:

[1] 王昌达,鞠时光,周从华,等. 一种隐通道威胁审计的度量方法[J]. 计算机学报,2009,32(4):751-762.

[2] TRABELSI Z,EL-SAYED H, FRIKHA L,*et al*. A novel covert channel based on the IP header record route option[J]. International Journal of Advanced Media and Communication,2007,1(4):328-350.

[3] MOSKOWITZ I S,NEWMAN A R. Simple timing channels[C]// Proc of IEEE Symposium on Research on Security and Privacy. Washington DC:IEEE Computer Society, 1994:56-64.

[4] CABUK S, BRODLEY C E,SHIELDS C. IP covert timing channels: design and detection[C]//Proc of the 11th ACM Conference on Computer and Communications Security. New York:ACM,2004:178-187.

[5] SELLKE S H,WANG C, BAGCHI S, *et al*. TCP/IP timing channels:theory to implementation[C]//Proc of the 28th IEEE International Conference on Computer Communications. 2009:2204-2212.

[6] 钱玉文,赵邦信,孔建寿,等. 一种基于 Web 的可靠网络隐蔽时间信道的研究[J]. 计算机研究与发展,2011,48(3),423-431.

[7] 严庆,刘军,肖军模. 网络隐通道的构建方法研究[J]. 计算机工程,2009,35(2):139-141.

[8] 曹保江,李春茂,肖建,等. 网络化控制系统时延测量、分析与预测[J]. 计算机工程与应用, 2007,43(33):115-120.