一种基于扩频编码的可靠网络隐蔽信道设计方法

牛小鹏* 李清宝 王 炜
(解放军信息工程大学 郑州 450002)

摘 要：针对网络隐蔽信道在强噪声环境中信息传递错误率高的问题，该文提出一种基于 CDMA 扩频编码的可靠网络隐蔽信道设计方法。该方法利用数据包在传输过程中的包际时延传递隐蔽信息，发送方采用散列扩频编码，接收方采用信道噪声预测消除等技术进行信道抗干扰处理，提高了强噪声环境中隐蔽信道通信的可靠性。针对信道抗干扰性与信道传输率两个主要衡量指标互斥、综合性能难以达到最优的问题，提出了基于选定传输率的抗干扰能力最优化方法。在 TCP/IP 网络中构建了该隐蔽信道，并进行了隐蔽信息传输实验，结果表明该文方法与解决同类问题的其他方法相比隐蔽信道数据传输的综合抗干扰能力提高 20%左右。

关键词：信息安全；网络隐蔽时间信道；信道传输率；信道抗干扰性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2013)04-1012-05
DOI: 10.3724/SP.J.1146.2012.01106

A Robust Network Covert Channel Algorithm Based on Spread Coding

Niu Xiao-peng Li Qing-bao Wang Wei
(*PLA Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: In order to solve the problem that the covert timing channel works unstable in the noisy network, a method of designing robust covert channel is proposed. The method uses the interval time of network packets to transfer information, the sender codes covert information using hash spreading spectrum, and the receiver forecasts the channel noise and eliminates it. In order to solve the contradictory relationship between transmission rate and robustness, the strategy of maximizing robustness under fixed transmission rate is proposed. The experimental environment of this covert channel is constructed and several experiments are conducted. The results show that the ability to resist noise is increased about by 20%, compared with other methods on the same problem.

Key words: Information security; Network covert timing channel; Channel transmission rate; Channel robustness

1 引言

隐蔽信道是指利用公开合法的信道隐蔽传递秘密信息的通信技术，它是保密通信的重要工具之一[1]。随着网络技术的发展，对网络隐蔽信道的研究成为该领域的重点。网络隐蔽信道分为存储信道和时间信道[2]，存储信道通信方便但隐蔽性较弱，传递大容量信息时易被检测到。时间信道隐蔽性强，但是通信两端同步困难[3]。

Cabuk等人[2]提出了一种IP隐蔽时间信道 (IP Covert Timing Channel, IPCTC)，用固定时间段内有没有数据包的发送表示0和1，编码简单，通信过程缺少同步机制和抗干扰编码，信道的可靠性和隐蔽性低。钱玉文等人[4]设计实现了基于HTTP协议的网络隐蔽时间信道同步机制和通信协议，其鲁棒性和容量都优于传统隐蔽信道。文献[5]设计了n-m编码策略，按照独立同分布的原则随机产生包间时延，模拟正常网络流量，在一定程度上提高了隐蔽信道的隐蔽性和抗干扰性。但该文是基于网络信道噪声在一定范围内发生变化，不会出现过大噪声干扰的强假设。文献[6]提出利用CDMA扩频编码机制对隐蔽信息进行编码，论证了扩频编码技术可以显著提高隐蔽信道的抗干扰能力，能够有效抵抗信道中的各种噪声，不足之处是所设计的时延-码元映射函数比较简单，不能逼真模拟正常网络信道流量。文献[7]提出了基于概率分布的时延-码元映射函数，但没有消除时延信号中的噪声，当信道中存在强噪声时隐蔽通信的错误率较高，平均在10%以上，且通信两端缺少同步，可靠性差。

本文提出利用隐蔽存储信道发送同步信息，利用隐蔽时间信道传递隐蔽数据的可靠网络隐蔽信道(Robust Network Covert Channel, RNCC)。实验表

2012-08-31 收到，2012-11-21 改回
国家 863 计划项目(2009AA01Z434)和信息工程大学未来发展基金(Future 1201)资助课题
*通信作者：牛小鹏 xiaoyuer8082@163.com

明，RNCC可以在保证信道传输效率的基础上最大程度地降低信道传输错误率，提高抗干扰能力。

2 RNCC 系统模型

RNCC 结构如图1所示，发送方利用隐蔽存储信道将同步信息嵌入到合法数据包中，编码器对隐蔽信息进行散列扩频编码，再按照正常网络流量的统计特征将码元调制成数据包的间隔时延。接收方对接收到的时延信号做消噪处理，然后由解码器进行解码和解调，恢复出隐蔽信息。

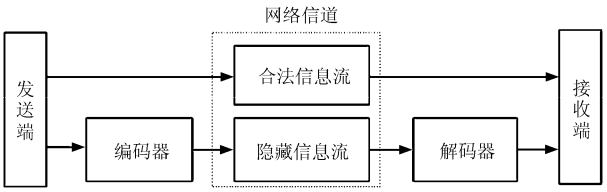

图 1 网络隐蔽信道系统模型

信息传输抗噪的方法包括两类：(1)通过在数据流中插入校验码来提高抗干扰能力；(2)通过编码机制保证信息的传递正确性。后者较前者具有更多的灵活性。对于隐蔽信息数据 b_k，用向量 $\boldsymbol{C}$ 对其扩频编码，结果为

$$\boldsymbol{S}=[s(1),s(2),\cdots,s(N)]=\sum_{k=1}^{K}s_k=\sum_{k=1}^{K}b_{i,k}\cdot\boldsymbol{C}_{f(i,k)} \quad (1)$$

其中 $\boldsymbol{C}$ 为具有正交性质的 Walsh-Hadamard 矩阵，每一列都可以作为扩频编码的向量码字，$f(i,k)$ 为隐蔽信息 $b_{i,k}$ 的索引哈希函数，利用该散列值在 $\boldsymbol{C}$ 中随机选取一列作为 $b_{i,k}$ 的扩频码字。

正常通信的网络数据包间隔具有随机性，并且相互独立具有相同的分布特征[2]，其值决定于数据流的包间隔时延概率分布函数。为了保证信道的隐蔽性，可以使用码字 $\boldsymbol{S}$ 产生与正常数据包间隔时延具有相同统计特征的时延信号。

文献[6]介绍了一种利用概率累积分布函数(Cumulative Distribute Function, CDF)的反函数生成服从特定分布随机变量的方法，即以区间[0,1]上服从均匀分布的随机变量序列作为任意分布的CDF 反函数的输入，得到满足该分布的随机变量。

按照概率累积分布函数的定义，信息码元的累积分布函数为

$$F_s(l)=\Pr[s\le l]=\sum_{l_m\le l}\Pr[s=l_m]=\sum_{l_m\le l}P_s[l_m] \quad (2)$$

对隐蔽信息的调制可分为两个阶段：(1)将扩频编码生成的码元向量映射到区间 $(0,1]$，得到均匀分布的随机变量序列 $\{u(1),u(2),\cdots,u(N)\}$；(2)以 $\{u(1),u(2),\cdots,u(N)\}$ 为输入，按式(2)计算得到与合法信息流具有相同分布的数据包间隔时延 D_t。第 1 阶段所使用的映射函数为

$$u(n)=F_s(l_{m-1})+[F_s(l_m)-F_s(l_{m-1})]\times v(n) \quad (3)$$

其中 $v(n)$ 是 $(0,1]$ 区间上服从均匀分布的随机变量，它将 $u(n)$ 的值映射到区间 $(F_s(l_{m-1}),F_s(l_m)]$ 中，避免用单值 $F_s(l_m)$ 表示 $s(n)$。

3 RNCC 的性能分析

网络信道是一个不可靠的信道，通信过程中可能存在丢包和延迟等现象，例如路由器、防火墙等网络设备在处理数据包时产生的延时，因此隐蔽信息在传递的过程中可能会被改变。为了使隐蔽通信在有噪声干扰的情况下仍然保持较高的正确率，就要求隐蔽信道具备抗干扰性，信息传递的错误率小于某一预定值，即 $P_e\le\varepsilon$，其中 $P_e=\mathrm{Bits}_e/\mathrm{Bits}_a$，$\varepsilon\in\Re^+$。$P_e$ 与信噪比 SNR(Signal-to-Noise Ratio)成反比关系[3]，$\mathrm{SNR}=E_s/E_x$，其中 E_s 是信号功率，E_x 是噪声功率。

目前比较常用的网络隐蔽信道检测方法是K-S测试(Kolmogorov-Smirnov test)[8]。令 $S(x)$ 表示携带隐蔽信息的数据流分布函数，$F(x)$ 表示正常合法数据流分布函数，则 H_s 可以表示为

$$H_s=\sup_x\left|F(x)-S(x)\right| \quad (4)$$

如果携带隐蔽信息的数据流与正常合法数据流之间的 H_s 不大于正常数据流之间的 H_s，则可认为该隐蔽信道具有较好的隐蔽性。为了便于分析，对隐蔽信道的主要性能参数作如下定义：

定义 1　隐蔽信道抗干扰系数 γ，为对原始信息编码调制后与编码调制前的信噪比之比值，即 $\gamma=\mathrm{SNR}_{\mathrm{po}}/\mathrm{SNR}_{\mathrm{pr}}$。

定义 2　隐蔽信道数据传输率 R，在连续的数据流中每个数据包间隔时延所能够传递的隐蔽信息位数，对于扩频系数为 N，信道数目为 K 的隐蔽信道，数据传输率为 $R=K/N$。

3.1 信道参数优化

编码调制前，$s(n)$ 仅代表原始信息位，将 $s(n)$ 映射到 $u_1(n)$，取值范围是 $(0,1/2]$ 和 $[1/2,1)$，分别代表原始隐蔽信息取0和1的概率。编码调制后，码元被转化成服从均匀分布的随机变量，共有 $M=K+1$ 种取值情况。在相同噪声分布的情况下，按照定义1抗干扰系数 γ 等于 $u(n)$ 与 $u_1(n)$ 的信号功率之比，即 $\gamma=N\cdot E_K/E_1$，N表示扩频系数，E_K 表示K个信道上 $u(n)$ 的信号功率，E_1 表示 $u_1(n)$ 的信号功率。对于取值区间在 $[a,b]$ 的随机变量，信号功率可以表示为 $(b-a)^2/12$ [7]。由于 $u(n)$ 共有M种取值可能，所以K个隐蔽信道的抗干扰系数 γ 可以表示为

$$\gamma = \frac{N}{M}\sum_{m=1}^{M}\left[\frac{1}{2}\frac{E_K(u(n)=l_m)}{E_1(u_1(n)=1)}+\frac{1}{2}\frac{E_K(u(n)=l_m)}{E_1(u_1(n)=-1)}\right]$$
$$= \frac{N}{M}\sum_{m=1}^{M}\frac{[F_s(l_m)-F_s(l_{m-1})]^2}{(1/2)^2} = \frac{4N}{M}\sum_{m=1}^{M}[P_s(l_m)]^2$$
$$= \frac{N}{K+1}\left(\frac{1}{2}\right)^{2K-2}\sum_{k=0}^{K}\binom{K}{k}^2$$
$$= \frac{N}{N\cdot R+1}\left(\frac{1}{2}\right)^{2\cdot N\cdot R-2}\sum_{k=0}^{\lfloor N\cdot R\rfloor}\binom{\lfloor N\cdot R\rfloor}{k}^2 \tag{5}$$

由式(5)可见，抗干扰系数 γ 与扩频系数 N 成正比，而数据传输率 R 与 N 成反比。如图 2 所示，在一定区间内 γ 随着 K 的增大逐渐下降；当 K 增大到一定程度，γ 趋近于 0，抗干扰能力处于极低水平，隐蔽信道几乎不能使用。而 R 与 K 成正比，随着 K 的增加线性增加，接近于 1。

由此可知，信道抗干扰能力与数据传输率两个主要衡量指标互斥，难以同时达到最优。为了使两个目标同时达到最佳状态，获得较好的抗干扰能力和数据传输率，需要按照一定的策略进行参数优化调节，获得最佳平衡。γ 可以从 0 趋近于正无穷，没有约束和比较标准，其值不易确定。而 $R\in(0,1]$，可以根据实际应用需求设定高或低的传输率。隐蔽信道的设计目的是传递秘密信息，数据量一般不大，但要求较高的准确率。因此可以设计如下策略：给定数据传输率 R，通过改变 N 的值，最大化抗干扰能力 γ。图 3 展示了将 R 固定为不同值时 γ 与 N 的关系。

参数选择过程如下，首先根据具体应用需求设定数据传输率 R，在固定 R 的条件下计算 $\gamma_{\max}$，以及扩频系数 N 和信道数目 K，文中所用到的参数设置如表 1 所示。

3.2 噪声消减

解码与编码过程相反，需要根据网络环境对载波信号做消噪处理。接收方得到的信号为 $\mathrm{cd}=d+x$，其中 x 是噪声，d 是包间时延。当 $x\le 20$ ms 时不用特殊处理，扩频编码机制和码元区间映射可以保证低错误率的信息传递；当 $x>20$ ms 时就会影响信息传递的正确率，即该信道通信环境的噪声门限 $d_t=20$ ms。信道消噪过程是先做信道噪声评估，得到平均包间隔时延 d_m 和最大包间隔时延 $d_{\max}$，然后根据 cd 的取值判断并消除噪声。接收方利用接收到的包间隔时延做解调和解码计算，如果 $\mathrm{cu}(n)\in(F_s(l_{m-1}),F_s(l_m)]$，则令 $\mathrm{cs}(n)=l_m$，然后用式(6)恢复隐蔽信息 cb_k。

$$\mathrm{cb}_k = \frac{1}{N}<\mathrm{cs},c_k>=\frac{1}{N}<s,c_k>+\frac{1}{N}<x,c_k>$$
$$= \sum_{i=1}^{K}\frac{b_i}{N}<c_i,c_k>+\frac{1}{N}<x,c_k>$$
$$= b_k+\frac{1}{N}<x,c_k> \tag{6}$$

表 1 隐蔽信道主要参数设置

R	$\gamma_{\max}$	N	K
0.05	40.000	40	2
0.10	12.375	40	4
0.20	3.9697	16	3
0.40	1.8044	8	3
0.80	0.5603	8	6

4 实验结果

4.1 测试环境及数据

为测试本文提出的网络隐蔽信道通信技术，设计实现了一个基于 TCP/IP 协议的网络通信程序 fileback(包括客户端和服务端)。

隐蔽通信实验在校园网的不同校区间进行，客户端和服务端间的物理距离为 10 km，丢包率为 0.6%，平均包间时延为 2.3452 ms。测试过程中在网络信道中施加两类噪声信号，分别为正态分布和均匀分布的噪声，具体参数如表 2 所示。均匀分布的随机变量比其它分布的随机变量具有更高的信息

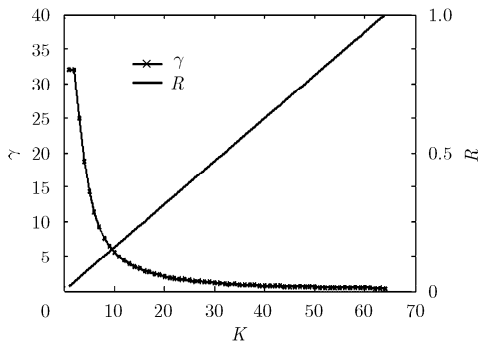

图 2 参数 K 对信道抗干扰能力与传输率 R 的影响

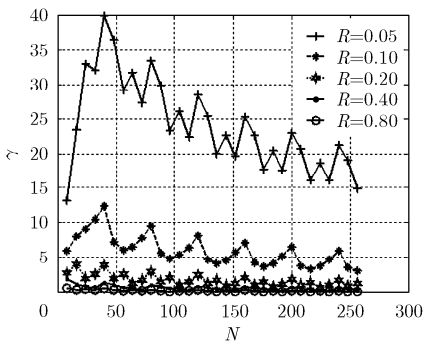

图 3 固定 R 的情况下 γ 与扩频系数 N 的关系

表 2 网络隐蔽信道数据传输错误率 P_e(%) 实验结果统计

算法	编码模式	无噪声	正态分布噪声 δ(ms)				均匀分布噪声 Δ(ms)			
			50	100	150	200	20	50	100	150
本文方法	$R=0.05$	0	1.07	1.07	1.07	1.79	1.07	1.43	2.78	3.93
	$R=0.10$	0	0.71	0.71	1.79	4.64	0.71	1.79	4.29	5.36
	$R=0.20$	0	2.14	9.29	11.07	12.50	4.64	6.07	10.00	10.00
	$R=0.40$	0	11.07	16.43	18.93	25.36	10.36	14.64	18.57	20.00
	$R=0.80$	0.36	16.43	22.81	26.07	23.57	9.64	21.43	26.07	26.43
方法1[7]	$\gamma=8$	0	5.71	6.43	5.36	9.29	15.00	33.21	40.36	45.71
	$\gamma=16$	0	1.07	1.79	1.07	1.79	4.64	18.93	34.29	37.86
方法2[5]	(1,1)	0	4.50	8.13	10.63	13.00	2.81	3.00	8.25	12.96
	(8,2)	0	10.13	14.06	14.69	15.76	5.12	11.53	14.19	15.69

熵[3,9]，因此均匀分布的噪声能表示隐蔽信道中最严重的噪声干扰，即网络环境最差情况。

4.2 结果分析

独立同分布的网络流量模型是其它高级流量模型的研究基础，正常网络数据流的包间隔时延可以用 i.i.d.Pareto 分布来刻画生成[10]。Pareto 分布的累积分布函数为

$$F_{\mathrm{CDF}}(x)=1-(b/x)^a,\ a>0,\ b>0,\ x>a \qquad (7)$$

其中 a 为指定变量的形状参数，b 为指定变量的位置参数。参考文献[5]和文献[7], a 取值为 0.95, b 取值为 10。为了保证信道的隐蔽性，数据包间隔时延按照 i.i.d. Pareto 分布生成。

表 2 给出了对网络隐蔽时间信道数据传输错误率 P_e 的测试结果汇总，方法 1，方法 2 分别是指文献[7]和文献[5]中的方法。实验结果表明 3 种隐蔽信道都能够在无噪声的自然信道中稳定传输数据，错误率低于 0.5%。当信道中存在正态或均匀分布的噪声干扰时，3 种方法受干扰的影响程度不同。

(1)总体比较分析　当信道中存在正态或均匀分布的噪声干扰时，3 种方法受干扰的影响程度不同，方法 1 对均匀分布的噪声比较敏感，方法 2 对正态分布的噪声比较敏感，而本文方法对两种噪声都有较好的抵抗能力。根据表 2 测试结果计算 3 种方法的隐蔽信道数据传输平均错误率，令正态噪声信道和均匀噪声信道的权重分别为 0.5，则 3 种方法的平均错误率分别为 8.49%, 16.405%和 9.19%，本文方法与后两种方法相比隐蔽信道数据传输错误率分别降低了 48%和 7%，综合抗干扰性能提高了 20%左右。

(2)噪声对抗干扰性能的影响　如前所述信道中存在噪声干扰，主要包括自然噪声和人为产生的噪声。当噪声时延小于噪声门限时不用特别处理，扩频编码机制和码元区域映射可以克服噪声干扰。但当噪声时延大于噪声门限时就需要在接收方对接收到的时延信号进行消噪处理。图 4 对比展示了在接收方按照文中提出的消噪算法对收到的包间时延进行消噪处理后的错误率和没有进行消噪处理的错误率。

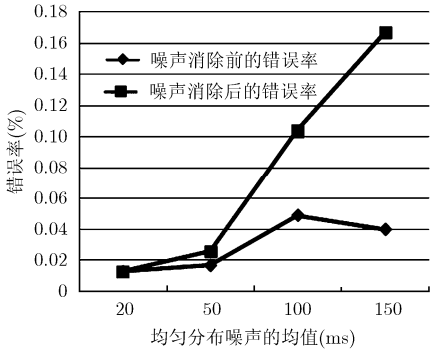

图 4 噪声消除算法对隐蔽通信错误率的影响

(3)3 种方法间的抗干扰性能比较　如图 5 所示，当信道中存在正态分布的噪声时，3 种方法在最佳参数配置下的数据通信错误率。可以看出本文方法和方法 1 都优于方法 2，这主要是因为前两种方法采用 CDMA 扩频编码，该编码方式用多位信号表示一位数据，具有天然的抗干扰性。当 $\delta=50$ 和 $\delta=100$ 时，本文方法略优于方法 1，而当 $\delta=150$ 和 $\delta=200$ 时方法 1 反而优于本文方法。这是由于两种方法的参数设置策略不同，方法 1 按照牺牲数据传输率换取高抗干扰性的策略进行参数设置，而本文方法是在综合考虑数据传输率和抗干扰性两个因素的基础上最大化抗干扰能力，因此本文方法的综合性能要优于方法 1。

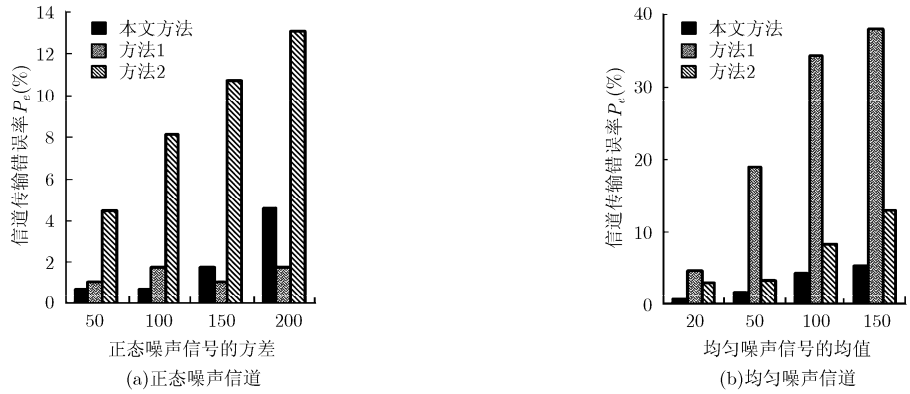

图 5 噪声信道中 3 种方法的抗干扰性

如图 5 所示，当信道中存在人为产生的均匀分布噪声时，3 种方法在最佳参数配置下的数据通信错误率。可以看出在该类噪声环境下本文方法优于方法 1 和方法 2，这主要是因为本文方法在接收方进行噪声消除处理，减弱了噪声信号对隐蔽信息的破坏程度。

(4)隐蔽性测试　对携带隐蔽信息的数据流包间时延做 K-S 测试，正常合法数据流与携带隐蔽信息的数据流之间的 H_s 是 0.023，而正常合法数据流之间的 H_s 是 0.027，其统计特征近似，表明本文所提出的网络隐蔽信道具有较强隐蔽性，可以在一定程度上抵抗网络数据流审计监测。

5 结束语

综上所述，本文给出了一种在强噪声干扰环境中网络隐蔽信道的设计方法，为在网络上实现隐蔽通信提供了一条新的途径。本文使用模拟的方法研究网络隐蔽信道的可靠性，在信道抗干扰性测试过程中使用正态和均匀分布的噪声模拟隐蔽信道的一般工作环境和最差工作环境，下一步将继续在实际应用环境中对网络隐蔽信道做测试，并增强其抗检测性。

参 考 文 献

[1] Lampson B. A note on the confinement problem[J]. *Communication of the ACM*, 1973, 10(16): 613–615.

[2] Cabuk S, Brodley C E, Shields C, *et al*.. IP covert timing channels: design and detection[C]. Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington DC, 2004: 178–187.

[3] Bukke Devendra Naik, Sarath Chandra Boddukolu, and Pothula Sujatha. Connecting entropy-based detection methods and entropy to detect covert timing channels[J]. *Advances in Computing and Information Technology*, 2012, 176(1): 279–288.

[4] 钱玉文, 赵邦信, 孔建寿. 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.
Qian Y W, Zhao B X, and Kong J S. Robust covert timing channel based on web[J]. *Journal of Computer Research and Development*, 2011, 48(3): 423–431.

[5] Sellke S H, Wang C C, Bagchi S, *et al*.. TCP/IP timing channels: theory to implementation [C]. Proceedings of the 28th IEEE Conference on Computer Communications, Rio de Janeiro, Brazil, 2009: 2204–2212.

[6] Liu Y L, Ghosal D, Armknecht F, *et al*.. Hide and seek in time-robust covert timing channels[C]. Proceedings of the 14th European Symposium on Research in Computer Security, Saint-Malo, France, 2009: 120–135.

[7] Liu Y L, Ghosal D, Armknecht F, *et al*.. Robust and undetectable steganographic timing channels for i.i.d. traffic [C]. Proceedings of the 12th Information Hiding Conference, Calgary, Alberta, Canada, 2010: 193–207.

[8] 王永吉, 吴敬征, 曾海涛. 隐蔽信道研究[J]. 软件学报, 2010, 21(9): 2262–2288.
Wang Y J, Wu J Z, and Zeng H T. Covert channel research[J]. *Journal of Software*, 2010, 21(9): 2262–2288.

[9] Liu X and Dai Y Q. A typical network covert timing channel with uniformly distributed noise[J]. *Chinese Journal of Electronics*, 2011, 4(20): 730–734.

[10] Houmanasdr A and Borisov N. CoCo: coding-based covert timing channels for network flows [C]. Proceedings of the 13th International Conference on Information Hiding, Prague, Czech Republic, 2011: 314–328.

牛小鹏： 男，1982 年生，博士，研究方向为网络信息安全.

李清宝： 男，1967 年生，博士，教授，主要研究方向为网络信息安全、系统结构等.

王　炜： 男，1975 年生，博士，讲师，主要研究方向为网络信息安全、系统结构、片上多处理器网络等.