网络时间隐蔽通道的拟合模型特性研究

杨 鹏 赵 辉 鲍忠贵
(北京跟踪与通信技术研究所 北京 100094)

摘 要 随着计算机网络的飞速发展,网络安全越来越受到人们的关注。在众多的攻击手段中,网络隐蔽通道已成为威胁计算机安全的重要来源之一。由于其隐蔽性较高、不易被发现和传输速率高等特点,网络时间隐蔽通道已成为该领域的研究热点之一。针对网络时间隐蔽通道的传输过程,构建了一种模型,并详细阐述了该模型中运用扩展码对隐蔽信息进行编码和调制的过程。在此基础上,分析了该模型下编码符号的概率分布状况,并与正常信道中的泊松分布拟合函数做了比较全面的对比。针对隐蔽通道的特性——隐蔽性和数据传输速率,首次分析了模型中的参数对其隐蔽性和传输速率的影响,并得到了二者之间的变化关系,这对今后网络时间隐蔽通道的构建工作具有一定的指导意义。

关键词 隐蔽通道,隐蔽性,数据传输速率,模型,编码
中图法分类号 TP309.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.028

Analysis on Fitting Model of Network Covert Timing Channel

YANG Peng ZHAO Hui BAO Zhong-gui
(Beijing Institute of Tracking and Telecommunications Technology, Beijing 100094, China)

Abstract With the rapid development of computer network, the security of computer network has caused more and more peoples' attention. Among lots of methods of network attack, network covert channels have become one of the main threats to the security of computers. Because of its undetectable nature and high data transmission rate, covert timing channel has become one of current research hot spots in the field of information security. This paper constructed a model for the transmission process of network covert timing channel. The model describes how to encode and modulate covert messages using spreading code. On the basis, we analyzed the probability distribution of the constructed model, then made a more comprehensive contrast with the Poisson distribution which is used to fit the legitimate channel. Aiming at analyzing the concealment and data transmission rate of covert channels, we first analyzed the parameters which impact the above properties of covert timing channels, and also discussed the relationship between these properties, which has certain significance for the future work of network covert timing channels.

Keywords Covert channel, Concealment, Data transfer rate, Model, Coding

1 引言

隐蔽通道的概念由 Lampson 于 1973 年提出[1],被定义为"在不违背主机安全策略的前提下能够利用正常信道从一个进程(用户)向另一个进程(用户)传递机密信息"[2]。早期隐蔽通道的研究主要集中在系统隐蔽通道上,随着网络技术的飞速发展,计算机网络安全越来越受到人们的关注,隐蔽通道的概念也逐渐向网络过渡,成为威胁计算机系统安全的重要来源之一。根据利用共享资源的方式不同,网络隐蔽通道可以分为网络存储隐蔽通道和网络时间隐蔽通道。网络存储隐蔽通道是将隐蔽信息填充到数据包中的预留位或扩展位,之后随着网络数据包一起发送,并被接收方接收,但是这种隐蔽通道由于改变了原有数据包的结构,容易被检测,因此实用价值较小[3]。

网络时间隐蔽通道主要通过调制正常信道数据包的时间间隔来传递隐蔽信息。这种方法的隐蔽性较强,现已成为该领域的一个研究热点。最简单的网络时间隐蔽通道利用数据包在一定时间段内是否缺失来表示隐蔽信息,即在规定时间内到达,则代表比特"1";反之,在规定时间内缺失,则代表比特"0"[4]。但是该编码模式的规律太明显,隐蔽通道与正常信道易被区分。为了减小隐蔽通道对噪声的敏感性,Girling 等通过增加数据包时间间隔来增加鲁棒性[5],但减小了通道的传输速率。Shah 提出了一种实用的隐蔽通道——Jittle Bug[6],该隐蔽通道通过用户远程登录时的按键时间间隔来调制隐蔽信息,但是该方式的同步机制非常脆弱,一旦同步机制被破坏,发送方和接收方之间的隐蔽通道便会停止工作。为了解决发送方和接收方之间的同步问题,Cabuk 等提出一种基于锁相环的新型时间隐蔽通道[7],在该隐蔽通道中,接收方可以通过判断网络延迟的长短,动态地调整时间间隔来对隐蔽信息进行解码。Fahimeh Rezaei 等通过改变接收方的门限来增加隐蔽通道的鲁棒性[8]。上述隐蔽通道将隐蔽信息嵌入到数据包时间间隔中会破坏正常信道的统计特性,如数据

到稿日期:2015-11-14 返修日期:2016-05-29
杨 鹏(1991-),男,硕士生,主要研究方向为操作系统隐蔽通道检测,E-mail:yangpeng199107@163.com;赵 辉(1957-),女,硕士,研究员,主要研究方向为航天测控信息系统结构设计;鲍忠贵(1971-),男,硕士,研究员,主要研究方向为航天测控软件设计。

包时间间隔的分布[7]、相关性[9]、分布熵[10]等，相应的检测方法也被陆续提出。除此之外，Pradhumna L 等提出使用支持向量机来区分隐蔽通道与正常信道[11]；Omar Darwish 等人提出使用分层熵来检测网络时间隐蔽通道，并确定了分析效果最佳的数据包数量[12]。

为了抵抗这些检测方法，使得隐蔽通道与正常信道的特性更加相符，人们开始对隐蔽通道的模型展开研究，Liu Yali 提出了一种应用扩展码的模型[13]，并对模型中的编码做了具体的分析，应用采样定理对该模型的编码进行近似，它能够对正常信道的通信进行较好的模拟；Amir Houmansadr 等利用离散同分布(i. i. d)来模拟隐蔽通道的通信[14]，采用了不同的编码方式，并对这几种编码方式的性能进行了比较；Liu Yali 等同样利用离散同分布(i. i. d)对隐蔽通道的通信进行了建模[15]，提出了可靠性的指标，并对影响该指标的因素进行了分析；Steven Gianvecchio 分析了隐蔽通道的全部设计流程：分析并拟合了正常通信－编码－传输－译码，随后设计了一种隐蔽通道，并检验了该隐蔽通道的有效性[16]。

为了更好地研究网络时间隐蔽通道的特性，本文采用现有的网络时间隐蔽通道模型，并使用泊松分布对正常信道进行模拟，分析了二者之间的差异。在该模型的基础上，本文还首次对影响网络时间隐蔽通道的隐蔽性和数据传输速率的因素进行了分析，得到了这些因素与网络时间隐蔽通道特性之间的变化关系，对今后隐蔽通道的构建工作具有一定的指导意义。

2 网络时间隐蔽通道模型

2.1 模型构架

隐蔽通道的模型架构如图 1 所示。

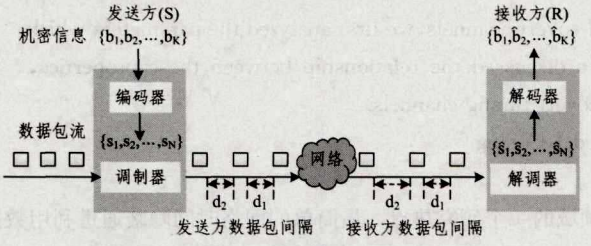


图 1 网络隐蔽通道的模型构架

b_i：隐蔽信息中的第 i 位信息比特。

s_i：应用扩展码编码后的第 i 位编码符号。

d_i：发送方发送的第 i 个数据包时间间隔。

$\hat{d}_i$：接收方接收到的第 i 个数据包时间间隔。

$\hat{s}_i$：接收方译码后的第 i 位编码符号。

$\hat{b}_i$：接收方解码的隐蔽信息中的第 i 位信息比特。

N：编码过程中的扩展因子。

K：编码过程中的并行编码数量。

$R_t=\frac{K}{N}$：每个数据包的传输比特(bit per packet，bpp)。

假设发送方(S)和接受者(R)位于隐蔽通道的两端。发送方 S 能够获得机密信息，并将机密信息传递给接收方 R。为了能够在不被察觉的情况下传递机密信息，发送方 S 需要将机密信息嵌入到正常信道的数据包流中。假设发送方 S 获得的隐蔽信息为$\{b_1,b_2,\cdots,b_K\}$，对这些信息进行编码得到编码符号$\{s_1,s_2,\cdots,s_N\}$，然后对编码符号进行调制得到数据包的时间间隔序列$\{d_1,d_2,\cdots,d_N\}$，最后将时间间隔序列加入到正常数据包流中。接收端 R 接收到的数据包时间间隔为$\{\hat{d}_1,\hat{d}_2,\cdots,\hat{d}_N\}$，对接收到的时间间隔序列进行解调得到编码符号$\{\hat{s}_1,\hat{s}_2,\cdots,\hat{s}_N\}$，最后对这些编码符号进行译码，接收方 R 便得到机密信息的比特$\{\hat{b}_1,\hat{b}_2,\cdots,\hat{b}_K\}$。

2.2 编码与调制

Liu Yali 等提出使用扩展码来增加隐蔽通道的鲁棒性[13]。通过扩展码可以有效地消除网络上噪声和抖动的影响，但是这种方法同样会减少隐蔽通道的容量，影响隐蔽通道的传输速率。下面详细分析扩展码在隐蔽通道中的应用。

假设要传递的隐蔽信息为$\{b_1,b_2,\cdots,b_K\}$，其中每个比特的取值范围为$\{-1,1\}$。接下来应用扩展码对隐蔽信息进行编码。

$$\vec{C}_i=b_i\cdot\vec{c}_i \tag{1}$$

其中，$\vec{c}_i$为编码向量，且 $\vec{c}_i=(c_1,c_2,\cdots,c_N)\in\{\pm1\}^N$。为了有效地提高传输速率，采用 K 路并行传输，则：

$$\vec{S}=(s_1,s_2,\cdots,s_N)=\sum_{i=1}^{K}\vec{C}_i=\sum_{i=1}^{K}b_i\cdot\vec{c}_i \tag{2}$$

接收方接收到传输的编码符号后，对其进行解码。为了能够复原隐蔽信息，要求$\{\vec{c}_0,\vec{c}_1,\vec{c}_2,\cdots,\vec{c}_K\}$是一组正交向量组，$\vec{c}_0$为一个全 1 向量。接收端的复原过程如下：

$$\begin{aligned}\frac{1}{N}\langle\vec{S},\vec{c}_j\rangle&=\frac{1}{N}\langle\sum_{i=1}^{K}b_i\cdot\vec{c}_i,\vec{c}_j\rangle\\&=\frac{1}{N}\sum_{i=1}^{K}b_i\langle\vec{c}_i,\vec{c}_j\rangle\\&=\frac{1}{N}\cdot b_j\cdot N=b_j\end{aligned} \tag{3}$$

在上述的编码过程中，N 为扩展向量的长度，K 为每次传递的隐蔽信息的数量，$K\leqslant N$。而隐蔽通道中每个数据包的传输比特(bpp)的大小为 $R_t=\frac{K}{N}$，当 $K=N$ 时，R_t 达到最大值 1。运用上述编码方式可以有效地增加网络时间隐蔽通道的隐蔽性和鲁棒性。下面分析编码元的概率分布。

计算编码符号 s_j 的概率分布。假设在每个向量$\vec{c}_i$中的 1 和－1 均是以$\frac{1}{2}$的概率均匀分布的，且隐蔽信息中 1 和－1 的分布也是均匀分布的。则对应于某一具体的 s_j，有：

$$s_j=\sum_{i=1}^{K}b_i\cdot\vec{c}_i(j) \tag{4}$$

若 s_j 的值为 l，对应的$\vec{c}_i(j)$中值为 1 的个数为 k_1，值为－1的个数为 k_2，则由编码的方式可以得到如下等式关系：

$$k_1+k_2=K,k_1-k_2=l \tag{5}$$

则编码符号的概率密度函数为：

$$P(s_j=l)=P(k_2=\frac{K-l}{2})$$

$$P(s_j=l)=\begin{cases}\binom{K}{\frac{K-l}{2}}\cdot(\frac{1}{2})^K, & K-l\text{ 为偶数}\\0, & \text{其他}\end{cases} \tag{6}$$

其概率分布函数为：

$$F_s(l)=P(s_i\leqslant l)=\sum_{l_m\leqslant l}P_s(l_m) \tag{7}$$

其中，$-K\leqslant l\leqslant K$。

从隐蔽通道模型的编码符号的概率密度表达式中可以看出，该编码符号的概率密度函数符合二项分布。

接下来说明调制与解调过程。本文将编码符号调制为数

据包时间间隔 t_i 采用的方式：

$$t_i=\alpha+\beta s_i \tag{8}$$

其中，β 为缩放系数，该系数在每次隐蔽信息的传输过程中为固定值；α 为平移系数，该系数遵循[0，T]之间的随机均匀分布，对于每个不同的数据包时间间隔 d_i 有不同的 α，发送方 S 和接收方 R 之间共享该系数的随机数生成种子。

在真实网络中进行传输时，需要考虑网络抖动、延迟对数据包时间间隔的影响。假设传输过程中的抖动为 x，则接收方 R 接收到的数据包时间间隔为 $\hat{t}_i=t_i+x$，接收方 R 对数据包时间间隔进行解码，则接收到的隐蔽信息为：

$$\begin{aligned}
\hat{b}_j&=\frac{1}{N}\langle\frac{1}{\beta}\hat{\vec{t}},\vec{c_j}\rangle=\frac{1}{N\beta}\langle\hat{\vec{t}},\vec{c_j}\rangle\\
\hat{b}_j&=\frac{1}{N\beta}\langle\vec{t},\vec{c_j}\rangle+\frac{1}{N\beta}\langle\vec{x},\vec{c_j}\rangle\\
\hat{b}_j&=\frac{\alpha}{N\beta}\langle\vec{c_0},\vec{c_j}\rangle+\sum_{i=1}^{K}\frac{\beta b_i}{N\beta}\langle\vec{c_i},\vec{c_j}\rangle+\frac{1}{N\beta}\langle\vec{x},\vec{c_j}\rangle\\
\hat{b}_j&=b_j+\frac{1}{N\beta}\langle\vec{x},\vec{c_j}\rangle
\end{aligned} \tag{9}$$

3　仿真结果与分析

Vern Paxson 等指出对于远程登录和文件传输等过程[17]，数据包的发送能够很好地应用泊松分布来拟合；而对于其他的一些数据包传输过程，则与泊松分布存在一定的偏差。本文采用泊松分布来拟合正常信道的数据包传输过程。

泊松分布的概率密度公式为：

$$P(X=k)=\frac{e^{-\lambda}\lambda^k}{k!} \tag{10}$$

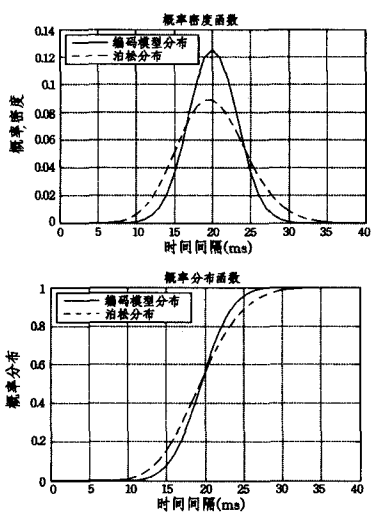


图 2　隐蔽通道编码符号与泊松分布的相关概率函数对比

本文设定隐蔽通道编码符号中的参数 $N=40$，$K=40$，泊松分布中的参数 $\lambda=20$。从图 2 中可以看出，编码符号的概率密度与泊松分布的概率密度形状相似，但是具体的概率值有一定的差异；二者的概率分布函数同样形状相似，概率值存在一定的差异。

3.1　隐蔽性影响因素

Kolmogorov-Smirnov 检验用来测试样本是否来自某一特定分布的方法。它的检验方法是对样本数据的累积频数分布与特定理论分布进行比较，若两者间的差距很小，则推论该样本取自特定分布族。

为了使隐蔽通道不易被发现，隐蔽通道与正常信道的数据包时间间隔应具有同样的概率分布，即使二者的概率分布存在差异，差异也应该尽可能小。为了检测隐蔽通道构造模型的有效性，本文应用 Kolmogorov-Smirnov 检验（KS 检验）[18]对隐蔽信道与正常信道进行检验。在上述模型中，待检测样本的数据包时间间隔分布函数为 $F_s(x)$，正常信道的数据包时间间隔分布函数为 $F_p(x)$，则应用 KS 检测的公式如下：

$$\begin{aligned}
D&=\sup_x|F_s(x)-F_p(x)|\\
D&=\sup_x|\sum_{k\leqslant x}\frac{e^{-\lambda}\lambda^k}{k!}-\sum_{k\leqslant x}P_s(k)|
\end{aligned} \tag{11}$$

其中，$F_s(x)$ 是隐蔽通道中编码符号 $s=x$ 的概率分布函数，$F_p(x)$ 为正常信道的拟合泊松分布。KS 测试的结果越小说明隐蔽通道与正常信道的相似度越高。在编码符号的扩展因子 N 固定的情况下，本文研究并行编码数 K 和泊松分布的参数 λ 对 KS 测试结果的影响，由于其意义不明显，本文改为研究每个数据包的传输比特 $R_t=K/N$ 和泊松分布的参数 λ 对 KS 测试结果的影响，测试结果如图 3 所示。

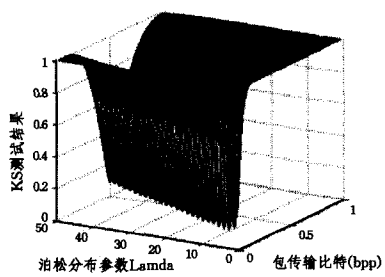
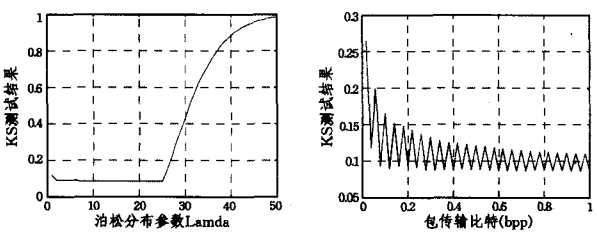


图 3　泊松分布参数和包传输比特与 KS 测试结果的关系

从上述结果可以看出：在编码符号扩展因子 N 固定的情况下，KS 测试结果与包传输比特和泊松分布参数 λ 具有密切的关系，在一些测试结果较好的位置，测试结果能够达到 0.086；即隐蔽通道模型与正常信道泊松分布拟合的概率分布最大差值为 0.086；但是在一些泊松分布参数和包传输比特的取值处，KS 测试结果较差，近似等于 1，此时本文中构建的模型与正常信道中的泊松分布完全不同。为了更好地研究包传输比特（bpp）和泊松分布参数 λ 与 KS 测试结果的关系，分别列出只考虑一个因素的情况下的 KS 测试结果，如图 4 所示（所有结果均在 $N=50$ 的情况下得出）。



(a)KS 测试结果与泊松分布参数 λ 的关系　(b)KS 测试结果与包传输比特（bpp）的关系

图 4　KS 测试结果的影响因素

从图 4 中可以看出，当泊松分布参数 λ 位于范围[1，25]内时，总存在一个包传输比特（bpp）使得 KS 测试结果能够位于 0.08～0.09 之间，这说明此时隐蔽通道中的编码符号与正常信道中泊松分布拟合的概率分布函数相符程度比较高；而当泊松分布参数 λ 位于范围[26，50]时，KS 测试结果逐渐变大，这说明隐蔽通道中的编码符号与正常信道中泊松分布拟合的概率分布函数逐渐偏离。对于每一个包传输比特（bpp），总存在一个泊松分布参数，使得 KS 测试结果取得较小值，而且随着包传输比特（bpp）的增加，KS 测试结果逐渐减小，说

明隐蔽通道中的编码符号与正常信道中泊松分布拟合的概率分布函数相符程度逐渐增加。

下面就图 4 做 3 点说明：1)在图 4(a)中，只有当泊松分布参数 λ 位于[1,25]之间时，KS 测试结果才会很好，这是由于初始设定隐蔽通道扩展因子 $N=50$ 和 $K\leqslant N$ 引起的，则编码过程中的并行编码数量 $K\leqslant 50$，只有当泊松分布参数 λ 与编码过程中的并行编码数量的一半即 $0.5K$ 相等或近似时，隐蔽通道中的编码符号 s_i 才会和正常信道中泊松分布拟合的概率密度函数近似，从而使得二者的 KS 测试结果较小。2)图 4(b)中 KS 测试结果随包传输比特(bpp)而出现间隔波动是由隐蔽通道中编码符号 s_i 的概率密度函数决定的，该编码符号 s_i 符合二项分布，当编码过程中的并行编码数量 K 为偶数时，编码符号 s_i 的概率密度函数的最大值只有一个，此时与泊松分布的概率密度函数的拟合效果更好，因而 KS 测试结果更小；而当编码过程中的并行编码数量 K 为奇数时，编码符号 s_i 的概率密度函数的最大值有两个，此时拟合效果有一定偏差，因而 KS 测试结果要大一些。3)得到的上述结果是由于事先设定隐蔽通道扩展因子 $N=50$ 所致。在实际的隐蔽通道构造过程中，通常先采集正常信道中的数据包时间间隔，并用泊松分布对采集数据进行拟合，获得泊松分布参数 λ，然后确定隐蔽通道扩展因子 N 和编码过程中的并行编码数量 K，对正常信道中数据包的泊松分布进行拟合，总能确定一组合适的参数 N 和 K 使得隐蔽通道与正常信道的 KS 测试结果比较小，满足隐蔽通道的隐蔽性要求。

3.2 数据传输速率的影响因素

隐蔽通道须具有鲁棒性和隐蔽性，以致能够抵抗网络传输过程中抖动和时延的影响，并且不易被检测发现。除此之外，数据传输速率也是隐蔽通道的一个重要特性。设传输的信息比特量为 I，传输时间为 t_{avg}，则数据传输速率 $S=I/t_{avg}$。下面研究在本文构造的隐蔽通道编码模型下影响数据传输速率的因素。在编码符号的扩展因子 N 固定的情况下，研究并行编码数 K 和泊松分布的参数 λ 对数据传输速率的影响，由于该意义不明显，本文改为研究每个数据包的传输比特 $R_t=K/N$ 和泊松分布的参数 λ 对数据传输速率的影响。将数据传输速率应用到本文的模型中，即：

$$S=\frac{I}{t_{avg}}=\frac{K}{N\cdot t_{avg}}$$

$$S=\frac{K}{N\cdot\sum_{i=1}^{K}F_p^{-1}(F_s(s=i))\cdot P_s(s=i)} \tag{12}$$

其中，$F_p^{-1}(\cdot)$为正常信道中泊松分布拟合的概率分布逆函数，$F_s(\cdot)$为隐蔽通道中编码符号的概率分布函数，$P_s(\cdot)$为隐蔽通道中编码符号的概率密度函数。泊松分布参数与包传输速率和数据传输速率的关系如图 5 所示。

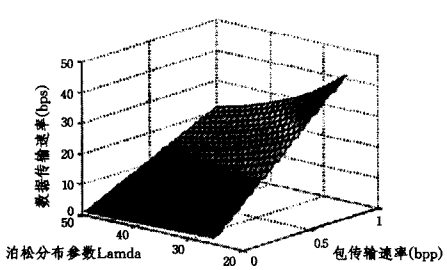


图 5 泊松分布参数与包传输速率和数据传输速率的关系

从图 5 中可以看出：1)随着包传输速率(bpp)的增大，数据传输速率(bit per second，bps)增加。包传输速率(bpp)还代表了数据包的利用率，数据包的利用率越高，数据传输速率(bps)越高。同时，包传输速率(bpp)代表了编码的冗余状况，冗余越小，隐蔽通道的抗干扰特性越差。二者相互矛盾，不可能同时满足。在实际的隐蔽通道构建过程中，包传输速率(bpp)的具体设定需要依据隐蔽通道的具体要求。2)随着泊松分布参数 λ 的增大，数据包传输速率(bps)逐渐减小。参数 λ 为泊松分布的均值，代表实际传输过程中数据包时间间隔的均值，随着数据包时间间隔均值的增大，数据包传输速率(bps)减小。

结束语 本文构建了一种网络时间隐蔽通道的模型，并详细阐述了在模型中运用扩展码对需要传输的信息进行编码和调制的过程。在此基础上，分析了该模型下调制后传输的编码符号的概率分布状况，并与正常信道中泊松分布拟合函数做了比较全面的对比。同时针对隐蔽通道特性——隐蔽性和数据传输速率，针对该模型首次分析了隐蔽通道中编码与调制过程中的参数对其隐蔽性和传输速率的影响，给出了详细的分析过程，并得到了一些有益的结论：1)隐蔽通道检测方法——KS 测试的结果与泊松分布参数 λ 和包传输速率(bpp)有密切的关系，随着包传输速率(bpp)的增大，KS 测试结果逐渐变好，泊松分布参数 λ 对 KS 测试结果的影响同时还与隐蔽通道模型中的扩展因子 N 有关，具体的分析见 2.1 节；2)随着包传输速率(bpp)的增大，数据传输速率(bps)增加；随着泊松分布参数 λ 的增大，数据包传输速率(bps)逐渐减小。

本文采用泊松分布模型来拟合正常信道，该模型对正常信道中的远程登录和文件传输等过程的数据包时间间隔具有较好的拟合效果，但是对于其他的数据包传输过程不能完全体现正常信道中数据包时间间隔的分布情况。通过仿真实验发现，采用文中的隐蔽通道模型可以很好地拟合正常信道的特性，并对影响隐蔽通道特性的参数做了具体的研究。在以后的工作中，将对正常信道中数据包时间间隔的拟合进行更加深入的研究。

参 考 文 献

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

[2] ZANDER S, ARMITAGE G, BRANCH P. A survey of covert channels and counter measures in computer network protocols [J]. Communication Surveys & Tutorials, 2007, 9(3): 44-57.

[3] QIAN Yu-wen, ZHAO Bang-xin, KONG Jian-shou, et al. Robust Covert Timing Channel Based on Web[J]. Journal of Computer Research and Development, 2011, 48(3): 423-431. (in Chinese)
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.

[4] PADLIPSKY M A, SNOW D W, KARGER P A. Limitations of end-to-end encryption in secure computer networks[R]. Mitre Corp Bedford Ma, 1978.

[5] GIRLING C G. Covert Channels in LAN's[J]. IEEE Transactions on Software Engineering, 1987(2): 292-296.

[6] SHAN G, MOLINA A, BLAZE M. Keyboards and Covert Channels[C]// USENIX Security. 2006.

[7] 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. ACM, 2004: 178-187.

(下转第 154 页)

因为某个关键字的分数过高而影响排序结果，提高了检索的准确性。未来将着重于采用不同的加密方法对索引进行加密，使索引具有更高的安全性。

参 考 文 献

[1] FENG Chao-sheng, QIN Zhi-guang, YUAN Ding. Techniques of Secure Storage for Cloud Data[J]. Chinese Journal of Computers, 2015, 38(1): 150-163. (in Chinese)
冯朝胜，秦志光，袁丁. 数据安全存储技术[J]. 计算机学报，2015，38(1)：150-163.

[2] SHEN Zhi-rong, XUE Wei, SHU Ji-wu. Surveyon the Research and Development of Searchable Encryption Schemes[J]. Journal of Software, 2014, 25(4): 880-895. (in Chinese)
沈志荣，薛巍，舒继武. 可搜索加密机制研究与进展[J]. 软件学报，2014，25(4)：880-895.

[3] SONG D X, WAGNER D, PERRING A. Practical Techniques for Searches on Encrypted Data[C]// IEEE Symposium on Security and Privacy, 2000: 44-55.

[4] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: Improved definitions and efficient constructions[C]// Proc of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 79-88.

[5] CAO Ning, WANG Cong, LI Ming, et al. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data[C]// Proc of INFOCOM. Shanghai: IEEE. 2011: 829-837.

[6] WONG W K, CHEUNG W L, KAO B, et al. Secure kNN computation on encrypted databases[C]// Proc of SIGMOD. New York: ACM, 2009: 139-152.

[7] CHENG Fang-quan, PENG Zhi-yong, SONG Wei, et al. An Efficient Privacy-Preserving Rank Query over Encrypted Data in Cloud Computing[J]. Chinese Journal of Computers, 2012, 35(11): 2215-2227. (in Chinese)
程芳权，彭智勇，宋伟，等. 云环境下一种隐私保护的高效密文排序查询方法[J]. 计算机学报，2012，35(11)：2215-2227.

[8] ZHANG Wei, XIAO Sheng, LIN Ya-ping, et al. Secure Ranked Multi-keyword Search for Multiple Data Owners in Cloud Computing[C]// Proc of Dependable Systems and Networks (DSN). Atlanta: IEEE, 2014: 276-286.

[9] IBRAHIM A, JIN H, YASSIN A, et al. Secure Rank-ordered Search of Multi-keyword Trapdoor over Encrypted Cloud Data [C]// Proc of Services Computing Conference (APSCC). Guilin: IEEE, 2012: 263-270.

[10] KAMARA S, PAPAMANTHOU C. Parallel and Dynamic Searchable Symmetric Encryption[M]// Financial Cryptography and Data Security. Berlin: Springer Berlin Heidelberg, 2013: 258-274.

[11] XIA Zhi-hua, WANG Xin-hui, SUN Xing-ming, et al. A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 7(2): 340-352.

[12] WANG Cong, CAO Ning, REN Kui, et al. Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1467-1479.

[13] SUN Wen-hai, WANG Bing, CAO Ning, et al. Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(11): 3025-3035.

[14] ZHANG Wei, LIN Ya-ping, XIAO Sheng, et al. Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing[J]. IEEE Transactions on Computers, 2016, 65(5): 1566-1577.

[15] ZERR S, OLMEDILLA D, NEJDL W, et al. Zerber^{+R}: Top-k retrieval from a confidential index[C]// Proc of EDBT. New York: ACM, 2009: 439-449.

[16] Lucene3. 5[OL]. http://jakarta. apache. org/lucene.

[17] LI Hong-wei, YANG Yi, TOM L, et al. Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(3): 312-325.

(上接第 148 页)

[8] REZAEI F, HEMPEL M, SHRESTHA P L, et al. Achieving robustness and capacity gains in covert timing channels[C]// 2014 IEEE International Conference on Communications (ICC). IEEE, 2014: 969-974.

[9] BERK V, GIANI A, CYBENKO G, et al. Detection of covert channel encoding in network packet delays[R]. Department of Computer Science, Dartmouth College, 2005.

[10] GIANVECCHIO S, WANG H. Detecting covert timing channels: an entropy-based approach[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 307-316.

[11] SHRESTHA P, HEMPEL M, REZAEI F, et al. A Support Vector Machine-based Framework for Detection of Covert Timing Channels[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 274-283

[12] DARWISH O, AL-FUQAHA A, ANAN M, et al. The role of hierarchical entropy analysis in the detection and time-scale determination of covert timing channels[C]// 2015 International Conference onWireless Communications and Mobile Computing (IWCMC). IEEE, 2015: 153-159.

[13] LIU Y, GHOSAL D, ARMKNECHT F, et al. Hide and seek in time—robust covert timing channels[M]// Computer Security-ESORICS 2009. Springer Berlin Heidelberg, 2009: 120-135.

[14] HOUMANSADR A, BORISOV N. CoCo: coding-based covert timing channels for network flows[M]// Information Hiding. Springer Berlin Heidelberg, 2011: 314-328.

[15] LIU Y, GHOSAL D, ARMKNECHT F, et al. Robust and undetectable steganographic timing channels for iid traffic[M]// Information Hiding. Springer Berlin Heidelberg, 2010: 193-207.

[16] GIANVECCHIO S, WANG H, WIJESEKERA D, et al. Model-based covert timing channels: Automated modeling and evasion [M]// Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2008: 211-230.

[17] PAXSON V, FLOYD S. Wide area traffic: the failure of Poisson modeling[J]. IEEE/ACM Transaction on Networking (ToN), 1995, 3(3): 226-244.

[18] RICHARDSON A M. Nonparametric Statistics: A Step-by-Step Approach[J]. International Statistical Review, 2015, 83(1): 163-164.