·网络空间安全· 文章编号：1000-3428(2020)02-0154-05 文献标志码：A 中图分类号：TP393

基于 Markov 模型的 HTTP 参数排序隐蔽信道检测方法

沈国良[1]，翟江涛[1]，戴跃伟[2]

（1. 江苏科技大学 电子信息学院，江苏 镇江 212003；2. 南京信息工程大学 计算机与软件学院，南京 210000）

摘 要： 网络隐蔽信道是利用网络协议中的保留、可选或未定义等字段在网络不同主机间建立秘密消息传输的通信信道，其中 HTTP 协议作为万维网上最常用的协议之一，是网络隐蔽信道的良好载体。为有效检测基于 HTTP 协议的隐蔽信道，提出一种基于 Markov 模型的隐蔽信道检测方法。以 Host、Connection、Accept 和 User-Agent 为关键字，建立数据包的 Markov 模型并计算其状态转移概率矩阵，利用待测数据包与正常数据包 2 个概率矩阵之间的相对熵，判别是否存在隐蔽信道通信。实验结果表明，当隐蔽信道中的异常数据超过 70% 时，该方法检测率可达 97% 以上。

关键词： HTTP 协议；隐蔽信道检测；Markov 模型；相对熵；检测率

开放科学（资源服务）标志码（OSID）：

中文引用格式： 沈国良，翟江涛，戴跃伟. 基于 Markov 模型的 HTTP 参数排序隐蔽信道检测方法[J]. 计算机工程，2020，46(2)：154-158，169.

英文引用格式： SHEN Guoliang，ZHAI Jiangtao，DAI Yuewei. HTTP parameter sorting covert channel detection method based on Markov model[J]. Computer Engineering，2020，46(2)：154-158，169.

HTTP Parameter Sorting Covert Channel Detection Method Based on Markov Model

SHEN Guoliang[1]，ZHAI Jiangtao[1]，DAI Yuewei[2]

（1. School of Electronics and Information，Jiangsu University of Science and Technology，Zhenjiang，Jiangsu 212003，China；
2. School of Computer and Software，Nanjing University of Information Science and Technology，Nanjing 210000，China）

【Abstract】 The network covert channel is a communication channel that establishes secret message transmission between different hosts on the network by utilizing reserved，optional or undefined fields in the network protocols. HTTP protocol，as one of the most commonly used protocols on the World Wide Web，becomes a good carrier of network covert channels. In order to effectively detect the HTTP protocol-based covert channel，this paper proposes a covert channel detection method based on Markov model. Taking Host，Connection，Accept and User-Agent as keywords，this method establishes the Markov model of data packet and calculates the state transition probability matrix of this model. The relative entropy between the data packet to be tested and the normal data packet is used to determine whether the covert channel exists or not. Experimental results show that when the abnormal data in the covert channel exceeds 70% ，the detection rate of this method can reach more than 97% .

【Key words】 HTTP protocol；covert channel detection；Markov model；relative entropy；detection rate

DOI： 10.19678/j.issn.1000-3428.0053783

0 概述

1973 年 LAMPSON 提出“covert channel”概念，其最初的定义是建立在多安全等级（Multi-Level Security，MLS）的自动化信息系统（Automated Information System，AIS）中，主要针对在不同主体和对象间的访问控制及安全分类。如今，其主要针对高度互联的网络，实体为网络应用程序或网络节点[1]，因而隐蔽信道的另一个更广泛更具适应性的定义为“策略上被拒绝但性质上允许的通信信道”。根据该定义，隐蔽信道可以延伸到网络传输的各个协议中，尤其是占据一半流量的 HTTP 协议，成为隐

基金项目： 国家自然科学基金（61702235，61472188，61602247，U1636117）；江苏省自然科学基金（BK20150472，BK20160840）。

作者简介： 沈国良（1994—），男，硕士研究生，主研方向为多媒体与信息安全；翟江涛（通信作者），副教授；戴跃伟，教授、博士生导师。

收稿日期： 2019-01-22 **修回日期：** 2019-03-21 **E-mail：** jiangtaozhai@gmail.com

蔽通信的良好载体。

HTTP 隐蔽信道分为存储式隐蔽信道[2]、时间式隐蔽信道[3]和网络行为隐蔽信道[4]。存储式隐蔽信道主要是利用 HTTP 协议报文中部分不关键的字段名或值嵌入隐密消息以实现隐蔽通信,如将某些保留、可选用或未定义的字段修改为经过编码的隐蔽数据[5]。传统的 HTTP 存储式隐蔽信道包括对 URI[6]、Cookies[7]、User-Agent[8]以及网页重定向等元素进行编码嵌入隐蔽信息实现隐蔽通信。时间式隐蔽信道主要利用网络传输 HTTP 数据包的时间特性来隐藏信息[9],通常使用数据包的收发时间以及包间时延等特性,例如 On-off 是一种典型的时间式隐蔽信道[10],它由信息发送端和接收端约定一个时间间隔,在此期间若有数据包发送代表隐秘信息“1”,无数据包发送则代表隐秘信息“0”。网络行为隐蔽信道往往是在用户访问网络的行为中编码嵌入消息并表现为用户的一系列操作[11],如 LiHB[12]通过数学组合的编码方式将 N 个请求分配到 M 条流中,接收端只要解码不同流对应的请求数量就能接收到隐蔽信息。

为了对抗隐蔽通信的非法使用,实现网络安全的可管可控,研究者们也陆续研究各种检测算法。文献[13]提出网络场景检测方法为用户提供使用潜在隐蔽信道的场景,但是面对实际网络中的复杂场景,其检测性能并不理想。文献[14]通过基于直方图的算法对正常通信时间序列与隐蔽通信的时间序列分别建模,并提出一种基于 Kolmogorov-Smimov(KS)统计量的检测算法。文献[15]根据时间式隐蔽信道的特点,提出检测波形形状的检测方法。上述 2 种方法对数据包的包间间隔等时间特性进行统计分析,取得了较好的检测效果,但不适用于检测网络行为信道。文献[16]提出基于校正熵的统计检测方法,并取得良好的检测率,但该方法并不能实现对存储式信道的检测。针对存储式信道的检测,文献[17-18]采用基于 SVM 的机器学习检测算法,利用正常数据和含密数据的差异进行检测;文献[19]提出基于 K-means 聚类的检测方法,对 HTTP 协议 GET 消息编码的隐蔽信道进行检测。

HTTP 协议中的参数排序隐蔽信道利用请求报文自身排序编码隐蔽信息,而上述检测方法主要通过包间间隔提取特定属性,无法对该信道进行检测。因此,根据信道需要频繁改变其报文的特性,本文提出一种基于 Markov 模型的 HTTP 参数排序隐蔽信道检测方法。

1　HTTP 协议中的隐蔽信道

HTTP 是万维网能够可靠交换文件(包括文本、声音、图像等各种多媒体文件)的重要基础。HTTP 的报文分为请求报文和响应报文。HTTP 请求报文由请求行、请求头部和请求正文组成,如图 1 所示。其中,请求头部包含有关客户端环境以及请求正文的有用信息。请求头部由“关键字:值”对组成,每行一对,关键字和值之间使用英文符号“:”分隔。采用 Wireshark 捕获到的 HTTP 请求报文如图 2 所示,其中 Host、Connection、User-Agent 及 Accept 等都是比较常见的报文信息,提供了使用浏览器类型、接收对象类型等信息。

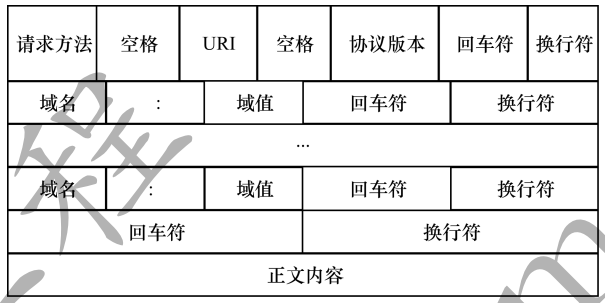

图 1　HTTP 请求报文的一般格式

Fig. 1　General format of HTTP request message

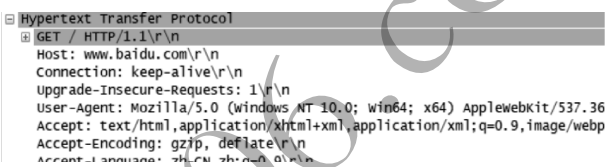

图 2　Wireshark 捕获的 HTTP 请求包

Fig. 2　HTTP request packet captured by Wireshark

HTTP 协议的参数排序通信隐藏算法[20]对序列 $\{A_i|0\leqslant i<n\}$ 中的所有对象进行特定排序。该算法在不改变对象之间顺序的前提下,使其中每一个对象可以在序列中出现或者不出现,所有对象全部出现的情况称为原始排序。对象出现代表发送隐秘信息“1”,对象不出现代表发送隐蔽信息“0”,因此,该算法也称为二进制排序算法。如图 3 所示,信息发送方用户客服端发起请求,接收方可以是假定的服务器,其中基准报文即为原始排序,以6 条关键字构造隐蔽信息通道,全部对象出现,用 111111 表示。在 2 次二进制排序报文中,接收方分别接收到 001110 和 110001 的隐蔽信息。

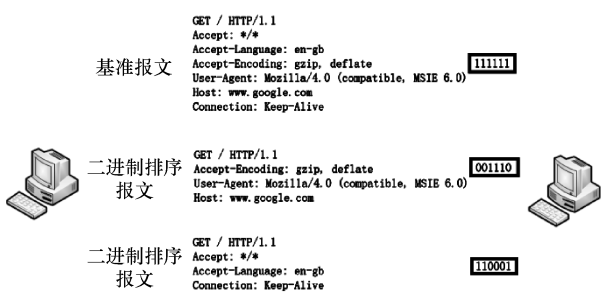

图 3　参数排序隐蔽通信的原理

Fig. 3　Principle of parameterized covert communication

该方法不会在 HTTP 报文中插入额外的字符,

只是通过改变其原有的排序达到隐藏消息的目的。因为在不同操作系统、浏览器下对于同一功能产生的 HTTP 报文表述形式差别很大,所以在 HTTP 报文中这些关键字经常被忽略。因此,利用上述特性构建的 HTTP 参数排序隐蔽信道,不会引起正常通信的异常,并且在少量样本下,人们无法判断该数据包是正常通信或者隐蔽通信引起的关键字缺失。但是该隐蔽信道的通信与正常通信的区别在于,隐蔽通信为了传输信息需要频繁改变报文,而正常通信的报文通常变化不会很大,且变化频率较低。假设 HTTP 数据包的报文对应一种状态,那么隐蔽通信的状态转换将比正常通信更为频繁。因此,可以通过大量数据建立正常通信和隐蔽通信的模型来衡量两者的差异性。Markov 模型是一种成熟的统计模型,其核心思想是每个状态值只取决于前面一个状态而与其他状态无关[21]。本文将数据包报文转化为对应的状态,通过建立正常通信和隐蔽通信的 Markov 模型状态转移概率矩阵,用相对熵来衡量两者之间的差异。

2 基于 Markov 模型的检测算法

2.1 Markov 链

Markov 链是一个时间和状态都是离散的马尔可夫过程。假设数据链 $X=\{x_1,x_2,\cdots,x_n\}$ 中任意一个变量 x_t 的值都在有限集 $E=\{0,1,\cdots,n\}$ 中,即当 $n\geqslant 1$ 时,$i_1,i_2,\cdots,i_n\in E$,则式(1)成立。

$$p\{x_n=i_n|x_{n-1}=i_{n-1},x_{n-2}=i_{n-2},\cdots,x_1=i_1\}=p\{x_n=i_n|x_{n-1}=i_{n-1}\} \tag{1}$$

数据链 $X=\{x_1,x_2,\cdots,x_n\}$ 即为一个具有可数状态的 Markov 链,其每个状态值只取决于前面一个状态而与其他状态无关。对于任意 $i,j\in E$,从时刻 $n-1$ 到时刻 n 的转移概率由式(2)给出。

$$p(x_n=i_n|x_{n-1}=i_{n-1})=\{x_n=j|x_{n-1}=i\}=p_{ij} \tag{2}$$

其中,p_{ij} 是系统从状态 i 变化到状态 j 的转移概率。假设一个系统的有限状态集 E 最多有 δ 个值,Markov 链 X 的状态转移概率矩阵可以用式(3)表示,其中满足每一行的转移概率和为 1,即 $\sum_{j=1}^{\delta}p_{ij}=1$。

$$\boldsymbol{P}=\begin{bmatrix}p_{11} & p_{12} & \cdots & p_{1\delta}\\ p_{21} & p_{22} & \cdots & p_{2\delta}\\ \vdots & \vdots & & \vdots\\ p_{\delta 1} & p_{\delta 2} & \cdots & p_{\delta\delta}\end{bmatrix} \tag{3}$$

序列 $X=\{x_1,x_2,\cdots,x_n\}$ 的状态转移概率矩阵可由下式给出:

$$p_{ij}=\frac{\{x_t|x_t=i,x_{t+1}=j\}}{\{x_t|x_t=i\}} \tag{4}$$

Markov 链的初始状态为:

$$Q=\{q_1,q_2,\cdots,q_\delta\} \tag{5}$$

其中,q_i 表示状态值为 $i(i=1,2,\cdots,\delta)$ 的概率,q_i 满足式(6)。

$$q_i=\frac{N_i}{N} \tag{6}$$

其中,N 表示序列的总长度,N_i 表示序列中状态值为 i 的总个数。

在 HTTP 协议中,客户端发送的请求报文中的关键字可能出现或者不出现,将所有可能排列情况视为独立状态,一个 HTTP 数据包的报文状态就是一个随机且有限的状态集,其当前状态只与上一个状态有关,因此,可以使用 Markov 链构建 HTTP 数据包的状态模型。

在 HTTP 参数排序隐蔽信道中,每一个关键字的出现与否都是组成某一时刻状态的因素,由于关键字种类繁多且正常通信中使用极少数,为了便于呈现,本文选取其中 4 个最为常见的关键字构建隐蔽信道,分别为 Host、Connection、Accept 和 User-Agent。通过 HTTP 数据包关键字的状态对应的二进制序列,计算得到 HTTP 数据包的状态位。

$$E_k=8\times E_{\text{Host}}+4\times E_{\text{Connection}}+2\times E_{\text{Accept}}+1\times E_{\text{User-Agent}} \tag{7}$$

由于每一个关键字都有 2 种取值,因此可计算得到 HTTP 数据包共有 16 种状态位,即 $E=\{0,1,\cdots,15\}$。

2.2 Markov 转移概率矩阵

对一个 HTTP 包数据集 $T_n=\{t_1,t_2,\cdots,t_n\}$,根据式(3)和式(4)求得其 Markov 链状态转移概率矩阵,建模过程为:提取数据包中的关键字,转化为二进制序列,利用式(7)计算得到 HTTP 包的状态,训练并得到 Markov 模型转移概率矩阵。因为要检测信道是否为隐蔽信道,所以除了要建立用于比较的实际 HTTP 包 Markov 模型转移概率矩阵,还要建立每一个待测数据集的 Markov 模型转移概率矩阵。

2.3 本文检测算法

本文采用相对熵对建立的模型进行比较,相对熵可以用来衡量 2 个概率分布之间的差异。假设 $p(x)$ 和 $q(x)$ 是离散随机变量 X 中的 2 个概率分布,则 p 和 q 的相对熵为:

$$D(p\parallel q)=\sum_x p(x)\ln\frac{p(x)}{q(x)} \tag{8}$$

$p(x)$ 和 $q(x)$ 分布相同,则相对熵等于 0;两者之间差异越大,则相对熵越大。本文利用相对熵的定义来计算正常数据流和待测数据流的 Markov 模型的状态转移概率矩阵的差异,计算公式为:

$$D(\boldsymbol{M}^{(p)}\parallel\boldsymbol{M}^{(q)})=\sum_{i,j}M_{ij}^{(p)}\ln\left(\frac{M_{ij}^{(p)}\sum_j M_{ij}^{(q)}}{\sum_j M_{ij}^{(p)}M_{ij}^{(q)}}\right) \tag{9}$$

其中,$\boldsymbol{M}^{(p)}$ 和 $\boldsymbol{M}^{(q)}$ 为 2 个转移概率矩阵,$M_{ij}^{(p)}$ 表示转

移概率矩阵 $\boldsymbol{M}^{(p)}$ 中 p_{ij} 的值,$M_{ij}^{(q)}$ 表示转移概率矩阵 $\boldsymbol{M}^{(q)}$ 中 p_{ij} 的值,可由式(4)求得。

2 个矩阵的差异越大,则其相对熵越大。因此,可以通过设定阈值来判断数据流是否异常,大于阈值则为隐蔽通信数据流,小于阈值则为正常通信数据流。正常通信数据流由于 HTTP 包的报文信息比较稳定,没有出现 4 个关键字均不出现的情况,所以部分状态值的数量为 0,导致当利用式(3)和式(4)计算数据流转移概率矩阵时,出现 0 元素及部分元素无意义,从而无法用式(9)计算 2 个模型之间的相对熵。因此,设定这些元素为一个很小的概率 $p_{ij} = 1.0 \times 10^{-6}$。同样,将这种方法应用到待测数据流的转移概率矩阵建立中。基于 Markov 模型的检测算法总体流程如图 4 所示。

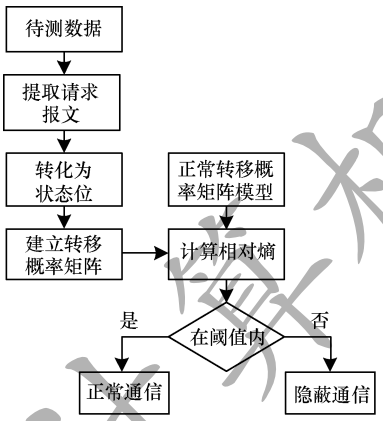

图 4　本文算法检测流程

Fig. 4　Detection process of algorithms herein

3　实验与结果分析

本文实验收集 40 000 个正常 HTTP 数据包和 20 000 个异常数据包。正常数据包通过 Fiddler 捕捉用户电脑与互联网之间的 HTTP 通信得到。将待发送消息编码成二进制信息,并以每 4 位嵌入一个 HTTP 包,根据第 1 节介绍的隐蔽信道构建方式,结合发送的二进制信息利用 Fiddler 篡改正常数据包报文中的 4 个关键字,获取异常数据包。实验首先通过模型训练设置合适的相对熵阈值,这是判断数据流是否异常的关键;其次设定一个合适的窗口大小,因为窗口过小容易减小待测模型与正常模型之间的差异,从而降低检测效果,窗口过大会影响检测速度;最后计算在正常数据流中嵌入 50% ~100% 的异常数据包时的检测率。

3.1　相对熵阈值的选定

本文实验分别取 10 000 个正常和含密的 HTTP 数据包作为训练集,其余用作测试集。以 1 000 窗口大小分割测试集为 20 组,含密数据和正常数据各 10 组。计算每一组中各个状态值的数量,并求出 10 组数据的均值,结果如图 5 所示。可以看出,异常数据包状态值从 0 到 9 数量较为均匀,在 100 上下浮动,状态值大于 8 的数据包数量均在 50 左右;正常数据包状态值低于 8 的数量为 0,这是因为正常数据包中都包含 Host 关键字,并且大部分状态值都是 15。根据建立训练集的 Markov 转移概率矩阵与实际模型求相对熵,结果如图 6 所示。

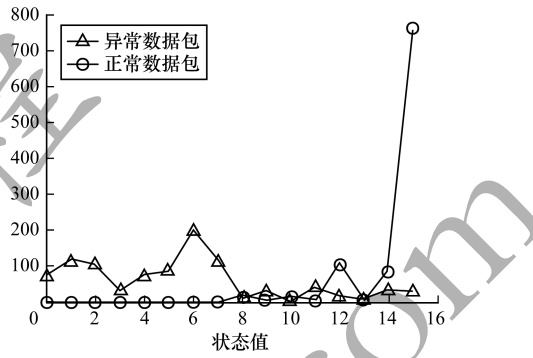

图 5　每组中的状态值数量均值

Fig. 5　Mean number of status values in each group

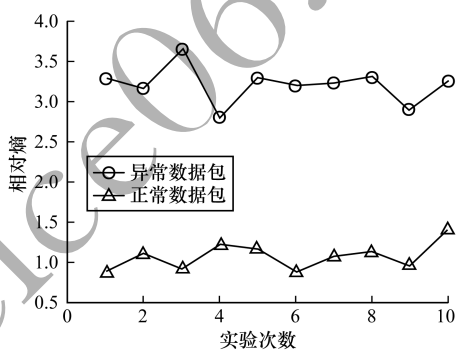

图 6　训练集与正常模型相对熵的值

Fig. 6　Relative entropy values of training set and normal model

从图 6 可知,异常数据流与选定的实际模型之间相对熵较大,正常数据流则偏小,结合图 5 中的结果,这是因为正常数据流中状态值为 12、14 和 15 的数据包占多数,与实际模型差异较小,而异常数据流中各个状态位的数据包较为均匀,与实际模型差异较大。其中,与异常数据流的最小相对熵值接近 2.5,与正常数据流的最大相对熵值接近 1.5,因此,设定阈值为 2,即当测试集与实际模型的相对熵值超过 2 时,判定为异常数据流,否则为正常数据流。

3.2　窗口大小的选定

为了分析窗口大小对检测率的影响,在设定相对熵阈值为 2,按不同窗口对测试集切割分为若干组,计算其检测率,结果如图 7 所示。

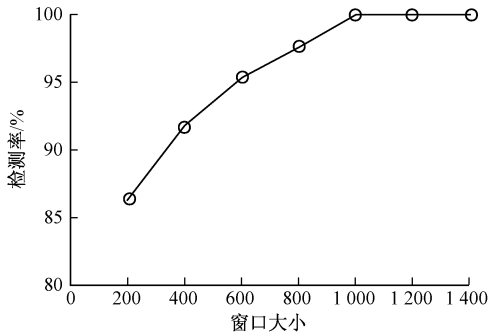

图 7 不同窗口下的检测率

Fig. 7 Detection rate in different window sizes

从图 7 可以看出,窗口较小对实验的检测率影响较大。这是因为较小数据包构建的异常数据流模型容易在局部与实际模型相似,大幅减小了相对熵的值。而当窗口大于等于 1 000 时,该方法均可取得较好的检测效果,因此,可将窗口设置为 1 000。

3.3 嵌入率对检测结果的影响

嵌入率是指在一个数据流中包含的异常数据包占总数据包的比例。在相对熵阈值为 2,窗口大小为 1 000 情况下,计算不同嵌入率下的检测率和误报率,结果如图 8 所示。由于嵌入率较低时,检测率偏低,因此在图 8 中只显示嵌入率大于 50% 的数据。

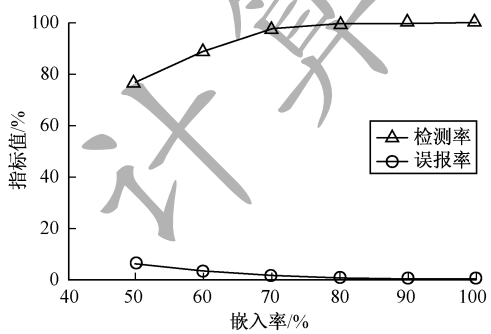

图 8 不同嵌入率下的检测率和误报率

Fig. 8 Detection rate and false alarm rate at different embedding rates

从图 8 可以看出,嵌入率在 50% 至 60% 的区间内,检测率较低。这是因为数据包中大量正常数据包的存在,使得由状态 15 向状态 15 的转移依旧占据主导地位,导致与实际模型计算相对熵时偏小,最终影响检测率。在嵌入率不小于 70% 时,所有状态值的数量趋于平均,加大了与实际模型的差异,检测率可以保持在 97% 以上。当嵌入率为 100% 时,检测率高达 99% ,并且保持极低的误报率。

4 结束语

本文分析基于 HTTP 的二进制排序隐蔽信道特征,利用隐蔽通信的状态转换比正常通信更频繁的特点,将基于 Markov 模型的检测方法用于隐蔽信道的检测,并以待测数据包和正常数据包的转移概率矩阵之间的相对熵作为判别标准。实验结果表明,该方法在窗口大小为 1 000 时,能够对嵌入率超过 70% 的异常数据流保持较高的检测率。但是本文没有考虑到该方法对于其他隐蔽通信方式的适用性,下一步将对其通用性进行研究。

参考文献

[1] GEISLER D, MAZURCZYK W, KELLER J. Towards utilization of covert channels as a green networking technique[C]//Proceedings of the 13th International Conference on Availability, Reliability and Security. New York, USA: ACM Press, 2018: 1-10.

[2] LIU Fang, LI Dongdong, ZHAO Yuntao, et al. The covert communication detection model based on key field of header in HTTP protocol[J]. Fire Control and Command Control, 2018, 43(11): 40-45. (in Chinese)
刘芳,李东东,赵运弢,等. HTTP 协议报文头域关键字段的隐蔽通信检测模型[J]. 火力与指挥控制,2018,43(11):40-45.

[3] ZHANG Lihua. Research on Anti-interference Technology of covert channel in time network[D]. Nanjing: Nanjing University of Science and Technology, 2017. (in Chinese)
张立华. 时间式网络隐蔽信道抗扰技术研究[D]. 南京:南京理工大学,2017.

[4] KOGOS K G, SELIVERSTOVA E I, EPISHKINA A V. Review of covert channels over HTTP: communication and countermeasures[C]//Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. Washington D. C., USA: IEEE Press, 2017: 459-462.

[5] LIANG Jun. The improvement and optimization of the network storage covert channel test simulation[J]. Computer Simulation, 2017, 34(2): 406-409. (in Chinese)
梁竣. 网络存储隐蔽信道检测的改进与优化仿真[J]. 计算机仿真,2017,34(2):406-409.

[6] LIU Zhengyi, SONG Tian. Covert sequence channel based on HTTP/2 protocol[J]. Journal of Computer Research and Development, 2018, 55(6): 1157-1166.

[7] JOHNSON M, LUTZ P, JOHNSON D. Covert channel using man-in-the-middle over HTTPS[C]//Proceedings of 2016 International Conference on Computational Science and Computational Intelligence. Washington D. C., USA: IEEE Press, 2016: 917-922.

[8] WANG Fei. Research on design and detection technology of covert channels based on WEB[D]. Hefei: University of Science and Technology of China, 2014. (in Chinese)
王飞. 基于 WEB 的隐蔽信道设计与检测技术研究[D]. 合肥:中国科学技术大学,2014.

[9] ZHANG Xiaosing, LIANG Chen, ZHANG Quanxin, et al. Building covert timing channels by packet rearrangement over mobile networks[J]. Information Sciences, 2018, 445: 66-78.

[10] BELOZUBOVA A, EPISHKINA A, KOGOS K. Random delays to limit on/off covert channel[C]//Proceedings of the 18th Mediterranean Electrotechnical Conference. Washington D. C., USA: IEEE Press, 2016: 1-5.

(下转第 169 页)

(上接第 158 页)

[11] QI Wen, DING Wanfu, WANG Xinyu, et al. Construction and mitigation of user-behavior-based covert channels on smartphones[J]. IEEE Transactions on Mobile Computing,2017,17(1):44-57.

[12] SHEN Yao, HUANG Liusheng, WANG Fei, et al. LiHB:lost in HTTP behaviors-a behavior-based covert channel in HTTP[C]//Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. New York,USA:ACM Press,2015:55-64.

[13] QIAN Yuwen, SONG Huaju, ZHAO Bangxin, et al. Study on the detection algorithm of covert network behavior channel based on corrected entropy[J]. Systems Engineering and Electronics, 2013, 35(6): 1312-1317. (in Chinese)
钱玉文,宋华菊,赵邦信,等. 基于校正熵的网络行为隐蔽信道的检测算法[J]. 系统工程与电子技术,2013,35(6):1312-1317.

[14] 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.

[15] QIAN Yuwen, SONG Huaju, SONG Chao, et al. Network covert channel detection with cluster based on hierarchy and density[J]. Procedia Engineering, 2012, 29:4175-4180.

[16] SAYADI S, ABBES T, BOUHOULA A. Detection of covert channels over ICMP protocol[C]//Proceedings of 2017 IEEE/ACS International Conference on Computer Systems and Applications. Washington D. C., USA:IEEE Press,2017:1247-1252.

[17] SUR A, NAIR A S, KUMAR A, et al. Steganalysis of network packet length based data hiding[J]. Circuits, Systems,and Signal Processing,2013,32(3):1239-1256.

[18] CABUK S, BRODLEY C E, SHIELDS C. IP covert channel detection[J]. ACM Transactions on Information and System Security,2009,12(4):1-29.

[19] LI Meng. Research on several typical network steganalysis algorithms[D]. Zhenjiang: Jiangsu University of Science and Technology,2019. (in Chinese)
李萌. 几种典型网络隐写检测算法研究[D]. 镇江:江苏科技大学,2019.

[20] MA Wenyan. Several new application layer covert channels on the HTTP protocol[J]. Computer CD Software and Applications, 2014(15): 179-180. (in Chinese)
马文岩. HTTP 协议上几种新的应用层隐蔽通道[J]. 计算机光盘软件与应用,2014(15):179-180.

[21] HAN Chunhao. Research and application of network traffic classification[D]. Beijing: Beijing University of Chemical Technology,2017. (in Chinese)
韩春昊. 网络流量分类研究与应用[D]. 北京:北京化工大学,2017.

编辑　刘盛龄