基于量子神经网络的启发式网络隐蔽信道检测模型*

唐彰国，李焕洲，钟明全，张 健
（四川师范大学 网络与通信技术研究所，成都 610066）

摘 要：为了提高隐蔽信道的检测率，讨论了传统的隐蔽信道检测技术的原理并对其特点作了详细的对比研究；通过对网络隐蔽通道特点的归纳和分析，找到可以描述网络隐蔽通道的若干属性，并提出基于网络隐蔽通道特征指纹的检测思想，归纳出隐蔽信道在协议域、统计规律、行为特征等方面表现出的通信指纹信息，在此基础上，设计并实现了一个基于量子神经网络的启发式网络隐蔽信道检测模型。测试结果表明该检测模型运行高效、检测结果较准确。

关键词：隐蔽信道；量子神经网络；通信指纹；启发式；检测
中图分类号：TP393 **文献标志码**：A **文章编号**：1001-3695(2012)08-3033-03
doi:10.3969/j.issn.1001-3695.2012.08.059

Heuristic detection model of covert channel based on quantum neural network

TANG Zhang-guo, LI Huan-zhou, ZHONG Ming-quan, ZHANG Jian
(*Institute of Computer Network & Communication Technology*, *Sichuan Normal University*, *Chengdu* 610066, *China*)

Abstract: In order to improve the detection rate of the covert channel, this paper discussed the covert channel detection technique, and gave a detail contrast research of related characters. Through the induction and analysis for the characteristics of network covert channel, this paper found some attributes to describe the network covert channels, and proposed an identification method based on network communication fingerprint. The communication fingerprints of covert channel were summarized such as in the protocol field, statistical regularities and behavior characteristics. On that basis, it designed and implemented a heuristic detection model of covert channel based on quantum neural network. Test results indicate that the system runs efficient and the results are more accurate.

Key words: covert channel; quantum neural network; communication fingerprint; heuristic; detection

随着互联网的蓬勃发展，对互联网上的信息和内容进行控制显得尤为重要，然而近年来出现的新型网络窃密技术，能够通过采用隐蔽信道、动态加密等技术突破现有安全设备，将攻击代码、涉密文件等数据送到目标主机。因此，对隐蔽信道开展研究并提出相应的监控措施具有重要的现实意义。隐蔽信道是指允许进程以危害系统安全策略的方式传输信息的通信信道，其研究领域包括信道识别、度量、消除、限制、审计和检测几个技术层面，其中最关键、最困难的一环就是隐蔽通道的检测和识别，表现在理论上还没有一个严谨普适的方法，在实践上没有有效的自动化分析工具。目前，对网络隐蔽信道检测的研究大部分集中在基于已知隐蔽信道类型的检测，而对未知的网络隐蔽信道的检测还没有一个通用的有效方法，因此需要应用人工智能等新方法新思想找出网络隐蔽信道的潜在特征，并构造一个通用的检测模型，从而可以获得更好的检测率以及对异常网络信道的准确预测。基于此，本文以互联网隐蔽信道信息流的特征为研究对象，通过对隐蔽通道的控制机制和通信机制进行分析，归纳描述网络隐蔽通道的若干属性，发现其通信特征、网络行为特征、使用特征等方面的特异性，并提出基于网络隐蔽信道通道特征指纹集的检测思想，实现一个通用的基于量子神经网络的网络隐蔽通道检测模型。

1 主流隐蔽信道检测技术的原理和现状

1.1 网络隐蔽信道检测原理

目前国际上先后提出了多种隐蔽通道分析方法，有代表性的是信息流分析法、无干扰法、共享资源矩阵法、改进 SRM 法、语义信息流法、隐蔽流树法、基于源代码搜索法和回溯搜索法等。这些方法大都没有深入探讨和揭示隐蔽通道相应的通信构成要素，没有将具体的机密信息传递过程抽象成一般性过程，更没形成统一的信息传递模型。为了能清楚揭示隐蔽信通道的存在场景和机密信息传递过程，考虑到隐蔽信道的构建者与检测者之间的对抗关系，可以借用博弈论来进行理论上的建模[1]。为了不失一般性，引入协议隐写算法集和隐蔽信道分析算法集，基于此构建隐蔽信道的对抗模型如图 1 所示。

该模型以期望隐蔽数据传输作为支付函数建模构建者与检测者之间的博弈对抗关系，并将对抗的主体归纳为作用在网络数据包之上的协议隐写算法集和隐蔽信道分析算法集，此外，网络数据信息流能否构成隐蔽通道的关键在于它能否真正被主体用于非法通信，而不是流经过的变量[2]。因此，基于网络数据流的隐蔽信道检测过程实际上是辨别输入的网络数据

收稿日期：2011-11-29；**修回日期**：2012-01-02 **基金项目**：四川省应用基础研究资助项目(07JY029-011)；四川省教育厅资助项目(12ZB105)

作者简介：唐彰国(1978-)，男，广西桂林人，讲师，硕士，主要研究方向为信息安全(tangzhangguo@sicnu.edu.cn)；李焕洲(1974-)，男，四川阆中人，教授，博士，主要研究方向为网络监控、可信计算；钟明全(1975-)，男，四川内江人，讲师，硕士，主要研究方向为通信与信息安全；张健(1975-)，女，四川宜宾人，讲师，博士研究生，主要研究方向为网络安全.

包或数据流是恶意隐蔽活动还是合法通信的分类问题,模型的核心是如何构建高效、通用的分析算法或智能学习算法。

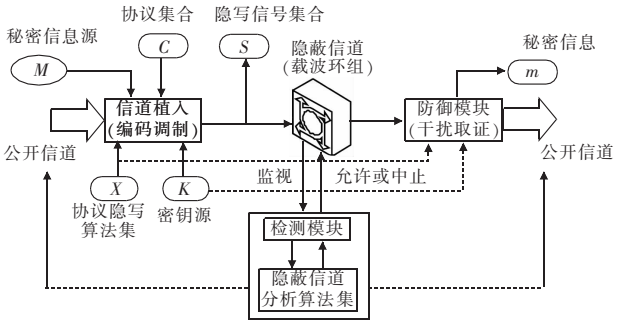

图 1 隐蔽信道的对抗模型

1.2 网络隐蔽信道检测技术综述

网络隐蔽信道的检测包括存储隐蔽信道检测和时间隐蔽信道检测[3]。网络存储隐蔽信道主要利用了网络协议的存储域携带隐蔽信息,包括网络数据包的协议控制部分、扩展数据部分和常规数据部分。对于将附加信息保存在包头的保留字段、未用字段和填充字段中的隐蔽信道,例如 IP 头的 TOS、DF 以及 TCP 头的标志、RST 字段等,其检测方法一般只要对每个数据包的特殊位进行监视,一旦发现这些数据位取值或取异常值,则可初步判定存在利用这些数据位传输信息的隐蔽信道。对于采用包头中的常用字段保存隐蔽信道,如 IP 头中的标志 ID、生存时间 TTL 和 TCP 的初始化序列号 ISN、时间戳等,其检测方法一般通过检验字段值的概率分布是否与自然生成的字段间存在差异,从而判断这些字段值是否被蓄意控制以便传输数据。为了获得更通用的检测模型,Sohn 等人利用 SVM 来检测 IPID 和 ISN 隐蔽信道,并于 2003 年将该方法用于检测基于 ICMP 协议负载的隐蔽信道。Tumoian 使用神经网络来检测 ISN 隐蔽信道,取得了较高的检测率,另外信息熵、决策树等智能方法也有应用。网络时间隐蔽信道的构建方法可以归纳为对数据包进行时间调制、包大小调制和发包行为调制,其对应的检测方法主要采用针对数据包的时间数据进行统计分析,计算检测指标,并根据指标值判断是否构成了隐蔽信道。

1.3 已有方法的比较

总结现有的隐蔽信道检测技术,为了便于比较本文将其归结为三个层次四大类。三个层次分别是语法、语义和语用[4],四大类分别是:a)特征检测,是指针对数据包固定字段的检测,识别数据包形式上的信息即语法信息,通过搜索特征进行数据分析匹配,这种机制适用于已知的隐蔽通道,而无法对加密数据进行检测,不能归纳攻击模式和识别新型的隐蔽通道;b)行为检测,是指提取出正常网络使用模式下的某些特征,识别的是协议使用的目的和效用价值等语用信息,如通过对所监控的网络建立流量模型,对监控的网络数据流通过实时统计的行为与模型的阈值差异发出警告,以此作为判断是否含有隐蔽信息的依据;c)统计检测,是基于通信协议的运行规则识别多个数据包之间的相互关系信息即语义信息,数据包在嵌入隐蔽信息后,其统计特性通常会改变;d)人工智能检测,如神经网络将隐蔽信道的特征、规律及效用等信息通过神经元之间的连接构成模式图来学习理解,虽然这种模式图不能显式地表达成有意义的解析式,但其固有的模糊性和兼容性能较好地满足基于“全信息”的分类要求。为了横向比较各种技术的差异,表 1 从以下几个方面来对这几种方法进行评价和比较。

表 1 现有网络隐蔽信道检测技术的识别能力对比

	基于特征方法	基于行为方法	基于统计方法	基于智能方法
检测对象	数据包的协议域	网络数据流	网络数据流	网络数据包
检测结果的准确性	漏报率高	误报率高	误报率较高、漏报率较低	漏报率中
检测结果可解析性	好	一般	较好	一般
未知信道识别能力	一般	较好	较好	好

2 基于量子神经网络的启发式隐蔽信道检测模型

2.1 检测模型及流程

模型采用以数据为中心的观点把隐蔽信道检测作为一个数据分析任务,通过对网络数据流的分析检测是否存在隐蔽信道的使用行为,遵循信息抽象级别的概念,设计基于量子神经网络的识别模型,整体架构如图 2 所示。模型引入通信指纹的概念描述隐蔽信道的共性特征,通信指纹包含多维属性,如协议特征(五元组、包载荷等)、行为特征(流量、链路长度等)、统计特征(包间隔、包延迟、包大小等)。将这些指纹特征作为神经网络的输入而不是使用原始数据包,其优点是由于在输入层加入先验信息,这种分层启发式方法能在保证很高的检测精度、通用性和适应性的同时,大幅缩减了输入信息的维度和分析量,能在复杂背景噪声下进行快速检测并进行精确识别。

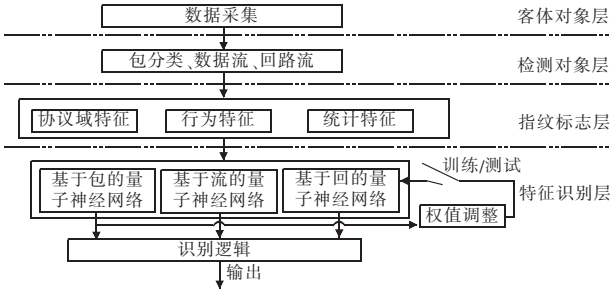

图 2 识别模型逻辑

模型的工作流程包括在线实时模式和离线检测模式,前者以数据报文为检测对象,后者以数据包文件为检测对象,导入数据报文或数据包文件后进行分类预处理,提取网络隐蔽通道的若干属性如通信特征、网络行为特征、使用特征等方面的特异性,按照协议、行为和统计三方面分别进行归一化处理,并作为指纹特征向量输入相应的量子神经网络,通过开关训练并使用该网络;最后通过一定的识别逻辑对三个神经网络的输出进行数据融合,从而实现对隐蔽信道的自动识别、检测和预警。

2.2 构建隐蔽信道指纹特征输入向量

网络隐蔽通道是在通信过程中泄露信息的,所以该模型主要监视通信过程中的网络流量、数据包、时间戳等符合网络隐蔽通道特点的属性,针对这些属性,对它们进行编码,并把每个属性作为一个分量,最后形成 n 维向量,这个 n 维向量就表示某个时刻网络中的状况。为了启发式地构造神经网络的输入,需要按照先验知识对输入进行分类指导和预处理,本文模型检测的客体对象分为离散包、会话流、数据回三个层次。其中,离散包特征是指通过分析单个的数据包来判断其是否包含秘密数据,这种层次的分析适合于基于协议字段的隐写方法,如利用 IP 分段标志、基于 IP 偏移、TCP 紧急指针等。流特征针对隐藏在连续的多个数据包中的异常信息,一般应用层 FTP、SMTP、POP3 等协议的隐蔽信道存在于会话流中。数据回特征

是指通信信道的双向信息流是否满足特定约束,包括链路特征、流量特征及带宽特征。包、流和回三个层次体现检测时利用信息的不同层次和不同的复杂程度[5]。

表 2　隐蔽信道指纹特征输入向量

信息类型	信息载体	输入向量	数据类型	特征含义
语法(特征类)	数据包	协议域	字符型、数值型	协议字段携带隐蔽信息
语义(统计类)	会话流	包大小、包延迟	数值型	行为调制携带隐蔽信息
语用(行为类)	数据回	链路、流量、带宽	数值型、布尔型	协议使用异常

神经网络算法是一个数值计算过程,它的输入和输出都是数值向量,因此神经网络不能直接与外界通信[6],需要将外部输入样本转换为输入向量并规格化到[0,1]区间。

a)字符型。如网络层、传输层和应用层各协议的隐写字段一般用字符型表示,对于字符型特征需要进行字符数值化,可将 TCP、UDP 等协议进行十进制编码,如用 1 表示 TCP,2 表示 UDP 等。计算公式为 $y=x/(a+1)$,其中 x 为协议的序号,a 为最大序号,y 为转换后的实数值。

b)数值型。如包大小、包延迟等,用数值型表示。对数值型数据进行归一化处理,采用线性插值法将其映射到[0,1]区间内数值,方法是若有一数组$[a_i]$在区间$[a_1,a_n]$内,通过公式 $x_i=x_1+(x_n-x_1)\frac{a_i-a_1}{a_n-a_1}$可将其中的 a_i 映射为区间$[x_n,x_1]$上的数。

c)布尔型。用于描述两个相反的逻辑状态,如链路是否过长、流量是否过大、带宽是否异常等,状态值为真则在指纹数组中相应字段用 1.0 表示;反之用 0.0 表示。

2.3　量子神经网络构造及算法选择

网络隐蔽信道检测的实质是一个数据分类问题。神经网络具有大规模并行处理、网络全局作用等优点,可以通过训练和学习产生一个非线性映射,自适应地对数据产生聚类,并对所选择的系统度量也不要求满足某种统计分布条件,因此与传统的智能方法相比具备了非参量化统计分析的优点。Karayiannis等人于 1997 年提出了基于多层激励函数的量子神经网络模型,该模型的输入层和输出层同于前向神经网络,在隐层的激励函数则采用多个 sigmoid 函数的线性叠加,隐层的神经元就能够表示更多的状态,而一个 sigmoid 函数只能表示两个状态,这种在隐层采用多层激励函数的方法是借用了量子理论中量子叠加的思想。理论和实验均证明多层激励函数的量子神经网络模型对具有不确定性、两类模式之间存在交叉数据的模式识别问题,使分类有更多的自由度,它应用到模式分类方面更有优越性[6]。

根据对指纹特征及其客体对象的分类,相应地构造了三个三层结构的量子神经网络,其中,基于包(语法)的神经网络以协议字段为输入向量,本文选取应用层、网络层和传输层协议的 11 个协议字段作为检测对象,其结构设计为 11-10-1;基于流(语义)的神经网络以统计特征为输入向量,如平均数据包大小、小数据包和大数据包比例、数据包模型变化、所有发送/接收数据包的总数和连接时间等,其结构设计为 5-18-1;基于回(语用)的神经网络以链路、流量和带宽等行为特征为输入向量,其结构设计为 3-10-1,对于三个神经网络的输出采用模糊逻辑进行信息融合。DR-QSOFM 量子神经元模型将样本的领域信息作为模型输入的一部分,与样本的特征向量一起参与权重向量的调整。DR-QSOFM 神经元由输入向量、权重向量、量子旋转门、传递函数组成,其中输入向量包含样本的特征向量和目标向量两个部分,模型结构如图 3 所示。其中,转换函数 f_m 将处于实数态的特征向量 X 和目标向量 T 转换成对应的量子态输入$|X\rangle$和$|T\rangle$,权重向量也为量子态,$|W\rangle$表示特征向量与量子旋转门 U_i 的连接权重,$|V\rangle$表示目标向量与 U_i 的连接权重;量子旋转门 U_i 在量子态特征向量、目标向量和权重向量的作用下进行相位旋转,然后再反作用于$|W\rangle$,使权重向量的方向朝着输入模式的方向进行调整,不断地向样本的中心位置移动,f_o 表示传递函数,将 DR-QSOFM 神经元的输出映射成一个实数,相应的量子神经网络的学习及分类算法参见文献[7]。

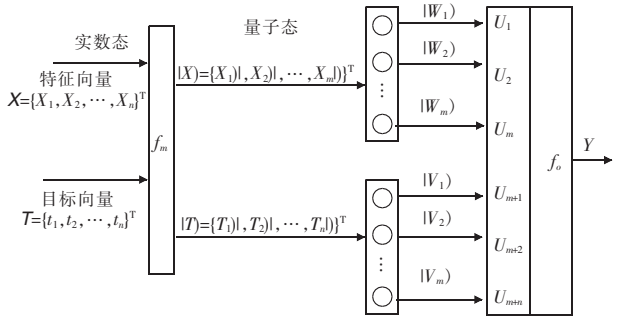

图 3　DR-QSOFM 神经元模型

构造模型的过程一般分为训练和测试两个阶段,在构造模型之前,要求将数据集随机地分为训练数据集和测试数据集。在训练阶段,使用训练数据集,通过分析由属性描述的数据来构造模型。在测试阶段,使用测试数据集来评估模型的分类准确率,如果认为模型的准确率可以接受,就可以用该模型对其他数据进行分类。

3　测试及结果分析

实验从检测率和训练时间两个方面,对本文提出的基于量子神经网络的识别方法相比传统的 BP 神经网络进行了验证比较。模型经过训练和学习后才可进行实际的测试。

模型的训练:首先搭建网络通信环境,在网络出口部署网络抓包软件。在训练阶段通过获取 Covert_TCP、NUSHU、Cctt 和 Loki2 等网络隐蔽通道软件的通信数据来得到该实验的数据集。选取数据集中的 6 000 条记录,其中正例和反例各为3 000条,作为神经网络算法的训练数据集。表 3 给出了 BP 神经网络与量子神经网络在收敛时间、训练次数和误差方面的比较。

表 3　BP 神经网络与量子神经网络的收敛时间、训练次数和误差比较

网络类型	收敛时间	训练次数	误差
BP 神经网络	3 min 28 s	1 968	0.020 553
量子神经网络	1 min 6 s	218	0.001 326

模型的使用:为了模拟真实通信环境,在校园某实验室运行 Active Port Forwarder、Covert_TCP、NUSHU、Cctt、Loki2、HttpTunnel、CMDshell 等隐蔽信道构建工具,以校园网通信流为背景噪声,通过导入校园网络中心实验当天的抓包数据进行测试,不同时段的信道离散在数据文件中,检测的统计结果如表 4 所示。

表 4　网络隐蔽信道检测技术的识别能力对比

信道数目	BP 神经网络		量子神经网络	
	检测率	检错率	检测率	检错率
300	89.1	10.9	95.8	4.2
212	90.3	9.7	94.6	5.4
368	88.5	11.5	93.2	6.8
568	91.7	8.3	96.5	3.5

(下转第 3038 页)

用如下公式表述：

$$K = \mathrm{MD5}(\mathrm{domain} + \mathrm{randomNum})$$

其中：K 表示密钥；MD5 表示散列函数；domain 表示域名；randomNum 表示随机数。

代理服务器解析数据源的 Set-Cookie 或者 Cookie 信息，并将此数据作为需要加密（解密）的数据。DES 加密（解密）程序获取要处理的字符串，将字符串分割成每 8 Byte 一组；然后分别对其进行一次标准 DES 加密（解密）；最后，将处理结果返回给代理模块。

5 测试

为了检验 Cookie 保护的有效性，本文使用 VS2010 的编译环境，对代码进行了编译，实现了可执行程序，并运行于实际网络环境中搭建的服务器上。测试机浏览器设置代理为代理服务器 IP，测试端口为 8086。测试方法：选取测试网站若干，在使用 Cookie 保护代理服务器和不使用 Cookie 保护代理服务器两种情况下分别访问并登录测试网站，通过比较检测 Cookie 保护系统是否将 Cookie 加密，若已加密，表示保护成功，反之保护失败；之后模拟一次获取 Cookie 的跨站脚本攻击，检测合法 Cookie 是否被攻击者获取，如果攻击者获取到的是非法 Cookie，则保护成功，反之保护失败。选取的测试网站为人人网、新浪网、天涯社区。测试结果如表 1 ~3 所示。

表 1 人人网测试结果

类别	Cookie 值
未保护	t = 197cc7995628221fb5058abf038440e5
保护	t = 2K 饢 S&8?? 絛 N 卤 > D? 浒? 3 姐 u 赋
模拟 XSS	t = 垭；? b 鳟蠼紳 & 粤訴踃赚迭? 阖 5 闶? J?

表 2 新浪网测试结果

类别	Cookie 值
未保护	vjuids = －4293816cd. 133cf82c8c6. 0. d023
保护	vjuids = ? H 卑俚瘪 g 騕腴 Y\S 跡? 8?% 繒?
模拟 XSS	vjuids = 夢騺 < 爆`| z 釩 2oE 紬勸椵? Z 啜

表 3 天涯网测试结果

类别	Cookie 值
未保护	sso = r = 861119083&sid = &wsid = D
保护	sso = zk]Gb 徹 4 淮琉閏? 7p 硕 O	@ . 黏?
模拟 XSS	sso = h? 薘嚪 iykW

测试结果表明，使用了本系统的网页 Cookie 均被加密后存储在浏览器中，且 XSS 攻击者获取到的 Cookie 没有被正确解密，Cookie 可被有效保护。

6 结束语

本文介绍了 Cookie 与 XSS 攻击，针对窃取 Cookie 类型的 XSS 攻击，提出了一种新的 Cookie 保护方法，并对其进行了实现。基于代理的 Cookie 保护，并利用 DES 算法或者其他加密算法对 Cookie 加密和解密，达到保护 Cookie 的目的。通过实际环境的测试，结果表明，可有效地防止 Cookie 被 XSS 攻击者窃取。这种 Cookie 保护框架可被有效地利用于 XSS 防御当中，以缓解目前日益泛滥的 XSS 攻击。

参考文献：

[1] JOHNS M, ENGELMANN B, POSEGGA J. XSSDS: server-side detection of cross-site scripting attacks[C]//Proc of Computer Security Applications Conference. Anaheim: IEEE, 2008: 335-344.

[2] GEBRE M T, LHEE K S, HONG M P. A robust defense against content-sniffing XSS attacks[J]. Digital Content, Multimedia Technology and its Applications, 2010, 9(1): 315-320.

[3] Network Working Group. RFC 2109, HTTP state management mechanism[S]. Washington DC: Internet Society, 1997.

[4] STEPHEN J, REDDY P, NAIDU D. Prevention of cross site scripting with E-Guard algorithm[J]. International Journal of Computer Applications, 2011, 22(5): 30-34.

[5] VARJABEDIAN R. Bullet proof cookies[EB/OL]. (2010-05)[2011-06]. http://www.codeproject.com/KB/aspnet/BulletProofCookies.aspx.

[6] JASON B, ELIE B, DIVIJ G. State of the art: automated black-box Web application vulnerability testing[J]. Security and Privacy, 2010, 5(1): 332-345.

[7] ZHOU Y, EVANS D. Why aren't HTTP-only cookies more widely deployed[C]//Proc of the 4th Web 2.0 Security and Privacy Workshop. 2010: 1-5.

[8] DIERKS T, RESCORLA E. RFC 4346, The transport layer security (TLS) protocol version 1.1[S]. US: IETF, 2006.

（上接第 3035 页） 由表 4 可知，基于量子神经网络的检测模型的统计检测率均在 90% 以上，对相同的数据样本其检测率和虚警率相比 BP 神经网络有明显优势。综合以上测试可以发现，基于量子神经网络的识别方法相比传统的 BP 神经网络在显著提高训练速度的同时保持了较好的检测效果，从技术上解析其原因可归结为：使用先验信息对输入进行预处理减少了训练时间，利用三个不同的量子神经网络在特征表达方面的互补性提高了检测率。

4 结束语

本文采用启发式的多特征检测思想，引入通信指纹的概念扩展了通信特征的范围，实现了网络隐蔽信道的通用检测模型，取得了较好的实验结果。未来的工作：a）针对不同的网络隐蔽信道的通信特点，研究统一化、规范化、形式化的通信特征描述方法；b）采用更可靠的方法如证据理论对多个神经网络模型的可信度进行分析评价和合成，进一步提高模型预测的精度也是下一步研究的重点。

参考文献：

[1] 刘光杰，戴跃伟，赵玉鑫，等. 隐写对抗的博弈论建模[J]. 南京理工大学学报：自然科学版，2008，32(2)：199-204.

[2] 陈喆，刘文清，王亚弟，等. 基于信息流分析的隐蔽通道分类与标志[J]. 计算机应用研究，2010，27(7)：2631-2635.

[3] 王永吉，吴敬征，曾海涛，等. 隐蔽信道研究[J]. 软件学报，2010，21(9)：2262-2288.

[4] 钮心忻，杨义先. 信息隐写与隐写分析研究框架探讨[J]. 电子学报，2006，34(12)：2421-2424.

[5] 吴传伟. 网络协议隐写检测技术的研究[D]. 南京：南京理工大学，2008.

[6] 朱大奇，桑庆兵. 光电雷达电子部件的量子神经网络故障诊断算法[J]. 电子学报，2006，34(3)：573-576.

[7] 张亮，陆余良，房珊瑶. 基于量子自组织神经网络的 DeepWeb 分类方法研究[J]. 计算机科学，2010，38(6)：205-210.