

基于多项式基的非对称量子纠错码的构造

邓楠¹, 李雷¹, 赵生妹²

(1. 南京邮电大学理学院, 江苏南京 210003;

2. 南京邮电大学通信与信息工程学院, 江苏南京 210003)

摘要:量子纠错码在量子计算和量子通信中起着至关重要的作用。文中区别于之前关于量子纠错码的研究,之前大多关于量子纠错码的研究都在对称的量子信道上,所谓对称的量子信道是指量子比特翻转的错误概率与量子相位翻转的错误概率相等的信道。文中的研究侧重在非对称的量子信道上,所谓非对称性体现在量子相位翻转的错误概率与量子比特翻转的错误概率不相等,前者大于后者,利用经典多项式码,基于多项式基构造映射,满足了构造定理的条件,从而构造了一类非对称量子纠错码。

关键词:自正交码;量子纠错码;非对称量子纠错码;多项式码;多项式基

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)08-0143-03

Construction of Asymmetric Quantum Error-correcting Codes Based on Polynomial Basis

DENG Nan¹, LI Lei¹, ZHAO Sheng-mei²

(1. College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. Institute of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Quantum error-correcting codes play a very important role in both quantum computation and quantum communication. It is different from the previous research work in quantum error-correcting codes that focuses on code constructions for symmetric quantum channels, the so-called symmetric quantum channel is the channel that phase-shift and qubit-flip errors have equal probabilities. It focuses on the asymmetric quantum channels, the so-called asymmetric quantum channel is the channel that phase-shift and qubit-flip errors have different probabilities, and the former is greater than the later. By the classical polynomial codes, obtained the correct codes to meet the theorem's conditions, and a family of asymmetric quantum error-correcting codes is obtained based on the polynomial basis.

Key words: self-orthogonal code; quantum error-correcting code; asymmetric quantum-error correcting code; polynomial codes; polynomial basis

0 引言

近几年来量子纠错码的研究进展很快。在1995-1996年, P. Shor 和 A. M. Steane 简化了量子错误的复杂的机制, 变为了逐位纠错的物理模型, 用有限个 Pauli 算子来表示每个量子位上的错误。然后, Shor^[1]构造了第一个量子纠错码 $[[n, k, d]] = [[9, 1, 3]]$ 。不久这个码被改进为7位和(最佳的)5位。在1998

年, Calderbank^[2]等人给出了量子纠错码理论的数学形式以及构造二元量子码的系统的数学方法。此后, 量子纠错码的研究发展迅速, 人们用已知的经典码(Reed-Muller码、Reed-Solomon码、BCH码、LDPC码等)来构造好的量子码[3~9], 并且开始利用量子信道的非对称特点来构造非对称量子纠错码。

量子信道的非对称性是 Ioffe 和 Mezard 于2007年在文献[10]中提出的, 已知的量子计算设备中的绝大部分都存在降相位时间 T_2 比对应的松弛时间 T_1 小的事实, 其关系为 $\frac{1}{T_1} = \frac{1}{(2T_2)} + \Gamma_p$ 。在一般情况下, 松弛将会导致比特与相位翻转都发生错误, 而降相位将仅仅导致相位翻转错误的发生。由于 T_1 与 T_2 的这种非对称性, 将会导致量子比特翻转的错误概率小于量子相位翻转的错误概率。即在量子计算和量子通信的

收稿日期: 2011-12-15; 修回日期: 2012-03-19

基金项目: 国家自然科学基金(61070234, 61071167); 江苏省高校自然科学基金(04KJB110097, 08KJB520023); 南京邮电大学攀登计划项目(NY207064)

作者简介: 邓楠(1986-), 女, 硕士, 研究方向为信息安全与量子信息技术; 李雷, 博士, 教授, 研究方向为信息安全、模式识别与智能系统。

物理实现中, X 错误和 Z 错误所发生的概率是不同的, 后者的概率要大得多。Ioffe 和 Mezard 还在文献[10]中利用 BCH 码和 LDPC 码构造了非对称量子纠错码。早在 1996 年, Steane^[11]就指出研究非对称量子码的重要意义。

非对称量子纠错码近些年来的发展很快, 取得了一些重要成果。Aly 于 2008 年在文献[12]中利用 RS 码和 BCH 码构造了非对称量子纠错码。Sarvepalli 等人于 2008 年在文献[7]中利用 LDPC 码构造了非对称量子 LDPC 码。在文献[13]中, Yeow Meng Chee 等人于 2010 年利用 MDS 码构造了非对称量子 MDS 码, Yeow Meng Chee 等人于 2011 年还在文献[14]中基于 CSS^[4]构造定理得到纯的非对称量子 MDS 码。文中利用经典多项式码, 基于多项式基构造新的映射, 得到满足构造定理条件的一类码字, 从而构造一类非对称量子纠错码。

1 基本理论知识

首先, 介绍一些基本的理论知识。

记 F_q 为元素 q 的有限域, 设 p 是一个素数, m 是一个正整数, 且令 $q = p^m$ 。

q 元线性分组码 C 是 F_q 上的 n 维线性空间 F_q^n 的一个 k 维线性子空间, 记为 $[n, k, d]$, 其中 d 为 C 的所有非零码字 c 的最小 Hamming 重量, 记为 $d = wt(C)$ 。

有限域 F_q 上的 Euclidean (又称作欧氏) 内积的定义如下所述:

设 $u = (u_0, u_1, \dots, u_{n-1}), v = (v_1, v_2, \dots, v_{n-1}) \in F_q^n$, 则 u 和 v 的欧氏内积定义为

$$uv = \sum_{i=0}^{n-1} u_i v_i$$

线性分组码 C 的欧氏对偶码定义如下: $C^\perp = \{u \in F_q^n : uc = 0, c \in C\}$ 。显然, C^\perp 是线性码 $[n, n-k]$ 。如果 $C \subseteq C^\perp$, 则称 C 是自正交码。

定理 1^[2] (CSS 构造) 如果存在自正交的线性码 $C = [n, k]$, 则存在量子纠错码 $[n, n-2k, d]$, 其中 $d = \min\{wt(c) \mid c \in C^\perp/C\}$, 这里 $wt(c)$ 表示 F_q^n 中向量 c 的 Hamming 重量。

由文献[10]可知, 非对称量子纠错码是基于量子比特翻转的错误概率小于量子相位翻转的错误概率的事实进行构造的, 并且针对不同类型的错误非对称量子纠错码的纠错能力也有所不同。基于此, 由文献[7, 10, 12]可以知道非对称量子纠错码的定义。

定义 1^[7, 10, 12] q 元非对称量子纠错码 Q , 记为 $[[n, k, \frac{d_z}{d_x}]]$, 是 F_q 上 q^k 维的 Hilbert 空间 C^q 的一个子空间, 它能同时纠正 $\lfloor (d_z - 1)/2 \rfloor$ 个量子相位翻转

的错误和 $\lfloor (d_x - 1)/2 \rfloor$ 个量子比特翻转的错误, 并且, 能同时发现 $(d_z - 1)$ 个量子相位翻转的错误和 $(d_x - 1)$ 个量子比特翻转的错误。

因此, 若 $d_z > d_x$, 则可知相位翻转对量子系统的影响要大于量子比特翻转对量子系统的影响。

文献[7, 10, 12]中提出:

定理 2^[7, 10, 12] 设 C_1 和 C_2 分别是参数 $[n, k_1, d_1]$ 和 $[n, k_2, d_2]$ 的经典 q 元线性码, 并且 $C_1^\perp \subseteq C_2$ (从而 $C_2^\perp \subseteq C_1$, 并且 $k_1 + k_2 - n \geq 0$)。则存在参数为 $[[n, k_1 + k_2 - n, \frac{d_z}{d_x}]]$ 的非对称量子码, 其中

$$d_z = \max\{w_H(C_1/C_2^\perp), w_H(C_2/C_1^\perp)\}$$

$$d_x = \min\{w_H(C_1/C_2^\perp), w_H(C_2/C_1^\perp)\}$$

进而, 如果 $w_H(C_1/\{0\}) = w_H(C_1/C_2^\perp)$, 并且 $w_H(C_2/\{0\}) = w_H(C_2/C_1^\perp)$, 则这个量子码 (对于 d_z/d_x) 是纯的。

由定理 2 构造的非对称量子码叫做加性量子码。

2 一类非对称量子纠错码的构造

定义 2 F_q^n 中的子集合

$C = \{c_f = (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \in F_q^n \mid f(x) \in F_q[x], \deg f \leq k-1\}$ 为 q 元线性码, 参数为 $[n, k, d]_q$, 称为多项式码。

定理 3^[15] F_q^n 中的子集合

$C = \{c_f = (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \in F_q^n \mid f(x) \in F_q[x], \deg f \leq k-1\}$ 为 q 元线性码, 参数为 $[n, k, d]_q$, 其中 $d = n - k + 1$, 从而为 MDS 码。

例 1^[15]: 设 $2 \leq n \leq q, 1 \leq k_1 \leq k_2 \leq n$ 。给出多项式码

$$D_1 = \{c_f = (f(\alpha_1), \dots, f(\alpha_n)) \in F_q^n : \psi f(x) \in F_q[x], \deg f \leq k_1 - 1\}$$

$$D_2 = \{c_f = (f(\alpha_1), \dots, f(\alpha_n)) \in F_q^n : \psi f(x) \in F_q[x], \deg f \leq k_2 - 1\}$$

则 D_1 和 D_2 均是 MDS 码, 参数分别为 $[n, k_1, d_1]$ 和 $[n, k_2, d_2]$, 其中, $d_1 = n - k_1 + 1, d_2 = n - k_2 + 1$

由 $k_1 \leq k_2$ 可知 $D_2 \subseteq D_1$ 。对偶码 D_1^\perp 和 D_2^\perp 也是 MDS 码, 参数分别为 $[n, n - k_1, d_1^\perp]_q$ 和 $[n, n - k_2, d_2^\perp]_q$, 其中, $d_1^\perp = k_1 + 1, d_2^\perp = k_2 + 1$ 。

取 $C_1 = D_1, C_2 = D_2^\perp$ 则 $C_2^\perp \subseteq C_1$ 。由此构造出加性量子码 Q , 参数为 $[[n, k, \frac{d_z}{d_x}]]_q$, 其中 $k = k_1 + n - k_2 - n = k_1 - k_2$, 而 d_z 和 d_x 分别是 $n - k_1 + 1$ 和 $k_2 + 1$ 中的最大值和最小值。

定义 3 形如 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ (其中 α 是 n 次元) 的基称为多项式基。

由此可以看出,多项式码中对应的多项式是由不同的多项式基生成的。

构造如下映射:

定义4 映射 $\varphi: F_q^n \rightarrow F_p^m, q=p^m, \varphi(c) = (a_0, a_1, \dots, a_{m-1}), c_i = \sum_{j=0}^{m-1} a_j \alpha_i^j$, 其中, $a_j \in F_p$ 。矩阵表示如下:

$$\begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{m-1} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^{m-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_{m-1} \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \dots \\ f(\alpha_n) \end{pmatrix} = c_f = C$$

其中, $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ 是 F_q 在 F_p 上的多项式基, $\alpha \in F_p, \alpha \neq 0$ 。

在文献[3]中,马文平等利用迹映射构造非对称量子纠错码,文中利用多项式基来构造一类非对称量子纠错码。

定理4 如果 C 是 F_q 上长度为 n 的自正交码,则 $\varphi(C)$ 是 F_p 上长度为 m 的自正交码。

证明:设 $c = (c_1, c_2, \dots, c_n), d = (d_1, d_2, \dots, d_n) \in F_q^n$ 为 C 的任意两个码字,其中 $c_i = \sum_{j=0}^{m-1} a_j \alpha_i^j, d_i = \sum_{j=0}^{m-1} b_j \alpha_i^j$, 由于 C 是自正交码,则有

$$cd = \sum_{i=1}^n c_i d_i = \sum_{i=1}^n \left(\sum_{j=0}^{m-1} a_j \alpha_i^j \right) \left(\sum_{k=0}^{m-1} b_k \alpha_i^k \right) = 0$$

即 $\sum_{j=0}^{m-1} \sum_{k=0}^{m-1} \alpha_i^{j+k} a_j b_k = 0$, 又因为 $\alpha \neq 0$, 所以

$$\varphi(c)\varphi(d) = \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} a_j b_k = 0.$$

因此, $\varphi(C)$ 是 F_p 上长度为 m 的自正交码。

根据定理1和定理4,可以得到如下的定理,从而可以构造得到一类量子纠错码。

定理5 设 C 是 F_q 上长度为 n 的自正交码, $C^\perp \subseteq C$, 则存在参数为 $[m, m-2k, d]$ 的量子纠错码。

证明:由定理4,因为 C 是 F_q 上长度为 n 的自正交码,可以得到 $\varphi(C)$ 是 F_p 上长度为 m 的自正交码。即 $\varphi(C)^\perp \subseteq \varphi(C)$ 。所以由定理1可以得到:存在参数为 $[m, m-2k, d]$ 的量子纠错码。

由定理4,同理,可以得到如下引理:

引理1 设 C_1 和 C_2 分别是参数 $[n, k_1, d_1]$ 和 $[n, k_2, d_2]$ 的经典 q 元线性码,并且 $C_1^\perp \subseteq C_2$ (从而 $C_2^\perp \subseteq C_1$, 并且 $k_1 + k_2 - n \geq 0$)。则有 $\varphi(C_1^\perp) \subseteq \varphi(C_2)$, $\varphi(C_2^\perp) \subseteq \varphi(C_1)$ 。

特别地,当 C_1 和 C_2 分别是循环码时, $C_1^\perp \subseteq C_2$, $C_2^\perp \subseteq C_1$, 从而有 $\varphi(C_1^\perp) \subseteq \varphi(C_2)$, $\varphi(C_2^\perp) \subseteq \varphi(C_1)$ 。

根据定理2和引理1,可以得到如下的定理,从而

可以构造得到一类非对称量子纠错码。

定理6 设 C_1 和 C_2 分别是参数 $[n, k_1, d_1]$ 和 $[n, k_2, d_2]$ 的经典 q 元线性码(特别地, C_1 和 C_2 分别为循环码), 并且 $C_1^\perp \subseteq C_2, C_2^\perp \subseteq C_1$, 则存在参数为 $[[m, k_1 + k_2 - m, \frac{d_1}{d_2}]]$ 的非对称量子纠错码。

证明:因为 C_1 和 C_2 分别是参数 $[n, k_1, d_1]$ 和 $[n, k_2, d_2]$ 的经典 q 元线性码(特别地, C_1 和 C_2 分别为循环码), 并且 $C_1^\perp \subseteq C_2, C_2^\perp \subseteq C_1$, 由引理1得到 $\varphi(C_1^\perp) \subseteq \varphi(C_2), \varphi(C_2^\perp) \subseteq \varphi(C_1)$ 。所以根据定理2得到:存在参数为 $[[m, k_1 + k_2 - m, \frac{d_1}{d_2}]]$ 的非对称量子纠错码。

3 结束语

文中根据 CSS 构造定理和非对称量子纠错码的构造定理,基于多项式基构造映射,得出满足构造定理条件的码字。从而分别构造得到一类量子纠错码和一类非对称量子纠错码。如何设计构造新的性能好的非对称量子纠错码以及在实际的物理背景下如何应用这些量子码将是未来研究的重点。

参考文献:

- [1] Shor P W. Scheme for reducing decoherence in quantum memory[J]. Phys Rev A, 1995, 52(4): 2493-2496.
- [2] Calderbank A R, Rains E M, Shor P M, et al. Quantum error correction via codes over GF(4)[J]. IEEE Trans. on Inf. Theory, 1998, 44(4): 1369-1387.
- [3] 钱建发, 马文平. 新的非对称量子纠错码的构造[J]. 电子与信息学报, 2009, 31(12): 2922-2925.
- [4] Chen H, Ling S, Xing C. Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound[J]. IEEE Trans. on Inf. Theory, 1998, 47(4): 2055-2058.
- [5] 马智, 冯克勤. 量子纠错码的 Gilbert-Varshamov 界和有限酉几何[J]. 自然科学进展, 2002(11): 1202-1204.
- [6] 郑大钟, 赵千川. 量子计算和量子信息(2)[M]. 北京: 清华大学出版社, 2005.
- [7] Sarvepalli P K, Klappenecker A, Rotteler M. Asymmetric quantum LDPC codes[C]//Proceeding of the IEEE International Symposium on Information Theory. Toronto, Canada: [s. n.], 2008: 305-309.
- [8] Aly S A, Klappenecker A, Sarvepalli P K. On quantum and classical BCH codes[J]. IEEE Trans. on Inf. Theory, 2007, 53(3): 1183-1188.
- [9] Grassl M, Geiselmann W, Beth T. Quantum Reed-Solomon Codes[J]. Applicable Algebra in Engineering, Communication and Computation, 1999, 13: 231-241.

(下转第149页)

80.13 的测试设备上部署即时通讯实时监测系统,主机配置如下:操作系统为 Fedora Core8(内核版本为 2.6.23),CPU 为英特尔 Pentium D,主频为 2.80GHz,物理内存为 1G,网卡为 RTL8139 Fast Ethernet Adapter。

运行测试设备上的即时通讯实时监测系统,对监测子网内的三台终端的 MSN 聊天行为进行实时监测,在终端聊天的过程中,监测系统将解析的结果实时地呈现在界面上,并将信息存储到数据库中从而备份数据,便于管理员后续的统计操作。

如图 6 所示,从 GTK 界面显示的结果上看,本系统能够有效地对 MSN 文本消息进行实时解析和还原,达到实时监测的目的。

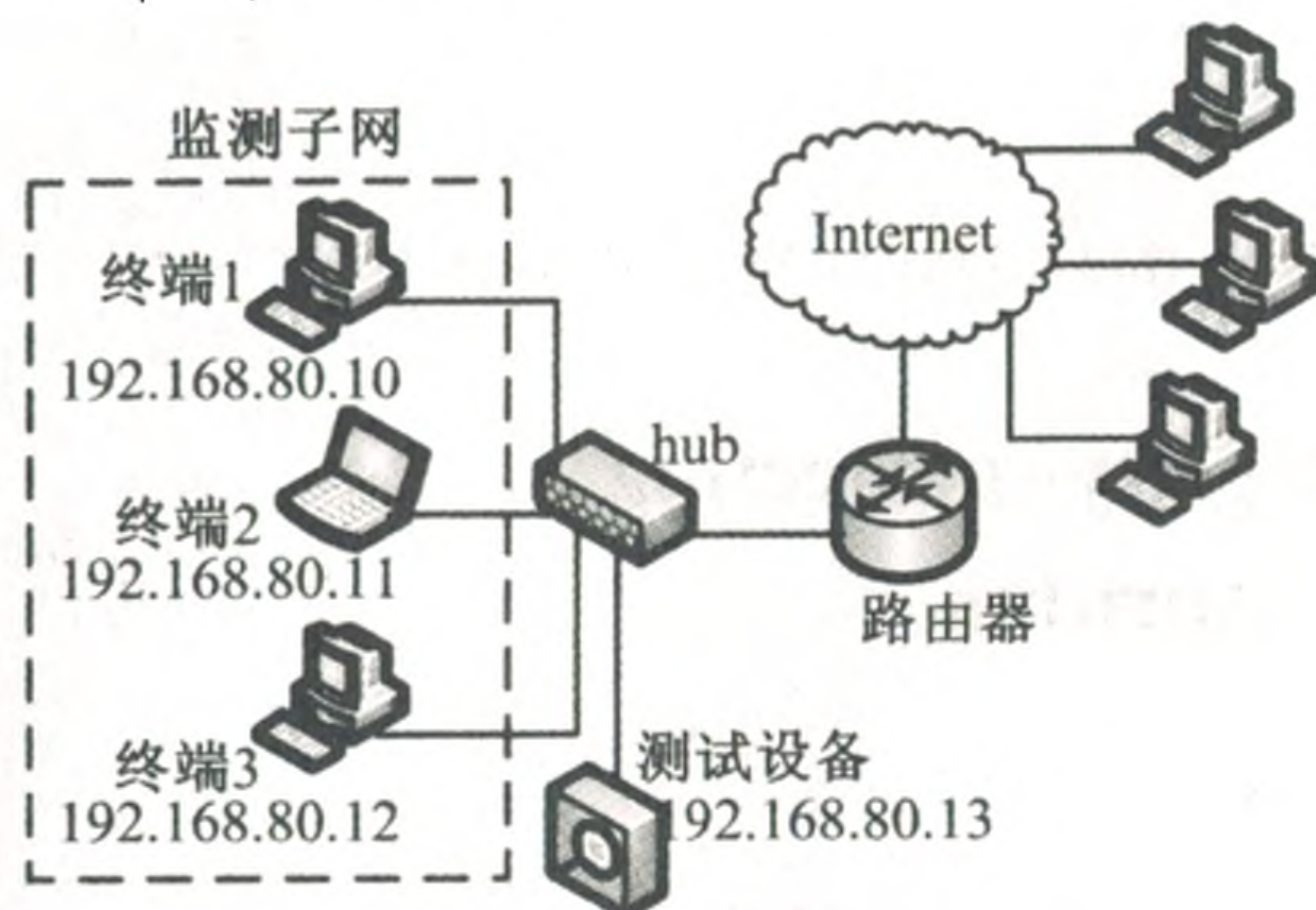


图5 系统测试环境图

No.	监测的 IP	监测的账号	数据方向	对方的账号	聊天内容
1	192.168.80.10	msntest_01@hotmail.com	---->	bjtlq@hotmail.com	最近忙吗?
2	192.168.80.10	msntest_01@hotmail.com	<----	bjtlq@hotmail.com	还好, 不是很忙!
3	192.168.80.12	msntest_03@hotmail.com	<----	yzulq@hotmail.com	能将你们公司的申请
4	192.168.80.11	msntest_02@hotmail.com	---->	bhnry@hotmail.com	小刘, 工资涨了吗?
5	192.168.80.12	msntest_03@hotmail.com	---->	yzulq@hotmail.com	不能哦, 公司机密!
6	192.168.80.10	msntest_01@hotmail.com	---->	bjtlq@hotmail.com	哦, 我们很忙阿!
7	192.168.80.11	msntest_02@hotmail.com	<----	bhnry@hotmail.com	没有, 涨的太慢了!
8	192.168.80.12	msntest_03@hotmail.com	<----	yzulq@hotmail.com	这么守规矩阿
9	192.168.80.11	msntest_02@hotmail.com	---->	bhnry@hotmail.com	你不如到我们公司吧

图6 系统测试结果图

4 结束语

针对目前即时通讯软件带来的网络安全问题,详

细分析了 MSN 通信机制和 MSN 通信协议。通过利用 Libnids 网络安全开发包设计并实现了即时通讯实时监测系统,实现了对监测子网内部用户聊天内容的实时监测。最后在真实的环境下对系统功能进行了测试,测试结果表明:系统能够正确地实现监测子网内部对即时通讯软件的实时监测。

下一步的研究工作包括:

1) 实现关键字过滤模块和阻断模块,根据通信过程中传递的敏感词进行会话阻断;

2) 研究其他主流即时通信协议(飞信、QQ),完成对它们的信息监测。

参考文献:

- [1] 中国互联网络信息中心. 第 28 次中国互联网络发展状况统计报告[EB/OL]. [2011-07-19]. <http://www.cnnic.net.cn/dtygg/dtgg/201107/W020110719521725234632.pdf>.
- [2] 张云川. 即时通信企业级应用研究[J]. 企业经济, 2005(6): 96-97.
- [3] Day M, Sugano H. A Model for Presence and Instant Messaging[S]. RFC 2778, 2000.
- [4] Mintz M. MSN Messenger Protocol[EB/OL]. 2004-10. <http://www.hypothetic.org/docs/msn>.
- [5] 刘彬, 赵荣彩, 丛建刚. 即时通信协议分析与监控技术研究[J]. 计算机应用研究, 2007, 24(9): 260-262.
- [6] 黄红桃, 彭宏, 吴建培, 等. 基于 MSN 协议的网络行为审计系统的设计与实现[J]. 计算机工程, 2007, 33(15): 255-257.
- [7] 付安民, 张玉清. 即时通实时监控系统的设计与实现[J]. 通信学报, 2008, 29(10): 165-172.
- [8] 刘文涛. 网络安全开发包详解[M]. 北京: 电子工业出版社, 2005.
- [9] 严华, 蔡瑞英. 即时通信监控系统的设计与实现[J]. 计算机技术与发展, 2009, 19(7): 242-244.
- [10] Day M, Aggarwal S, Mohr G. Instant Messaging/Presence Protocol Requirements[S]. RFC 2779, 2000.
- [11] Owens M. The Definitive Guide to SQLite[M]. [s. l.]: Apress, 2006.
- [12] 宋国伟. GTK+2.0 编程范例[M]. 北京: 清华大学出版社, 2002.

(上接第 145 页)

- [10] Ioffe L, Mezard M. Asymmetric quantum error-correcting codes[J]. Phys. Rev. A, 2007, 75(3): 86-90.
- [11] Steane A M. Simple quantum error-correcting codes[J]. Phys. Rev. Lett, 1996, 77(6): 793-797.
- [12] Aly A. Asymmetric and symmetric subsystem BCH codes and beyond[J/OL]. 2008. <http://arxiv.org/abs/0803.0764v1>.
- [13] Chee Y M, Jitman S, Ezerman M F, et al. On Asymmetric

Quantum MDS Codes[J/OL]. 2010-06-09. <http://arxiv.org/abs/1006.1694v1>.

- [14] Chee Y M, Ezerman M F, Jitman S, et al. Pure Asymmetric Quantum MDS Codes from CSS Construction[J/OL]. 2011-09-15. <http://arxiv.org/abs/1006.1694v2>.
- [15] 冯克勤, 陈豪. 量子纠错码[M]. 北京: 科学出版社, 2010.

参考文献(15条)

1. Shor P W Scheme for reducing decoherence in quantum memory 1995(04)

2. Calderbank A R;Rains E M;Shor P W Quantum error correction via codes over GF(4)[外文期刊] 1998(04)

3. 钱建发;马文平 新的非对称量子纠错码的构造[期刊论文]-电子与信息学报 2009(12)

4. Chen H;Ling S;Xing C Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound 1998(04)

5. 马哲;冯克勤 量子纠错码的Gilbert-Varshamov界和有限西几何[期刊论文]-自然科学进展 2002(11)

6. 郑大坤;赵千川 量子计算和量子信息(2) 2005

7. Sarvepalli P K;Klappenecker A;Rotteler M Asymmetric quantum LDPC codes 2008

8. Aly S A;Klappenecker A;Sarvepalli P K On quantum and classical BCH codes[外文期刊] 2007(03)

9. Grassl M;Geiselmann W;Beth T Quanta Reed-Solomon Codes 1999

10. Ioffe L;Mezard M Asymmetric quantum error-correcting codes 2007(03)

11. Steane A M Simple quantum error-correcting codes 1996(06)

12. Aly A Asymmetric and symmetric subsystem BCH codes and beyond 2008

13. Chee Y M;Jitman S;Ezerman M F;et al On Asymmetric Quantum MDS Codes 2010

14. Chee Y M;Ezerman M F;Jitman S Pure Asymmetric Quantum MDS Codes from CSS Construction 2011

15. 冯克勤;陈豪 量子纠错码 2010