

基于纠缠的数据链路层量子通信协议^{*}

周南润^{1)†} 曾贵华²⁾ 龚黎华¹⁾ 刘三秋³⁾

1) 南昌大学电子信息工程系, 南昌 330031)

2) 上海交通大学电子工程系, 上海 200240)

3) 南昌大学物理系, 南昌 330031)

(2006 年 9 月 26 日收到, 2006 年 12 月 8 日收到修改稿)

利用量子力学中的纠缠关联性, 提出了数据链路层的量子通信协议. 该协议把线路分为忙闲时段, 量子纠缠态的分发预先在闲时段完成, 数据经由经典链路发送, 确认帧经由量子纠缠信道发送. 量子信息的传输可以是瞬时的, 因此两个发送成功的数据帧之间的最小时间间隔可以大为减小. 研究表明该协议能有效地提高数据链路的最大吞吐量, 改善数据链路层停止等待协议的性能.

关键词: 量子通信, 纠缠, 停止等待协议, 数据链路

PACC: 0365, 4250, 4230Q

1. 引言

量子信息学是量子力学与信息科学相结合的产物, 包括量子密码、量子通信、量子计算和量子测量等. 近年来, 量子信息学在理论和实验上都取得了重要突破, 引起各国政府、科技界和信息产业界的高度重视. 量子力学中的奇特物理现象在信息领域中有着独特的功能, 在提高计算速度、保障信息安全、增大信息容量和提高检测精度等方面可以突破现有的经典信息系统的极限^[1-13]. 利用量子力学的基本原理和特性可以很好地解决经典情况下一些无法解决的难题. 例如, Gisin 小组提出了一个 Byzantine 问题的量子解决方案^[14], 而分布式计算中古老的 Byzantine 问题在经典情况下被证明是无法解决的. 文献^[15, 16]利用量子光学中的 EPR (Einstein, Podolsky and Rosen) 关联对的非定域关联性以及量子远程通信, 设计了一个量子同步通信协议, 通过在不可靠的信道上传递纠缠粒子, 逐步建立可靠的信道, 解决了两军问题, 该协议在经典通信和量子通信中连接的建立与释放, 通信 QoS (quality of service) 和网络性能提高等方面有重要应用价值.

众所周知, 数据链路层协议的作用是在不太可靠的物理链路上实现可靠的数据传输^[17]. 实用的停

止等待协议 ARQ (automatic repeat request) 的优点是比较简单, 缺点是通信信道的利用率不高. 连续 ARQ 协议和选择重传 ARQ 协议可以适当克服这些缺点. 当传播时延很大, 例如卫星通信, 停止等待协议就很不适用, 这时必须采用连续 ARQ 协议. 如果信道的传输质量很差因而误码率较大时, 连续 ARQ 协议不一定优于停止等待协议. 为了进一步减小两个发送成功的数据帧之间的最小时间间隔, 有效地提高数据链路的最大吞吐量, 改善数据链路层停止等待协议的性能, 本文结合量子力学中特有的纠缠现象和量子信息的传输特性, 对数据链路层的停止等待协议进行改进, 提出基于纠缠的数据链路层量子通信协议.

2. 数据链路层的停止等待协议

当网络中两个结点要通信时, 数据的发方 A 必须确知收方 B 是否已经处在准备接收的状态. 因此必须对数据链路进行管理, 即建立、维持和释放数据链路. 发方发送数据的速率必须使收方来得及接收, 因而必须采用流量控制技术.

对于数据链路层的停止等待协议, 设 t_f 是一个数据帧的发送时延, 数据帧沿链路从 A 到 B 的传播

^{*} 国家自然科学基金(批准号: 10647133, 60472018), 江西省自然科学基金(批准号: 0512007), 江西省教育厅科技项目(批准号 [2007] 22 号)和南昌大学引进人才科研启动费资助的课题.

[†] E-mail: znr21@163.com, znr21@sju.org

时延为 t_p , B 收到数据帧所花的处理时间为 t_{pr} , 发送确认帧 ACK 的发送时延为 t_a , 传播时延为 t_p , 设 A 处理确认帧的时间也为 t_{pr} , 则对停止等待协议, 两个发送成功的数据帧之间的最小时间间隔 t_T 为

$$t_T = t_f + 2t_p + 2t_{pr} + t_a. \quad (1)$$

设含帧丢失的数据帧出错概率为 p , 并假设确认帧不会出现差错, 而且允许重传的次数不受限制, 则正确传送一个数据帧所需的平均时间 t_{AV} 为

$$t_{AV} = t_T + (1-p) \sum_{i=1}^{\infty} i p^i t_T = \frac{t_T}{1-p}, \quad (2)$$

数据链路的最大吞吐量为

$$\lambda_{\max} = 1/t_{AV} = (1-p)/t_T. \quad (3)$$

从 (3) 式可知, 对给定的数据链路而言, 数据帧含帧丢失的出错概率变化不大, 要提高链路的最大吞吐量, 必须减小两个发送成功的数据帧之间的最小时间间隔 t_T . 处理时延 t_{pr} 和确认帧的发送时延 t_a 一般都远小于传播时延 t_p , 因而在经典情况下提高数据链路的最大吞吐量一般依靠提高线路的传输速率.

3. 数据链路层的量子通信协议

量子力学表明: 构成自旋 EPR 对的两个反方向飞行的粒子, 经过足够长时间之后, 它们空间波包肯定已不再交叠, 但它们的自旋态依然彼此关联: 各自的自旋取向均依赖于对方而处于一种不确定状态. 一旦对其中一个粒子做自旋取向测量, 使其产生坍缩, 则另一粒子虽然处于遥远而未知的地方, 也将瞬间同时发生自旋态的坍缩. 这是一种瞬时的、不受相对论定域因果律约束的、不可从中阻断的关联坍缩^[18]. 量子远程通信和纠缠交换的出色实验证实了这种难以理解的现象. 不考虑信息中经典部分的传递, 单单就信息中量子部分的传递——量子态的关联坍缩而言, 不论是转移复系数的量子远程通信还是转移纠缠模式的量子纠缠交换, 都具有以下三个共同的特性^[18]: 1) 转移是瞬间实现的; 2) 转移时无需预先知道对方在哪里; 3) 转移过程不会为任何障碍所阻隔. 换言之, 除了建立量子信道的的时间, 量子信息的传输可以不需要时间. 我们利用量子力学中的这一特性, 经由量子信道发送确认帧, 可以缩短超时重传时间, 提高数据链路的最大吞吐量.

状态的改变是一个客观的物理过程, 量子态的

关联坍缩是可以实验观测的. 本文采用量子远程通信来发送确认帧. 量子远程通信过程中信息分为两部分, 量子信息(瞬时的超空间转移)和经典信息(不大于光速), 最终信息传递速度不大于光速. 实际数据链路有忙闲时段之分, 假如我们在闲时段分发 EPR 关联粒子对, 建立量子纠缠信道, 在忙时段通过传递量子信息确认帧便可以提高通信的效率. 为叙述方便, 假设通信双方约定确认帧(确认量子信息)处于量子态 $|\phi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$, 发方和收方在链路闲时段所共享的 EPR 关联对始终处于纠缠态 $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$. 收方发送确认信息时, 制备一粒子处于确认帧量子态 $|\phi\rangle$, 并采用可以识别 Bell 基 $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$ 和 $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$ 的装置对新制备的粒子 $|\phi\rangle$ 和预先共享的一个粒子进行联合测量, 有

$$|\psi\rangle = \frac{1}{2} \left[|\psi^-\rangle \left(-\frac{1}{\sqrt{5}}|0\rangle - \frac{2}{\sqrt{5}}|1\rangle \right) + |\psi^+\rangle \left(-\frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle \right) + |\phi^-\rangle \left(\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle \right) + |\phi^+\rangle \left(-\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle \right) \right], \quad (4)$$

B 测量所得的结果可能是 Bell 基中的某一个, 出现概率都是 1/4. 到了设定的测量时间, 发方测量与收方相对应的纠缠粒子, 如果收方发出了确认帧, 收方粒子所处量子态必定为 $-\frac{1}{\sqrt{5}}|0\rangle - \frac{2}{\sqrt{5}}|1\rangle$, $-\frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$, $\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$ 和 $-\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$ 之一, 出现的概率都是 1/4. 当出现上述四个状态中的任何一个时, 就表明数据帧已正确接收. 这四个量子态是非正交的, 非正交态的区分可以参看文献[3, 15, 19]. 值得指出的是, 非正交量子态不可以区分, 但是在允许破坏量子态的前提下, 区分非正交量子态是可行的.

根据以上确认帧的传送和检测方法, 数据链路层的量子通信协议(量子停止等待协议)的算法描述如下:

在发送结点 S :

S1) 从主机取出一个数据帧。

S2) $V(S) \leftarrow 0$, {发送状态变量初始化}。

S3) $N(S) \leftarrow V(S)$, {将发送状态变量的数值写入发送序号}。

将数据帧送交发送缓存。

S4) 将发送缓存中的数据帧发送出去。

S5) 设置等待测量计时器,并等待, {选择适当的超时重传时间}。

S6) 到了测量时间,进行量子测量,判定确认帧是否发回,若发回,从主机取一个新的数据帧;

$V(S) \leftarrow [1 - V(S)]$; {更新发送状态变量,变为下一个序号}。

转到 S3)。

S7) 若未发回,转到 S4), {重传数据帧}。

在接收结点 R:

R1) $V(R) \leftarrow 0$ 。

R2) 等待。

R3) 当收到一个数据帧,就检查有无产生传输错误,若有错,不发送否认帧,直接转到 R2); 否则执行后续算法。

R4) 若 $N(S) = V(S)$, 则执行后续算法; 否则丢弃此数据帧,并转到 R2)。

R5) 将收到的数据帧中的数据部分送交主机。

R6) $V(R) \leftarrow [1 - V(R)]$, 同时执行量子测量,发送量子确认帧。

与经典停止等待协议算法在接收发生错误时必须发送否认帧不同的是,量子停止等待协议算法只发送确认帧,不发送否认帧。若在设定的时间内发方没有收到确认帧,就重传数据帧,若在设定的时间内收到了确认帧,则发送新的数据帧。这适当减轻了链路的负载。

对于量子停止等待协议,处理时延包含经典处理时延 t_{pr} 和量子处理时延 t_{Qpr} ,但是经典处理和量子处理可以同时进行,因而总处理时延 $T_{pr} < t_{pr} + t_{Qpr}$,实际上总处理时延可以取为 $T_{pr} = \max(t_{pr}, t_{Qpr})$ 。由于确认帧的发送时延 t_a 和量子处理时延 t_{Qpr} 可以有重叠,为分析方便,设 $t_{pr} + t_a \geq t_{Qpr} > t_a$, 那么两个发送成功的数据帧之间的最小时间间隔 T_T 为

$$T_T = t_f + t_p + 2t_{pr} + t_a = t_T - t_p. \quad (5)$$

数据链路的最大吞吐量为

$$\Lambda_{\max} = \frac{1-p}{T_T} = \frac{1-p}{t_T - t_p}. \quad (6)$$

令 $\lambda_p = \frac{1-p}{t_p}$, 因为 $t_T > t_p$, 由(3)式得 $\lambda_p > \lambda_{\max}$, 即 0

$< \frac{\lambda_{\max}}{\lambda_p} < 1$. 整理(6)式得

$$\Lambda_{\max} = \frac{1}{\frac{1}{\lambda_{\max}} - \frac{1}{\lambda_p}} = \frac{\lambda_{\max}}{1 - \frac{\lambda_{\max}}{\lambda_p}} > \lambda_{\max}. \quad (7)$$

由(6)和(7)式可知,该协议的最大吞吐量比经典停止等待协议有明显的改善。一般而言,处理时间和确认帧的发送时延都远小于传播时延,即 $t_T = t_f + 2t_p$, $T_T = t_f + t_p$, 因而基于纠缠的数据链路层量子通信协议对网络性能改善是显著的。当数据帧较短,线路传输速率较高,一个数据帧的发送时延 t_f 较小,而链路较长时,传播时延 t_p 较大,该协议比经典停止等待协议强得多。

在计算机通信的早期人们就已发现,对于经常产生误码的实际链路,只要加上合适的控制规程,就可以使通信变为比较可靠,例如面向字符的 IMP-IMP 协议和 BSC 协议。充分发掘量子信息学的特殊原理,可以在不可靠的信道上建立可靠的信道,也可以通过量子与经典相结合的方式减少某一阶段经典通信的时间。量子信息的传递可以是瞬时的,但是量子信道的建立还是需要时间的,所以该通信协议就是通过在闲时段预先建立量子信道以便在经典通信阶段节约时间。一个网络最主要的性能指标就是吞吐量和平均时延,吞吐量代表服务的数量,平均时延代表服务的质量。因此该量子停止等待协议在提高网络通信性能方面有明显的意义。

通过设置多个不同的 $|\phi\rangle$ 态,可以类似地实现连续量子 ARQ 协议。同样的道理,连续量子 ARQ 协议比连续 ARQ 协议优越。对于传播时延很大的卫星通信,停止等待协议很不适用。量子停止等待协议虽然比停止等待协议有较大的改进,但是在卫星通信这种大传播时延的情况下,其性能一般仍不如连续量子 ARQ 协议。因此,从数据链路最大吞吐量的角度看,连续量子 ARQ 协议才是最优的数据链路层通信协议。

值得指出的是,分发纠缠光子是在空闲时段完成,因此系统需要量子内存,而目前量子内存尚不实用。然而研究中经常借助量子内存,例如 Biham 等人对量子密码网络的研究中就借助了量子内存^[20]。为避免分发纠缠态时遇到高优先级的通信,可以将纠缠态的分发设置为最高优先级,以避免对量子缓存的需求。

4. 结 论

利用量子力学中的纠缠关联性和量子信息传输的瞬时性,提出了数据链路层的量子通信协议.该协议把线路分为忙闲时段,量子纠缠态的分发在闲时段完成,建立纠缠量子信道,数据发送过程中的确

认量子信息经由纠缠量子信道以量子远程通信的方式传送.由于确认量子信息传输的瞬时性,有效地改善了数据链路层停止等待协议的性能.该协议的实现比经典的停止等待协议复杂,因而只在时间起关键作用的通信过程中才能真正体现其优势,比如战争情报等时间性强的通信.随着量子信息技术的不断发展,该协议实现的成本必将大为降低.

- [1] Li C Z, Huang M Q, Chen P X, Liang L M 2000 *Quantum communication and quantum computation* (Changsha: National Defense University of Science and Technology Press) (in Chinese) [李承祖、黄明球、陈平形、梁林梅 2000 量子通信和量子计算 (长沙:国防科技大学出版社)]
- [2] Zhou N, Zeng G, Xiong J 2004 *Electron. Lett.* **40** 1149
- [3] Zhou N R, Zeng G H 2005 *Chin. Phys.* **14** 2164
Zhou N R, Zeng G H, Nie Y Y *et al* 2006 *Physica A* **362** 305
- [4] Nielsen M A, Chuang I L 2000 *Quantum computation and quantum information* (Cambridge University Press)
- [5] Zhang Y Q, Jin X R, Zhang S 2006 *Chin. Phys.* **15** 2252
- [6] Yang J 2005 *Chin. Phys.* **14** 2149
- [7] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese) [王 剑、陈皇卿、张 权、唐朝京 2007 物理学报 **56** 673]
- [8] Zheng X J, Fang M F, Cai J W 2006 *Chin. Phys.* **15** 2840
- [9] Zhou N R, Zeng G H, Zeng W J, Zhu F C 2005 *Opt. Commun.* **254** 380
- [10] Feng F Y, Zhang Q 2007 *Acta Phys. Sin.* **56** 1924 (in Chinese) [冯发 勇、张 强 2007 物理学报 **56** 1924]
- [11] Wu T, Ye L, Ni Z X 2006 *Chin. Phys.* **15** 2506
- [12] Gao T, Yan F L, Wang Z X 2005 *Chin. Phys.* **14** 893
- [13] Zhou X Q 2007 *Acta Phys. Sin.* **56** 1881 (in Chinese) [周小清 2007 物理学报 **56** 1881]
- [14] Fitz M, Gisin N, Maurer U 2001 *Phys Rev Lett.* **87** 217901
- [15] Zhou N R, Zeng G H, Zhu F C, Liu S Q 2006 *J. Shanghai Jiaotong Univ.* **40** 5 (in Chinese) [周南润、曾贵华、朱甫臣、刘三秋 2006 上海交通大学学报 **40** 5]
- [16] Zhou N R 2005 *Ph. D. Thesis* (Shanghai Jiaotong University) (in Chinese) [周南润 2005 博士学位论文 (上海交通大学)]
- [17] Xie X R 2000 *Computer network* 2nd edition (Dalian: University of Technology Press) p46 (in Chinese) [谢希仁 2000 计算机网络 (第二版) (大连:大连理工大学出版社)第 46 页]
- [18] Zhang Y D 2006 *Principles of quantum information physics* (Beijing: Science Press) p115, 212 (in Chinese) [张永德 2006 量子信息物理原理 (北京:科学出版社)第 115, 212 页]
- [19] Peres A 1988 *Phys. Lett. A* **128** 19
- [20] Biham E, Huttner B, Mor T 1996 *Phys. Rev. A* **54** 2651

Quantum communication protocol for data link layer based on entanglement^{*}

Zhou Nan-Run^{1)†} Zeng Gui-Hua²⁾ Gong Li-Hua¹⁾ Liu San-Qiu³⁾

¹⁾ *Department of Electronics Information Engineering, Nanchang University, Nanchang 330031, China*

²⁾ *Electronic Engineering Department, Shanghai Jiaotong University, Shanghai 200240, China*

³⁾ *Department of Physics, Nanchang University, Nanchang 330031, China*

(Received 26 September 2006 ; revised manuscript received 8 December 2006)

Abstract

By exploiting the entanglement correlation in quantum mechanics, a quantum communication protocol for data link layer is proposed. The protocol divides the link into busy time and leisure time, where the data is sent via classical channel and the distribution of quantum entanglement is supposed to be completed at leisure time and the acknowledge frame is sent via quantum entanglement channel. The transmission of quantum information can be instantaneous; therefore the minimum time span between two successfully delivered data frames can be significantly reduced. It is shown that the proposed protocol enhances the maximum throughput effectively and improves the performance of the stop-and-wait protocol of data link layer.

Keywords : quantum communication, entanglement, stop-and-wait protocol, data link

PACC : 0365, 4250, 4230Q

^{*} Project supported by the National Natural Science Foundation of China (Grant Nos. 10647133 and 60472018), the Natural Science Foundation of Jiangxi Province, China (Grant No. 0512007), the Research Foundation of the Education Dept. of Jiangxi Province (Grant No. [2007] 22), and the Scientific Research Starting Foundation for the Recruit Talent of Nanchang University of China.

[†] E-mail : znr21@163.com, znr21@sjtu.org