文章编号:1000-5862(2013)05-0492-05

基于量子双向传态的多方量子通信网络的构建方案

邹　昕,叶志清*

(1. 江西师范大学物理与通信电子学院,江西 南昌 330022;2. 江西省光电子与通信重点实验室,江西 南昌 330022)

摘要:利用量子双向传态技术构建了一个量子通信网络,从而实现安全的多方通信. 对该方案的通信安全性和网络工作效率进行了分析,并提出了改进方法,使得该方案更具有实用价值.

关键词:量子通信网络;量子双向传态;身份认证;6 粒子团簇态;安全性

中图分类号:TN 918　　**文献标志码**:A

0　引言

通信使人们的生活发生了翻天覆地的变化,从最初的烽火传递信息,到如今的电话、互联网等,人们甚至可以身处大洋两岸,却清楚地看到对方,科技革命带给人们无限憧憬. 在能够满足基本通信需求后,人们对通信的要求进一步提高,进而考虑通信的安全性和高效性. 由于科技革命带动技术的飞速发展,经典通信已经逐渐不能满足人类对信息传输的需求. 因此,量子通信应运而生. 一般说来,量子通信主要有 2 种方式:量子密钥分发[1-4]及量子安全直接通信[5-9]. 在 BB84 协议及量子隐形传态[10]被提出后的若干年间,量子通信在理论和实践上都取得了重大成果;而在现实生活中,通信离不开网络,当量子通信跟网络相结合的时候,才能在最大限度地发挥通信效用的同时,增强其保密性,从而提高通信质量,方便人们的生活.

本文提出了利用量子双向传态技术来构建一个量子通信网络,从而实现安全的多方通信的方案. 由于使用多粒子团簇态[11-14]为量子信道,使得通过局域操作破坏它的性质比 GHZ 态类困难得多,从而提高了通信的安全性,使该方案更具有实用价值.

1　量子网络通信原理:量子双向传态

通信方之一的 Alice 有待传态 $|\xi\rangle_A^I=(a_0|0\rangle+a_1|1\rangle)_A$,另一通信方 Bob 有待传态 $|\eta\rangle_B^I=(b_0|0\rangle+b_1|1\rangle)_B$,且通信双方与控制方 Charlie 共享一个 6 粒子纠缠态

$$|\psi\rangle_{A_1B_1A_2B_2C_1C_2}^E=\frac{1}{2}\begin{pmatrix}|\phi^+\rangle_{A_1B_1}\otimes|\phi^+\rangle_{A_2B_2}\otimes|00\rangle_{C_1C_2}+\\|\phi^-\rangle_{A_1B_1}\otimes|\phi^-\rangle_{A_2B_2}\otimes|01\rangle_{C_1C_2}+\\|\psi^+\rangle_{A_1B_1}\otimes|\psi^+\rangle_{A_2B_2}\otimes|10\rangle_{C_1C_2}+\\|\psi^-\rangle_{A_1B_1}\otimes|\psi^-\rangle_{A_2B_2}\otimes|11\rangle_{C_1C_2}\end{pmatrix},\tag{1}$$

其中 $|\phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$,$|\psi^\pm\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$,整个量子体系的系综态为

$$|\Psi_s\rangle_{AA_1B_1B_2A_2C_1C_2B}=|\xi\rangle_A^I\otimes|\psi\rangle_{A_1B_1B_2A_2C_1C_2}^E\otimes|\eta\rangle=$$

$$|\xi\rangle_A^I\otimes\frac{1}{2}\begin{pmatrix}|\phi^+\rangle_{A_1B_1}\otimes|\phi^+\rangle_{A_2B_2}\otimes|00\rangle_{C_1C_2}+\\|\phi^-\rangle_{A_1B_1}\otimes|\phi^-\rangle_{A_2B_2}\otimes|01\rangle_{C_1C_2}+\\|\psi^+\rangle_{A_1B_1}\otimes|\psi^+\rangle_{A_2B_2}\otimes|10\rangle_{C_1C_2}+\\|\psi^-\rangle_{A_1B_1}\otimes|\psi^-\rangle_{A_2B_2}\otimes|11\rangle_{C_1C_2}\end{pmatrix}\otimes|\eta\rangle_B^I=$$

$$\frac{1}{2}\begin{pmatrix}|\xi\rangle_A^I\otimes|\phi^+\rangle_{A_1B_1}\otimes|\eta\rangle_B^I\otimes|\phi^+\rangle_{B_2A_2}\otimes|00\rangle_{C_1C_2}+\\|\xi\rangle_A^I\otimes|\phi^-\rangle_{A_1B_1}\otimes|\eta\rangle_B^I\otimes|\phi^-\rangle_{B_2A_2}\otimes|01\rangle_{C_1C_2}+\\|\xi\rangle_A^I\otimes|\psi^+\rangle_{A_1B_1}\otimes|\eta\rangle_B^I\otimes|\psi^+\rangle_{B_2A_2}\otimes|10\rangle_{C_1C_2}+\\|\xi\rangle_A^I\otimes|\psi^-\rangle_{A_1B_1}\otimes|\eta\rangle_B^I\otimes|\psi^-\rangle_{B_2A_2}\otimes|11\rangle_{C_1C_2}\end{pmatrix}.\tag{2}$$

通信开始时,Alice 先对己方粒子(A,A_1)进行一次基于 Bell 基的联合测量,然后将测量的结果公开;Bob 对他的(B,B_2)粒子同样也进行联合测量,且公开测量结果. 通过分析易知,Alice、Bob 均有 4 种可能的测量结果:$|\phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$和$|\psi^\pm\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$,得到的概率均为 1/4. 假设通信双方测量的结果均为$|\phi^+\rangle$,那么由

$$|\xi\rangle_A^I\otimes|B\rangle_{A_1B_1}^{(i)}=$$

收稿日期:2013-05-19

基金项目:国家自然科学基金(61368001)和江西省自然科学基金(20114BAB202003)资助项目.

通信作者:叶志清(1960-),男,浙江建德人,教授,主要从事光量子通信和光电子器件的研究.

$$\frac{1}{2}\sum_{r=0}^{3}|B\rangle_{AA_1}^{(r)}\otimes\left[\sigma_{B_1}^{(i)}\sigma_{B_1}^{(r)})|\xi\rangle_{B_1}^{I}\right], \quad (3)$$

$$|\eta\rangle_B^I\otimes|B\rangle_{B_2A_2}^{(i)}=$$

$$\frac{1}{2}\sum_{s=0}^{3}|B\rangle_{BB_2}^{(s)}\otimes\left[\sigma_{A_2}^{(i)}\sigma_{A_1}^{(s)})|\eta\rangle_{A_2}^{I}\right], \quad (4)$$

其中$|B\rangle^{(i)}\{i=0,1,2,3\}=\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$,$\sigma^{(i)}\{i=0,1,2,3\}=\{I,\sigma_z,\sigma_x,\sigma_x\sigma_z\}$,可知系综态必塌缩为

$$|\Psi\rangle_{B_1A_2C_1C_2}=$$

$$\frac{1}{2}\begin{pmatrix}|\xi\rangle_{B_1}^{I}\otimes|\eta\rangle_{A_2}^{I}\otimes|00\rangle_{C_1C_2}+(\sigma_z|\xi\rangle_{B_1}^{I})\otimes\\(\sigma_z|\eta\rangle_{A_2}^{I})\otimes|01\rangle_{C_1C_2}+(\sigma_x|\xi\rangle_{B_1}^{I})\otimes\\(\sigma_x|\eta\rangle_{A_2}^{I})\otimes|10\rangle_{C_1C_2}+(\sigma_x\sigma_z|\xi\rangle_{B_1}^{I})\otimes\\(\sigma_x\sigma_z|\eta\rangle_{A_2}^{I})\otimes|11\rangle_{C_1C_2}\end{pmatrix}. \quad (5)$$

若双方进行通信得到了 Charlie 的允许,他就测量己方粒子所处态并将测量结果告知 Alice 和 Bob. 这里,如果 Charlie 得到的结果是$|01\rangle_{C_1C_2}$,那么 Alice 必知己方粒子 A_2 所处的态为$(\sigma_z|\eta\rangle_{A_2}^{I})$. 因此,她对 A_2 进行幺正变换 σ_z,便能够在该粒子上将 Bob 想要传递的初态重建出来;相应地,Bob 对粒子 B_1 进行一次幺正变换 σ_z,就能够将 Alice 的初态重建于自己的粒子上. 这便是一个完整的双向传态过程.

2　量子通信网络的构建

以上述原理为基础,提出了一个构建量子通信网络的方案,并进行简要的安全性分析. 整个方案分为网络通信系统构建、用户注册认证和网络通信 3 个阶段.

2.1　通信系统构建阶段

该通信网络为星型网,拥有一个中心服务器(Center Server,简称 CS)和若干区域服务器(Domain Server,简称 DS)DS_1、DS_2、DS_3…,每个区域服务器负责它管辖区域(Domain)内各个客户端服务器(User Server,简称 US)US_1、US_2、US_3…之间的通信,且各个 US、DS 以及 CS 之间已事先共享足够多的处于 6 粒子团簇态的粒子作为通信量子信道,如图 1 所示.

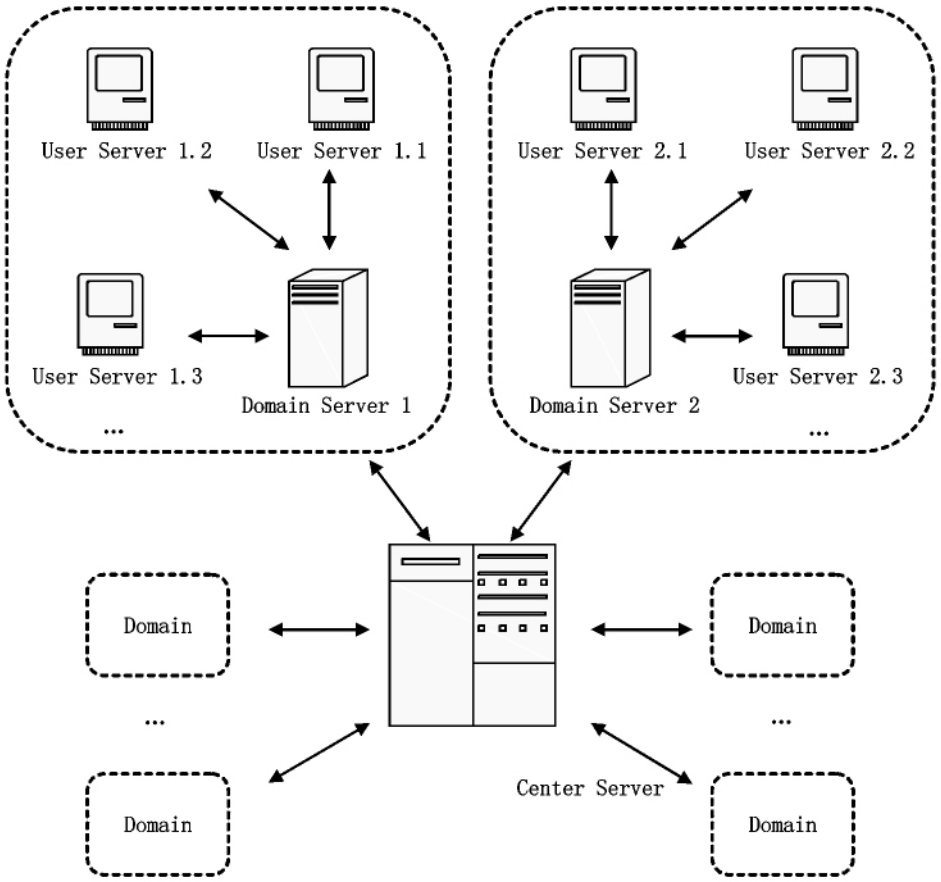

图 1　量子信道的构建

2.2　注册认证阶段

假设有一用户通过 US 与 DS 通信,若他们以前没有通信过,那么需要先进行第 1 次登记,即所谓注册[15]. US 将根据用户提供的姓名、密码等个人特征

信息,制备出一些处于特殊量子态粒子,这便是用户信息的载体. 通过量子隐形传态技术,可以使 DS 获取特定用户的个人信息,DS 将这些数据存储并通知 US 注册成功. 当用户再次登录,在客户端服务器 US 输入自己的个人信息时,通过与注册阶段类似的方式,DS 获得用户的特征信息并与事先存储的信息比较,若完全一致,则身份认证通过;否则认证不通过[16].

2.3 网络通信阶段

2.3.1 同网络内通信 (i)用户通过身份认证并登录成功后,区域服务器(DS)自动记录在客户端服务器(US)登录的用户状态为在线,以备通信. (ii)假设用户 A 在 DS_1 管辖范围内的 $US_{1.1}$ 上登录,他想与位于本网络内的用户 B 通信. 首先,A 通过 $US_{1.1}$ 向 DS_1 发出通信请求,DS_1 收到请求后在自己所管辖区域内查找,若确定 B 在本网络(假设用户 B 在 $US_{1.2}$ 登录)且状态为在线,则通知 $US_{1.1}$ 和 $US_{1.2}$ 开始通信. 根据量子双向传态原理,利用 $US_{1.1}$、$US_{1.2}$ 和 DS_1 事先共享的 6 粒子团簇态为量子信道,用户 A 和 B 即可完成他们之间的双向通信,如图 2 所示.

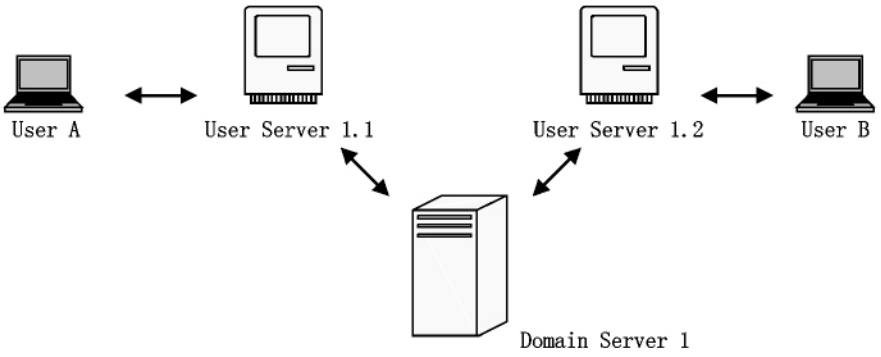

图 2 同网络通信

这里,各个客户端服务器向区域服务器提出申请的机会均等,而区域服务器以"先到先服务"的原则,优先响应更早提出通信请求的客户端服务器.

2.3.2 跨网络通信 (i)与同网络内通信一样,用户通过身份认证并登录成功后,区域服务器(DS)自动记录在客户端服务器(US)登录的用户状态为在线,以备通信. (ii)假设用户 A 在 DS_1 管辖范围内的 $US_{1.1}$ 上登录,他想与位于另一网络内的用户 H 通信(假设用户 H 在客户端 $US_{2.1}$ 上登录,$US_{2.1}$ 位于 DS_2 管辖范围之内). 首先,A 通过 $US_{1.1}$ 向 DS_1 发出通信请求,DS_1 收到请求后在自己所管辖区域内查找,发现没有用户 H 的登录信息,则向中心服务器(CS)提出申请,希望 CS 找到 H 的信息;CS 随即发送全网广播,要求记录了 H 状态信息的 DS 反馈信息. DS_2 在自己的数据库中发现 H 的信息,且此时 H 已通过 $US_{2.1}$ 登录,则向 CS 报告已经找到用户 H,且 H 状态为在线,可以进行通信(若 H 没有登录,则通报已找到 H 但是状态为不在线);CS 随即向 DS_1、DS_2 发出通知,允许用户 A、H 通信. 此时,利用 $US_{1.1}$、$US_{2.1}$ 和 CS 事先共享的 6 粒子团簇态为量子信道,A、H 可以成功实现双向通信,如图 3 所示.

这里,各个区域服务器向中心服务器提出申请的机会均等,中心服务器以"先到先服务"为原则,处理通信请求并参与通信.

3 通信安全性及效率分析

3.1 注册及认证阶段的安全性

在注册以及认证过程中,用户的操作均在 US 上进行,而具有用户个人信息的量子态在联合测量后会遭到破坏,由此可知用户在离开 US 后信息不会泄露. 若攻击者使用纠缠攻击,由于本方案中承载用户信息的量子态是未知的,而通过纠缠攻击无法获知,所以得不到任何有关用户的个人信息. 况且,这种攻击方式还会使得原有粒子之间的纠缠性遭到破坏,进而导致认证失败. 再者,攻击者由于没有用户的密码,也无法获知量子态,故无法冒名通过认证[15]. 由此看来,注册及认证阶段的安全性是有保障的.

3.2 双向传态的安全性

基于量子物理世界的一些基本定理,如量子不可克隆定理、测不准原理等,攻击者在量子通信中既不能得到精确的密文,也不能对量子态进行反复测量. 如果在量子信道上传送的量子态被攻击者改变,则结果将被改变,说明攻击者的行为能被发现;如果攻击者窃听量子信道,则纠缠态的纠缠性一定会被破坏,因此量子态不能传递到目的地. 即使攻击者获得了控制的测量结果,没有服务器上的纠缠粒子,也

无法重建通信双方待传的态,由此看来,量子态在量子信道上的传递是安全、可靠的.

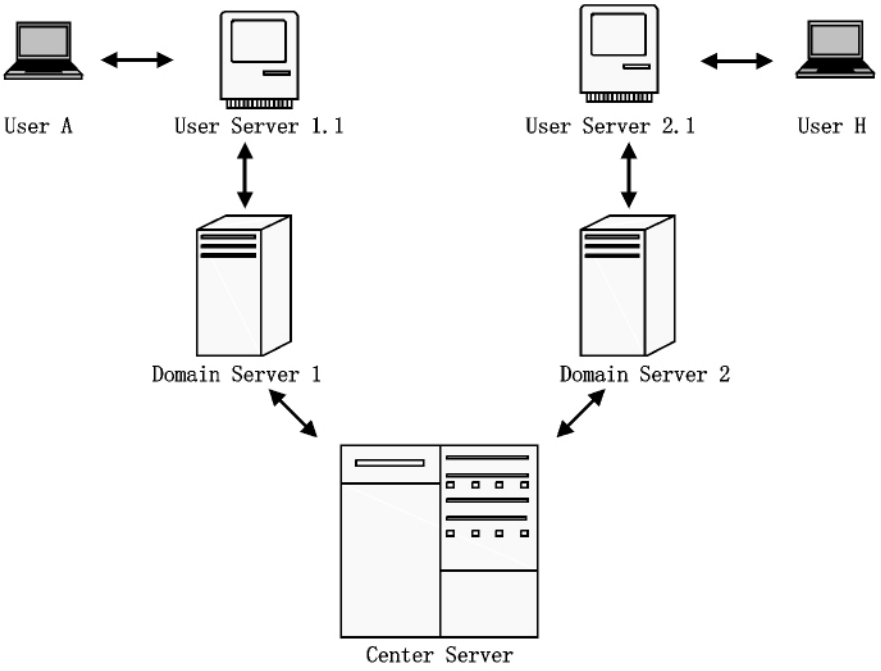

图 3　跨网络通信

3.3　服务器工作效率

在跨网络通信的过程中,存在 2 个问题:(i)需要借助中心服务器发送广播以查找另一网络中的用户,如果每次跨网通信都需要发送广播,不仅费时而且增加开销,通信效率低下;(ii)每次只能处理完一组通信之后再处理另外一组,无法满足用户实时通信的需求. 对此,提出 2 点改进方案:(a)各区域服务器应定时更新管辖区内客户端服务器上用户的登录情况,并及时向中心服务器通报,这样可以减少中心服务器发送广播的次数,从而有效减少开销,提高效率;(b)应选用高性能的服务器作为中心服务器,需要具备并行处理事件的能力,例如在控制一对通信组通信的同时,可以响应其他区域服务器的请求(如查找特定用户).

最后,尽管在身份认证、服务器之间发出请求并响应的过程中,需要使用经典信道,但经典信道不会用来传递任何与用户本身相关的信息,而只会用来传递必要的指令,因此,攻击者想从经典信道获取或窃听用户的机密信息是无法实现的. 综上所述,该网络通信系统是安全、可靠的,而且在改进服务器性能之后可以更好地满足通信需求.

4　结论

本文提出了利用量子双向传态技术来构建一个量子通信网络,从而实现安全的多方通信的方案. 该方案分为网络通信系统构建、用户注册认证和网络通信 3 个阶段. 首先构建了一个网络通信系统,包括客户端服务器、区域服务器和中心服务器,它们事先共享足够多的团簇态作为量子信道以供注册认证和网络通信使用;然后根据文献[14-15]的思想,完成用户的身份注册及认证;最后基于量子双向传态技术,实现同网和跨网通信. 与此同时,对通信的安全性和网络工作效率进行了分析,并提出了改进方法,使得该方案更具有实用价值.

5　参考文献

[1] Chen Hui, Zhu Shixiong, Zhu Fuchen. Introduction of quantum private communication [M]. Beijing: Beijing Institute of Technology Press, 2010: 86-104.

[2] Dai Kui, Song Hui. Introduction of technology of quantum information [M]. Changsha: National University of Defense Technology Press, 2001: 65-67.

[3] 陈晖,朱甫臣. 一次量子通信 QKD 和 QA 协议 [J]. 通信技术, 2003(6): 87-88.

[4] Zhou Chunyuan, Wu Guang, Chen Xiuliang, et al. Quantum private communication in 50 kilometer fiber [J]. Science in China (Series G: Physics, Mechanics & Astronomy), 2003, 33(6): 538-543.

[5] Deng Fuguo, Long Guilu, Liu Xiaoshu. Two-step quantum

direct communication protocol using the Einstein-Podolsky-Rosen pair block [J]. Phys Rev A,2003,68:42317.

[6] Deng Fuguo, Long Guilu. Secure direct communication with a quantum one-time pad [J]. Phys Rev A,2004,69:52319.

[7] Lucamarini M, Mancini S. Secure deterministic communication without entanglement [J]. Phys Rev Lett,2005,94:140501.

[8] Wang Chuan, Deng Fuguo, Li Yansong, et al. Quantum secure direct communication with high-dimension quantum superdense coding [J]. Phys Rev A,2005,71:44305.

[9] Wang Chuan, Deng Fuguo, Long Guilu. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state [J]. Opt Commun, 2005, 253:15-20.

[10] Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Phys Rev Lett, 1993, 70:1895-1899.

[11] Li Dachuang, Cao Zhuoliang. Teleportation of two-particle entangled state via cluster state [J]. Commun Theor Phys, 2007,47:464-466.

[12] Hong Zhihui, Nie Yiyou, Huang Yibin, et al. Controlled quantum teleportation via four particle cluster states [J]. Chinese Journal of Quantum Electronics, 2008, 25(4): 458-461.

[13] Wang Xinwen, Shan Yongguang, Xia Lixin, et al. Dense coding and teleportation with one-dimensional cluster states [J]. Phys Lett A,2007(1):7-11.

[14] Dong Ping, Xue Zhengyuan, Yang Ming, et al. Generation of cluster states [J]. Phys Rev A,2006,73(3):33818.

[15] Li Yuanhua, Liu Junchang, Nie Yiyou. Quantum identification scheme of cross-center based on four-particle cluster state [J]. Chinese Journal of Quantum Electronics,2011, 28(1):52-57.

[16] Zhou Nanrun, Zeng Guihua, Zeng Wenjie, et al. Cross-center quantum identification scheme based on teleportation and entanglement swapping [J]. Opt Commun,2005,254:380-388.

The Scheme of a Quantum Communication Network's Construction

ZOU Xin, YE Zhi-qing*

(1. College of Physics and Communication Electronic, Jiangxi Normal University, Nanchang Jiangxi 330022, China;
2. Key Laboratory of Photoelectronic & Telecommunication of Jiangxi Province, Nanchang Jiangxi 330022, China)

Abstract: Making using the technology of two-way quantum teleportation, a quantum communication network to implement securely multipoint communication has been constructed. The scheme's security and network communication efficiency were analyzed, and the improved methods, making the scheme more practical.

Key words: quantum communication network; two-way quantum teleportation; quantum identity authentication; cluster states; security

(责任编辑:冉小晓)