软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(1)):158−163

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

异构家庭网络中融合量子信息技术的安全通信协议*

马鸿洋, 王淑梅

(青岛理工大学 理学院,山东 青岛 266033)

通讯作者: 马鸿洋, E-mail: hongyang_ma@aliyun.com

摘 要: 随着量子信息技术与家庭网络技术日益紧密结合,采用量子密钥确保家庭网络的通信安全已经成为大势所趋.针对目前数字家庭通信网络的安全日益复杂和多样化的问题,提出了异构家庭网络中融合量子信息技术的安全通信协议,智能终端设备、家庭网关、业务管理平台内的服务器共享量子 GHZ 态,根据 GHZ 三重态的内在特性,从而实现业务管理平台内的服务器对智能终端设备的合法性访问和数据处理.该协议利用现有手段可以实现.

关键词: 异构;数字家庭网络;量子信息技术;GHZ 态

中文引用格式: 马鸿洋,王淑梅.异构家庭网络中融合量子信息技术的安全通信协议.软件学报,2013,24(Suppl.(1)):158−163. http://www.jos.org.cn/1000-9825/13017.htm

英文引用格式: Ma HY, Wang SM. Security communication protocol integrate quantum information technology in heterogeneous home network. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(1)):158−163 (in Chinese). http://www.jos.org.cn/1000-9825/13017.htm

Security Communication Protocol Integrate Quantum Information Technology in Heterogeneous Home Network

MA Hong-Yang, WANG Shu-Mei

(School of Sciences, Qingdao Technological University, Qingdao 266033, China)

Corresponding author: MA Hong-Yang, E-mail: hongyang_ma@aliyun.com

Abstract: With the merging of quantum information and home network technologies, the adoption of quantum key to ensure the security of home network communication has become a critical topic. To address the problem of digital home network security with increased complexity and variety, this paper proposes a secure communication protocol in integrated quantum information technology in heterogeneous digital home network where GHZ states are shared by intelligent terminal equipments, family gateways and servers within business management platform. Based on the inherent triplet-state characteristics of quantum GHZ states, legitimacy of communications between servers within business management platform and intelligent terminal equipments can be validated, and information can also be protected. This protocol can be implemented by existing approaches.

Key words: heterogeneous; digital home network; quantum information technology; GHZ state

随着数字家庭网络的迅速发展及其量子信息技术的成熟,两者的融合成为未来无线网络发展的一个重要方向.数字家庭网络[1,2]是指利用家庭网关将公共网络功能和应用扩展到家庭中,以无线通信的方式连接各种智能家电终端,并提供语音、多媒体、敏感数据、设备控制和系统管理等功能.由于家庭网络中使用无线通信,其无所不在的电磁波为家庭用户提供便捷服务,也因其信息暴露在空中而引起通信安全的危机.

众多研究人员在数字家庭网络安全方面提出了多种安全通信方案.章坚武等人提出了基于改进的用户数据报协议的智能家庭网关通信模式,利用 LPC2103 微控制器与 RTL8019AS 智能模块,实现数字家庭网络信息的

* 基金项目: 国家自然科学基金(61173056); 山东省高等学校科技计划(J11LG07); 青岛市科技计划基础研究项目(12-1-4-4-(6)-JCH)

收稿时间: 2013-05-02; 定稿时间: 2013-08-22

安全处理和控制[3].赵跃华等人提出了异构的数字家庭网络中嵌入式系统的紧凑安全策略,利用 HTTP 摘要认证和 SSL 安全协议,实现身份认证的嵌入式网关的安全通信[4].

量子信息技术[5]是一种新的技术手段,其对于信息的加密不再是依靠常规加密技术,而是依靠物理特性.该技术在未来网络通信的发展过程中具有重要的战略意义.其相关理论及实验研究成果众多[6,7].1982 年,Bennett 等人提出了 BB84 通信协议[8].1991 年,Ekert 提出了 EPR 协议通信[9].Ma 等人提出了多簇多量子节点的量子密钥共享协议[10].Li 等人提出了四粒子组成的团簇态实现跨中心、分布式的量子密钥通信以及身份认证[11].

本文提出了异构家庭网络中融合量子信息技术的安全通信协议以及智能终端设备、家庭网关、业务管理平台内的服务器共享的 GHZ 态,根据 GHZ 三重态的内在特性,实现了业务管理平台内的服务器对智能终端设备的合法性访问和数据处理.本文第 1 节介绍异构家庭网络与量子信息技术的相关知识.第 2 节阐述异构家庭网络中融合量子信息技术的安全通信协议.第 3 节是通信协议的安全性理论分析.第 4 节是结束语.

1 异构家庭网络与量子信息技术的相关知识

1.1 异构家庭网络系统简介

异构的数字家庭网络系统包括家庭网关、智能终端设备、业务管理平台内的服务器,还有量子密钥通信设备等.

家庭网关是整个异构数字家庭网络的关键部件,是无线数据输入和输出的控制中心;智能终端设备是异构数字家庭网络的被控对象,例如,智能电视、家庭通信域的手机、智能冰箱、智能水电表、智能监控设备等;业务管理平台内的服务器是通过网关采集智能终端设备信息的硬件设备.为了避免繁冗的布线,本协议的数据通信采用无线通信技术.

家庭网关采用 IPv4 或 IPv6 协议进行编制网络地址.如果采用 IPv4 协议编制,则该地址包括网络号和主机号,一般是 C 类地址,而且该地址由接入网络的上一级网关按照一定规则分发配置.对于内部智能终端、业务管理平台内服务器的地址均由家庭网关统一分配,但整个异构数字家庭网络对外呈现唯一的 IP 地址号.如果采用 IPv6 协议编制,则家庭网关、智能终端、业务管理平台内的服务器均有独立的 IP 地址号.这些地址由接入网络的上一级网关按照一定规则分发配置,家庭网关不需要参与 IP 地址的分发和管理业务.本协议 IP 地址按照 IPv4 协议来配置.

三者之间的通信所使用的信道有量子信道与经典信道,量子信道是利用量子 GHZ 态传输量子信息,用虚线表示;经典信道是无线通信技术中使用“0”、“1”码来传输信息,用实线表示,如图 1 所示.

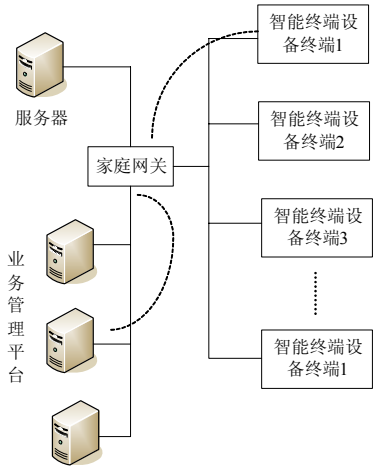


图 1 异构家庭网络构成结构图

1.2 异构家庭网络协议参考模型

本协议考虑无线通信和量子通信的需要,借鉴 OSI 7 层模型的思想,根据系统的实际情况,设计了异构家庭网络的五层协议模型,如图 2 所示.该模型不仅满足不同层数据控制的需求,而且还满足量子通信的要求.

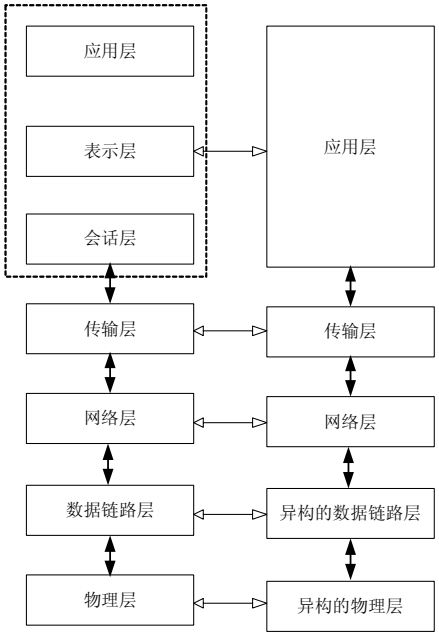


图 2 异构家庭网络协议参考模型

(1) 异构的物理层

该层不仅要能传输常规的“0”、“1”码,而且能传输量子信息.在实现条件上,一部分采用无线通信编码方式;另一部分采用能处理量子信息的设备,包括量子关联光源的制备设备、量子态的测量设备.该层的作用是使用无线通信设备和量子通信设备为上层提供物理连接,控制数据的出错率.

(2) 异构的数据链路层

该层一方面采用无线通信的载波监听多路访问/冲突检测协议,另一方面进行量子信息的数据传输.

(3) 网络层

根据 IPv4 或 IPv6 协议配置的 IP 地址,实现异构家庭网络内部之间的经典信息和量子信息的路由控制.

(4) 传输层

该层处理经典信息和量子信息端到端连接控制以及拥塞控制,其中,要解决量子信息的拥塞控制必须考虑量子信息的存储设备.

(5) 应用层

该层是定义家庭用户在网络中的接口功能,为其提供常规的多种服务,例如信息查询、信息处理等软件服务.

1.3 量子信息技术及其GHZ态的简介

量子信息技术是将微观粒子作为信息载体,利用微观粒子所特有的量子性质——纠缠、不确定性、相关性等,实现在经典通信、经典计算、经典密码学等领域无法完成的项目.其中,量子密码是到目前为止所公认的绝对安全的理论.这种理论上的无条件安全性是指,通过理论可以证明,即使窃听者具有任意物理学所能提供的攻击手段和无限大的计算能力,该密码依然可以保证双方或者多方通信信息的安全性.

本协议所用的量子密钥——GHZ 态[12],是以 Greenberger,Horne,Zeilinger 这 3 位科学家的名字联合命名的,其表达式为

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)_{ABC} \tag{1}$$

其原理如下:首先,3 个参与者 Alice,Bob 和 Charlie 分别各自持有 GHZ 态的一个粒子;其次,Alice,Bob 和 Charlie 随机测量他们分别持有的粒子的状态;最后,Charlie 在公共信道上宣布其测量结果,Alice,Bob 根据 Charlie 公布的测量结果,依据 GHZ 三重态的内在相干性,Alice 和 Bob 则获知密钥信息.

2 异构家庭网络中融合量子信息技术的安全通信协议

该通信协议分为 4 个部分:系统初始化、各自联合判定阶段、数据通信阶段、通信注销阶段.其中,假设家庭网关是可信的第三方.

2.1 系统初始化

Step 1. 业务管理平台内的服务器按照家庭网关为其配置的 IP 地址进行经典数据的路由转发,向家庭网关发送启动数据传输的数据帧.

Step 2. 家庭网关收到请求数据帧后,进行量子 GHZ 态的初始化,将 3 个粒子 A,B,C 分发给业务管理平台内的服务器、智能终端设备以及自身.

2.2 各自联合判定阶段

Step 3. 家庭网关需要验证业务管理平台内的服务器的身份.业务管理平台内的服务器、智能终端设备各自随机沿 x 和 y 的方向测量自己手中的粒子.

Step 4. 业务管理平台内的服务器、智能终端设备将其测量基(x 或 y)发给家庭网关,但各自保存自己的量子比特值,该结果只有自己知道,并不公布.

Step 5. 家庭网关根据业务管理平台内的服务器、智能终端设备的测量基,测量自己手中的粒子.将式(1)变形为式(2)~式(5):

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left[\left(|+x\rangle_A|+x\rangle_B+|-x\rangle_A|-x\rangle_B\right)\left(|0\rangle_C+|1\rangle_C\right)+\left(|+x\rangle_A|-x\rangle_B+|-x\rangle_A|+x\rangle_B\right)\left(|0\rangle_C-|1\rangle_C\right)\right] \tag{2}$$

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left[\left(|+y\rangle_A|+x\rangle_B+|-y\rangle_A|-x\rangle_B\right)\left(|0\rangle_C-i|1\rangle_C\right)+\left(|+y\rangle_A|-x\rangle_B+|-y\rangle_A|+x\rangle_B\right)\left(|0\rangle_C+i|1\rangle_C\right)\right] \tag{3}$$

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left[\left(|+x\rangle_A|+y\rangle_B+|-x\rangle_A|-y\rangle_B\right)\left(|0\rangle_C-i|1\rangle_C\right)+\left(|+x\rangle_A|-y\rangle_B+|-x\rangle_A|+y\rangle_B\right)\left(|0\rangle_C+i|1\rangle_C\right)\right] \tag{4}$$

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left[\left(|+y\rangle_A|+y\rangle_B+|-y\rangle_A|-y\rangle_B\right)\left(|0\rangle_C-|1\rangle_C\right)+\left(|+y\rangle_A|-y\rangle_B+|-y\rangle_A|+y\rangle_B\right)\left(|0\rangle_C+|1\rangle_C\right)\right] \tag{5}$$

其中,$|+x\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right),|-x\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right),|+y\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+i|1\rangle\right),|-y\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-i|1\rangle\right),|0\rangle=\frac{1}{\sqrt{2}}\left(|+x\rangle+|-x\rangle\right),|1\rangle=\frac{1}{\sqrt{2}}\left(|+x\rangle+|-x\rangle\right)$.

由式(2)可知,家庭网关可以根据业务管理平台内的服务器、智能终端设备的测量基,可知自己的测量结果.如果沿着+x 方向测量 A,B 粒子,则 C 粒子的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$,反之,沿着+$x$ 与–x 方向测量 A,B 粒子,则 C 粒子的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$;由式(3)可知,如果沿着 +$y$ 与 +x 方向测量 A,B 粒子,则 C 粒子的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle-i|1\rangle\right)$,反之,沿着+$y$ 与–x 方向测量 A,B 粒子,则 C 粒子的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle+i|1\rangle\right)$;由式(4)可知,如果沿着

+*x* 与+*y* 方向测量 *A*,*B* 粒子,则 *C* 粒子的量子态是 $\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)$,反之,沿着+*x* 与–*y* 方向测量 *A*,*B* 粒子,则 *C* 粒子的量子态是 $\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)$;由式(5)可知,如果沿着+*y* 方向测量 *A*,*B* 粒子,则 *C* 粒子的量子态是 $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$,反之,沿着+*y* 与–*y* 方向测量 *A*,*B* 粒子,则 *C* 粒子的量子态是 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. 这样,根据业务管理平台内的服务器、智能终端设备的测量基的不同情况,家庭网关得到不同的量子态.

Step 6. 家庭网关完成测量后,将其结果按照家庭网关为其配置的 IP 地址进行路由转发给业务管理平台内的服务器、智能终端设备,其中,结果是 $\{|+x\rangle,|-x\rangle,|+y\rangle,|-y\rangle\}$ 中的一个情况.

Step 7. 业务管理平台内的服务器、智能终端设备根据式(2)~式(5)结合自己的测量结果和家庭网关转发过来的测量结果,就可以判定对方所拥有的量子态.这样,业务管理平台内的服务器、智能终端设备获得共同的量子比特串,记为共同的量子密钥.

2.3 数据通信阶段

Step 8. 业务管理平台内的服务器将自己手中的量子比特发送给智能终端设备,智能终端设备接收量子密钥后,与自己的量子比特进行核对,如果相符,那么允许在本地进行数据处理的相关操作.

2.4 通信注销阶段

Step 9. 业务管理平台内的服务器接收完数据后,再按照家庭网关为其配置的 IP 地址进行经典数据的路由转发,向家庭网关发送停止数据传输的数据帧.

3 安全分析

本通信协议因为是异构结构,其安全性通过量子密钥来保证,本文仅从量子信息的角度分析其安全性:

(1) 假设存在外部窃听者,与智能终端设备、家庭网关构造新的 GHZ 态,这三者之间的所拥有的粒子为 *E*,*F*,*G*,其表达式为 $|\psi\rangle_{EFG}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{EFG}$,窃听者执行相关测量,所采用的 GHZ 态基矢为:$\frac{1}{\sqrt{2}}(|000\rangle\pm|111\rangle)$,$\frac{1}{\sqrt{2}}(|001\rangle\pm|110\rangle)$,$\frac{1}{\sqrt{2}}(|010\rangle\pm|101\rangle)$,$\frac{1}{\sqrt{2}}(|100\rangle\pm|011\rangle)$.

A,*B*,*C*,*E*,*F*,*G* 这 6 个粒子所构成的系统是

$$|\psi\rangle_{ABC}|\psi\rangle_{EFG}=\frac{1}{2}\left[\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{BCE}\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{AFG}+\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{BCE}\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{AFG}+\right.$$
$$\left.\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)_{BCE}\frac{1}{\sqrt{2}}(|011\rangle+|100\rangle)_{AFG}+\frac{1}{\sqrt{2}}(|001\rangle-|110\rangle)_{BCE}\frac{1}{\sqrt{2}}(|011\rangle-|100\rangle)_{AFG}\right] \quad (6)$$

通过式(6),可知窃听者必须在智能终端设备、家庭网关、业务管理平台内的服务器这三者的帮助下才能获得下面 4 个测量结果中的一个,其中,4 个测量结果为 $\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{BCE}$,$\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{BCE}$,$\frac{1}{\sqrt{2}}(|001\rangle-|110\rangle)_{BCE}$,$\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)_{BCE}$. 当然,三者是不可能提供这种额外帮助的,所以窃听者无法得到相关信息.

(2) 假设存在内部窃听者业务管理平台内的服务器.某个服务器并没有获得家庭网络发送的粒子,但是想获得读取智能终端设备的权限,需要自己伪造相关测量数据.而根据 GHZ 三重态的内在特性可推知,GHZ 三重态的一个粒子的量子比特是无法获得其他两个粒子的量子态的.该服务器将伪造的量子态其发送给智能终端设备,必定因为较大错误率而被拒绝访问.

4 结束语

本文提出了异构家庭网络中融合量子信息技术的安全通信协议,在智能终端设备、家庭网关、业务管理平台内的服务器三者之间共享量子 GHZ 态,实现业务管理平台内的服务器对智能终端设备的合法访问.另外,本文还提出了异构家庭网络协议参考模型,但是该模型还需要进一步的细化.

References:

[1] Vaidya B, Park JH, Yeo SS, Rodrigues JJPC. Robust one-time password authentication scheme using smart card for home network environment. Computer Communications, 2011,34:326−336.

[2] Miguel V, Cabrera J, Jaureguizar F, García N. Distribution of high-definition video in 802.11 wireless home networks. IEEE Trans. on Consumer Electronics, 2011,57(1):53−61.

[3] Zhang JW, Yan H, Bao JR. Design of intelligent family gateway and its application in Internet of things. Computer Engineering, 2011,37(18):246−251 (in Chinese with English abstract).

[4] Zhao YH, Du YH, Bao MG. Implementation of security in embedded Web gate based on authentication. Computer Engineering, 2004,30(23):111−113 (in Chinese with English abstract).

[5] Razavi M. Multiple-Access quantum key distribution networks. IEEE Trans. on Communications, 2012,60(10):3071−3079.

[6] Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 1992,68(21):3121−3124.

[7] Zhang YL, Wang YN, Xiao XR, Jing L, Mu LZ, Korepin VE, Fan H. Quantum network teleportation for quantum information distribution and concentration. Physical Review A, 2013,87(2):22302.

[8] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proc. of the IEEE Int'l Conf. on Computers Systems and Signal Processing. Bangalore: IEEE, 1984. 175−179.

[9] Ekert AK. Quantum cryptography based on bell's theorem. Physical Review Letters, 1991,67(6):661−663.

[10] Ma HY, Chen BQ, Guo ZW, Li HS. Development of quantum network based on multiparty quantum secret sharing. Cannadian Journal of Physics, 2008,86(9):1097−1101.

[11] Li YH, Liu JC, Nie YY. Quantum identification scheme of cross-center based on four-particle cluster state. Chinese Journal of Quantum Electronics, 2011,28(1):52−57 (in Chinese with English abstract).

[12] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Physical Review A, 1999,59(3):1829−1834.

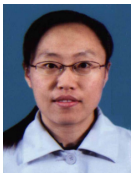
附中文参考文献:

[3] 章坚武,颜欢,包建荣.智能家庭网关设计及其物联网应用.计算机工程,2011,37(18):246−251.

[4] 赵跃华,杜云海,包明国.智能家庭网络安全解决方案.计算机工程,2004,30(23):111−113.

[11] 李渊华,刘俊昌,聂义友.基于团簇态的跨中心量子网络身份认证方案.量子电子学报,2011,28(1):52−57.

马鸿洋(1976－),男,山东青岛人,博士,副教授,主要研究领域为量子信息安全,无线网络,信息论.
E-mail: hongyang_ma@aliyun.com



王淑梅(1975－),女,副教授,主要研究领域为计算机网络.
E-mail: shlxb@qtech.edu.cn