doi:10.3788/gzxb20124110.1256

基于特洛伊木马攻击的多用户树型量子信令损伤模型及修复策略

李超,聂敏

(西安邮电大学 通信与信息工程学院,西安 710061)

摘 要:提出了一个多用户量子信令树型传输系统,并详细阐述了信令的传输过程.研究了系统中信令受到特洛伊木马攻击的损伤模型及其修复的必要性.将量子密钥分发的思想引入量子信令安全的直接通信中,分析了采用非正交量子态,以克服特洛伊木马攻击的问题,从而提高了信令传输的安全性.对多用户量子信令树型传输系统进行改进,提出了新的广义的多用户量子信令树型拓扑传输模型.研究结果表明,本文所提出的对多用户信令攻击的修复策略可有效地防止特洛伊木马攻击,从而保证信令传输过程安全有效的进行.

关键词:多用户量子信令;信令传输;树型拓扑;特洛伊木马攻击

中图分类号:G301 **文献标识码**:A **文章编号**:1004-4213(2012)10-1256-5

0 引言

随着量子通信的发展,量子保密通信的研究不断深入,量子密钥分发协议[1-3]也越来越完善,可以在发送端和接收端协商出绝对安全的量子密钥,从而利用此密钥对信息进行一次一密,就可以通过经典信道进行绝对安全的通信.量子通信近年来又产生了一个新的分支——量子安全直接通信[4-6].2002年,Bostrom 和 Felbinger 提出了“ping-pong”协议[7].2003 年,邓富国等利用块传输的思想,提出了两步的量子安全直接通信方案协议[8].2007 年,邓富国等又提出了利用单光子实现的经济的量子安全直接通信网络[9].但量子信令传输的安全性研究尚未展开.为此,本文在分析了在特洛伊木马攻击(Trojan Horse Attacking Strategy, THAS)[10-12]的前提下,提出了多用户量子信令树型拓扑模型,利用量子态的不同偏振来承载不同的信令消息.将量子密钥分发思想引入量子信令安全的直接通信,采用非正交量子态来克服特洛伊木马攻击,使得攻击者不能精确地获得传输信令,从而提高了信令传输的安全性.

1 多用户量子信令树型传输系统

本文提出的多用户树型拓扑量子信令模型,其信令传输过程如图 1.

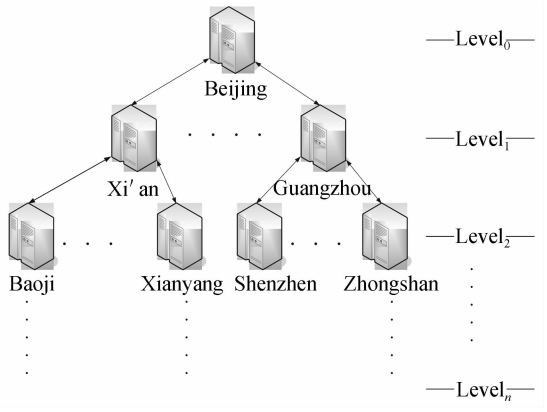

图 1 多用户量子信令树型拓扑传输模型

Fig. 1 Transmission model of multi-user quantum signaling tree topology

假设北京用户要将其信令传送给各地,首先将信令传送到各大区中心和直辖市,比如西安、南京、沈阳、成都、重庆等,然后由各大区中心再到该大区的省会城市,再由各省会城市向其省内其它城市传输,以此类推.同样,若各地市想要向北京传送信令消息,也要逐级上传.也就是说,每两个量子交换机之间都是多路双向信令的传送方式.

在量子信令交换机中,每个用户都有不同的身份编码(ID).主叫用户通过交换机识别被叫用户的 ID 号,完成路由的建立和通信过程.在通常情况下,为了扩大系统的传输容量,采用量子波分系统,即不同用户根据不同的光子频率进行编码和接收信令.

基金项目:国家自然科学基金(No. 61172071)和陕西省自然科学基础研究计划(No. 2010JM8021)资助

第一作者:李超(1987—),女,硕士研究生,主要研究方向为量子通信、移动通信. Email: lc32514@163.com

导 师:聂敏(1964—),男,教授,博士后,主要研究方向为量子通信、移动通信、现代通信网理论和关键技术. Email: niemin@xupt.edu.cn

收稿日期:2012-05-31;**修回日期**:2012-07-18

所以，接收端根据用户的 ID 号可正确区分用户身份.

量子信令形如

$$|\varphi\rangle=a|H\rangle+b|V\rangle \tag{1}$$

式中 a 及 b 均为复数，满足 $|a|^2+|b|^2=1$. H 和 V 为单光子在水平和垂直方向的偏振，且单光子的偏振方向可取水平与垂直之间的任意角度. 由于圆周上有无数个点即 a 和 b 的取值有无穷多个，所以所传信令以 a 和 b 的不同取值来进行区分，只要满足 $|a|^2+|b|^2=1$ 即可.

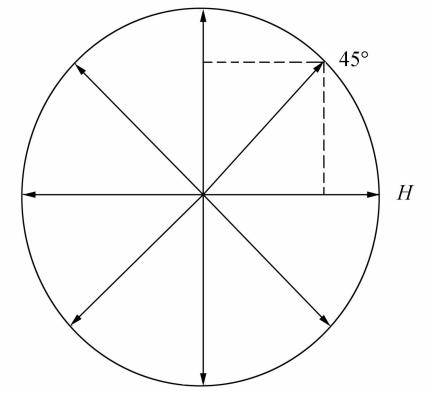

图 2　单光子的偏振方向

Fig. 2　Single photon polarization

为保证信令安全有效地传输，在量子信令交换机的输出端必须进行加密操作. 过程如下：每个信道中有 k 对用户分别传送各自的信令，发端(Alice)和收端(Bob)共享一个 EPR 对作为信令密钥，表示如下

$$K=|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|0_a0_b\rangle+|1_a1_b\rangle) \tag{2}$$

将携带信令信息的光子(信令粒子)和密钥粒子经过一个量子受控非门完成加密操作，该过程可表示为

$$|\Phi^c\rangle=C_{mk}|\Phi^+\rangle|\varphi\rangle=|0_a0_b\rangle\otimes|\varphi\rangle+|1_a1_b\rangle X_m|\varphi_m\rangle \tag{3}$$

C_{mk} 代表信令粒子与密钥粒子上的量子受控非(Controlled-Not 或 CNOT)门操作[13]. 这个门有两个量子输入比特，分别是控制量子比特和目标量子比特. 若控制量子比特置为 0，则目标量子比特保持不变；若控制量子比特置为 1，则目标量子比特将翻转. 其矩阵表示 U_{CN} 为

$$U_{CN}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \tag{4}$$

X_m 是对信令粒子的量子非门. 也就是说，当密钥 EPR 对处于 $|0_a0_b\rangle$ 时，信令粒子处于 $|\varphi\rangle$；EPR 对处于 $|1_a1_b\rangle$ 时，信令粒子处于 $X_m|\varphi\rangle$.

考虑量子信令采用树型拓扑传输. 一个完整的信令传输过程，在该树型拓扑模型中可逐段进行，各段加密和传输方式相同. 每段传输的是多路信令(可表示为：$|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_n\rangle$)，信令从树根节点(北京)到叶子节点(各地市)准确无误地传输.

2　特洛伊木马攻击模型

图 3 为特洛伊木马攻击过程. 从图中可看出，Alice 将信令经过加密(图中的信封代表原始信令，带锁的信封代表信令被加密)发送给 Bob，而 Bob 在接收端经过解密来还原信令. 攻击者 Eve 事先在 Alice 设备中植入木马(图中的木马 Trojan horse)，待 Alice 对信令进行加密后，将反馈信息(图中带钥匙的信封)传送给 Eve，此时 Eve 可通过反馈信息获得信令信息.

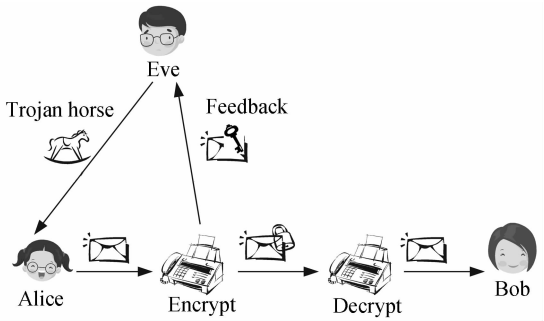

图 3　特洛伊木马攻击过程

Fig. 3　Trojan horses attack process

通常情况下，攻击者在中途进行信令拦截，而特洛伊木马攻击的特点是，一开始就在发送方或接收方的服务器(量子信令交换机)中植入木马. 所以，特洛伊木马攻击成功的前提是：攻击者不被发现的前提下，事先在量子信令交换机中植入木马. 所植入的木马可区分本征态 $|0\rangle$ 和 $|1\rangle$，并向攻击者反馈信息. 这样，式(3)经加密后的信令变为

$$\widehat{|\Phi^c\rangle}=|0_a(h_{\parallel})0_b\rangle\otimes|\varphi\rangle+|1_a(h_{\perp})1_b\rangle\otimes X_m|\varphi\rangle \tag{5}$$

式中，$h_{\parallel}$、$h_{\perp}$ 为木马对攻击者的反馈信息，其分别代表对 $|0\rangle$ 和 $|1\rangle$ 的反馈，这样，根据上式攻击者可得出所传输信令为 $|\varphi\rangle$ 或 $X_m|\varphi\rangle$，从而最终完全获得信令消息.

3　修复策略

对于树型拓扑信令传输系统来说，如果受到传统的攻击，只会造成一小段信令消息被窃取. 但是如果受到特洛伊木马攻击，因为木马事先隐藏在交换机中，从该交换机进出的所有信令都会受到威胁. 特别是根节点(北京)的交换机，一旦遭到了特洛伊木马攻击，整个信令传输系统的所有信令都有可能被窃取. 所以，对树型信令拓扑而言，特洛伊木马攻击

的危害性极大.

根据不可克隆定理,如果量子比特为正交态,测量基可精确测量构成测量基的每一个量子比特;若量子比特由非正交量子比特组成,则不可克隆.所以,防止特洛伊木马攻击的关键是:制备一组 Alice 和 Bob 共享的非正交的纠缠态.

选用两组基$|0\rangle$,$|1\rangle$和$|+\rangle$,$|-\rangle$如图 4.

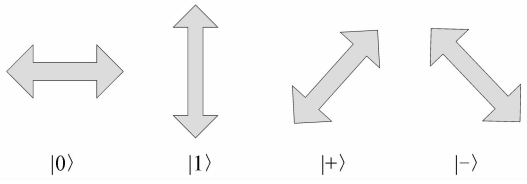

图 4 两组正交基

Fig. 4 Two groups of orthogonal basis

Alice 和 Bob 制备了一组 EPR 纠缠对,每对可表示为

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|0_a0_b\rangle+|1_a1_b\rangle)=\frac{1}{\sqrt{2}}(|+_a+_b\rangle+|-_a-_b\rangle) \tag{6}$$

其中,$|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$. Alice 和 Bob 随机的在$\{I,H\}$中选择一种操作,应用到她(他)的 EPR 粒子上,直到所有的 EPR 对完全操作.I为单位操作

$$|\psi_1\rangle=I|\Phi^+\rangle=|\Phi^+\rangle \tag{7}$$

H为 Hadamard 门,对于双量子比特来说

$$H=\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix} \tag{8}$$

$$|\psi_2\rangle=H|\Phi^+\rangle=\frac{1}{2}(|1_a+_b\rangle+|0_a-_b\rangle)=\frac{1}{\sqrt{2}}(|+_a1_b\rangle+|-_a0_b\rangle) \tag{9}$$

Alice 和 Bob 获得一组由$\{|\psi_1\rangle,|\psi_2\rangle\}$组成的随机序列,作为密钥,且经计算$\langle\psi_1|\psi_2\rangle\neq0$.内积不为零也就是说密钥由非正交量子比特构成.

此时新构建的密钥为

$$|K\rangle=c_1|\psi_1\rangle+c_2|\psi_2\rangle \tag{10}$$

加密后的信令消息为

$$|\Phi^c\rangle=C_{mk}|K\rangle|\varphi\rangle=(\frac{c_1}{\sqrt{2}}|0_a0_b\rangle+\frac{c_2}{\sqrt{2}}|0_a-_b\rangle)\otimes|\varphi\rangle+(\frac{c_1}{\sqrt{2}}|1_a1_b\rangle+\frac{c_2}{\sqrt{2}}|1_a+_b\rangle)\otimes X_m|\varphi\rangle \tag{11}$$

假设在发送端植入木马,所传输的信令为

$$|\Phi^c(r)\rangle=C_{am}\{c_1|\psi_1(r)\rangle+c_2|\psi_2(r)\rangle\}|\varphi\rangle=(\frac{c_1}{\sqrt{2}}|0_a(h_{\parallel})0_b\rangle+\frac{c_2}{\sqrt{2}}|0_a(h_?)-_b\rangle)\otimes|\varphi\rangle+(\frac{c_1}{\sqrt{2}}|1_a(h_\perp)1_b\rangle+\frac{c_2}{\sqrt{2}}|1_a(h_?')+_b\rangle)\otimes X_m|\varphi\rangle \tag{12}$$

这里,$h_?$和$h_?'$代表不确定的反馈信息.即使攻击者在 Alice 和 Bob 中植入两个木马分别可检测$|0\rangle$,$|1\rangle$和$|+\rangle$,$|-\rangle$,因为密钥的选择完全是随机的,攻击者也不会获得精确的信令消息.

4 多用户树型传输协议分析

以上所进行的分析,是针对端到端的情况.对于树型拓扑信令传输系统而言,攻击者可以选择任意交换机来植入木马,且能获得发往此交换机以及从此交换机发出的所有信令消息.这对于树型传输系统来说危害性极大.如果在树的根部就植入木马,整个系统的所有信令消息都会受到威胁.

假设在信道中有k组信令传输,就信令形式而言,不同的(a,b)组合对应不同的频率f(或波长λ),表示如下

$$\begin{aligned}&(a_1,b_1)\rightarrow\lambda_1\\&(a_2,b_2)\rightarrow\lambda_2\\&\quad\vdots\qquad\vdots\\&(a_k,b_k)\rightarrow\lambda_k\end{aligned} \tag{13}$$

对于多用户树型传输,每个用户在发端分别进行加密然后传输,攻击者植入的木马可以检测到所有该交换机中用户的状态.所以为防止特洛伊木马攻击,在树型系统中,所有的用户都要使用随机的非正交叠加态作为密钥进行加密,即可保证信令传输的安全.

在树型拓扑传输模型中,每两个量子交换机之间都是多路双向信令的传送方式.如果攻击者为盲目攻击,即任意在一个交换机中植入木马,则由上文的修复策略中可得其不能得到完全的确定反馈,假设其获得信息的最大概率为a;如果攻击者为有选择性的攻击,即确定攻击某个交换机(A),窃取指定两个交换机(A 到 B)之间传输的信令,由于攻击者不能够区分信令的来向和去向,只能够收到所有经过 A 的信令的反馈信息,所以并不能准确地选择 A 与 B 之间的信令.假设 A 有m个输入方向,n个输出方向,则攻击者成功获取其中一个重要信息的概率为$1/amn$.所以就树型拓扑结构来说,树的分支越多,攻击者成功获取信令消息的概率就越小,相对系统越安全.所以将图 1 的多用户量子信令树型拓扑传输模型进行改进,如图 5.

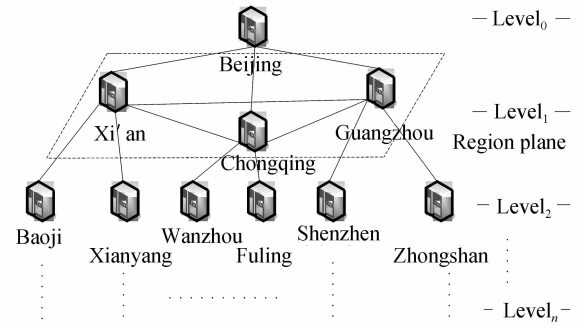

图 5　广义的多用户量子信令树型拓扑传输模型

Fig. 5　General transmission model of multi-user quantum signaling tree topology

首先将原来的 1 级系统中的大区中心城市和直辖市改为省会城市和直辖市，再由各省会城市向其省内其它城市传输，这样分支的部分增多可确保一定的安全性；其次，在树型拓扑模型中，根节点受到攻击将会很严重，也就是说 0 级与 1 级之间的安全性很重要，所以将 1 级系统中各城市相连构成大区平面，若这两级的交换机受到攻击，则信令可通过其互连迂回传送. 再次，大区平面的构建使得重要枢纽城市之间的信令传送不再经过北京，为根节点减少负担.

5　结论

本文构建了一个多用户量子信令树型拓扑传输模型，并对其安全性进行了分析. 选用不同的偏振角度来标记不同的信令，使得同时可进行多用户的传输. 在传输过程中为了确保其安全性，假定偏振角度以每秒 3 000 次的频率进行有规律的变更，降低了被攻击的可能性. 具体对对系统受到特洛伊木马攻击进行了分析，研究结果表明使用非正交态方案能有效地防止特洛伊木马攻击. 对于树型拓扑的特殊性，新的广义的多用户量子信令树型拓扑传输模型，使得在整个信令传输网中信令消息被窃取的可能性降低，确保信令传输安全有效的进行. 本文的研究为今后量子信令传输安全性的发展可提供必要的技术支持.

参考文献

[1] ZHAO Yi, QI Bing, MA Xiong-feng, *et al*. Experimental quantum key distribution with decoy states[J]. *Physical Review Letters*, 2006, **96**(7):070502-1-070502-4.

[2] QUAN Dong-xiao, PEI Chang-xing, ZHU Chang-hua, *et al*. New method of decoy state quantum key distribution with a heralded single-photon source[J]. *Acta Physica Sinica*, 2008, **57**(9): 5600-5604.
权东晓，裴昌幸，朱畅华，等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报，2008，**57**(9)：5600-5604.

[3] CHEN Xia, WANG Fa-qiang, LU Yi-qun, *et al*. A differentialphase shift key distribution QKD system combing wit hefficient BB84 scheme[J]. *Acta Photonica Sinca*, 2008, **37**(5): 1052-1056.
陈霞，王发强，路铁群，等. 结合高效 BB84 协议的差分密钥分发系统[J]. 光子学报，2008，**37**(5)：1052-1056.

[4] LIU Dan, PEI Chang-xing, QUAN Dong-xiao, *et al*. A new quantum secure direct communication scheme with authentication[J]. *Chinese Physics Letters*, 2010, **27**(5): 050306.

[5] CHEN Zhi-xin, TANG Zhi-lie, LIAO Chang-jun, *et al*. Practical security problem of six states Q KD protocol[J]. *Acta Photonica Sinica*, 2006, **35**(1): 126-129.
陈志新，唐志列，廖常俊，等. 实际量子密钥分配扩展 BB84 协议窃听下的安全性分析[J]. 光子学报，2006，**35**(1)：126-129.

[6] QUAN Dong-xiao, PEI Chang-xing, LIU Dan, *et al*. Qne-way quantum secure direct communication based on single photons [C]. 2009 Forth Internal Conference on Communications and Networking in China, Xi′ an, China, Aug. 26-28, 2009. (EI: 20095112557671).

[7] BOSTROEM K, FELBINGER T. Deterministic secure direct communication using entanglement [J]. *Physical Review Letters*, 2002, **89**(18): 187902.

[8] DENG Fu-guo, LONG Gui-lu, LIU Xiao-shu. Two-step quantum direct communication protocol using t he Einstein-Podolsky-Rosen pair block[J]. *Physical Review A*, 2003, **68**(4): 042317.

[9] DENG Fu-guo, LI Xi-han, LI Chun-yan, *et al*. Economical quantum secure direct communication network wit h single photons[J]. *Chinese Physics*, 2007, **16**(12): 355323559.

[10] GISIN N, FASEL S, KRAUS B, *et al*. Trojan-horse attacks on quantum-key-distribution systems[J]. *Physical Review A*, 2006, **73**(2): 022320.

[11] GISIN N, RIBORDY G, TITTEL W, *et al*. Quantum cryptography[J]. *Review of Modern Physics*, 2002, **74**(1): 145

[12] DENG Fu-guo, LI Xi-han, ZHOU Hong-yu, *et al*. Improving the security of multiparty quantum secret sharing against Trojan horse attack[J]. *Physical Review A*, 2005, **72**(4): 044302.

[13] 尹浩，马怀新. 军事量子通信概论[M]. 北京：军事科学出版社，2006：109-110.

Damage Model of Quantum Signaling of Multi-user Based on Malicious Attack and Repair Strategy

LI Chao, NIE Min

(*School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an* 710061, *China*)

Abstract: A quantum signaling tree transmission system of multi-user is presented, and the transmission process of signaling is described. The damage model of Trojan horse attack to signaling in the transmission process and the repair necessity are studied. The idea of quantum key distribution is introduced to the safety of quantum signaling in direct communication, and non-orthogonal quantum states are analyzed to overcome the problem of Trojan horse attack that will improve the safety of the signal transmission. Quantum signaling tree transmission system of multi-user is improved, and a new general transmission model of multi-user quantum signaling tree topology is presented. The result shows that repair strategy of multi-user quantum signaling transmission system being attacked can effective detect the Trojan horse attack, and increases distance of security transmission, to ensure the signaling transmission process safely and effectively.

Key words: Multi-user quantum signaling; Signaling transfer; Tree topology; Trojan horse attack