光子学报 2012, 41(10) 1256-1260 DOI: 10.3788/gzxb20124110.1256 ISSN: 1004-4213 CN: 61-1235/O4

论文

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

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.

Keywords: Multi-user quantum signaling Signaling transfer Tree topology Trojan horse attack

收稿日期 2012-05-31 修回日期 2012-07-18 网络版发布日期

DOI: 10.3788/gzxb20124110.1256

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

通讯作者: 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

作者简介:

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,路轶群,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. 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.

本刊中的类似文章

1. 李超, 聂敏, 刘晓慧.基于恶意攻击的多用户量子信令损伤模型及 诱骗态修复策略[J]. 光子学报, 2012,41(3): 339-342

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人		邮箱地址	
反馈标题		验证码	1501