

基于蛛网结构的量子卫星广域网构建策略及性能仿真

聂敏 韩凯捷 杨光 张美玲 孙爱晶 裴昌幸

Construction strategy and performance simulation of quantum satellite wide area network based on cobweb structure

Nie Min Han Kai-Jie Yang Guang Zhang Mei-Ling Sun Ai-Jing Pei Chang-Xing

引用信息 Citation: *Acta Physica Sinica*, 70, 140303 (2021) DOI: 10.7498/aps.70.20210556

在线阅读 View online: <https://doi.org/10.7498/aps.70.20210556>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

您可能感兴趣的其他文章

Articles you may be interested in

基于量子隐形传态的量子保密通信方案

Quantum communication scheme based on quantum teleportation

物理学报. 2017, 66(23): 230303 <https://doi.org/10.7498/aps.66.230303>

基于部分测量增强量子隐形传态过程的量子Fisher信息

Enhancement of quantum Fisher information of quantum teleportation by optimizing partial measurements

物理学报. 2018, 67(14): 140304 <https://doi.org/10.7498/aps.67.20180330>

中纬度地区电离层偶发E层对量子卫星通信性能的影响

Influence of the ionospheric sporadic E layer on the performance of quantum satellite communication in the mid latitude region

物理学报. 2017, 66(7): 070302 <https://doi.org/10.7498/aps.66.070302>

基于量子算法的量子态层析新方案

A novel scheme of quantum state tomography based on quantum algorithms

物理学报. 2019, 68(14): 140301 <https://doi.org/10.7498/aps.68.20190157>

基于袋鼠纠缠跳跃模型的量子状态自适应跳变通信策略

An adaptive quantum state-hopping communication strategy based on kangaroo entanglement hopping model

物理学报. 2019, 68(11): 110301 <https://doi.org/10.7498/aps.68.20190163>

基于量子游走的仲裁量子签名方案

Arbitrated quantum signature scheme based on quantum walks

物理学报. 2019, 68(12): 120302 <https://doi.org/10.7498/aps.68.20190274>

基于蛛网结构的量子卫星广域网 构建策略及性能仿真*

聂敏¹⁾ 韩凯捷^{1)†} 杨光¹⁾²⁾ 张美玲¹⁾ 孙爱晶¹⁾ 裴昌幸³⁾

1) (西安邮电大学通信与信息工程学院, 西安 710121)

2) (西北工业大学电子信息工程学院, 西安 710072)

3) (西安电子科技大学, 综合业务网国家重点实验室, 西安 710071)

(2021年3月24日收到; 2021年4月26日收到修改稿)

量子卫星通信是通信领域的研究热点和前沿, 具有理想的信息安全性和覆盖面广的优势, 对于构建全球范围的量子卫星广域网具有重要意义, 而远距离传输信息时网络的可靠性、安全性和路由中继等问题仍需改进. 为了构建性能良好的量子卫星广域网, 本文提出利用蜘蛛网作为一种独特的自然通信拓扑结构, 将自然界蛛网演进为人工蛛网拓扑, 量子信息的传输采用 N 阶量子隐形传态路由方案, 其传输时延基本不变, 在此基础上构建蛛网网络拓扑量子广域网传输模型, 并对构建的网络模型的误码率、吞吐率、安全密钥生成率进行仿真分析. 用抗毁度作为衡量网络拓扑结构可靠性的指标, 以 9 节点环型网和 9 节点蛛网为例进行定量和定性分析, 得出蛛网拓扑具有更高的可靠性. 当噪声的平均功率谱密度给定且不存在中继时, 量子态的传输距离越大误码率越大, 这时要考虑引入中继; 当传输距离和噪声功率谱密度一定的情况下, 误码率随着中继节点个数的增多而减小, 因此在蛛网拓扑下要选择合适的路由过程. 随着量子卫星分发纠缠光子对成功概率的增大, 吞吐率逐渐增加; 随着网络中传输时延的增大, 吞吐率逐渐减小, 但在该路由方案下传输时延基本不变, 且蛛网结构的传输时延很小, 因此本文中提出的基于 N 阶量子隐形传态的蛛网网络拓扑量子广域网的吞吐率不会有明显的降低. 当量子信息的传输距离不断增大时, 网络密钥生成率逐渐减小; 随着网络中继节点个数的增多, 密钥生成率逐渐增加. 由此可见, 利用蛛网拓扑以及 N 阶量子隐形传态路由方案构建量子卫星广域网具有很好的优势.

关键词: 蜘蛛网拓扑, N 阶量子隐形传态路由方案, 量子卫星广域网

PACS: 03.67.Hk, 03.67.-a

DOI: 10.7498/aps.70.20210556

1 引言

发展量子卫星通信是我国重点战略发展计划, 其发展的最终目标是构建全球广域量子通信网络体系^[1]. 量子密钥分发 (quantum key distribution, QKD) 以其无条件安全性引起了学者的广泛关注^[2], 1984 年 Bennett 和 Brassard 提出了第一个

无条件安全传输的 BB84 协议, 1992 年 Bennett 在此前研究的基础上又提出了 B92 协议. 但在实际 QKD 实现过程中会存在很多安全漏洞, 2012 年 Lo 等^[3] 首次提出测量设备无关量子密钥分配 (measurement-device-independent quantum key distribution, MDI-QKD) 协议, MDI-QKD 的提出不仅保证 QKD 协议理论上的安全性, 也消除了窃听者的攻击, 且使通信距离扩大. 随着该协议理论

* 国家自然科学基金 (批准号: 61971348, 61201194)、陕西省国际科技合作与交流计划项目 (批准号: 2015KW-013) 和陕西省自然科学基金基础研究计划 (批准号: 2021JM-464) 资助的课题.

† 通信作者. E-mail: 3191696125@qq.com

基础的不断完善, 近几年该领域的实验得到了快速的发展, 2020年潘建伟等^[4]提出了远距离自由空间 MDI-QKD 方案, 实现了在 19.2 km 的城市大气通道上的第一个自由空间 MDI-QKD, 这项实验标志着我国向着基于卫星的 MDI-QKD 迈出了第一步. 同年 Yin 等^[5]实现了基于纠缠的无中继千公里量子保密通信, 这些研究进一步表明通过量子卫星构建全球量子通信网络的方案是可行的.

2016年8月, 我国成功发射了世界第一颗量子科学实验卫星“墨子号”^[6]; 2017年9月, 总长 2000 多公里的“京沪干线”量子保密通信网络正式开通, 同时“京沪干线”与“墨子号”成功对接, 首次实现了洲际量子保密通信^[7]; 2011年, 周小清等^[8]研究了量子隐形传态网络的互联与路由策略. 2012年, 连涛和聂敏^[9]通过分析环境噪声对量子信令远距离传输的影响, 提出了基于纠缠交换的量子信令中继策略. 2013年, 刘晓慧等^[10]提出了传输时延小的多阶量子隐形传态量子路由方案, 并分析了其路由策略. 2021年聂敏等^[11]根据球形蒲公英量子卫星网络的结构特性, 提出了一种两端纠缠交换的量子路由方案. 2021年1月陈宇翱等^[12]提出了约 4600 km 的天地一体化量子通信网络.

通信网络的传输能力主要与网络的拓扑结构和路由策略有关, 自然界中的蛛网结构相比于其他结构(树型、星型、环型等)可靠性高、可扩展性好、传输时延小, 迄今为止国内外有关基于蛛网网络拓扑的量子卫星广域网构建策略研究尚未完全展开. 受自然界蛛网的启发, 本文对其进行标准化处理, 在此基础上分析蛛网结构和量子卫星通信网络之间的相似性, 构建量子卫星广域网, 进一步分析基于 N 阶量子隐形传态的量子卫星广域网的误码率、吞吐率以及安全性问题, 通过仿真研究, 为构建性能良好的量子卫星广域网奠定基础.

2 蜘蛛网网络拓扑

2.1 蛛网结构及其捕食策略

蛛网结构中圆网是最具代表性的, 且在圆网结构的基础上可以继续进化为别的类型的网^[13]. 自然界中的圆形蜘蛛网如图 1 所示, 结构图如图 2, 其呈现椭圆形并具有一定的对称性, 由捕丝、拖丝、旋转螺旋丝组成, 拖丝按功能又可以划分为框架丝、锚定丝、径向丝. 捕丝具有一定的黏性, 可将

猎物粘住; 径向丝支撑整个网结构的稳定^[14], 且具有很强的延展性, 可以通过径向丝的振动为蜘蛛提示猎物的位置.

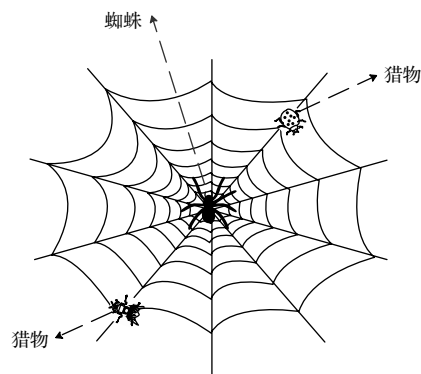


图 1 自然界圆形蜘蛛网

Fig. 1. Round spider web in nature.

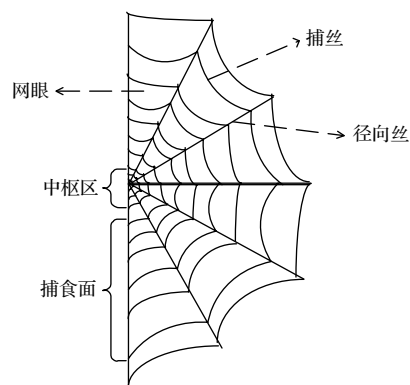


图 2 蛛网结构图

Fig. 2. Cobweb structure diagram.

蜘蛛一般停留在中心区域, 当猎物撞击蛛网时黏性的捕丝会粘住猎物. 因蜘蛛的视觉能力很差, 蜘蛛捕食主要依靠丝线的振动来判断猎物的位置, 振动信号沿径向衰减率是沿周向衰减率的 $1/6$ ^[15], 因此传递蛛网内的振动信息主要是沿着径向丝快速传递到中心区域, 蜘蛛沿着径向丝抵达猎物身边.

2.2 人工蛛网演进过程

人工蛛网演进过程如图 3 所示. 蛛网是由星型、环型拓扑演进而来, 其中星型结构简单且容易管理; 环型拓扑的信息传输误码率很低, 但可靠性差. 蛛网网络拓扑 (spider network topology, SNT) 除结合这两种拓扑结构的优点之外, 还有很强的抗毁能力, 当通信链路发生故障断开或者出现拥塞时, 由于网络中任意一个节点到另外一个节点的路

径不止一条,可以选择其他路径实现链路之间的连接,使得信息有效传输.

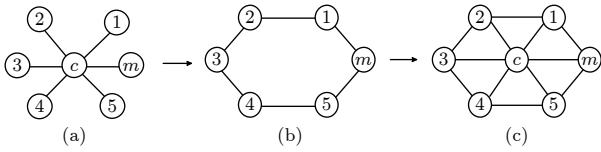


图3 人工蛛网演进过程 (a) 星型; (b) 环型; (c) 蛛网
Fig. 3. Evolution of artificial cobweb: (a) Star; (b) ring; (c) spiderweb.

2.3 SNT 与环型拓扑的性能分析

1) 可靠性定量分析

网络抗毁性考虑的是网络拓扑在节点或边失效后继续维持功能的能力,点(边)连通度是最早被用来刻画网络抗毁性的测度指标.因此本文网络抗毁度从网络拓扑结构的角度出发,分析网络发生故障前网络保持连通的能力,根据链路连通性分析网络可靠性.以9节点环型网络和9节点SNT为例进行定量分析,验证蛛网结构的高可靠性.抗毁度的计算过程如下,首先计算完整的网络拓扑的连通度,然后算出每个节点的重要度,删除掉重要度最大的节点以及节点相连接的链路,查看网络中是否有节点连接,重复上述过程直到网络中没有节点相连,从而计算出网络的抗毁度.

假设网络拓扑 H 有 g 个节点,删除其中的 c 个节点后,网络拓扑可以表示为 $H(c)$,最终删除 m 个节点可以使得网络中的所有节点均为孤立节点,根据参考文献 [16,17] 可知,网络抗毁度定义为

$$W(H) = \sum_{c=0}^{m-1} E(c), \quad (1)$$

其中 $E(c)$ 表示删掉 c 个节点之后网络的连通度,表达式为:

$$E(c) = \sum_{a=1}^{g-c-1} \sum_{b=a+1}^{g-c} e_c(a, b), \quad (2)$$

式中 $e_c(a, b)$ 表示删掉 c 个节点之后节点 a 和节点 b 之间的连通度,可表示为:

$$e_c(a, b) = \sum_{d=1}^p \frac{1}{J(d)}, \quad (3)$$

p 为节点 a 到达节点 b 之间的路径条数,且均为互不相交的路径; $J(d)$ 为节点 a 到节点 b 之间的第 d 条路径所需要经过的链路个数.

由上述的分析过程,计算得到9节点环型网的抗毁度为

$$W(H_1) = E(0) + E(1) + E(2) + E(3) + E(4) = 49.53, \quad (4)$$

9节点SNT的抗毁度为

$$W(H_2) = E(0) + E(1) + E(2) + E(3) + E(4) = 90.13. \quad (5)$$

因此蜘蛛网络拓扑结构相比环型网络拓扑结构具有更高的可靠性.

2) 可靠性定性分析

参考文献 [18], 假设链路失效的概率为 r , 链路有效的概率为 s , 网络的全端可靠性为 $K(H, S)$, H 代表网络的拓扑结构, $H - q$ 是网络 H 中除去 q 后获得的网络, H/q 是网络中将 q 所连接的两个节点进行合并后得到的网络.只分析因链路失效而导致的不可靠性,因子定理为

$$K(H, s) = sK(H/q) + rK(H - q), \quad (6)$$

通过分解环型拓扑,可以得到环型拓扑的可靠性为

$$K(H_1, s) = 6s^5 - 5s^6, \quad (7)$$

单层人工蛛网网络拓扑结构经过分解,最终可得到其可靠性为

$$K(H_2, s) = 292s^6 - 1246s^7 + 2272s^8 - 2256s^9 + 1282s^{10} - 394s^{11} + 51s^{12}. \quad (8)$$

仿真实验结果如图4所示,横轴为链路有效率 s ,纵轴为可靠性 K .当链路有效率为0.7时,环型拓扑的可靠性为0.42,蛛网拓扑的可靠性为0.81.因此蛛网结构在可靠性方面更具优势,随着节点个数的增多,网络中任意两个节点之间的通信路径不止一条,网络全端可靠性增加.

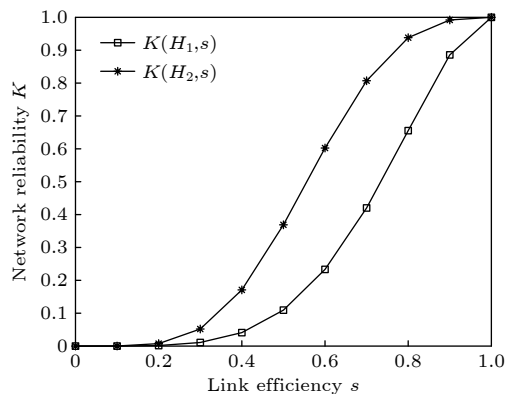


图4 环型与蛛网拓扑的网络可靠性分析

Fig. 4. Network reliability analysis of ring and cobweb topologies.

3 基于 N 阶量子隐形传态路由方案

实现量子通信的关键是量子态远程传送和量子路由, 不同用户之间需要共享量子纠缠^[19,20]. 在进行远距离节点的量子态传输时, 主要存在以下两个问题: 一是量子终端的存储容量有限, 当网络中有很多中继节点时, 其中一个量子设备不可能存储所有可能与之通信的量子设备的纠缠光子对; 二是自由空间中充满了各种环境噪声, 进行远距离的 EPR 光子对的分发是不可能的. 而 N 阶量子隐形传态路由方案是不受这两个问题的限制, 可将量子信息从源节点 Alice 传输到另外一个远距离且不与之共享 EPR 纠缠光子对的目的节点 Bob 处, 需在各个中间节点处进行量子测量和量子门操作, 通过中间节点完成量子态的传输^[10]. 该路由方案原理如图 5 所示

3.1 二阶量子隐形传态

以二阶量子隐形传态过程为例进行分析, 假设 Alice 为源节点, Bob 为目的节点, David 为中间交换节点, 逻辑线路图如图 6 所示.

首先给 Alice 和 David 分发 EPR 纠缠光子对, 给 David 和 Bob 分发 EPR 纠缠光子对, 纠缠态分别表示为

$$|\varphi^+\rangle_{A_2D_1} = \frac{1}{\sqrt{2}} (|0\rangle_{A_2}|0\rangle_{D_1} + |1\rangle_{A_2}|1\rangle_{D_1}), \quad (9)$$

$$|\varphi^+\rangle_{D_2B} = \frac{1}{\sqrt{2}} (|0\rangle_{D_2}|0\rangle_B + |1\rangle_{D_2}|1\rangle_B), \quad (10)$$

所以在开始进行信息传输时, 总的五量子比特系统可以表示为

$$\begin{aligned} |I\rangle \otimes |\varphi\rangle_{A_2D_1D_2B} &= \frac{1}{2} |I\rangle \otimes (|0\rangle_{A_2}|0\rangle_{D_1} + |1\rangle_{A_2}|1\rangle_{D_1}) \otimes (|0\rangle_{D_2}|0\rangle_B + |1\rangle_{D_2}|1\rangle_B) \\ &= \frac{1}{2} (\alpha|0\rangle + \beta|1\rangle)_{A_1} \otimes (|0\rangle_{A_2}|0\rangle_{D_1} + |1\rangle_{A_2}|1\rangle_{D_1}) \otimes (|0\rangle_{D_2}|0\rangle_B + |1\rangle_{D_2}|1\rangle_B); \end{aligned} \quad (11)$$

接着 Alice 和 David 对他们的两个量子比特进行量子门 CNOT 操作, 得到如下结果:

$$\begin{aligned} &\frac{1}{2} [\alpha|0\rangle_{A_1} \otimes |0\rangle_{A_2}|0\rangle_{D_1} \otimes (|0\rangle_{D_2}|0\rangle_B + |1\rangle_{D_2}|1\rangle_B) \\ &+ \alpha|0\rangle_{A_1} \otimes |1\rangle_{A_2}|1\rangle_{D_1} \otimes (|1\rangle_{D_2}|0\rangle_B + |0\rangle_{D_2}|1\rangle_B) \\ &+ \beta|1\rangle_{A_1} \otimes |1\rangle_{A_2}|0\rangle_{D_1} \otimes (|0\rangle_{D_2}|0\rangle_B + |1\rangle_{D_2}|1\rangle_B) \\ &+ \beta|1\rangle_{A_1} \otimes |0\rangle_{A_2}|1\rangle_{D_1} \otimes (|1\rangle_{D_2}|0\rangle_B + |0\rangle_{D_2}|1\rangle_B)]; \end{aligned} \quad (12)$$

然后 Alice 和 David 分别对他们的第一个量子比特进行哈德曼门操作, 得到如下结果:

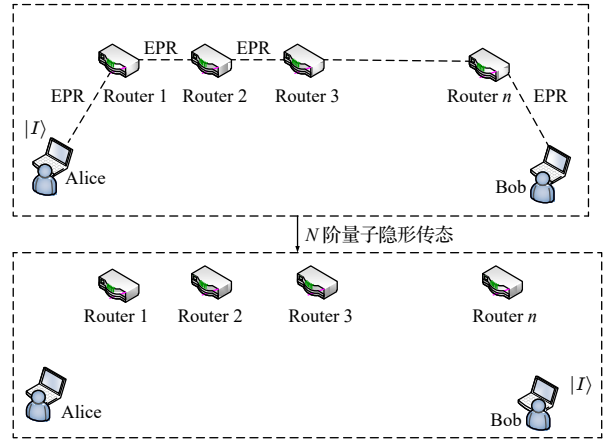


图 5 基于 N 阶量子隐形传态的量子路由方案

Fig. 5. Quantum routing scheme based on N -order quantum teleportation.

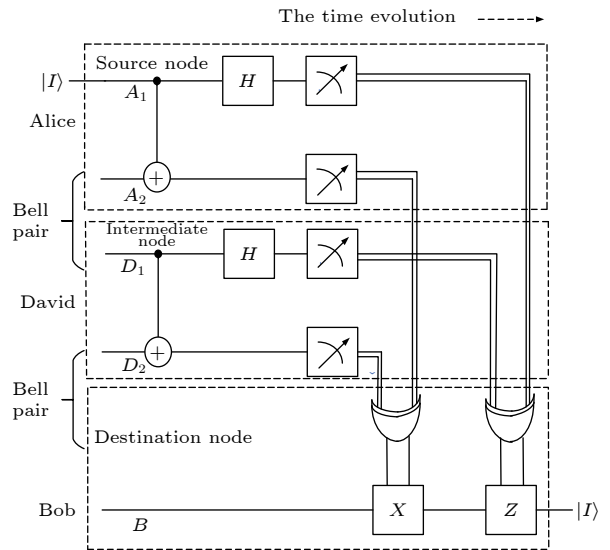


图 6 二阶量子隐形传态逻辑线路图

Fig. 6. Second-order quantum teleportation logic circuit diagram.

$$\begin{aligned} & \frac{1}{4} [(|0\rangle_{A_1}|0\rangle_{D_1} + |1\rangle_{A_1}|1\rangle_{D_1}) \otimes (|0\rangle_{A_2}|0\rangle_{D_2} + |1\rangle_{A_2}|1\rangle_{D_2}) \otimes (\alpha|0\rangle + \beta|1\rangle)_B \\ & + (|0\rangle_{A_1}|0\rangle_{D_1} + |1\rangle_{A_1}|1\rangle_{D_1}) \otimes (|0\rangle_{A_2}|1\rangle_{D_2} + |1\rangle_{A_2}|0\rangle_{D_2}) \otimes (\alpha|1\rangle + \beta|0\rangle)_B \\ & + (|0\rangle_{A_1}|1\rangle_{D_1} + |1\rangle_{A_1}|0\rangle_{D_1}) \otimes (|0\rangle_{A_2}|0\rangle_{D_2} + |1\rangle_{A_2}|1\rangle_{D_2}) \otimes (\alpha|0\rangle - \beta|1\rangle)_B \\ & + (|0\rangle_{A_1}|1\rangle_{D_1} + |1\rangle_{A_1}|0\rangle_{D_1}) \otimes (|0\rangle_{A_2}|1\rangle_{D_2} + |1\rangle_{A_2}|0\rangle_{D_2}) \otimes (\alpha|1\rangle - \beta|0\rangle)_B]. \end{aligned} \quad (13)$$

由上述计算结果可以看出, 只要 Bob 获得了 Alice 和 David 的两个量子比特的状态信息, 就可以知道自己的状态信息. 例如 Bob 已知 Alice 的两个量子比特分别为 $|0\rangle_{A_1}|0\rangle_{A_2}$, David 的两个量子比特分别为 $|0\rangle_{D_1}|1\rangle_{D_2}$, 那么 Bob 的量子比特一定是 $\alpha|1\rangle + \beta|0\rangle$. Bob 得知自己的状态信息后, 就可以对其进行相应的量子门操作恢复出 Alice 传输给它的信息 $|I\rangle = \alpha|0\rangle + \beta|1\rangle$. Bob 需要进行的量子门操作如表 1 所列.

表 1 已知测量结果后的量子门操作
Table 1. Quantum gate operation after known measurement results.

A_1 异或 D_1	A_2 异或 D_2	量子门操作
0	0	无
0	1	X门
1	0	Z门
1	1	X门和Z门

3.2 三阶量子隐形传态

在分析二阶量子隐形传态的基础上, 讨论三阶量子隐形传态的具体过程, 其需要借助两个中间节点完成量子态传送. 源节点为 Alice, 目的节点为 Bob, 中间节点分别为 David 和 Gina, 逻辑线路图如图 7 所示.

与二阶量子隐形传态过程类似, 在开始进行传输时总的七量子比特系统可以表示为

$$\begin{aligned} & |I\rangle \otimes |\varphi\rangle_{A_2 D_1 D_2 G_1 G_2 B} \\ & = \frac{1}{2} |I\rangle \otimes (|0\rangle_{A_2}|0\rangle_{D_1} + |1\rangle_{A_2}|1\rangle_{D_1}) \\ & \quad \otimes (|0\rangle_{D_2}|0\rangle_{G_1} + |1\rangle_{D_2}|1\rangle_{G_1}) \\ & \quad \otimes (|0\rangle_{G_2}|0\rangle_B + |1\rangle_{G_2}|1\rangle_B) \\ & = \frac{1}{2} (\alpha|0\rangle + \beta|1\rangle)_{A_1} \\ & \quad \otimes (|0\rangle_{A_2}|0\rangle_{D_1} + |1\rangle_{A_2}|1\rangle_{D_1}) \\ & \quad \otimes (|0\rangle_{D_2}|0\rangle_{G_1} + |1\rangle_{D_2}|1\rangle_{G_1}) \\ & \quad \otimes (|0\rangle_{G_2}|0\rangle_B + |1\rangle_{G_2}|1\rangle_B), \end{aligned} \quad (14)$$

接着采用与二阶过程同样的操作, Alice, David 和 Gina 对他们的两个量子比特进行量子门 CNOT 操作, 然后 Alice, David 和 Gina 分别对他们的第一个量子比特进行哈德曼门操作. Bob 已知测量结果以后需要进行量子门操作, 如表 2 所列.

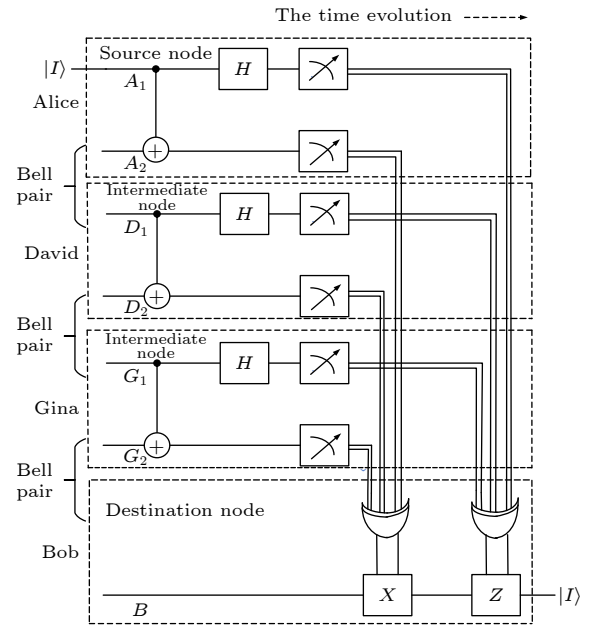


图 7 三阶量子隐形传态逻辑线路图

Fig. 7. Third-order quantum teleportation logic circuit diagram.

表 2 已知测量结果后的量子门操作
Table 2. Quantum gate operation after known measurement results.

A_1 异或 D_1 异或 G_1	A_2 异或 D_2 异或 G_2	量子门操作
0	0	无
0	1	X门
1	0	Z门
1	1	X门和Z门

综上所述, 随着网络规模的不断扩大, 就需要使用一个或者一个以上的中继节点完成远距离量子态传送, 即 N 阶量子隐形传态过程. 由二阶以及三阶量子隐形传态逻辑线路图可知, 各个节点的量子门操作和量子测量是同步完成的, 完成多个节点路由时间与量子隐形传态时间相同.

3.3 量子路由方案仿真分析

已有的路由方案很多,常用的包括量子中继路由方案、量子纠缠交换路由方案等.参考文献 [10], 设采用量子中继路由方案时,传输时间 T 为

$$T = (n + 1)T_1, \quad (15)$$

其中 T_1 表示在量子信息的传输过程中完成量子隐形传态的时间, n 是路由过程使用的中继节点数目.

采用量子纠缠交换路由方案时,传输一个量子态所需要的时间 T' 为

$$T' = T_1 + nT_2, \quad (16)$$

其中 T_2 表示量子纠缠交换时间.

采用 N 阶量子隐形传态路由方案时,传输一个量子态所需要的时间 T'' 为

$$T'' = w + h + T_1, \quad (17)$$

其中 w 为在广域网的位置数据库中查找用户具体位置所需的时间, h 为量子卫星分发纠缠光子对的时间. 假设 $T_1 = 0.8 \mu\text{s}$, $T_2 = 0.7 \mu\text{s}$, $w = 0.01T_1$, $h = 0.01T_1$.

仿真结果如图 8 所示, 当 $n = 4$ 时, $T = 4 \mu\text{s}$, $T' = 3.6 \mu\text{s}$, $T'' = 0.82 \mu\text{s}$; 当 $n = 10$ 时, $T = 8.8 \mu\text{s}$, $T' = 7.8 \mu\text{s}$, $T'' = 0.82 \mu\text{s}$. 由此可见, 随着中继节点个数的增多, 前两种路由方案传输时延有明显的增大, 而 N 阶量子隐形传态路由方案传输一个量子态的时间基本保持不变, 传输时延小.

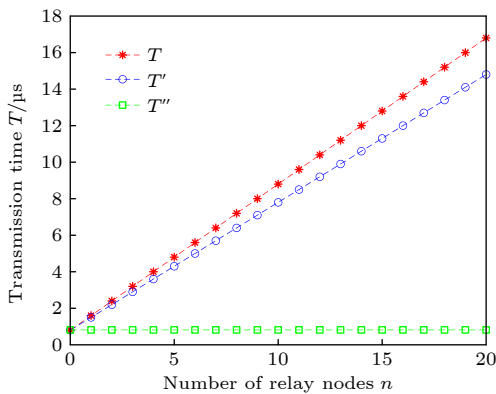


图 8 三种路由方案量子态传输时间与中继节点个数的关系

Fig. 8. Relationship between the quantum state transfer time and the number of relay nodes.

4 基于 SNT 的量子卫星广域网网络模型

自然界中的蛛网结构与量子卫星通信网络有

很多的相似性.

1) 蜘蛛捕食猎物的大小决定所构建蛛网的大小, 说明蛛网具有很强的可扩展性, 因此要实现可靠性高的量子卫星广域网, 就要采用蛛网网络拓扑结构, 一个网络的通信总需求决定了它的通信容量、大小和性能要求.

2) 蛛网中的每个节点代表网络中的一台路由器, 量子信息通过路由器进行传输. 蛛丝的强度代表着通信网络数据流的大小, 捕丝的延展性代表了它们适应通信流的能力.

3) 在捕食过程中如果蛛网出现断裂, 蜘蛛不会立即去修复破损的网, 而是利用其继续捕食, 说明蛛网具有很强的抗毁性, 它将在夜晚根据环境变化以及捕食经验构建新的网. 根据以上几点的相似性, 以 7 节点 SNT 为例, 将其拉伸为立体结构来构建量子卫星广域网, 其立体蛛网结构图如图 9 所示.

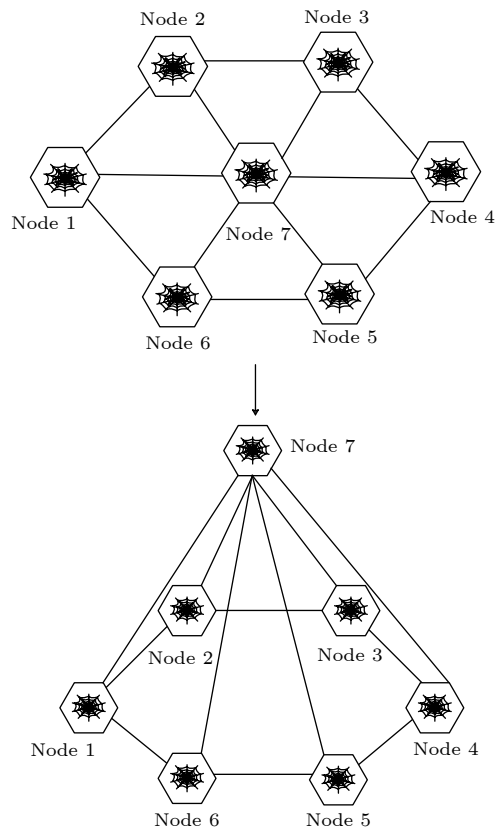


图 9 六边形逻辑蛛网拓扑模型

Fig. 9. Hexagonal logic spider web topology model.

图 10 是 SNT 量子卫星广域网模型, 量子卫星广域网由量子卫星 (quantum satellite)、量子无线基站 (router)、量子全局位置数据库 (QGPW)、量子局部位置数据库 (QLPW) 以及地面通信用户组

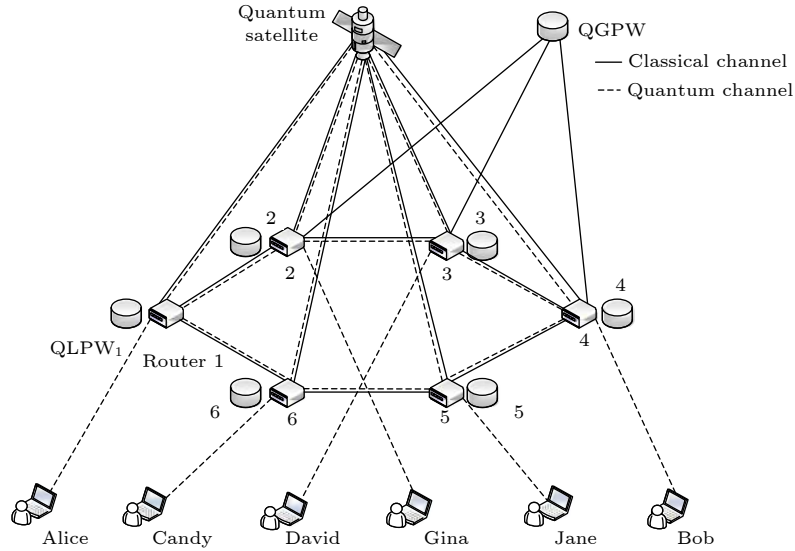


图 10 基于蛛网拓扑的量子卫星广域网

Fig. 10. Quantum satellite wide area network based on cobweb topology.

成. 蛛网的中间节点作为 quantum satellite, 其余蛛网节点为各个不同的基站, 作为中继转发, 每个基站都配有一个 QLPW, 用来查找各个用户的具体位置. 量子卫星的主要任务是生成纠缠光子对, 并将其发送给各个基站, 建立卫星与各个基站之间的量子信道, 实现量子信息的传输.

假设源节点 Alice 要给目的节点 Bob 发送信息, 初始 Alice 先给 Router1 发送一个请求, 即将量子信息发送给 Bob, 然后 Router1 通过 QGPW 查询自己的位置信息, 识别 Bob 在哪个基站下面, QGPW 的优点在于可以找到符合网络的最短路径路由, 使信息高效传输. 由图 10 可知网络中只有一个量子卫星, 通过 QGPW 可以查询到 Alice 和 Bob 在同一颗卫星下, 此时 QGPW 会通知 Router1 的目的用户 Bob 的具体位置, 同时在通信的过程中, Router1 请求 quantum satellite 发送纠缠光子对给相应的基站, 建立起卫星与基站之间的量子信道, 利用 N 阶量子隐形传态路由方案有效传送 Alice 所要传送给 Bob 的信息.

5 基于 N 阶量子隐形传态的量子卫星广域网性能仿真

5.1 量子信息传输误码率分析

由于存在环境噪声、人为干扰等因素会导致通

信链路失效, 使纠缠粒子的状态发生变化, 从而产生错误的传输. 设量子信息传输误码率为 P_T ^[9], 公式为

$$P_T = \left[\frac{[L/(n+1)]^2 \lambda^2 \sigma^2}{f_T^2 f_R^2 F_T F_R (1 - L_p)} \right], \quad (18)$$

式中 σ^2 是噪声平均功率谱密度, 其余各参量的含义如表 3 所列.

为了减小大气环境对传输链路产生的衰减效应, 应该选择合适的光波长, 根据文献 [21], 应选择透射率较高的大气窗口, 因此本文取 $\lambda = 1550 \text{ nm}$ 进行分析. 其余参数设置为 $n = 0$, $f_T = f_R = 32 \text{ mm}$, $F_T = F_R = 1$, $L_p = 5\%$, 噪声的平均功率谱密度分别为 1, 2 和 3 dB/km.

首先分析在无中继节点的情况下, 误码率 P_T 与传输距离 L 之间的关系. 仿真结果如图 11 所示.

当 σ^2 一定时, 星地之间传输距离越大, 误码率越大. 在 $\sigma^2 = 1 \text{ dB/km}$ 条件下, 当传输距离为 2000 km 时, 误码率为 0.049; 当传输距离为 4000 km 时, 误码率达到 0.197. 在量子信息在星地之间的传输距离一定的条件下, σ^2 越大, 误码率也越大, 当传输距离为 3000 km, $\sigma^2 = 1 \text{ dB/km}$ 时误码率为 0.111; $\sigma^2 = 3 \text{ dB/km}$ 时误码率达到 0.332. 因此在没有中继的情况下, 传输更远距离时误码率增大, 就需要考虑引入中继.

表 3 量子信息传输误码率各参量含义

Table 3. Meaning of parameters of bit error rate in quantum information transmission.

L	n	λ	f_T	f_R	F_T	F_R	L_p
星地间传输距离	中继节点个数	光子波长	发送端望远镜孔径	接收端望远镜孔径	发端望远镜传输因子	收端望远镜传输因子	链路损耗

当星地之间的传输距离 L 为 4000 km 时, 分析功率谱密度 σ^2 、中继节点个数 n 与误码率 P_r 的关系, 仿真结果如图 12 所示, 误码率的其余参量取值同图 11.

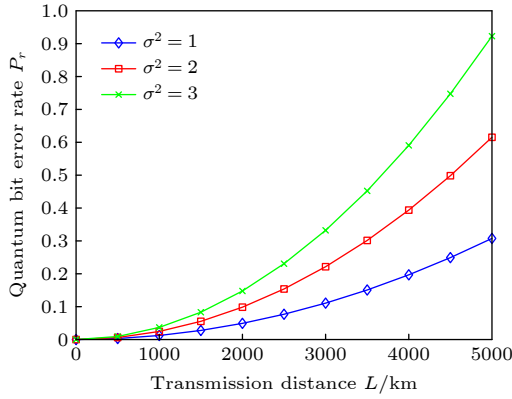


图 11 误码率与传输距离的关系

Fig. 11. Relationship between BER and transmission distance.

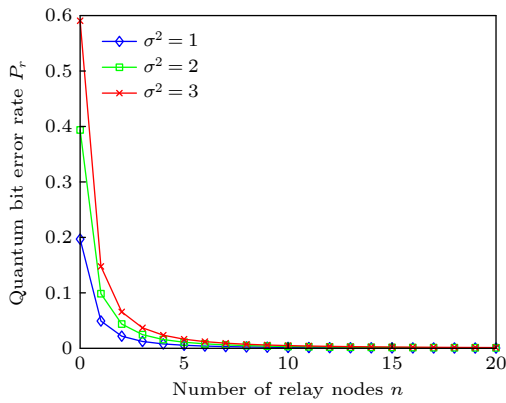


图 12 误码率与中继节点个数的关系

Fig. 12. Relationship between bit error rate and the number of relay nodes.

当 σ^2 一定时, 误码率随着 n 的增大而减小, 当中继节点数取为 6 或者更大时, 误码率几乎保持不变, 因此在量子卫星广域网中进行信息传输时要选择合适的路由过程, 使得信息有效传输.

5.2 量子广域网吞吐率分析

基于 N 阶量子隐形传态的量子卫星广域网中, 设成功分发纠缠光子对的概率为 P_1 、在 QGPW 中成功查找位置信息的概率为 P_2 、成功进行量子门操作的概率为 P_3 、接收端成功接收量子信息的概率为 P_4 . 那么成功将一个量子态信息传输至目的节点的概率为

$$P = P_1 \times P_2 \times P_3 \times P_4. \quad (19)$$

在 N 阶量子隐形传态的过程中, 生成纠缠粒子对的时间为 h 、在位置数据库中查找信息的时间为 w 、进行量子门操作的时间为 j 、在中继节点处的传输时延为 T'' . 而在 N 阶量子隐形传态的过程中, 传输一个量子态的时间不会随着中继节点个数的增多而增大, T_1 是量子隐形传态的平均时间, 所以

$$T'' = w + h + T_1. \quad (20)$$

因此成功传输一个量子态所需要的时间为

$$T_t = w + h + j + T''. \quad (21)$$

则在量子卫星广域网中传输量子信息时网络吞吐率可以定义为

$$Q = \frac{P}{T_t} = \frac{P_1^n \times P_2 \times P_3 \times P_4}{w + h + j + T''}, \quad (22)$$

其中 w, h, j 的大小相比于 T'' 很小, 可以忽略不计, 所以

$$Q = \frac{P}{T_t} = \frac{P_1^n \times P_2 \times P_3 \times P_4}{T_1}. \quad (23)$$

令 $T_1 = 0.8 \mu\text{s}$, 分析吞吐率 Q 与 P_1, n 的关系. 根据文献 [22] 可知, 在理想条件下概率均设为 0.8, 所以令 P_2, P_3, P_4 均为 0.8, 仿真结果如图 13 所示.

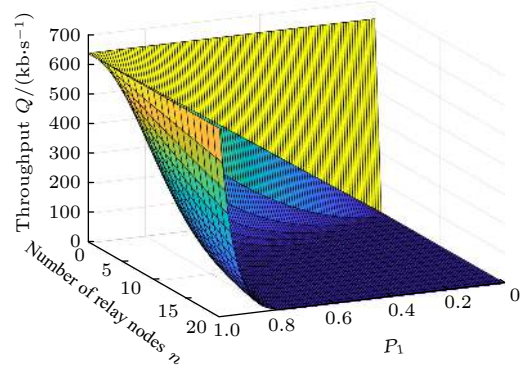


图 13 吞吐率 Q 与 P_1 以及中继节点个数 n 的关系

Fig. 13. Relationship between throughput rate Q and P_1 and the number of relay nodes n .

由仿真结果可知, 在传输时延不变的条件下, 随着 P_1 的增大, 吞吐率 Q 也在逐渐增加, 最大可以达到 640 kb/s; 随着中继节点个数 n 的增大, 吞吐率逐渐降低. 因此在蛛网拓扑结构下, 要选择合适的路由过程使得量子信息的吞吐率尽可能大.

令 $P_1 = P_2 = P_3 = P_4 = 0.8$ 时, 分析吞吐率 Q 与传输时延 T_t 的关系, 其中中继节点个数分别取 2, 4, 6, 仿真结果如图 14 所示.

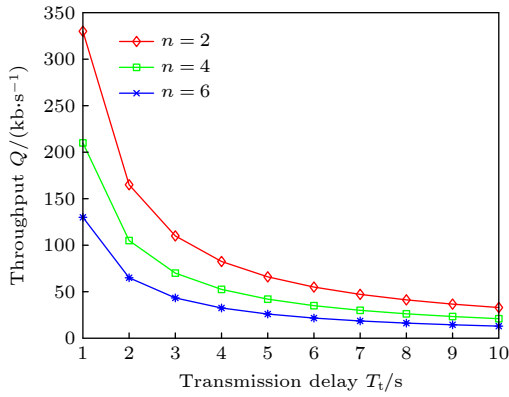


图 14 吞吐率与传输时延的关系

Fig. 14. Relationship between throughput Q and transmission delay.

随着网络中传输时延的增大, 吞吐率 Q 逐渐减小. 但在 N 阶量子隐形传态路由方案下, 传输时延基本不变, 且在蛛网网络拓扑下可选路径多, 传输时延小, 因此本文提出的基于 N 阶量子隐形传态的蛛网网络拓扑量子广域网的吞吐率不会随着传输时延的增大有明显的降低.

5.3 安全密钥生成率分析

网络的安全性主要是指在一定链路条件下所能获得的最高安全密钥生成率. 在量子卫星广域网通信过程中, 进行量子信息传输时仅考虑理想的单光子源, 在单个脉冲中含 u 个光子的概率为^[23]

$$P_u = \frac{\varphi^u}{u!} \exp(-\varphi), \quad (24)$$

式中 φ 为平均光子数, 在一般的量子通信实验中, φ 取值为 0.1^[23], 来获取准单光子源. 根据诱骗态方案, 可知单光子的计数率为

$$R_1 = 10^{-\gamma L/10}, \quad (25)$$

式中 γ 为量子信道衰减系数, 通常取值为 0.2 dB/km, L 为量子信息的传输距离. 考虑单光子计数率后, 可以得到安全密钥生成率为

$$G = P_u R_1 [1 - H(P_T)] - S_\varphi H(P_T), \quad (26)$$

$$H(P_T) = -P_T \log_2 P_T - (1 - P_T) \log_2 (1 - P_T), \quad (27)$$

$$S_\varphi = 1 - \exp(-R_1 \varphi). \quad (28)$$

根据 (18) 式、(27) 式和 (28) 式可知, 影响密钥生成率的参数主要为量子信息的传输距离 L , 中

继节点个数 n , 噪声平均功率谱密度 σ^2 .

1) 在不考虑中继的情况下, 仿真分析密钥生成率与传输距离的关系, 仿真结果如图 15 所示. 当 σ^2 取 3 dB/km, 传输距离 $L = 2500$ km 时, 密钥生成率为 0.023 bit/s; 传输距离为 $L = 4000$ km, 密钥生成率减小至 0.008 bit/s, 因此当量子信息的传输距离增大时, 网络误码率增大, 从而导致安全密钥生成率逐渐减小.

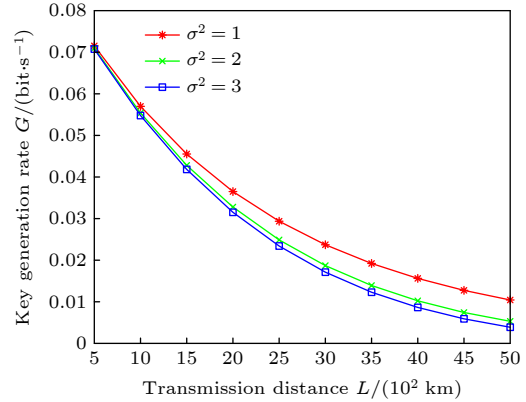


图 15 密钥生成率与传输距离的关系

Fig. 15. Relationship between key generation rate and transmission distance.

2) 由上述结果可知, 随着密钥生成率的降低要考虑引入中继. 当量子信息的传输距离为 3500 km 时, 仿真得到网络密钥生成率与 n 的关系如图 16 所示, 随着 n 的不断增大, 密钥生成率增加, 在蛛网网络拓扑结构中, 任意两个节点之间的通信路径不止一条, 迂回路由多, 可以在网络中选择合适的中继节点个数, 找到最优路径, 使得网络的密钥生成率达到最大, 网络安全性更高.

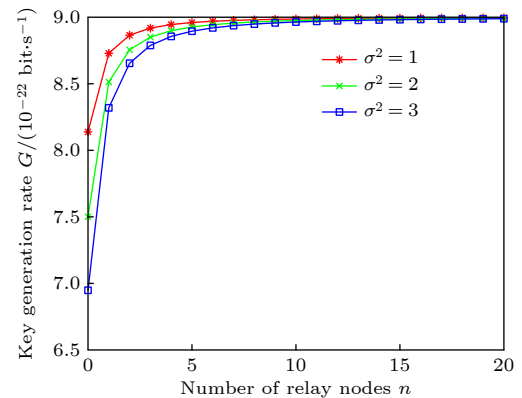


图 16 密钥生成率与中继节点个数的关系

Fig. 16. Relationship between key generation rate and number of relay nodes.

综上,对网络安全密钥生成率的仿真实验可知,本文提出的基于蛛网拓扑的量子卫星广域网中继传输模型,一定程度上改进了信息传输的安全性问题,保证了量子信息通过中继节点传输时的安全性.

6 结 论

本文利用蛛网网络拓扑构建量子卫星广域网, SNT 具有高可靠性,且 N 阶量子隐形传态路由方案的传输时延小. 增加中继节点数可以有效降低网络的误码率,增大量子卫星成功分发纠缠光子对的概率可以提升网络吞吐率,虽然吞吐率会随着传输时延的增大而减小,但在该路由方案下传输时延基本不变,且 SNT 的传输时延小,所以量子卫星广域网的吞吐率不会有明显的降低,且其在一定程度上改进了信息传输的安全性. 因此采用该路由方案以及蛛网网络拓扑构建量子卫星广域网可靠性高、误码率低、吞吐率大,这为建立全球范围的量子卫星广域网奠定了理论基础.

参考文献

- [1] Peng Z C, Pan J W 2016 *Bull. Chin. Acad. Sci.* **31** 1096 (in Chinese) [彭承志, 潘建伟 2016 中国科学院院刊 **31** 1096]
- [2] Zhu W 2016 *M. S. Thesis* (Beijing: Beijing University of Posts and Telecommunications) (in Chinese) [朱武 2016 硕士学位论文 (北京: 北京邮电大学)]
- [3] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
- [4] Cao Y, Li Y H, Yang K X, Jiang Y F, Li S L, Hu X L, Maimaiti A, Li C L, Zhang W J, Sun Q C, Liu W Y, Xiao J, Liao S K, Ren J G, Li H, You L X, Wang Z, Yin J, Lu C Y, Wang X B, Zhang Q, Peng C Z, Pan J W 2020 *Phys. Rev. Lett.* **125** 260503
- [5] Yin J, Li Y H, Liao S K, Meng Y, Cao Y, Zhang L, Ren J G, Cai W Q, Liu W Y, Li S L, Shu R, Huang Y M, Deng L, Li L, Zhang Q, Liu N L, Chen Y A, Lu C Y, Wang X B, Xu F H, Wang J Y, Peng C Z, Artur K. Ekert, Pan J W 2020 *Nature* **582** 501
- [6] Zhang Z H, Ma L Y 2018 *Forum Sci. Tech. Chin.* **34** 1 (in Chinese) [张志会, 马连轶 2018 中国科技论坛 **34** 1]
- [7] Liao S K, Cai W Q 2018 *Phys. Rev. Lett.* **120** 030501
- [8] Zhou X Q, Wu Y W, Zhao H 2011 *Acta Phys. Sin.* **60** 040304 (in Chinese) [周小清, 邬云文, 赵晗 2011 物理学报 **60** 040304]
- [9] Lian T, Nie M 2012 *Acta Photo. Sin.* **41** 1251 (in Chinese) [连涛, 聂敏 2012 光子学报 **41** 1251]
- [10] Liu X H, Nie M, Pei C X 2013 *Acta Phys. Sin.* **62** 200304 (in Chinese) [刘晓慧, 聂敏, 裴昌幸 2013 物理学报 **62** 200304]
- [11] Nie M, Guo J W, Wei R Y, Yang G, Zhang M L, Sun A J, Pei C X 2021 *Laser & Optoelect. Prog.* **57** 1 (in Chinese) [聂敏, 郭建伟, 卫容宇, 杨光, 张美玲, 孙爱晶, 裴昌幸 2021 激光与光电子学进展 **57** 1]
- [12] Chen Y A, Zhang Q, Chen T Y, Cai W Q, Liao S K, Zhang J, Chen K, Yin J, Ren J G, Chen Z, Han S L, Yu Q, Liang K, Zhou F, Yuan X, Zhao M S, Wang T Y, Jiang X, Zhang L, Liu W Y, Li Y, Shen Q, Cao Y, Lu C Y, Shu R, Wang J Y, Li L, Liu N L, Xu F H, Wang X B, Peng C Z, Pan J W 2021 *Nature* **589** 214
- [13] Zhuo C H, Jiang P, Wang C H, Guo C 2006 *Sichuan J. Zoo* **26** 898 (in Chinese) [卓春晖, 蒋平, 王昌河, 郭聪 2006 四川动物 **26** 898]
- [14] Zhuo C H 2007 *M. S. Thesis* (Chengdu: Sichuan University) (in Chinese) [卓春晖 2007 硕士学位论文 (成都: 四川大学)]
- [15] Liu X S, Zhang L, Lin J W 2010 *First International Conference on Pervasive Computing, Signal Processing and Applications* Harbin, China, September 17–19, 2010 p224
- [16] Li B 2013 *M.S. Thesis* (Xi'an: Xidian University) (in Chinese) [李彬 2013 硕士学位论文 (西安: 西安电子科技大学)]
- [17] Zhao Z F 2013 *M. S. Thesis* (Harbin: Harbin Institute of Technology) (in Chinese) [赵振峰 2013 硕士学位论文 (哈尔滨: 哈尔滨工业大学)]
- [18] Liu X S, Zhang L, Zhou Y, Lin J W, Xu D G 2012 *Proc. CSEE* **32** 142 (in Chinese) [刘晓胜, 张良, 周岩, 林建伟, 徐殿国 2012 中国电机工程学报 **32** 142]
- [19] Bouwmeester D, Pan J W, Mattle K, Manfred E, Weinfurter H, Zeilinger A 1997 *Nature* **390** 575
- [20] Chen P, Deng F G, Long G L 2006 *Chin. Phys.* **15** 2228
- [21] Zhu Q L, Shi L, Wei J H, Zhu Y, Yang R, Zhao G H 2018 *Laser & Optoelect. Prog.* **55** 41 (in Chinese) [朱秋立, 石磊, 魏家华, 朱宇, 杨汝, 赵顾颢 2018 激光与光电子学进展 **55** 41]
- [22] Zhu C H, Pei C X, Ma H X, Yu X F 2006 *J. Xidian. Univ.* **6** 839 (in Chinese) [朱畅华, 裴昌幸, 马怀新, 于晓飞 2006 西安电子科技大学学报 **6** 839]
- [23] Li T F, Yang F, Li W, Cui S M 2015 *Tele. Engin.* **55** 959 (in Chinese) [李铁飞, 杨峰, 李伟, 崔树民 2015 电讯技术 **55** 959]

Construction strategy and performance simulation of quantum satellite wide area network based on cobweb structure*

Nie Min¹⁾ Han Kai-Jie^{1)†} Yang Guang¹⁾²⁾ Zhang Mei-Ling¹⁾
Sun Ai-Jing¹⁾ Pei Chang-Xing³⁾

1) (*School of Communication and Information Engineering, Xi'an University of Posts and Telecommunication, Xi'an 710121, China*)

2) (*School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China*)

3) (*State Key Laboratory of Integrated Service Networks, Xi'an University of Electronic Science and Technology, Xi'an 710071, China*)

(Received 24 March 2021; revised manuscript received 26 April 2021)

Abstract

Quantum satellite communication is a research hotspot and frontier in the field of communication. It has the advantages of ideal information security and wide coverage, which is of great significance in constructing a global quantum satellite wide area network. However, problems such as network reliability, security and routing relay still need to be improved when transmitting information over long distances. In this paper, the spider web is used as a unique natural communication topology to transform the natural spider web into an artificial spider web topology. The quantum information transmission adopts N-order quantum teleportation routing scheme, and the transmission delay is basically unchanged. On this basis, the spider web topology quantum wide area network transmission model is constructed. The bit error rate, throughput rate and security key generation rate of the network model are simulated and analyzed. Taking 9-node ring network and 9-node cobweb for example, the quantitative analysis and qualitative analysis are both conducted in this paper. The results show that the cobweb topology has higher reliability. When the average power spectral density of the noise is given and there is no relay, the bit error rate increases with the transmission distance increasing, so the introduction of relay should be considered. When the transmission distance and noise power spectral density are constant, the bit error rate decreases with the number of relay nodes increasing, so the appropriate routing process should be selected in the spider web topology. With the increase of the probability of transmitting entangled photon pairs, the throughput rate gradually increases. With the increase of transmission delay in the network, the throughput rate Q gradually decreases. However, the transmission delay is basically unchanged in this routing scheme, and the transmission delay of cobweb structure is very small. Therefore, the throughput rate of the topology quantum WAN of cobweb network based on N-order quantum teleportation proposed in this paper will not significantly decrease. When the transmission distance of quantum information increases, the network key generation rate decreases gradually. With the increase of the number of network relay nodes, the key generation rate increases gradually. Thus, it can be seen that using cobweb topology and N-order quantum teleportation routing scheme to construct a quantum satellite WAN has good advantages.

Keywords: spider web topology, N-order quantum teleportation routing scheme, quantum satellite wide area network

PACS: 03.67.Hk, 03.67.-a

DOI: 10.7498/aps.70.20210556

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61971348, 61201194), the International Scientific and Technological Cooperation and Exchange Program in Shaanxi Province, China (Grant No. 2015KW-013), and Natural Science Basic Research Program of Shaanxi, China (Grant No. 2021JM-464).

† Corresponding author. E-mail: 3191696125@qq.com