量子簇分片传输方案

王新良,黄青改,张中卫

(河南理工大学 物理与电子信息学院,河南 焦作 454000)

摘 要:在量子通信网络中,量子路由器因自身性能的限制,使其能够存储转发的量子簇长度是有限的。由于量子城域网和广域网数据量庞大,会导致大量量子簇因长度限制问题无法转发而只能以量子分组的形式进行数据传输。为了解决上述问题,提出了一种量子簇分片传输方案,其将不能够直接被量子路由器存储转发的量子簇,通过分片将其分解为若干个长度较短的、能够直接被路由器存储转发的分片量子簇完成数据传输。仿真结果表明:在数据量庞大的城域网和广域网中,需要分片的量子簇数量多,对于提出的量子簇分片传输方案,与已有的量子簇数据传输方案相比,其能够以较少的纠缠资源和较短的传输时间完成量子分组的数据传输,具有较好的实际应用价值。

关键词:量子路由器; 量子簇; 分片; 量子纠缠

中图分类号:TN929 **文献标志码**:A **DOI**:10.3788/IRLA201847.1122004

Fragment transmission scheme of quantum cluster

Wang Xinliang, Huang Qinggai, Zhang Zhongwei

(School of Physics and Electronic Information, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: In the quantum communication network, quantum routers can store and forward quantum clusters with limited length. In the metropolitan area network(MAN) and wide area network(WAN), date volumes are very large, as a result, a large number of quantum clusters can not be stored and forwarded because of the length constraint problem and can only be transmitted in the form of quantum packets. In order to solve the above problem, a fragment transmission scheme of quantum cluster was proposed, it fragmented the quantum clusters, which were not able to be stored and forwarded by the quantum router, so that the fragmented quantum cluster could satisfy the storage and forwarding condition of routers and could be directly transmitted. The simulation results show that in the MAN and WAN, a large number of quantum clusters need to be fragmented because of the large amount of date, so compared with the existing data transmission scheme based on quantum cluster, the proposed fragment transmission scheme of quantum cluster can achieve the data transmission by consuming the short time and less quantum entanglement resources, and own the better practical value.

Key words: quantum router; quantum cluster; fragment; quantum entanglement

收稿日期:2018-06-05; **修订日期**:2018-07-13

基金项目:国家自然科学基金(61405055);河南省科技攻关计划(172102210274);
河南理工大学矿山信息化重点学科开放实验室开放基金(ky2015-18);河南理工大学博士基金(B2012-073)

作者简介:王新良(1980-),男,副教授,博士,主要从事量子通信、网络安全方面的研究。Email:junci158@163.com

0 引 言

20 世纪物理学史上最重要的成就之一是量子力学的创立，而量子通信是量子力学的基本原理和通信理论相互结合的学科。1993 年，Bennett[1]等人基于量子纠缠的原理提出了量子隐形传态方案，实现数据安全传输。1997 年 Bouwmeester[2]等人利用纠缠光子对作为量子信道第一次实现了量子隐形传态，同年 Towsend 等人[3]完成了多用户的量子通信网络实验。2003 年，Brassard 提出了一种采用波分复用技术的基于光纤的量子通信网络方案[4]，并且不会影响通信的性能。2013 年，参考文献[5]实现了距离超过 300 km 的纠缠粒子分发。2016 年，参考文献[6]提出了一种能够减少散射对入射偏振光影响的 PR 方法，对未来的水下量子保密通信具有重要的意义。2017 年，参考文献[7]提出了一种基于秘钥真随机性的、可进行篡改定位的、面向安全通信的空域水印算法来提高水印的安全性，可广泛应用于数字图像的安全传输中。以上文献针对量子通信距离的扩展、实际的应用进行了深入研究，为量子通信技术在互联网中的广泛使用提供了很好的应用基础。然而，互联网网络规模巨大，要将量子通信技术应用于互联网数据传输需要发展量子中继技术[8]实现远距离通信，量子中继技术能够为量子互联网提供底层的通信信道，但是如何在众多用户之间使用尽可能少的纠缠资源和时间开销完成数据传输，构建适合量子互联网数据传输的网络通信协议已成为当前一个重要的研究方向。

2007 年，参考文献[9]基于量子纠缠原理完成数据帧的确认，能够有效改善数据链路层停止等待协议的性能。2011 年，参考文献[10]将现行的交换机等互联设备增加纠缠粒子对发生器，在网络空闲时保持和相邻设备间的量子连结，将经典的互联网升级为量子隐形传态互联网，利用经典互联网的路由算法完成路由选择。2013 年，参考文献[11]在量子移动终端之间没有共享纠缠对的情况下，仍然可以完成量子态的无线传输，该量子路由方案可以用来构建量子无线广域网。2015 年，聂敏等[12]提出了一种基于分组交换的量子通信网络协议，能够节省大量的纠缠资源，适用于链路不稳定的量子通信网络。2016年，参考文献[13]采用基于纠缠交换的中继技术，通过优先选择最少中继节点的量子信道，实现多用户量子 VoIP 通信，能够极大地提高量子 VoIP 网络的性能。同年，王林飞等[14]针对大规模的量子通信网络提出了一种基于量子网络分层结构的量子分组传输方案，能够进一步减少量子分组信息在量子通信网络中的传输时间和纠缠资源。

上述文献中采用了多种研究方案在量子互联网中实现数据传输，然而，在实际的量子互联网中，完成路由存储转发的核心设备是量子路由器，在研究量子数据传输方案时，应当充分考虑量子路由器自身性能的限制；量子路由器是以量子分组或量子分组簇[14]为基本的路由选择单位，其需要首先将到达的量子分组或量子分组簇存入到接收缓存中，等待处理；而量子路由器的缓存是有限的，如果每个量子分组或量子分组聚合后的量子簇过长，可能会导致该量子分组或量子簇无法进入缓存而被直接丢弃，导致丢包率上升，对量子路由器性能及工作效率造成负面影响。因此，在实际工程应用中，量子路由器都会对能够转发的分组或分组簇限定一个最大转发长度，一旦量子分组或量子分组簇长度超过上限，量子路由器将直接把其丢弃，不对其进行转发。在参考文献[14]提出的量子簇数据传输方案没有考虑量子路由器关于量子簇转发长度的限制，如果聚合后的量子簇长度过大，该量子簇将直接被丢弃，导致数据丢失。

为了解决上述问题，文中提出了一种基于分层的量子簇分片传输方案，能够在确保数据正确传输的同时，进一步节省纠缠资源的消耗，降低量子分组传输时延。

1 量子簇分片报文格式

在参考文献[14]中依据经典互联网 IPv6 协议的 IP 报文格式特点给出了相应的量子分组报文格式和量子簇报文格式。在量子分组首部中，因为经典 IPv6 协议首部中的载荷长度字段为 16 位，在量子分组首部中对应的载荷长度字段通过密集编码[15]的方式使用 8 位量子位就能够实现 16 位载荷长度编码。

量子簇是量子分组按照目的地址进行聚合，之后再进行路由转发。量子簇当中的负载长度是聚合过程当中的所有量子分组长度之和。如果对同一网

络目的地址的量子分组进行无限制的聚合，其生成的量子簇长度可能就会超过量子路由器能够处理的上限，一旦长度超过上限，该量子簇将被量子路由器直接丢弃。

为了能够有效解决这一问题，在参考文献[14]中提出的量子簇报文格式的基础上提出了分片量子簇报文格式如图 1 所示，其字段具体内容如下。

Destination address	Traffic flow type	Payload length	Flag	Segment offset	Identification field	Payload data
(64 qubits)	(2 qubits)	Obtained by calculation	MF DF (1 qubit)	(7 qubits)	(8 qubits)	Maximum complete data obtained by aggregating all packets

图 1 分片量子簇报文格式

Fig.1 Packet format of fragment quantum cluster

(1) 目的地址字段：表示分片量子簇的目的地址；业务流类别字段用于区分量子分组、量子簇和分片量子簇；载荷长度字段表示分片量子簇中的有效载荷数据长度，根据分片后得到的分片量子簇中包含的各量子分组数据长度计算得出；有效载荷数据字段表示分片后该分片量子簇中包含的各量子分组数据。

(2) 标志字段：采用密集编码方式可实现 2 位二进制地址编码。当 2 位二进制地址编码为 00 时，表示数据允许分片，且已经是整个数据最后一个分片；当 2 位二进制地址编码为 01 时，表示数据允许分片，且后面还有数据分片；当 2 位二进制地址编码为 10 时，表示不允许分片；当 2 位二进制地址编码为 11 时，无意义。

(3) 片偏移字段：7 个量子位，片偏移指出，在较长的数据分片之后，某一数据分片在原来的数据当中的相对位置，且每个分片的长度是 8 字节的整数倍。

(4) 标识字段：在发送端，当聚合后的量子簇长度过大时，可将其按照分片量子簇格式将其分成若干个分片报文，并给每一个分片后的报文分配一个相同的报文标识。

2 基于分层结构的量子簇分片传输方案

在参考文献[14]中详细给出了量子分组及量子簇数据的传输方案，文中详细给出量子簇分片数据传输方案，具体过程如下。

2.1 分片量子簇聚合方案

假定某城域网路由器在时间 T 内收到了从局域网发送的 m 个量子分组，假定每个量子路由器能够处理的最大有效载荷长度为 A，分片量子簇聚合的具体步骤如下：

步骤(1) 设置硬件计时器 T，假定在计时器 T 超时之前某城域网路由器接收到 m 个量子分组，将 m 个量子分组按照目的地址进行分组，对每组中包含的量子分组执行步骤(2)；

步骤(2) 假定该组中包含 x 个量子分组，则计算 x 个量子分组的总长度，用 H 表示，如果 $H\leqslant A$，则可将 x 个量子分组直接合并后作为有效载荷数据，按照参考文献[14]中给出的量子簇报文格式添加上相应的量子簇首部，封装成量子簇报文后发送出去；如果 $H>A$，执行步骤(3)；

步骤(3) 因为路由器对转发的量子分组或量子分组簇长度存在限制，因此在分片的过程中，每个分片量子簇的有效载荷长度等于或者小于 A；将 x 个量子分组合并后得到一个大的量子数据序列，长度为 H，$k=[H/A]$；

步骤(4) 从得到的量子数据序列中取出前 A 个量子比特，添加上相应的分片量子簇首部后即可得到一个分片量子簇，将 k 的数值减 1，执行步骤(5)；

步骤(5) 如果 $k>1$，将 k 的数值减 1，重复执行步骤(4)；如果 $k=1$，则取出量子数据序列中剩余的量子比特，添加上相应的分片量子簇首部后即可得到一个分片量子簇；如果 $k=0$，量子簇分片结束，最终可得到 k 个分片量子簇，前 $k-1$ 片的有效载荷长度等于 A，第 k 片的有效载荷长度等于或者小于 A，并依据每个分片量子簇在原有量子数据序列中的相对位置计算其对应的片偏移字段。标志字段的设置如下：前 $k-1$ 片分片量子簇中 MF 位为 1，第 k 片分片量子簇的 MF 位为 0。

步骤(6) 经过分片之后的数据，按照分片量子簇格式添加上相应的分片量子簇首部后就得到了完整的分片量子簇，进行多次路由转发后到达最后一跳城域网路由器 D。在量子路由器 D 上，对分片量子簇进行重组。量子路由器通过解析获得每个分片量子簇首部中的标识字段，通过标识字段就可以找到

属于同一个量子簇的分片量子簇报文，然后依据分片量子簇报文中的片偏移量字段，对分片量子簇报文进行重新排序后得到的有效载荷数据就是发送端发送的量子数据序列。

步骤(7) 针对重组之后得到的量子数据序列，量子路由器 D 通过测量获得每个量子分组头信息，并且以密集编码的方式恢复其量子分组头信息，按照参考文献[14]中提出的量子分组传输方法将恢复的量子分组按照目的地址路由转发给各个局域网路由器。

2.2 分片量子簇数据传输方案

在参考文献[14]提出的量子网络分层结构当中，量子局域网当中的用户和量子路由器所要传输的是量子分组的形式，而量子城域网和广域网接收局域网发送的量子分组或者本地量子城域网和广域网发送的量子簇。

在文中提出的量子簇分片传输方案中，量子局域网当中的主机和量子路由器所要传输的数据仍然是量子分组的形式，与参考文献[14]相同；在量子城域网和量子广域网中，当量子分组聚合后，如果有效载荷长度小于等于 A，则量子数据以量子簇的报文格式进行存储转发；如果有效载荷长度大于 A，则量子数据以分片量子簇的格式进行存储转发；在城域网和广域网内，所要传输的量子簇或分片量子簇根据目的网络地址在路由表内进行路由转发。

由图 1 可知，在需要传送的分片量子簇报文格式中，包含首部和有效载荷数据信息，其中，在城域网和广域网的路由器之间存在相应的量子纠缠粒子对。基于参考文献[14]中量子簇数据传输方案的工作原理，文中在分片量子簇报文传输过程中，分片量子簇报文的首部信息基于密集编码原理[15]进行传送，分片量子簇报文的有效载荷数据信息基于量子隐形传态原理进行传送，详细步骤如下：

(1) 城域网路由器 B 针对自己所要发送的分片量子簇报文首部信息产生相应的量子纠缠对，将量子纠缠对中其中的一个留给自己，另外一个发送给下一跳路由器，假定最初制备的纠缠态是：

$$|\Phi^+\rangle=(|01\rangle+(|10\rangle)/\sqrt{2} \tag{1}$$

(2) 城域网路由器 B 通过对自己持有的量子比特执行不同的幺正变换实现两个经典比特编码，具体编码过程如下：如果城域网路由器 B 要传送的经典比特信息为 00，则对自己持有的量子比特执行幺正变换 I，该量子比特的纠缠态变为：

$$I|\Phi^+\rangle=|\Phi^+\rangle=(|01\rangle+(|10\rangle)/\sqrt{2} \tag{2}$$

如果城域网路由器 B 要传送的经典比特信息为 01，则对自己持有的量子比特执行幺正变换 σ_x，该量子比特的纠缠态变为：

$$\sigma_x|\Phi^+\rangle=|\Psi^+\rangle=(|00\rangle+(|11\rangle)/\sqrt{2} \tag{3}$$

如果城域网路由器 B 要传送的经典比特信息为 10，则对自己持有的量子比特执行幺正变换 σ_z，该量子比特的纠缠态变为：

$$\sigma_z|\Phi^+\rangle=|\Phi^-\rangle=(|01\rangle-(|10\rangle)/\sqrt{2} \tag{4}$$

如果城域网路由器 B 要传送的经典比特信息为 11，则对自己持有的量子比特执行幺正变换 $i\sigma_y$，该量子比特的纠缠态变为：

$$i\sigma_y|\Phi^+\rangle=|\Psi^-\rangle=(|00\rangle-(|11\rangle)/\sqrt{2} \tag{5}$$

(3) 城域网路由器 B 把自己所持有的编码后的纠缠粒子发送到下一跳路由器 C，之后下一跳路由器使用贝尔基进行联合测量，如果测量结果为 $|\Phi^+\rangle$，则路由器 C 获得的两个经典比特信息为 00；如果测量结果为 $|\Psi^+\rangle$，则路由器 C 获得的两个经典比特信息为 01；如果测量结果为 $|\Phi^-\rangle$，则路由器 C 获得的两个经典比特信息为 10；如果测量结果为 $|\Psi^-\rangle$，则路由器 C 获得的两个经典比特信息为 11；量子路由器通过进行联合测量就能够读取出分片量子分簇报文中包含的首部信息；

(4) 城域网路由器 B 将分片量子簇有效载荷数据编码在序列 τ 中，τ_i 为量子数据信息序列的第 i 个粒子，粒子 τ_i 对应的量子态为：$|\Phi\rangle_{\tau_i}=\alpha|0\rangle_{\tau_i}+\beta|1\rangle_{\tau_i}$，城域网路由器 B 产生纠缠粒子对为 E_i 和 F_i，其纠缠态为：

$$|\Phi^+\rangle_{E_iF_i}=(|01\rangle_{E_iF_i}+|10\rangle_{E_iF_i})/\sqrt{2} \tag{6}$$

城域网路由器 B 保留纠缠粒子 E_i，将纠缠粒子 F_i 发送给下一跳路由器；然后，城网路由器 B 将 $|\varphi\rangle_{\tau_i}$ 与 $|\Phi^+\rangle_{E_iF_i}$ 进行直积，可得：

$$\begin{aligned}|\varphi\rangle_{\tau_i}\otimes|\Phi^+\rangle_{E_iF_i}=&\frac{1}{2}|\Phi^+\rangle_{\tau_iF_i}=\frac{1}{2}|\Psi^+\rangle_{\tau_iE_i}(\alpha|1\rangle_{F_i}+\beta|0\rangle_{F_i})+\\&\frac{1}{2}|\Psi^-\rangle_{\tau_iE_i}(\alpha|1\rangle_{F_i}+\beta|0\rangle_{F_i})+\\&\frac{1}{2}|\Phi^+\rangle_{\tau_iF_i}(\alpha|0\rangle_{F_i}+\beta|1\rangle_{F_i})+\\&\frac{1}{2}|\Phi^-\rangle_{\tau_iF_i}(\alpha|0\rangle_{F_i}+\beta|1\rangle_{F_i})\end{aligned} \tag{7}$$

(5) 城域网路由器 B 对其拥有的两个量子比特 τ_i 和 E_i 按照 BELL 基进行联合测量，并将测得的结果发送给下一跳路由器，下一跳路由器按照下表对其保存的纠缠粒子 F_i 执行相应的幺正变换进行数据恢复得到量子比特 τ_i，重复上述过程下一跳路由器能够得到有效载荷数据编码序列 τ。之后将之前所得到的分片量子簇首部信息和有效载荷数据编码序列 τ 重新按照分片量子簇进行封装。

3 量子簇分片传输方案性能分析

假设某城域网对收到的局域网发送的量子分组聚合之后的量子簇的总数是 S，假定在 S 个量子簇中能够被路由转发的量子簇数量是 r，不能够被转发的量子簇个数是 $S-r$。在参考文献[14]中提供了两种城域网、广域网中的数据传输方式，一种是基于量子分组进行数据传输，一种是基于量子簇进行数据传输；因为路由器性能的限制，存在 $S-r$ 个聚合后的量子簇不能被量子路由器存储转发，在参考文献[14]提供的方案中，对于上述不能转发的量子簇中包含的量子分组只能够以量子分组的形式进行传送。

3.1 量子簇或分片量子簇个数、量子分组数与量子纠缠对数的关系

量子分组能够在量子局域网、量子城域网和量子广域网[14]中传输，量子簇和分片量子簇是在量子城域网和量子广域网中输。

在路由传输的过程当中，假设每个分组的长度均是 L，m 个量子分组从局域网目的地址出发，在城域网中聚合成量子簇或分片量子簇，在城域网和广域网之间通过量子路由器存储转发后转发到目的地址。假设在路由转发的过程当中，量子簇或分片量子簇在城域网和广域网经过的路由数量平均是 n(奇数)，每个分组的量子比特数用 N_1 表示，则：

$$N_1=L+146 \tag{8}$$

(1) 在 m 个量子分组传输的过程当中，按照参考文献[14]中提供的数据传输方案在城域网路由器上聚合得到 S 个量子簇，如果聚合之后的量子簇的载荷长度小于等于 A，则量子簇可以进行路由转发。假设满足路由器转发条件的量子簇数量为 r 个。则剩余的量子簇中包含的量子分组只能以单个分组的形式进行路由转发。则 m 个量子分组传输过程中需要的纠缠粒子对数是：

$$N=2N_1\cdot m+\sum_{i=1}^{r}[64+2+8\cdot r_i+N_1\cdot r_i]\cdot\frac{n-1}{2}+\sum_{i=r+1}^{S}S_i(64+2+8+N_1)\cdot\frac{n-1}{2} \tag{9}$$

式中：r_i、S_i 表示聚合之后的量子簇中第 i 个量子簇当中的量子分组数。以量子分组的形式所传输的量子分组的数量是 $\sum_{i=r+1}^{S}S_i$，且两者满足约束条件：

$$\sum_{i=1}^{r}r_i+\sum_{i=r+1}^{S}S_i=m$$

(2) 在文中提出的分片量子簇传输方案中，充分考虑了量子路由器存储转发性能的限制，能够在考虑量子路由器性能的基础上进行尽可能的聚合。由上可知，m 个量子分组聚合得到的 S 个量子簇中，有 r 个量子簇能够直接进行传送，则对这 r 个量子簇中包含的量子分组按照量子簇格式聚合封装后直接进行数据传送；对之后的 $S-r$ 个量子簇按照分片量子簇格式进行数据分片，假设分片之后得到的分片量子簇数量是 b，其中 b_j 表示分片之后第 j 个分片当中的所包含的平均量子分组个数，且满足条件：$\sum_{i=1}^{r}r_i+\sum_{j=1}^{b}b_j=m$。

则传输过程当中量子纠缠对总数是：

$$N'=2N_1\cdot m+\sum_{i=1}^{r}[64+2+8\cdot r_i+N_1\cdot r_i]\cdot\frac{n-1}{2}+\sum_{j=1}^{b}b_j(64+2+7+8+1+8\cdot b_j+N_1\cdot b_j)\cdot\frac{n-1}{2} \tag{10}$$

在两种方案传输的过程中，两者所消耗的纠缠对数之差为 N''，其中

$$N''=N-N' \tag{11}$$

设量子分组的平均有效长度 $L=10\ 000$，$m\subset[600,10\ 000]$，$n\subset[1,30]$，$r=20$，$r_i=30$，$b_j=20$。两种方案传输数据所需要的纠缠粒子对数的差值与量子分组和量子路由器之间的关系如图 2 所示。

由图 2 可知，当转发数据的量子路由器数量一定时，随着需要传输的量子分组数的增大，文中提出的数据传输方案只需要消耗较少的纠缠粒子对数就能够完成数据传输，而参考文献[14]中消耗的纠缠资源较多；如果需要传输的量子分组数一定时，当转发数据的量子路由器数量增加时，参考文献[14]完

成数据传输需要消耗更多的纠缠资源。

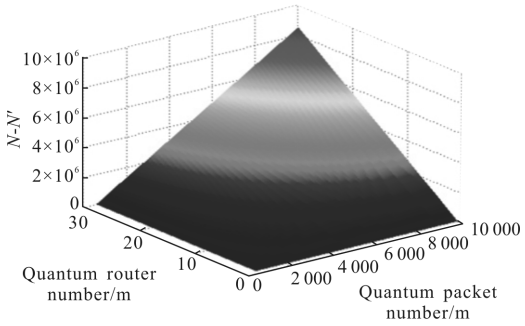

图 2 传输的量子分组数、经过的路由器数与量子纠缠对数之差的关系

Fig.2 Relationship among the quantum packet number, the quantum router number and the quantum entangled logarithm difference

假定 L=10 000, m=12 000, n=15, r_i=30, b_j=20, 则在两种不同传输方案中, 量子纠缠对数与之间的关系如图 3 所示。

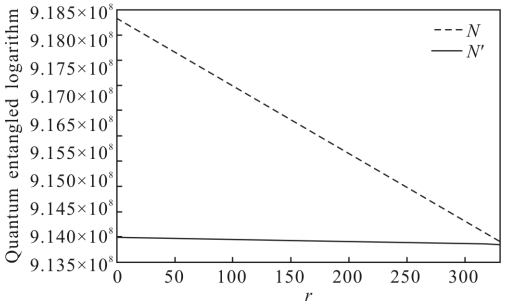

图 3 量子纠缠对数与 r 的关系

Fig.3 Relationship between quantum entangled logarithm and r

由图 3 可知, 当 r 最大时, 表示所有的量子簇都能够被量子路由器进行存储转发, 量子簇都能够被量子路由器进行存储转发, 此时文中和参考文献[14]提出的数据传输方案所消耗的纠缠粒子数相同; 然而在量子城域网和量子广域网中量子分组数量非常庞大, 如果采用参考文献[14]提供的方案, 会出现大量的聚合后的量子簇无法被量子路由器直接进行存储转发, 从而导致 r 数值往往比较小, r 的数值越小, 由图 3 可知, 文中提出的数据传输方案在相同情况下能够以更少的纠缠粒子数完成数据传输。

3.2 分片量子簇传输时延分析

量子隐形传态时间用 T_t 表示, 其中隐形传态包括纠缠对的产生与分发时间以及完成经典信息传输所需的时间。量子分组、量子簇和分片量子簇中每个量子位的读取时间为 t_r, 每个量子位的恢复时间是 t_R, 其中选择路由时间为 T_S, 量子分组达到路由器排队处理时间使用 $M/M/1$ 排队算法, 则每次路由平均排队的概率是 p, λ 表示每个量子路由器的分组到达率。其中能够直接被量子路由器进行存储转发的量子簇个数是 r, 每个量子簇当中包含的量子分组数是 r_i。

(1) 基于量子簇和量子分组传输方案的传输时延分析

由参考文献[14]可知, 在量子分组聚合的过程当中 r 个量子簇到达目的路由器所需的传输时间为:

$$T_r=[T_t\cdot r_i+74t_r\cdot r_i+t_R(66+8\cdot r_i)+T_S]\cdot r+(W'+T_S)\cdot\frac{n-1}{2}+(66+8\cdot r_i)\cdot t_r+(T_t+74+T_S)\cdot r_i \tag{12}$$

其中:

$$W'=\frac{p[T_t\cdot r_i+74t_r\cdot r_i+t_R(66+8\cdot r_i)+T_S]}{r-\lambda[T_t\cdot r_i+74t_r\cdot r_i+t_R(66+8\cdot r_i)+T_S]} \tag{13}$$

式中: W' 表示以单个量子簇传输数据时的平均排队时延。

对于聚合之后不能直接被量子路由器转发的量子簇所包含的量子分组, 按照单个量子分组的形式进行路由传输。需要传输的量子分组的个数是 $\eta=m-\sum_{i=1}^{r}r_i$, 则 η 个量子分组数据传输所需要的时间是:

$$T_\eta=[T_t+74(t_r+t_R)+T_S]\cdot(\eta+1)+(W+T_S)\cdot\frac{n-1}{2} \tag{14}$$

其中:

$$W=\frac{p[T_t+74(t_r+t_R)+T_S]}{1-\lambda[T_t+74(t_r+t_R)+T_S]} \tag{15}$$

式中: W 表示以单个量子分组传输数据时的平均排队时延。

由以上可知, m 个量子分组在城域网和广域网之间完成数据传输所需要的时间为:

$$T=T_r+T_\eta \tag{16}$$

(2) 文中是基于分片量子簇的方式完成数据传输, 假定传输的分片量子簇数量是 b, 每个分片量子簇当中包含的量子分组数是 b_j, 则传输的时间是:

$$T_b=[T_t\cdot b_j+90t_r\cdot b_j+t_R(82+8\cdot b_j)+T_S]\cdot b+(W'+T_S)\frac{n-1}{2}+(82+8\cdot b_j)\cdot t_r+(T_t+74+T_S)\cdot b_j \tag{17}$$

其中:

$$W''=\frac{p\cdot b[T_t\cdot b_j+90t_r\cdot b_j+t_R(82+8\cdot b_j)+T_S]}{b-\lambda[T_t\cdot b_j+90t_r\cdot b_j+t_R(82+8\cdot b_j)+T_S]} \tag{18}$$

式中：W''表示以单个分片量子簇传输数据时的平均排队时延。

由以上可知完成 m 个量子分组以文中提出的传输方案所需要的时间为 T'：

$$T'=T_r+T_b \tag{19}$$

假设 n=15，t_r=0.1 ns，t_R=0.1 ns，T_t=10 ns，T_S=1 ns，p=0.1，λ=0.3，r_i=30，b_j=20，m=10 000。则 r 与两种传输方案传输时间之间的关系如图 4 所示。

由图 4 可知，随着 r 的增加，两种传输方案的传输时间逐渐减小。r 的数值越小，与参考文献[14]提出的传输方案相比，文中提出的分片量子簇传输方案能够节省的传输时间就越多。由此可知，在实际工程应用中，文中提出的分片量子簇传输方案与参考文献[14]相比，所需的传输时延更小。

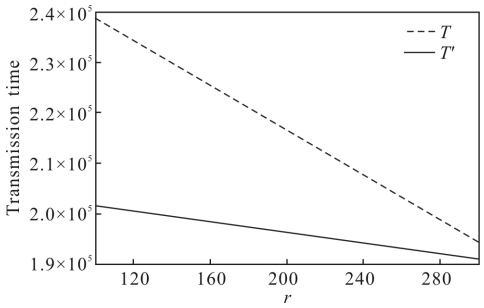

图 4 总传输时延与 r 的关系

Fig.4 Relationship between the total transmission time and r

假定 n=15，t_r=0.1 ns，t_R=0.1 ns，T_t=10 ns，T_S=1 ns，p=0.1，λ=0.3，r=50，r_i=30，b_j=20。则量子分组数与两种传输方案所消耗的传输总时间的关系如图 5 所示。

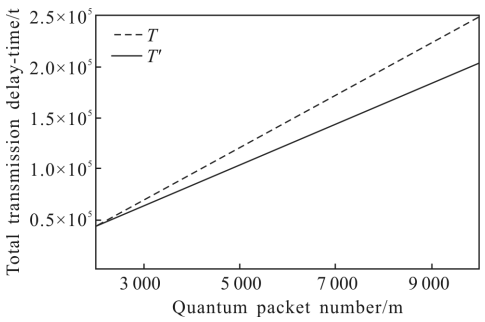

图 5 总传输时延与量子分组数的关系

Fig.5 Relationship between quantum packet and total transmission time

由图 5 可知，随着量子分组数的增加，两种传输方案完成数据传输所需的传输时间逐渐增大。而且量子分组数量越多，分片量子簇传输方案所节省的传输时间越多。

假设 n=15，t_r=0.1 ns，t_R=0.1 ns，m=10 000，r_i=30，r=50，λ=0.3，T_S=1 ns，$T_t\subset$[0.1 ns，25 ns]，b_j=20。则量子分组隐形传态时间与两种传输方案所消耗的传输时间差如图 6 所示。

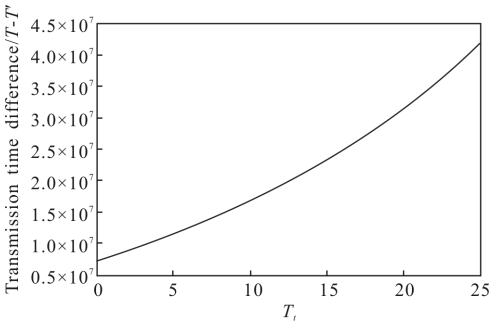

图 6 T_t 与两种方案传输时间差的关系

Fig.6 Relationship between T_t and transmission time difference of the two schemes

由图 6 可知，随着量子分组隐形传输时间的增加，与参考文献[14]提出的传输方案相比，文中提出的分片量子簇传输方案能够节省的传输时间就越多。

由上述仿真分析结果可知，与参考文献[14]提供的传输方案相比，当量子路由器数量或者量子分组数一定时，随着量子分组数或者量子路由器数量的增加，文中提出的传输方案消耗的纠缠资源数相对较少。在实际的量子网络通信当中，量子分组按照目的地址聚合之后，随着能够被路由器直接转发的量子簇数量的增加，文中提出的传输方案在数据传输时，消耗的纠缠资源和传输时延较小。当量子分组的数量或量子分组隐形传态时间越大时，文中提出的传输方案所消耗的传输时间与参考文献[14]相比减少的越明显。综上所述，文中提出的分片量子簇传输方案在纠缠资源消耗和传输时延方面与参考文献[14]相比均得到了有效的改善，具有较好的应用价值。

4 结 论

在量子互联网通信中，采用量子分组聚合的传输方案可以有效节省量子分组和量子簇在城域网之间传输的时延和纠缠资源。但是随着传输数据的增大，在聚合的过程当中，量子簇不是在一定时间内无限制的按照量子城域网网段聚合，超过量子路由器

路由转发的最大值时,量子路由器不能够缓存接收,从而导致数据丢失。文中提出了一种量子簇分片传输方案,其将不能够直接被量子路由器存储转发的量子簇,通过分片将其分解为若干个长度较短的能够直接被路由器存储转发的分片量子簇完成数据传输。仿真结果表明,当转发数据的量子路由器数量一定时,随着传输量子分组数的增大,文中提出的数据传输方案只需要消耗较少的纠缠粒子对数就能够完成数据传输,而参考文献[14]中消耗的纠缠资源较多;如果需要传输的量子分组数一定时,当转发数据的量子路由器数量增加时,参考文献[14]完成数据传输需要消耗更多的纠缠资源;当能够被量子路由器直接转发的量子簇数量越小,文中提出的数据传输方案在相同情况下能够以更少的纠缠粒子数和更少的传输时间完成数据传输。

参考文献:

[1] Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. ***Physical Review Letters***, 1993, 70(13): 1895.

[2] Pan J W, Bouwmeester D. Experimental quantum teleportation [J]. ***Nature***, 1997, 390(390): 575.

[3] Phoenix S J D, Barnett S M, Townsend P D, et al. Multi-user quantum cryptography on optical-networks [J]. ***Modern Opt***, 1995, 46(6): 1155-1163.

[4] Brassard G, Bussieres F, Godbout N, et al. Multi-user quantum key distribution using wave-length division multiplexing[C]//SPIE, 2003, 5260(6): 149-153.

[5] Inagaki T, Matsuda N, Tadanaga O, et al. Entanglement distribution over 300 km of fiber [J]. ***Optics Express***, 2013, 21(20): 23241-9.

[6] Xu Xiong, Tao Qiangqiang, Shen Fei, et al. Retrieving the polarization information for light communication [J]. ***Infrared and Laser Engineering***, 2016, 45(9): 0922002. (in Chinese)
许雄, 陶强强, 沈飞, 等. 基于偏振信息恢复的光通信[J]. 红外与激光工程, 2016, 45(9): 0922002.

[7] Wu Jianan, Wang Shigang, Zhang Di, et al. Binary image watermark fusionbased on quantum key true randomness [J]. ***Optics and Precision Engineering***, 2017,25 (11): 2968 - 2974. (in Chinese)
吴佳楠, 王世刚, 张迪, 等. 融合量子密钥真随机性的二值图像水印[J]. 光学 精密工程, 2017, 25(11): 2968-2974.

[8] Xue Le, Nie Min, Liu Xiaohui. A model of quantum signaling repeater and parameters simulation [J]. ***Acta Phys Sin***, 2013, 62(17): 170305. (in Chinese)
薛乐, 聂敏, 刘晓慧. 量子信令中继器模型及性能仿真[J]. 物理学报, 2013, 62(17): 170305.

[9] Zhou Nanrun, Zeng Guihua, Gong Lihua, et al. Quantum communication protocol for data link layer based on entanglement [J]. ***Acta Phys Sin***, 2007, 56 (9): 5066-5070. (in Chinese)
周南润, 曾贵华, 龚黎华, 等. 基于纠缠的数据链路层量子通信协议[J]. 物理学报, 2007, 56(9): 5066-5070.

[10] Zhou Xiaoqing, Wu Yunwen, Zhao Han. Quantum teleportation internetworking and routing strategy [J]. ***Acta Phys Sin***, 2011, 60(4): 35-40. (in Chinese)
周小清, 邬云文, 赵晗. 量子隐形传态网络的互联与路由策略[J]. 物理学报, 2011, 60(4): 35-40.

[11] Liu Xiaohui, Nie Min, Pei Changxing. Quantum wireless wide-area networking and routing strategy[J]. ***Acta Phys Sin***, 2013, 62(20): 200304. (in Chinese)
刘晓慧, 聂敏, 裴昌幸. 量子无线广域网构建与路由策略[J]. 物理学报, 2013, 62(20): 200304.

[12] Nie Min, Wang Linfei, Yang Guang, et al. Transmission protocol and its performance analysis of quantum communication network based on packet switching [J]. ***Acta Phys Sin***, 2015, 64(21): 210303. (in Chinese)
聂敏, 王林飞, 杨光, 等. 基于分组交换的量子通信网络传输协议及性能分析[J]. 物理学报, 2015, 64(21): 210303.

[13] Nie Min, Liu Guangteng, Yang Guang, et al. Voice over quantum IP routing based on least relay node constrained optimization strategy [J]. ***Acta Phys Sin***, 2016, 65 (12): 120302. (in Chinese)
聂敏, 刘广腾, 杨光, 等. 基于最少中继节点约束的量子VoIP 路由优化策略[J]. 物理学报, 2016, 65(12): 120302.

[14] Wang Linfei, Nie Min, Yang Guang, et al. A scheme of quantum packet transmission and its performance analysis based on hierarchical [J]. ***Acta Phys Sin***, 2016, 65 (13): 130302. (in Chinese)
王林飞, 聂敏, 杨光, 等. 一种基于分层的量子分组传输方案及性能分析[J]. 物理学报, 2016, 65(13): 130302.

[15] Yan Hongye. The scheme of quantum dense coding in quantum communication [D]. Dalian: Dalian University of Technology, 2010. (in Chinese)
闫红叶. 量子通信中的密集编码方案[D]. 大连: 大连理工大学, 2010.