Computers, Materials & Continua CMC, vol.64, no.3, pp.1629-1645, 2020

Continuous-Variable Quantum Network Coding Based on Quantum Discord

Tao Shang[1, *], Ran Liu[1], Jianwei Liu[1] and Yafei Hou[2]

Abstract: Establishing entanglement is an essential task of quantum communication technology. Beyond entanglement, quantum discord, as a measure of quantum correlation, is a necessary prerequisite to the success of entanglement distribution. To realize efficient quantum communication based on quantum discord, in this paper, we consider the practical advantages of continuous variables and propose a feasible continuous-variable quantum network coding scheme based on quantum discord. By means of entanglement distribution by separable states, it can achieve quantum entanglement distribution from sources to targets in a butterfly network. Compared with the representative discrete-variable quantum network coding schemes, the proposed continuous-variable quantum network coding scheme has a higher probability of entanglement distribution and defends against eavesdropping and forgery attacks. Particularly, the deduced relationship indicates that the increase in entanglement is less than or equal to quantum discord.

Keywords: Continuous variable, quantum network coding, quantum discord, entanglement distribution, Gaussian cloning.

1 Introduction

The main idea of network coding [Ahlswede, Cai, Li et al. (2000)] is to improve the network throughput by encoding the information of intermediate network nodes. By referring to network coding, quantum network coding (QNC) can improve network throughput and save network bandwidth, which has triggered the community's interest in the design of QNC. In 2006, Hayashi et al. [Hayashi, Iwama, Nishimura et al. (2007)] proposed the concept of QNC and the protocol for crossing two qubits over the butterfly network. The first QNC protocol XQQ (crossing two qubits) shows that QNC is possible in the butterfly network. In order to solve the problem that the fidelity of XQQ protocol is less than 1, Hayashi applied quantum teleportation to quantum network coding in 2007, and proposed a quantum network coding scheme based on the prior entangled state between two sending parties [Hayashi (2007)]. With the help of prior entanglement, new breakthroughs in QNC has been achieved [Wang, Luo, Xu et al. (2018); Nguyen, Babar,

[1] School of Cyber Science & Technology, Beihang University, Beijing, 100083, China.

[2] Graduate School of Natural Science and Technology, Okayama University, Okayama Prefecture, 700-8530, Japan.

[*] Corresponding Author: Tao Shang. Email: shangtao@buaa.edu.cn.

Received: 20 January 2020; Accepted: 10 April 2020.

Alanis et al. (2017); Li, Gao, Qin et al. (2018)]. To make long-distance quantum communication more efficient, Satoh et al. [Satoh, Le Gall and Imai (2012)] designed a QNC scheme for quantum repeaters in which adjacent nodes initially share one Einstein-Podolsky-Rosen (EPR) pair. The information carrier of all the above schemes is discrete variable, hence they are called discrete-variable quantum network coding (DVQNC) scheme. However, it is difficult for these schemes to prepare and detect single photons for encoding discrete information. For feasible applications in quantum communication, both theoretical and experimental investigations are increasingly concerned with continuous variables. In 2017, Shang et al. [Shang, Li and Liu (2017)] proposed two continuous-variable quantum network coding (CVQNC) schemes. The first scheme transmits two coherent states over butterfly network utilizing ADD/SUB operators and Gaussian cloning, and the fidelity of the first scheme is 1/2. The second scheme is based on continuous-variable quantum teleportation and transmit two coherent states faultlessly. In 2019, the CVQNC scheme against pollution attack [Shang, Li, Chen et al. (2019)] and quantum homomorphic signature scheme [Shang, Pei, Chen et al. (2019)] were proposed. From the perspective of transmitting classical information, these CVQNC schemes have better network throughput than the DVQNC schemes.

Entanglement is the underpinning of many fundamental quantum tasks and is regarded as a key resource in quantum information. In 2003, Cubitt et al. [Cubitt, Verstraete, Dür et al. (2003)] proposed a protocol called entanglement distribution by separable states (EDSS) protocol. It can be used to construct entanglement between two distant particles by sending a third particle which is not entangled with the two distant particles. In 2008, Mišta et al. [Mišta and Korolkova (2008)] found that the distribution of entangled states in Gaussian states is possible by using linear optics elements and a certain three-mode fully separable mixed Gaussian state which are available in experiments. Similarly, two modes of the state are entangled by mixing on two beam splitters in sequence, while the third particle is separable at all stages of the protocol. Then they proposed a simpler and more efficient protocol which results in continuous-variable entanglement distribution [Mišta and Korolkova (2009)]. Furthermore, it was shown that the amount of quantum discord between the distant particles and the carrier bounds the entanglement gain [Chuan, Maillard, Modi et al. (2012)]. In fact, discord results from the loss of information caused by quantum measurements, Ollivier et al. [Ollivier and Zurek (2001)] introduced it to quantify quantum correlation. We traced back the early roots of discord to the EPR-Bohr argument on completeness of quantum mechanics [Einstein, Podolsky and Rosen (1935); Wiseman (2013)], to Everett's thesis on universal wave function and relative-state formulation of quantum mechanics [DeWitt and Graham (2015)], to Lindblad's investigations of entropy and quantum measurements [Lindblad (1973)], etc. In the last decade, various aspects of discord was widely studied, such as calculation, operational meaning, ramifications, and applications. So it is worth devoting the study of entanglement from the perspective of quantum discord for efficient quantum communication.

In this paper, we design a CVQNC scheme based on quantum discord under the butterfly network. The scheme implements quantum entanglement distribution with less entanglement resources, because the continuous-variable EDSS (CV-EDSS) protocol provides new ideas of constructing entanglement via intermediate nodes in the butterfly network. The ADD operator and the SUB operator are applied to encode operation and

decode operation, while Gaussian cloning is used to simulate the copy operation of QNC. Also, considering practical advantage, we utilize continuous variables for QNC to increase the success probability of transmitting the ancillary mode to the corresponding target.

The main contributions of our work are:

(1) *A CVQNC scheme based on quantum discord is proposed.* The basic operation of ADD/SUB operators and Gaussian cloning are provided. Based on the butterfly network, two separable auxiliary modes are transmitted between source nodes and target nodes, achieving continuous-variable entanglement distribution. As a result, the fidelity of the link for transmitting the ancillary modes from sources to targets is $1/2$. Each target node receives $4\log_2 N$ bits of classical information via one network transmission. Also, our scheme can defend against eavesdropping and forgery attacks.

(2) *Theoretical results based on quantum discord are deduced.* The relationship between entanglement distribution and quantum discord is quantified and the theorem that the entanglement gain between source nodes and target nodes is less than or equal to quantum discord is deduced.

This paper is organized as follows. In Section 2, we introduce related works, including continuous-variable EDSS, ADD/SUB operators and Gaussian cloning. Section 3 gives a CVQNC scheme based on quantum discord. Section 4 focuses on the scheme analysis in term of performance and security. Section 5 is our conclusion.

2 Related works

2.1 Continuous-variable entanglement distribution by separable states (CV-EDSS)

By sending a separable ancillary mode c from Alice to Bob, the CV-EDSS protocol [Mišta Jr. and Korolkova (2009)] aims to entangle mode a at Alice with separable mode b at Bob (see Fig. 1).

Step 1. Alice prepares the mode a and the mode c in a pure single-mode squeezed state with covariance matrix (CM) γ_a and γ_c. Bob prepares the mode b in the vacuum state. The CMs are

$$\gamma_a = \begin{bmatrix} e^{\pm 2t} & 0 \\ 0 & e^{\mp 2t} \end{bmatrix}, \gamma_b = I, \gamma_c = \begin{bmatrix} e^{\pm 2t} & 0 \\ 0 & e^{\mp 2t} \end{bmatrix} \tag{1}$$

where the squeezing parameter is $t \geq 0$, I is a two-dimensional identity matrix. Then according to the Gaussian distribution with correlation matrix $Q(x)$, Alice and Bob respectively displace their own modes by random correlated displacements

$$Q(x) = x \begin{pmatrix} I - \sigma_z & \sqrt{2}(\sigma_z - I) & 0 \\ \sqrt{2}(\sigma_z - I) & 4I & \sqrt{2}(\sigma_z + I) \\ 0 & \sqrt{2}(\sigma_z + I) & \sigma_z + I \end{pmatrix} \tag{2}$$

where σ_z denotes the z Pauli matrix and $x \geq 0$. As a result, a three-mode fully separable Gaussian state with a CM Eq. 3 will be prepared.

$$\gamma_1 = \gamma_a \oplus \gamma_b \oplus \gamma_c + Q \tag{3}$$

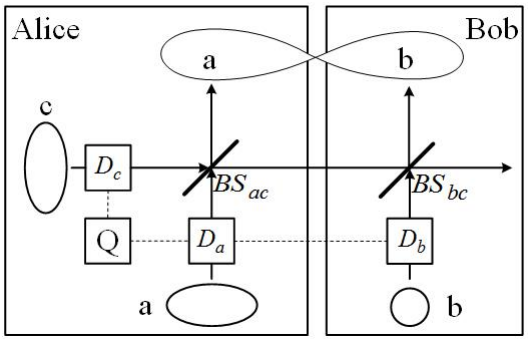

Figure 1: This is the process of continuous variables entanglement distribution by separable Gaussian states. Empty ellipses represent that modes a and c which are in the momentum and position-squeezed vacuum states, and empty circle represents that mode b is in a vacuum state

Step 2. The modes a and c are superimposed on a balanced beam splitter BS_{ac} described by the matrix

$$U_{ac} = \begin{pmatrix} \frac{1}{\sqrt{2}}I & 0 & \frac{1}{\sqrt{2}}I \\ 0 & I & 0 \\ \frac{1}{\sqrt{2}}I & 0 & -\frac{1}{\sqrt{2}}I \end{pmatrix} \tag{4}$$

Thus the CM turns to

$$\gamma_2 = U_{ac}\gamma_1 U_{ac}^T = \begin{bmatrix} mI & 2x\sigma_z & n\sigma_z \\ 2x\sigma_z & (1+4x)I & -2xI \\ n\sigma_z & -2xI & mI \end{bmatrix} \tag{5}$$

where $m = \cosh(2t) + x$, $n = \sinh(2t) - x$. The state is separable with respect to $b - ac$ splitting and for $x \geq \frac{e^{2t} - 1}{2}$, also with respect to $c - ab$ splitting.

Step 3. The mode c is mixed with mode b on a balanced beam splitter BS_{bc} described by the matrix

$$U_{bc} = \begin{pmatrix} I & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}I & \frac{1}{\sqrt{2}}I \\ 0 & \frac{1}{\sqrt{2}}I & -\frac{1}{\sqrt{2}}I \end{pmatrix} \tag{6}$$

Then the CM turns to

$$\gamma_3 = U_{bc}\gamma U_{bc}^T = \begin{pmatrix} mI & \frac{2x+n}{\sqrt{2}}\sigma_z & \frac{2x-n}{\sqrt{2}}\sigma_z \\ \frac{2x+n}{\sqrt{2}}\sigma_z & \frac{1+m}{2}I & \frac{1+4x-m}{2}I \\ \frac{2x-n}{\sqrt{2}}\sigma_z & \frac{1+4x-m}{2}I & \frac{1+8x+m}{2}I \end{pmatrix} \tag{7}$$

We denote the reduced state of the mode a and the mode b is the matrix $\gamma_{3,ab}^{(T_b)}$ and the CM $\gamma_{3,ab}$ is in the block form $\gamma_{3,ab} = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}$, where A, B and C are 2×2 submatrices.

By computing the lower symplectic eigenvalue υ of the matrix $\gamma_{3,ab}^{(T_b)}$, we conclude that the mode a and the mode b was finally entangled by the interference on the beam splitter BS_{bc}. The eigenvalue is

$$\upsilon = \sqrt{\frac{\kappa - \sqrt{\kappa^2 - 4\det(\gamma_{3,ab})}}{2}} \tag{8}$$

where

$$\det(\gamma_{3,ab}) = [\frac{1+\cosh(2t)}{2} + (e^{-2t} + \frac{1}{2})x]^2, \tag{9}$$

$$\kappa = \det(A) + \det(B) - 2\det(C) = m^2 + (n+2x)^2 + \frac{(m+1)^2}{4}. \tag{10}$$

By calculating the logarithmic negativity given by the formula $E_{\mathrm{N}} = \text{-}\log_2 \upsilon$, we can also quantify the amount of distributed entanglement. For $t > 0$ and $x = \frac{(e^{2t}-1)}{2}$, we get $\upsilon < 1$, therefore the modes a and b are entangled for an arbitrarily small nonzero squeezing parameter.

In this protocol, two modes of the state are entangled by mixing them sequentially with the third separable mode on two beam splitters. Beyond point-to-point communication, it can help construct the entanglement between sources and targets via intermediate nodes, especially in a butterfly network. By encoding the quantum states, the information of the third mode in EDSS will be hidden and guarantee that the modes a and b will be entangled ultimately between sources and targets.

2.2 ADD/SUB operators

After mixing two single-mode states $|\alpha_1\rangle = |x_1 + ip_1\rangle$ and $|\alpha_2\rangle = |x_2 + ip_2\rangle$ on a 50:50 beam splitter, the position and momentum operators will be

$$x_1' = (x_1 - x_2)/\sqrt{2}, p_1' = (p_1 - p_2)/\sqrt{2} \tag{11}$$

$$x_2' = (x_1 + x_2)/\sqrt{2}, p_2' = (p_1 + p_2)/\sqrt{2}. \tag{12}$$

Thus, we can obtain the add state of the two single-mode states by amplifying (x_2', p_2'). Similarly, we can obtain the subtract state by amplifying (x_1', p_1').We give a diagram of ADD/SUB operators (see Fig. 2). The $50:50$ beam splitter *BS* mixes the input states. One of the beams of BS is selected as the input of the noiseless linear amplifier (NLA). After the amplification process with a factor $g=\sqrt{2}$, we get the desired state $|\alpha_+\rangle=|\alpha_1+\alpha_2\rangle$ or $|\alpha_-\rangle=|\alpha_1-\alpha_2\rangle$.

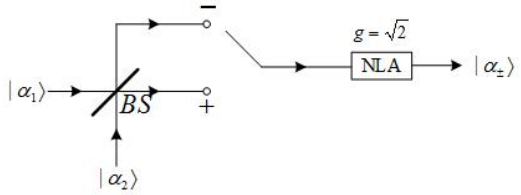

Figure 2: Diagram of ADD/SUB operators

Hence the ADD operator and the SUB operator are defined [Shang, Li and Liu (2017)] as follows:

$$ADD(|\alpha_1\rangle,|\alpha_2\rangle)=|(x_1+x_2)+i(p_1+p_2)\rangle \tag{13}$$

$$SUB(|\alpha_1\rangle,|\alpha_2\rangle)=|(x_1-x_2)+i(p_1-p_2)\rangle \tag{14}$$

We apply the ADD operator and the SUB operator to encode and decode coherent states (see Fig. 3).

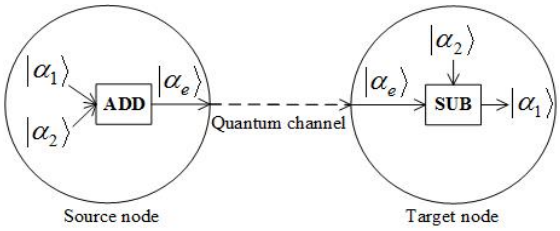

Figure 3: Encode and decode coherent states by applying the ADD operator and SUB operator

At the source node, we obtain the encoded state

$$|\alpha_e\rangle=ADD(|\alpha_1\rangle,|\alpha_2\rangle)=|(x_1+x_2)+i(p_1+p_2)\rangle \tag{15}$$

by applying the ADD operator to two coherent states $|\alpha_1\rangle=|x_1+ip_1\rangle$ and $|\alpha_2\rangle=|x_2+ip_2\rangle$.

At the target node, we obtain the decoded state

$$|\alpha_d\rangle=SUB(|\alpha_e\rangle,|\alpha_2\rangle)=|x_1+ip_1\rangle=|\alpha_1\rangle \tag{16}$$

by applying the SUB operator to $|\alpha_e\rangle$, $|\alpha_2\rangle$.

So the state $|\alpha_1\rangle$ or $|\alpha_2\rangle$ which is input to the ADD operator can be decoded by the SUB

operator.

2.3 Gaussian cloning (GC)

Cloning is an important step in the implementation of QNC. For discrete variables, quantum cloning techniques can be classified into two types. Definitive cloning performs unitary transformations during the entire cloning process. Probabilistic cloning performs unitary transformation and quantum measurement during cloning. Quantum no-cloning theorem governs both types of quantum cloning.

Duan et al. [Duan and Guo (1998a, 1998b)] proposed the probabilistic cloning technique which introduces quantum measurements to accurately clone a set of linearly independent quantum states with a certain probability. For continuous variables, approximate cloning schemes are used to simulate the copying operation. Cerf et al. [Cerf, Ipe and Rottenberg (2000)] proposed that the set of input states to be copied was restricted to Gaussian states and derived the optimal cloning fidelity. Here, we introduce a Gaussian cloning machine for continuous variables.

Gaussian cloning machine can be used to simulate the copying operation for coherent states. $|\alpha_0\rangle$ denotes the input coherent state and the output of the Gaussian cloning machine is

$$\hat{\rho} = \int d^2\alpha G(\alpha) |\alpha_0 + \alpha\rangle\langle\alpha_0 + \alpha| \tag{17}$$

where the displacement error $\alpha = x + ip$ consists of the position error x and the phase error p. x and p obey the bivariate Gaussian distribution with zero mean and a variance of $1/4$, i.e.,

$$P(x, p) = \frac{2}{\pi}\exp[-2(x^2 + p^2)]. \tag{18}$$

So the distribution function of

$$G(\alpha) = \frac{2}{\pi}\exp(-2|\alpha|^2). \tag{19}$$

The fidelity of the Gaussian cloning machine is calculated as follows:

$$f = \langle\alpha_0|\hat{\rho}|\alpha_0\rangle = \frac{2}{\pi}\int d^2\alpha e^{-3|\alpha|^2} = \frac{2}{3} \tag{20}$$

In summary, the set of input states to be copied is restricted to Gaussian states and the optimal cloning fidelity is $2/3$. So Gaussian cloning can be an effective operation used to simulate the copy operation of QNC.

3 CVQNC scheme based on quantum discord

The CV-EDSS protocol constructs entanglement between two distant locations. Gaussian cloning clones quantum states with a certain probability. These two basic operations provide basic conditions to design a CVQNC scheme. Fig. 4 shows the setting of the proposed CVQNC scheme.

Our CVQNC scheme is described as follows:

Step 1. (Preparation) The modes a_1, b_1, c_1 are prepared at the nodes s_1, t_1. The modes a_2, b_2, c_2 are prepared at the nodes s_2, t_2. Here a_1, c_1, a_2, c_2 are pure single-mode squeezed states and b_1, b_2 are the vacuum state. The CMs are

$$\gamma_{a_j} = \begin{bmatrix} e^{\pm 2t} & 0 \\ 0 & e^{\mp 2t} \end{bmatrix}, \gamma_{b_j} = I, \gamma_{c_j} = \begin{bmatrix} e^{\pm 2t} & 0 \\ 0 & e^{\mp 2t} \end{bmatrix}, j = 1,2. \tag{21}$$

Then Alice and Bob displace locally their modes by random correlated displacements distributed according to the Gaussian distribution with correlation matrix

$$Q_j(x) = x \begin{pmatrix} I - \sigma_z & \sqrt{2}(\sigma_z - I) & 0 \\ \sqrt{2}(\sigma_z - I) & 4I & \sqrt{2}(\sigma_z + I) \\ 0 & \sqrt{2}(\sigma_z + I) & \sigma_z + I \end{pmatrix}, j = 1,2. \tag{22}$$

As a result, they prepare by LOCC a three-mode fully separable Gaussian state with CM as follows:

$$\gamma_{1_j} = \gamma_{a_j} \oplus \gamma_{b_j} \oplus \gamma_{c_j} + Q_j, j = 1,2. \tag{23}$$

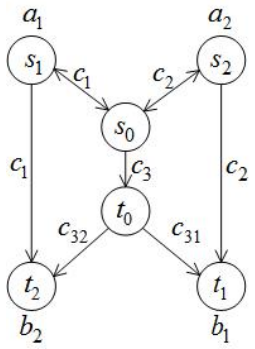

Figure 4: New CVQNC scheme

Step 2. At the node s_1, the modes a_1 and c_1 mix on a balanced beam splitter $BS_{a_1c_1}$. At the node s_2, the modes a_2 and c_2 mix on a balanced beam splitter $BS_{a_2c_2}$. Then we obtain two three-mode systems. The corresponding CMs are

$$\gamma_{2_j} = U_{a_jc_j} \gamma_1 U_{a_jc_j}^T = \begin{bmatrix} mI & 2x\sigma_z & n\sigma_z \\ 2x\sigma_z & (1+4x)I & -2xI \\ n\sigma_z & -2xI & mI \end{bmatrix}, j = 1,2 \tag{24}$$

where $m = \cosh(2t) + x$, $n = \sinh(2t) - x$, and the beam splitter is described by the matrix

$$U_{a_jc_j}=\begin{pmatrix}\frac{1}{\sqrt{2}}I & 0 & \frac{1}{\sqrt{2}}I\\ 0 & I & 0\\ \frac{1}{\sqrt{2}}I & 0 & -\frac{1}{\sqrt{2}}I\end{pmatrix}, j=1,2. \tag{25}$$

Step 3. s_1, s_2 send c_1, c_2 to the node s_0, respectively.

Step 4. (Encoding at node t_0) The new mode c_3 is introduced at s_0. By applying the ADD operator to c_1, c_2, we obtain the encoded state $c_3 = ADD(c_1, c_2)$.

Step 5. s_0 sends c_1 to t_2 via s_1 and s_0 sends c_2 to t_1 via s_1. c_3 is sent to the node t_0.

Step 6. At the node t_0, the Gaussian cloning of c_3 gives c_{31}, c_{32}. And c_{31}, c_{32} are sent to the node t_1, t_2, respectively.

Step 7. (Decoding at node t_1, t_2) At the node t_1, we obtain the decoded state $SUB(c_{31}, c_2) = c_1$ by applying the SUB operator to c_{31}, c_2. Similarly, at the node t_2, we obtain the decoded state $SUB(c_{32}, c_1) = c_2$ by applying the SUB operator to c_{32}, c_1.

Step 8. At the node t_1, the mode c_1 which from Step 7 mixes the mode b_1 on another balanced beam splitter $BS_{b_1c_1}$. At the node t_2, the mode c_2 which from Step 7 mixes the mode b_2 on balanced beam splitter $BS_{b_2c_2}$. The balanced beam splitter $BS_{b_jc_j}$ is described by the matrix

$$U_{b_jc_j}=\begin{pmatrix} & & \\ I & 0 & 0\\ 0 & \frac{1}{\sqrt{2}}I & \frac{1}{\sqrt{2}}I\\ 0 & \frac{1}{\sqrt{2}}I & -\frac{1}{\sqrt{2}}I\end{pmatrix}, j=1,2. \tag{26}$$

Then the CMs turn to

$$\gamma_{3_j}=U_{b_jc_j}\gamma U_{b_jc_j}^{T}=\begin{pmatrix} mI & \frac{2x+n}{\sqrt{2}}\sigma_z & \frac{2x-n}{\sqrt{2}}\sigma_z\\ \frac{2x+n}{\sqrt{2}}\sigma_z & \frac{1+m}{2}I & \frac{1+4x-m}{2}I\\ \frac{2x-n}{\sqrt{2}}\sigma_z & \frac{1+4x-m}{2}I & \frac{1+8x+m}{2}I\end{pmatrix}. \tag{27}$$

where $m=\cosh(2t)+x$ and $n=\sinh(2t)+x$. We compute the lower symplectic Eigenvalue υ of the matrix $\gamma_{3,ab}^{(T_b)}$ corresponding to the reduced state of the modes a and b to get the conclusion that mode a and mode b are finally entangled by the interference on the beam splitter $BS_{b_jc_j}$.

4 Scheme analysis

4.1 Performance analysis

In this section, we will provide performance analysis of our CVQNC scheme from the perspectives of fidelity and network throughput.

4.1.1 Fidelity

We consider the fidelity of the link $s_1 \to t_1$ for transmitting the mode c_1 and the link $s_2 \to t_2$ for transmitting the mode c_2.

Theorem 1: *With ideal ADD/SUB operators, the fidelity of the link* $s_i \to t_i$ *for transmitting the mode* c_i *is* $1/2$ *(i=1,2).*

Proof: If the ADD/SUB operators are ideal, the relationship between the variances of the inputs $|\alpha_1\rangle, |\alpha_2\rangle$ and the output $|\alpha_\pm\rangle$ is

$$\Delta^2 x_\pm = \Delta^2 x_1 = \Delta^2 x_2, \Delta^2 p_\pm = \Delta^2 p_1 = \Delta^2 p_2 \tag{28}$$

which indicates that this operation will not amplify quantum fluctuation. By applying the ideal ADD operation to c_1, c_2 at the node s_0, we obtain the quantum state

$$c_3 = \int d^2 q G(q) |c_1 + c_2 + q\rangle\langle c_1 + c_2 + q|, \tag{29}$$

where the displacement error q obeys a Gaussian distribution of

$$G(q) == \frac{2}{\pi} \exp(-2|q|^2). \tag{30}$$

After the GC operation at the node t_0, the replicas of c_3 are

$$\{c_{31}, c_{32}\} = \int d^2 r G(r) \int d^2 q G(q) |c_1 + c_2 + q + r\rangle\langle c_1 + c_2 + q + r|, \tag{31}$$

where r follows Gaussian distribution

$$G(r) == \frac{2}{\pi} \exp(-2|r|^2). \tag{32}$$

After applying the ideal SUB operator to c_{32}, c_1 at node t_1, the output is

$$\rho_{out}^1 = \int d^2 r G(r) \int d^2 q G(q) |c_1 + q + r\rangle\langle c_1 + q + r| \tag{33}$$

By using $|\langle c|c'\rangle|^2 = \exp(-|c - c'|^2)$ which is the property of coherent states, we calculate the fidelity of the link $s_1 \to t_1$ as follows:

$$F_1 = \langle c|\rho_{out}^1|c'\rangle = \frac{4}{\pi^2} \int d^2 r d^2 q e^{-(2|q|^2 + 2|r|^2 + |q+r|^2)} = \frac{1}{2} \tag{34}$$

For the reason of symmetry [Shang, Li and Liu (2017)], the fidelity of the link $s_2 \to t_2$ for transmitting the mode c_2 is also $1/2$.

4.1.2 Network throughput

Network throughput is one of criteria for evaluating the performance of network coding schemes. The extension from discrete variables to continuous variables means to vary from finite to infinite spaces. After one network transmission, the target node t_1 receives c_2, c_{31} and the target node t_2 receives c_1, c_{32}.

Theorem 2: Each target node receives $4\log_2 N$ bits of classical information via one network transmission.

Proof: Suppose that a coherent state $|x+ip\rangle$ is modulated with classical characters, each classical character x or p has N elements which are $0,1,\ldots,N-1$. The amount of information is

$$I(x_i) = -\log_2 p(x_i) = \log_2 \frac{1}{p(x_i)} = \log_2 N, \tag{35}$$

where $x_i \in 0,1,\ldots,N-1$. That is, the amount of information of a coherent state is $2\log_2 N$. So each target node receives $4\log_2 N$ bits via one network transmission.

Similarly, we suppose qubits $|0\rangle$ and $|1\rangle$ are used to carry classical bits 0 and 1. In this case, the information of one qubit is the same as that of one bit. Also, the network throughput of DVQNC schemes can be measured in terms of classical bits. In XQQ, each target node receives 2 bits of classical information. In the QNC scheme with prior entanglement between senders [Hayashi (2007)], each target node receives one bit of classical information.

Compared with the DVQNC schemes, the CVQNC schemes contain more information. As a result, our CVQNC scheme has a larger network throughput than the DVQNC schemes.

4.1.3 Network throughput

Quantum discord is in a primitive place than entanglement, so we can give insight into the role of discord in entanglement distribution. We calculate the relative entropy of entanglement [Piani, Gharibian, Adesso et al. (2011)] and the relative entropy of discord [Nielsen and Chuang (2007)] to search for a relationship between the increase in entanglement and quantum discord.

The von Neumann entropy of quantum state ρ is

$$S(\rho) = -tr(\rho \log \rho). \tag{36}$$

The quantum relative entropy between two states ρ and σ is defined as

$$S(\rho \| \sigma) = -S(\rho) - tr(\rho \log \sigma). \tag{37}$$

The relative entropy of entanglement in the bipartition x-versus-y is defined as

$$\varepsilon_{x:y}(\rho) = \min_{\rho_{x:y}} S(\rho \| \rho_{x:y}) \tag{38}$$

which is the minimum relative entropy between the joint state ρ of x and y, where

$$\rho_{x:y} = \sum_i p_i \rho_x^i \otimes \rho_y^i . \tag{39}$$

The relative entropy of discord is defined as

$$D_{x|y}(\rho) = \min_{\chi_{x|y}} S(\rho \| \chi_{x|y}) \tag{40}$$

which is the minimum relative entropy between ρ and the set of quantum-classical states

$$\chi_{x|y} = \sum_j p_j \chi_x^j \otimes |j\rangle\langle j|_y , \tag{41}$$

where $|j\rangle$ is an orthonormal basis for y [Abeyesinghe, Devetak, Hayden et al. (2009)].

The key step in our scheme is the transmission of ancillary modes c_i from source nodes s_i to target nodes t_i. The bipartitions $ac:b$ and $a:cb$ corresponds to the situations before and after the transmission of the ancillary modes. The difference between the relative entropy of entanglement in the bipartition $ac:b$ and the relative entropy of entanglement in the bipartition $a:cb$ can be limited [Madhok and Datta (2013)].

Lemma 1: *For any tripartite state ρ_{abc}, the difference of entanglement is bounded by the relative entropy of discord, i.e.,*

$$\left|\varepsilon_{a:bc}(\rho) - \varepsilon_{ac:b}(\rho)\right| \le D_{ab|c}(\rho) . \tag{42}$$

Reference [Bennett and Shor (1998)] indicates that under any completely positive trace-preserving map M the relative entropy is monotonic, i.e.,

$$S(\rho \| \sigma) \ge S(M(\rho) \| M(\sigma)) . \tag{43}$$

By combining it with lemma 1, we can obtain the following theorem.

Theorem 3: Assuming the initial state of a,b and c is u, and by means of a local encoding operation M_{ac}, the state will be $g = M_{ac}(u)$. We have

$$\varepsilon_{a:bc}(g) \le \varepsilon_{ac:b}(u) + D_{ab|c}(g) \tag{44}$$

Proof: A local operation on ac cannot increase entanglement in the $ac:b$, i.e.,

$$\varepsilon_{ac:b}(g) \le \varepsilon_{ac:b}(u) . \tag{45}$$

It can be deduced that

$$\varepsilon_{a:bc}(g) \le \varepsilon_{ac:b}(g) + D_{ab|c}(g) \le \varepsilon_{ac:b}(u) + D_{ab|c}(g) . \tag{46}$$

The local encoding operation M_{ac} in our scheme corresponds to the mixing operation of modes a_i and c_i on a balanced beam splitter $BS_{a_i c_i}$.

This theorem indicates that the increase in entanglement is less than or equal to quantum discord measured in the communication system. So quantum discord is a necessary prerequisite to the entanglement distribution.

4.2 Security analysis

The purpose of our CVQNC scheme based on quantum discord is to entangle two modes existing in source node and target node, respectively. In the process of entanglement

distribution, the quantum channels are tentatively used. After the evolution of the system, channels are unnecessary, so attackers cannot eavesdrop the links to obtain information.

We analyze whether the ancillary mode c_i can be calculated and forged by eavesdropping the modes transmitted in quantum channels. For the reason of symmetry, we analyze the link $s_1 \to t_1$ merely. In Step 2, the nodes s_1 entangles mode a_1 with the pair of modes (b_1c_1) by mixing modes a_1 and c_1, while mode c_1 is separable from subsystem a_1b_1. In Step 8, the nodes t_1 mixes modes b_1 and c_1 on a balanced beam splitter, while the mode c_1 still remains separable from subsystem a_1b_1.

Theorem 4: The mode c_i remains separable from subsystem a_ib_i at all times during the scheme.

Proof: The positive partial transpose (PPT) criterion declares that a three-mode Gaussian state with CM γ is separable with respect to bipartition $x-(yz)$ (where x,y,z is an even permutation of A,B,C) if and only if the matrix $\gamma^{(T_x)}$ satisfies the uncertainty relation [Giedke, Kraus, Lewenstein et al. (2001)], i.e.,

$$\gamma^{(T_x)} - i\Omega \geq 0 \tag{47}$$

For any matrix $\gamma^{(T_x)}$, there is a symplectic matrix S satisfying the condition $S\Omega S^T = \Omega$, such that

$$S\gamma^{(T_x)}S^T = diag(s_1, s_1, s_2, s_2, s_3, s_3). \tag{48}$$

The matrix $\gamma^{(T_x)}$ possesses three invariants denoted by $I_1, I_2, I_3 = \det(\gamma^{(T_x)})$ that can be calculated easily as coefficients of the characteristic polynomial of the matrix $\Omega\gamma^{(T_x)}$, i.e.,

$$\det(\gamma^{(T_x)} - \mu I) = u^6 + I_1u^4 + I_2u^2 + I^3. \tag{49}$$

The criterion declare that for CM γ the mode x is separable from the modes (yz) if and only if Eq. (50) holds [Serafini (2007)].

$$\sum = \prod_{j=1}^{3}(s_j^2 - 1) = I_3 - I_2 + I_1 - 1 \geq 0 \tag{50}$$

In Step 2, by choosing proper parameters d, r and x, the mode c_1 can be separable from the subsystem a_1b_1. The CM γ^2 turns to

$$\gamma_2^{(T_c)} = \Lambda_c\gamma^2\Lambda_c \tag{51}$$

after partial transposition, where $\Lambda_c = diag(1,1,1,1,1,-1)$. The matrix $\gamma_2^{(T_c)}$ possesses three invariants denoted $I_1, I_2, I_3 = \det(\gamma^2)$ which satisfy

$$\det(\gamma_2^{(T_c)} - \mu I) = u^6 + I_1u^4 + I_2u^2 + I_3. \tag{52}$$

The condition $\sum = I_3 - I_2 + I_1 - 1 \geq 0$ has a simple expression $\sum = x(wx + v)$, where

w and v are functions of d and r. Taking $e^{2(d-r)}=\frac{3}{2}$ and $e^{2(d+r)}=2$, we get $w>0$ and $v<0$. On this condition, the threshold value $x_{th}=-\frac{v}{w}\approx 1.04$ and hence for $x>x_{th}$, $\sum>0$ is valid. In consequence, the mode c_1 is separable from subsystem a_1b_1 in Step. 2.

In Step 8, for CM γ_3, supposing $e^{2(d-r)}=\frac{3}{2}$, $e^{2(d+r)}=2$ and $x=1.041$, we obtain $\sum\approx 0.3957>0$. Thus the mode c_1 remains separable from subsystem a_1b_1.

By using the separability criterion, we can get the conclusion that the mode c_i remains separable from a_ib_i at all times in our scheme.

Though the ancillary mode c_i can be eavesdropped in quantum channels, attackers or dishonest intermediate nodes cannot obtain any information about states a_i, b_i because the ancillary mode c_i is separable at all times. Attackers or dishonest intermediate nodes may forge the ancillary mode c_i, so the scheme will fail to construct entanglement. However, due to quantum uncertainty principle, it is rather complicated to forge the ancillary modes precisely. Once the entanglement construction fails, the scheme can restart from Step 1 and check if there exists an attacker or intermediate nodes are dishonest.

Theorem 5: *If the modes c_1, c_2 are successfully transmitted, the modes a_j and b_j will be entangled for an arbitrarily small nonzero squeezing.*

Proof: We denote the CM γ_{3,a_jb_j} in the block form $\gamma_{3,a_jb_j}=\begin{pmatrix} A & C \\ C^T & B \end{pmatrix}$, where A, B and C are 2×2 submatrices. The eigenvalue reads as

$$v=\sqrt{\frac{\kappa-\sqrt{\kappa^2-4\det(\gamma_{3,a_jb_j})}}{2}}, \tag{53}$$

$$\text{where } \det(\gamma_{3,ab})=\left[\frac{1+\cosh(2t)}{2}+(e^{-2t}+\frac{1}{2})x\right]^2, \tag{54}$$

$$\kappa=\det(A)+\det(B)-2\det(C)=m^2+(n+2x)^2+\frac{(m+1)^2}{4} \tag{55}$$

For $t>0$ and $x=\frac{(e^{2t}-1)}{2}$, we obtain $\upsilon<1$ [Mišta Jr. and Korolkova (2009)], therefore the modes a and b are entangled for an arbitrarily small nonzero squeezing.

5 Conclusion

In this paper, from the perspective of quantum discord, we proposed a feasible CVQNC scheme in which a tripartite state is established between sources nodes and target nodes.

By virtue of the CV-EDSS protocol, the scheme achieves quantum entanglement distribution from sources to targets on a butterfly network. The fidelity of the link for transmitting the ancillary modes from sources to targets is $1/2$. Our CVQNC scheme has a larger network throughput than the DVQNC schemes. Security analysis proves that our scheme defends against eavesdropping and forgery which means it can be applied to the case of high security. The proposed CVQNC scheme provides a model for constructing entanglement in quantum network and a guidance for future work.

Funding Statement: This project is supported by the National Natural Science Foundation of China (No. 61571024, No. 61971021), Aeronautical Science Foundation of China (No. 2018ZC51016), and the National Key Research and Development Program of China (No. 2016YFC1000307) for valuable helps.

Conflicts of Interest: There is no conflict of interests or disclose all the conflicts of interest regarding the manuscript submitted.

References

Abeyesinghe, A.; Devetak, I.; Hayden, P.; Winter, A. (2009): The mother of all protocols: restructuring quantum information's family tree. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 465, no. 2108, pp. 2537-2563.

Ahlswede, R.; Cai, N.; Li, S. Y.; Yeung, R. W. (2000): Network information flow. *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204-1216.

Bennett, C. H.; Shor, P. W. (1998): Quantum information theory. *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2724-2742.

Cerf, N. J.; Ipe, A.; Rottenberg, X. (2000): Cloning of continuous quantum variables. *Physical Review Letters*, vol. 85, no. 8, pp. 1754.

Chuan, T.; Maillard, J.; Modi, K.; Paterek, T.; Paternostro, M. et al. (2012): Quantum discord bounds the amount of distributed entanglement. *Physical Review Letters*, vol. 109, no. 7, pp. 070501.

Cubitt, T. S.; Verstraete, F.; Dür, W.; Cirac, J. I. (2003): Separable states can be used to distribute entanglement. *Physical Review Letters*, vol. 91, no. 3, pp. 037902.

DeWitt, B. S.; Graham, N. (2015): *The Many Worlds Interpretation of Quantum Mechanics*. Princeton University Press.

Duan, L. M.; Guo, G. C. (1998): A probabilistic cloning machine for replicating two non-orthogonal states. *Physics Letters A*, vol. 243, no. 5-6, pp. 261-264.

Duan, L. M.; Guo, G. C. (1998): Probabilistic cloning and identification of linearly independent quantum states. *Physical Review Letters*, vol. 80, no. 22, pp. 4999.

Einstein, A.; Podolsky, B.; Rosen, N. (1935): Can quantum-mechanical description of physical reality be considered complete? *Physical Review Letters*, vol. 47, no. 10, pp. 777.

Giedke, G.; Kraus, B.; Lewenstein, M.; Cirac, J. I. (2001): Separability properties of three-mode Gaussian states. *Physical Review A*, vol. 64, no. 5, pp. 052303.

Hayashi, M. (2007): Prior entanglement between senders enables perfect quantum network coding with modification. *Physical Review A*, vol. 76, no. 4, pp. 040301.

Hayashi, M.; Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita, S. (2007): Quantum network coding. *Annual Symposium on Theoretical Aspects of Computer Science*, pp. 610-621.

Li, D. D.; Gao, F.; Qin, S. J.; Wen, Q. Y. (2018): Perfect quantum multiple-unicast network coding protocol. *Quantum Information Processing*, vol. 17, no. 1, pp. 13.

Lindblad, G. (1973): Entropy, information and quantum measurements. *Communications in Mathematical Physics*, vol. 33, no. 4, pp. 305-322.

Madhok, V.; Datta, A. (2013): Quantum discord as a resource in quantum communication. *International Journal of Modern Physics B*, vol. 27, no. 1-3, pp. 1345041.

Mišta Jr., L.; Korolkova, N. (2008): Distribution of continuous-variable entanglement by separable Gaussian states. *Physical Review A*, vol. 77, no. 5, pp. 050302.

Mišta Jr., L.; Korolkova, N. (2009): Improving continuous-variable entanglement distribution by separable states. *Physical Review A*, vol. 80, no. 3, pp. 032310.

Nguyen, H. V.; Babar, Z.; Alanis, D.; Botsinis, P.; Chandra, D. et al. (2017): Towards the quantum internet: Generalized quantum network coding for large-scale quantum communication networks. *IEEE Access*, vol. 5, pp. 17288-17308.

Nielsen, M. A.; Chuang, I. (2007): Quantum computation and quantum information, *Mathematical Structures in Computer Science*, vol. 17, no. 6, pp. 1115-1115.

Ollivier, H.; Zurek, W. H. (2001): Quantum discord: a measure of the quantumness of correlations. *Physical Review Letters*, vol. 88, no. 1, pp. 017901.

Piani, M.; Gharibian, S.; Adesso, G.; Calsamiglia, J.; Horodecki, P. et al. (2011): All nonclassical correlations can be activated into distillable entanglement. *Physical Review Letters*, vol. 106, no. 22, pp. 220403.

Satoh, T.; Le Gall, F.; Imai, H. (2012): Quantum network coding for quantum repeaters. *Physical Review A*, vol. 86, no. 3, pp. 032331.

Serafini, A. (2007): Detecting entanglement by symplectic uncertainty relations. *JOSA B*, vol. 24, no. 2, pp. 347-354.

Shang, T.; Li, K.; Chen, R.; Liu, J. W. (2019): Continuous-variable quantum network coding against pollution attacks. *International Workshop on Quantum Technology and Optimization Problems*, pp. 196-206. Springer.

Shang, T.; Li, K.; Liu, J. W. (2017): Continuous-variable quantum network coding for coherent states. *Quantum Information Processing*, vol. 16, no. 4, pp. 107.

Shang, T.; Pei, Z.; Chen, R.; Liu, J. (2019): Quantum homomorphic signature with repeatable verification. *Computers, Materials & Continua*, vol. 59, no. 1, pp. 149-165.

Wang, F.; Luo, M. X.; Xu, G.; Chen, X. B.; Yang, Y. X. (2018): Photonic quantum network transmission assisted by the weak cross-Kerr nonlinearity. *Science China Physics, Mechanics & Astronomy*, vol. 61, no. 6, pp. 060312.

Wiseman, H. M. (2013): Quantum discord is Bohr's notion of non-mechanical disturbance introduced to counter the Einstein-Podolsky-Rosen argument. *Annals of Physics*, vol. 338, pp. 361-374.