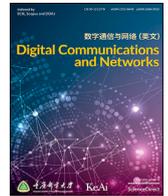




Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Information security through controlled quantum teleportation networks

Hala Hamdoun^{a,1}, Alaa Sagheer^{a,b,*}^a Center for Artificial Intelligence and Robotics (CAIRO), Department of Computer Science, Aswan University, Aswan, Egypt^b Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Saudi Arabia

ARTICLE INFO

Keywords:

Information security
Machine-to-machine communication
Intelligent secure systems
Quantum teleportation
Quantum networks

ABSTRACT

Information security is the backbone of current intelligent systems, such as the Internet of Things (IoT), smart grids, and Machine-to-Machine (M2M) communication. The increasing threat of information security requires new models to ensure the safe transmission of information through such systems. Recently, quantum systems have drawn much attention since they are expected to have a significant impact on the research in information security. This paper proposes a quantum teleportation scheme based on controlled multi-users to ensure the secure information transmission among users. Quantum teleportation is an original key element in a variety of quantum information tasks as well as quantum-based technologies, which plays a pivotal role in the current progress of quantum computing and communication. In the proposed scheme, the sender transmits the information to the receiver under the control of a third user or controller. Here, we show that the efficiency of the proposed scheme depends on the properties of the transmission channel and the honesty of the controller. Compared with various teleportation scheme presented recently in the literature, the most important difference in the proposed scheme is the possibility of suspicion about the honesty of the controller and, consequently, taking proper precautions.

1. Introduction

The new technologies, such as the Internet of Things (IoT), smart grids, and Machine-to-Machine (M2M) communication, herald a new era of computing whereby every conceivable object is equipped with, or connected to, a smart device, allowing a series of data and electronic information to be transmitted through the Internet [1,2]. This information is processed intelligently to create new services for users. Accordingly, the scope of security risks is expanded, and the risk of compromise of electronic information is increasing. In order to cope with this risk, research and investment in the field of electronic information security have been growing steadily, and various security paradigms are being steadily developed [3].

Information security refers to protecting information and systems from dishonest or unauthorized access and disruptions. Previously, information security issues have been studied in a technological context [4], but the growing threat of information security has extended researchers' attention to exploring reliable solutions and new paradigms that ensure secure information transmission [5,6]. Recently, quantum systems are promoting the technological revolution in the fields of computing and networking.

Regarding computation, the proper use of quantum computation opens up new possibilities. It makes feasible solutions to some problems that are computationally intractable to the classical networks and computers, such as factoring large numbers, detecting eavesdropping, and many other issues. There is no doubt that quantum networks and quantum computing systems will hybridize very soon, allowing applications to select the most efficient mechanism for accomplishing a particular function [7]. For networking, it is widely demonstrated that quantum networks will significantly affect the information security [8]. Like its classical counterpart, the quantum network supports the movement of information or data from place to place for the sake of distributed computation. The motivation for doing so is the same for both quantum and classical networks, such as the desire to connect people, to connect devices such as sensors or computers to share databases in separate locations, to name just a few. However, there are two significant differences between classical and quantum networking techniques, namely, the data type and the data transfer mechanism [9]. Regarding the data type, quantum networks, and thereby quantum computation, use the quantum bit that is usually called a qubit, rather than the classical bits used in classical computation. As for the transfer mechanism, it is called teleportation in quantum networks [9,10]. Quantum Teleportation (QT)

* Corresponding author.

E-mail addresses: hala@aswu.edu.eg (H. Hamdoun), asagheer@kfu.edu.sa (A. Sagheer).¹ Hala Hamdoun is a PhD candidate in computer engineering.

<https://doi.org/10.1016/j.dcan.2020.04.009>

Received 3 October 2018; Received in revised form 11 February 2020; Accepted 19 April 2020

Available online 4 June 2020

2352-8648/© 2020 Chongqing University of Posts and Telecommunications. Publishing Services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an

open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

is the crux of quantum networks for 20 years [11]. QT enables unknown quantum states to be teleported (or transferred) reliably from one object to another over a long distance, without the physical movement of the object itself (A recent article teleported quantum states across a distance of 1400 km [12]). Experimentally, the information encoded in quantum light moves and is reconstructed remotely, while the sender device remains in its original position. Here, the receiver, usually called Bob, can be any form of physical device different from the sender, who is commonly known as Alice [13]. In contrast, classical communication exchanges information by physically copying data and transmitting the copy. The rules of quantum mechanics prohibit the creation of independent copies of unknown arbitrary quantum information. Accordingly, from the perspective of information security, quantum networks are much safer than classical networks [7–14].

Since the early seminal work of Bennett et al. [15], which allowed teleportation of an arbitrary qubit between two remote locations, scientists have made noticeable progress with QT in both theoretical studies [16,17] and experimental applications [10,18,19]. The idea of quantum teleportation was generalized by Karlsson et al. to be Controlled Quantum Teleportation (CQT) [20]. Later on, with the rapid development of networking, the application of CQT in the field of information security has received extensive attention [6,21]. The principle of CQT is that the encoded information can be teleported successfully from a sender Alice to a receiver Bob only with the permission and further collaboration of the third user Charlie as a controller or supervisor [22]. This kind of information transmission can be extended to sharing a quantum secret among several receivers, which is the same as quantum state sharing [23]. Since CQT is very useful in cryptographic conferences and quantum networks, it has become a particularly interesting subject in recent years compared with the typical QT [22,23]. However, most recent contributions in CQT assumed the cooperation of all users of the networks. In other words, without the help and cooperation of Charlie, the teleportation process between Alice and Bob cannot be realized [22–24]. Intuitively, this limitation is not usually the case, especially when there is a suspicion that the controller is dishonest and, consequently, information security is at risk or, at least, the receiver Bob may not get the original information in a correct manner. In this paper, we propose that a multi-user-based CQT scheme achieves information transmission successfully. We analyze the security of the proposed scheme and discuss whether the controller is honest or dishonest. The efficiency of the proposed scheme is discussed by calculating the transmission fidelity of the teleported information in both cases, i.e. when the controller is either honest or dishonest. In addition, we investigate the robustness of the utilized channel in the presence of a dishonest controller, assuming the worst scenario. This paper is organized as follows: section 2 shows a few basic concepts in the quantum world that will help the reader to go through the paper. Section 3 provides a broad literature review and the motivation for writing this paper. Section 4 shows the proposed teleportation scheme. The efficiency of the proposed scheme is investigated in section 5. Finally, section 6 presents an overall discussion and conclusion of the paper.

2. Basic concepts from the quantum world

This section highlights the most important concepts in the area of quantum information that may help the reader to follow the paper. A classical bit is a kind of physical system that has two stable Boolean states: 0 and 1. Quantum bit, is a quantum system in which the Boolean states 0 and 1 are represented by a prescribed pair of normalized and mutually orthogonal quantum states labeled as $|0\rangle$ and $|1\rangle$. Qubits derive their extraordinary power from the coherent quantum superposition of both states. Actually, this phenomenon which is called *quantum parallelism* allows the states to be both 0 and 1 at the same time.

A collection of n qubits is called a *quantum register* of size n . A *quantum*

logic gate is a device that performs a fixed unitary operation on selected qubits in a fixed period. *Quantum network* is a device consisting of quantum logic gates whose computational steps are synchronized in time. *Entanglement* is a new kind of correlation between two or more subsystems of quantum systems [25]. It is a main ingredient of quantum communication theory that does not exist in any classical system. The basic idea of quantum entanglement is that two qubits can be intimately linked to each other even if they are separated by billions of light-years of space; a change induced in one qubit will affect the other. From entanglement comes the power of teleportation, which is based on entanglement and a classical channel [25].

Simply, *teleportation* can be defined as the process of transmitting quantum information from one location to another with the help of classical communication and a previously shared quantum channel between the sending and receiving locations. *Quantum channel* is a communication channel that can transmit quantum information and classical information. An example of quantum information is the state of a qubit. This qubit may be either in the normal (non-accelerated) state or the accelerated state. Physically, qubits take the form of photons resulting from changes in the electric field.

An important concept related to the teleportation is the transmission fidelity, which is also an essential part of communication theory. For any given communication scheme, the transmission fidelity is a quantitative measure of the accuracy of transmission. In other words, it measures whether the transmitted information is the same as the information sent or there is something missing during the teleportation. In this paper, we measure the transmission fidelity in order to investigate the efficiency and security of the controlled teleportation.

3. Literature review and motivation

Research work on quantum networking can be said to begin with Bennett's protocol, which originated around 1996. In the Bennet scheme, the quantum channel includes two qubits only, specifically, two users Alice and Bob [15]. The communication scheme runs when Alice applies a Bell measurement on her own qubit and the qubit of the unknown quantum information. Then, Bob reconstructs the unknown quantum information by applying an adequate unitary operation on his qubit according to Alice's measurement result.

The QT of single-qubit information using three-qubit information can be realized with two possible schemes: Standard Quantum Teleportation (SQT) and CQT [26]. In the former scheme, Alice gets two qubits of the shared information, whereas Bob gets only one qubit. Alice takes a Bell measurement on her qubits and then sends, via a classical channel, the result to Bob. To get an exact copy of the information sent, Bob performs an appropriate unitary transformation on his own qubit [26].

In the second scheme, Alice, Bob and the third user Charlie, share their qubits. The benefit of the third user here is to enhance the security of the teleportation process. For this reason, the teleportation process is called CQT, where Charlie has full control over the teleportation process and is considered a supervisor. It is widely demonstrated that CQT is very useful for the expected quantum computers [26,27]. Therefore, this article focuses on CQT.

CQT runs when Alice measures the standard two-qubit Bell measurement on her two qubits, and Charlie measures his qubit on the orthogonal basis of a single qubit. Both Alice and Charlie send their measurement results to Bob, who then performs a single transformation on his qubits to produce an exact copy of the information being sent. It is clear that if Charlie is not involved, Bob can never construct a copy of the original information. In other words, assuming that a fourth user (such as the eavesdropper) can successfully steal the particles of Alice and Bob successfully, the eavesdropper can never construct the original information because Charlie's role is mandatory for this operation [22,24,26].

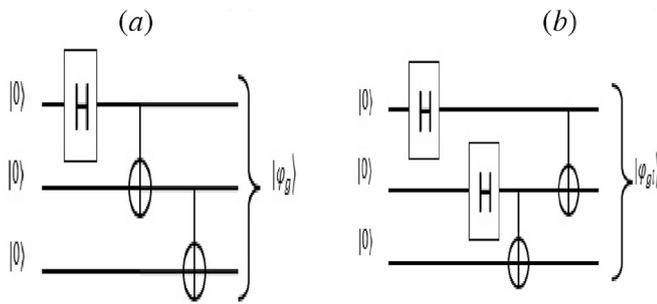


Fig. 1. (a) A quantum circuit for GHZ state generation. (b) A quantum circuit for GHZ-like state generation.

Due to its importance, CQT has attracted much concern. The first contribution was introduced by Karlsson et al. in Ref. [20], where the unknown information could be sent to one receiver according to the controller’s measurement outcome. After Karlsson’s scheme, many CQT protocols were proposed for teleporting unknown information using different quantum channels. For example, in Refs. [24,28], the authors applied a three-user CQT using three-qubits. The authors in Ref. [29] presented a general idea of constructing methods for multi-qubit quantum teleportation between two remote users with the control of other agents.

In [30], the authors proposed an improved CQT scheme using the quantum entanglement swapping procedure. The scheme assumes that Bob is dishonest and he is recognized by the trusted Charlie. So, after Alice gets the feedback information from Charlie, she can confirm Bob’s identity and send the quantum information to Bob. The scheme can effectively prevent the counterfeit identity attacks to ensure the security of quantum teleportation. Finally, in Ref. [22], the authors designed a quantum circuit that can construct information suitable for perfect CQT. They evaluated their scheme by calculating three items: teleportation transmission fidelity, success probability, and the controller’s power.

On the other hand, most previous studies have assumed that three users are in the normal or non-accelerated frame. However, the modern world exhibits complex and dynamic structures, which are difficult to handle with simple or general models. As such, modern applications of quantum communication may require more than one user so that all users of the quantum network are in an accelerated state [31]. In fact, the idea of having more than one accelerated qubits or users is not new in the field of quantum teleportation. In 2004, Alsing et al. presented the first teleportation scheme with a uniformly accelerated qubit [32]. Since then, many authors focused on this interdisciplinary field [33,34]. The authors of the current paper proposed a contribution using accelerated users to achieve the quantum teleportation task [35]. The current paper is an extension of that contribution.

From this brief review, it is clear that most of the previous works concerned with CQT assume that the three users, Alice, Bob and Charlie, are in cooperation [20,23,36]. However, it is possible that the controller Charlie may be dishonest and, consequently, the receiver Bob may not get the original information in the correct way. In this case, many questions are raised. What about information security? What happens if all three users are in the accelerated frame?

Both of these questions and the need to build a secure quantum communication network have prompted the authors of this paper to conduct a more in-depth study of the controlled teleportation scheme. Accordingly, the subject of this paper is to investigate the behavior of controlled quantum teleportation in both cases of the controller, either he/she is honest or dishonest. Also, this paper tries to find out a suitable communication channel in various situations. These concerns are addressed in this paper in terms of accelerated users.

4. The proposed teleportation scheme

This section addresses the proposed scheme that is an extension of our previous scheme published recently in Ref. [35]. And It is worth emphasizing that the main contribution of the current paper is that it considers the dishonest situation of the controller or the third user, whereas our previous work [35] assumed that all users are honest. In this case, we assume that the users share three types of qubit states with GHZ and GHZ-like states in different categories. Fig. 1 illustrates two circuits showing that both of these states can be generated, via local operations, as Hadamard gate and Controlled NOT (CNOT) gate.

Simply, the Hadamard gate transfers the state $|0\rangle$ or $|1\rangle$ into an equal superposition $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. The operation of CNOT gate operates on two qubits, which simply flips the state of the second qubit if and only if the first qubit is in state $|1\rangle$. It means that keeping the first qubit unchanged if it is in state $|0\rangle$. By applying these gates, as shown in Fig. 1, we can get the state vectors of the GHZ and GHZ-like states, which can be described as follows:

$$|\psi_g\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$

$$|\psi_{g\ell}\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle) \tag{1}$$

4.1. Preparing the quantum channels

Since we are interested in using the accelerated quantum qubit states to perform teleportation, we assume that the qubit states in Eq. (4) evolve in the acceleration, non-inertial frame, according to the following transformations:

$$|0_k\rangle_M = \cos r |0_k^+\rangle_I |0_k^-\rangle_{II} + \sin r |1_k^+\rangle_I |1_k^-\rangle_{II},$$

$$|1_k\rangle_M = |1_k^+\rangle_I |0_k^-\rangle_{II} \tag{2}$$

where $k = 0, 1, 2$ and 3 stand for the teleported information qubit, the first, second and third qubit of channel, respectively. The definition of the acceleration for one qubit with respect to the others, r , is given by $\tan r_k = \exp[-\pi\omega_k c/a_k]$, where $0 \leq r_k \leq \pi/4$. The parameter a_k is the acceleration of the qubits with respect to the speed of light, where $0 \leq a_k \leq \infty$. The parameter ω_k represents the frequency of the traveling qubit, and c represents the speed of light. The parameters $|n\rangle_I$ and $|n\rangle_{II}$ ($n = 0, 1$) indicate two causally disconnected regions in the Rindler space [37,38]. It is assumed that each of the two described quantum qubit states represents a channel that contains three qubits, where each qubit represents a user moving in a uniform acceleration. Using the transformation in Eq. (4.1), we get the final state in both Rindler regions I and II . By tracing out the quantum qubit states in the second region II , we get the final accelerated quantum qubit state in region I [39] of each quantum qubit state as follows:

1. The accelerated quantum GHZ-state in the first region, $\rho_g^{(I)}$, is described by an 8×8 matrix, where the non-zero elements are given as:

$$\begin{aligned} \rho_g^{(11)} &= C_1^2 C_2^2 C_3^2, & \rho_g^{(22)} &= C_2^2 C_3^2 S_1^2, \\ \rho_g^{(33)} &= C_1^2 C_3^2 S_2^2, & \rho_g^{(44)} &= C_3^2 S_1^2 S_2^2, \\ \rho_g^{(55)} &= C_1^2 C_2^2 S_3^2, & \rho_g^{(66)} &= C_2^2 S_1^2 S_3^2, \\ \rho_g^{(77)} &= C_1^2 S_2^2 S_3^2, & \rho_g^{(88)} &= S_1^2 S_2^2 S_3^2 + 1, \\ \rho_g^{(81)} &= \rho_g^{(18)} &= C_1 C_2 C_3 \end{aligned} \tag{3}$$

2. The accelerated quantum GHZ-like state in the first region, $\rho_{g\ell}^{(t)}$, is described by an 8×8 matrix, where the non-zero elements, in this case, are given as:

$$\begin{aligned}
 \rho_{g\ell}^{(22)} &= C_2^2 C_3^2, \rho_{g\ell}^{(25)} = \rho_{g\ell}^{(52)} = C_1 C_3 C_2^2, \\
 \rho_{g\ell}^{(23)} &= \rho_{g\ell}^{(32)} = C_1 C_2 C_3^2, \\
 \rho_{g\ell}^{(28)} &= \rho_{g\ell}^{(82)} = C_2 C_3, \\
 \rho_{g\ell}^{(33)} &= C_1^2 C_2^2, \rho_{g\ell}^{(35)} = \rho_{g\ell}^{(53)} = C_2 C_3 C_1^2, \\
 \rho_{g\ell}^{(38)} &= \rho_{g\ell}^{(38)} = C_1 C_3, \\
 \rho_{g\ell}^{(44)} &= S_2^2 C_3^2 + S_1^2 C_2^2, \\
 \rho_{g\ell}^{(47)} &= \rho_{g\ell}^{(74)} = C_1 C_3 S_2^2, \\
 \rho_{g\ell}^{(46)} &= \rho_{g\ell}^{(64)} = C_2 C_3 S_1^2, \\
 \rho_{g\ell}^{(55)} &= C_1^2 C_2^2, \rho_{g\ell}^{(58)} = \rho_{g\ell}^{(85)} = C_2 C_2 C_3, \\
 \rho_{g\ell}^{(66)} &= S_1^2 C_2^2 + S_3^2 C_2^2, \\
 \rho_{g\ell}^{(67)} &= \rho_{g\ell}^{(76)} = C_1 C_2 S_3^2, \\
 \rho_{g\ell}^{(77)} &= S_2^2 C_1^2 + S_3^2 C_1^2, \\
 \rho_{g\ell}^{(88)} &= S_1^2 (S_2^2 + S_3^2) + S_2^2 S_3^2 + 1
 \end{aligned}
 \tag{4}$$

where $C_k = \cos r_k, S_k = \sin r_k$ and $k = 1, 2, 3$ are the first, second, and third qubit of the corresponding channel, respectively.

4.2. Describing the proposed scheme

Now, after preparing the multi-qubit accelerated channels, the users are ready to perform the controlled quantum teleportation scheme [35]. A schematic diagram of the proposed teleportation scheme is depicted in Fig. 2. The locations of the three qubits named Alice, Bob and Charlie, are entangled with each other via a quantum channel. And the quantum information can be transmitted from one location to another, with the help of the classical communication and the previously shared quantum entanglement among the three locations. We can summarize the

proposed scheme into the following steps:

1. Alice combines the teleported state with her accelerated qubit.
2. Alice performs Bell Measurements (BM) on her two qubits.
3. Charlie makes the Von Neuman measurement on his qubit, then he and Alice send their measurements to Bob. This will help Bob to recover the teleported information.
4. Based on Alice’s and Charlie’s measurements, Bob applies one of the appropriate unitary operations, such as bit-flip (X), phase flip (Z), or bit-phase flip (Y) qubit operation, to get the initial teleported information.

Suppose that the information which Alice wishes to teleport to Bob is coded in quantum qubit $|+\rangle$ or $|-\rangle$,

$$\begin{aligned}
 |+\rangle &= \alpha|0\rangle_0 + \beta|1\rangle_0, \\
 |-\rangle &= \alpha|0\rangle_0 - \beta|1\rangle_0
 \end{aligned}
 \tag{5}$$

where $|\alpha|^2 + |\beta|^2 = 1$. Qubit 0 denotes the qubit which contains the coded information of the message that will be teleported, and qubits 1, 2 and 3 denote the three qubits of quantum channels that belong to Alice, Bob, and Charlie, respectively.

Now, we proceed to describe how the controller (Charlie) controls the teleportation of information between the sender (Alice) and the receiver (Bob), where the users share the accelerated channels which are described by Eq.(4.1), Eq.(4.1), and Eq.(4.2) for the GHZ and GHZ-like states, respectively.

1. The accelerated GHZ-state

Let us assume that the users share the accelerated GHZ state given in Eq.(4.1) as a quantum channel. In order to teleport the information, which is coded in Eq.(4.2), the users follow the steps as described in the proposed scheme. Table 1 shows the appropriate operations which can be performed by each user [35].

2. The accelerated GHZ-like state

In this case, the accelerated GHZ-like state, which is given in Eq.(4.1),

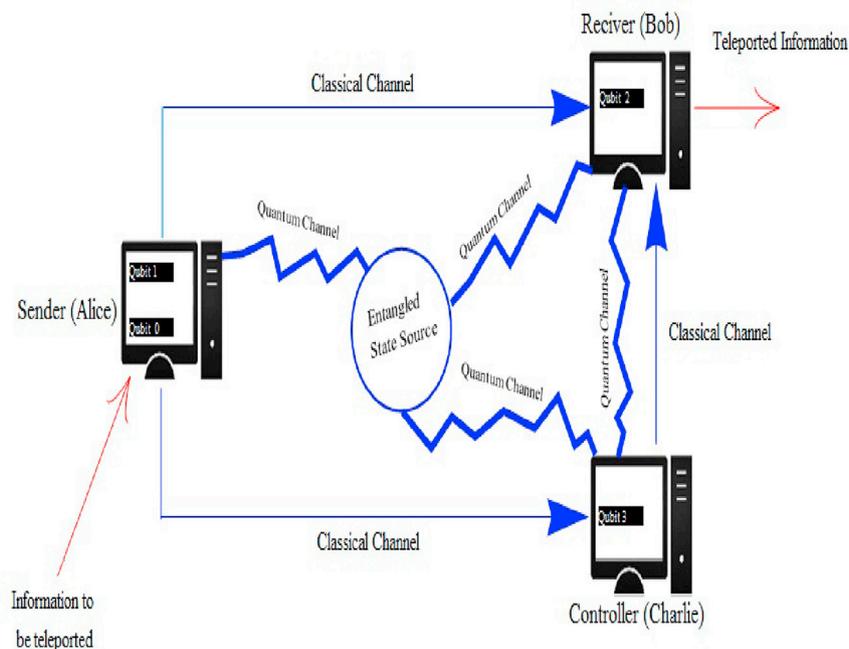


Fig. 2. A schematic diagram of the teleportation process [35].

is used as a quantum channel to perform the quantum teleportation scheme. Bob can retrieve the information by applying the appropriate operation depending on Alice’s and Charlie’s measurements, as shown in Table 2.

5. Efficiency of the proposed scheme

To investigate the effectiveness of the proposed scheme, we need to calculate the transmission fidelity of the teleported information. Fidelity is a quantum measurement method used to express the probability that one state passes a test to identify another state. For this reason, fidelity is called the transition probability.

Since the users cooperate to teleport the coded state from Alice to Bob, the transmission fidelity of the teleported state depends on the honesty or dishonesty of the controller. Mathematically, the transmission fidelity $\mathcal{F} = \text{tr}\{\rho_{\text{initial}}\rho_{\text{final}}\}$, where ρ_{initial} is given by the quantum qubit state of the coded information, and ρ_{final} is given by the quantum qubit state of the corresponding channel at Bob’s side. Therefore, we may have one of the following two cases.

5.1. Case of an honest controller

For the accelerated GHZ state, Bob can end the teleportation scheme by applying an adequate operation from those given in Table 1 in order to retrieve the teleported information. Bob gets the coded information with a transmission fidelity that depends on both Alice’s and Charlie’s measurements. For example, here we will consider two different cases of Alice’s measurements. Namely, we will consider the two cases when Alice measures ρ_{ψ}^+ and ρ_{ϕ}^+ , where Charlie’s measurement is x_+ in both cases. The transmission fidelity of the teleported information in the case of an honest controller is \mathcal{F}_{GHZ}^H . Then, \mathcal{F}_{GHZ}^H for both of Alice’s measurements, ρ_{ψ}^+ and ρ_{ϕ}^+ , is given respectively as:

$$\mathcal{F}_{GHZ}^H = (\alpha^4 C_1^2 C_2^2 (C_3^2 + S_3^2) + \alpha^2 \beta^2 S_1^2 C_2^2 (C_3^2 + S_3^2) + 2\alpha^2 \beta^2 C_1 C_2 C_3 + \alpha^2 \beta^2 C_1^2 S_2^2 (C_3^2 + S_3^2) + \beta^4 S_1^2 S_2^2 (C_3^2 + S_3^2) + \beta^4) \tag{6}$$

$$\mathcal{F}_{GHZ}^H = \alpha^4 S_1^2 S_2^2 (C_3^2 + S_3^2) + \alpha^2 \beta^2 C_1^2 S_2^2 (C_3^2 + S_3^2) + \alpha^2 \beta^2 S_1^2 C_2^2 (C_3^2 + S_3^2) + \beta^4 C_1^2 C_2^2 (C_3^2 + S_3^2) + 2\alpha^2 \beta^2 C_1 C_2 C_3 + \alpha^4 \tag{7}$$

Fig. 3 shows the behavior of transmission fidelity in the case of using GHZ state as a quantum channel. In the case of using GHZ-like state as a quantum channel, Bob gets the coded information with a transmission fidelity that depends on both Alice’s and Charlie’s measurements, similar to GHZ state. Here, we will also consider Alice measurements. Namely, we will consider the two cases when Alice measures ρ_{ψ}^+ and ρ_{ϕ}^+ , where Charlie’s measurement is 0 in both cases. The transmission fidelity of the teleported information in the case of an honest controller is \mathcal{F}_{gl}^H . Then,

Table 1 Bob’s unitary operations when Charlie measures at x-direction.

Alice’s measure	Charlie’s measure	Resulted state	Bob operation
ρ_{ψ}^-	x_+	$\alpha 0\rangle_0 + \beta 1\rangle_0$	I
ρ_{ψ}^+	x_+	$\alpha 0\rangle_0 - \beta 1\rangle_0$	Z
ρ_{ϕ}^-	x_+	$\alpha 1\rangle_0 + \beta 0\rangle_0$	X
ρ_{ϕ}^+	x_+	$\alpha 1\rangle_0 - \beta 0\rangle_0$	Y
ρ_{ψ}^-	x_-	$\alpha 0\rangle_0 + \beta 1\rangle_0$	Z
ρ_{ψ}^+	x_-	$\alpha 0\rangle_0 - \beta 1\rangle_0$	I
ρ_{ϕ}^-	x_-	$\alpha 1\rangle_0 + \beta 0\rangle_0$	Y
ρ_{ϕ}^+	x_-	$\alpha 1\rangle_0 - \beta 0\rangle_0$	X

Table 2 Bob’s unitary operations when Charlie measures “0” or “1”.

Alice’s measure	Charlie’s measure	Resulted state	Bob operation
ρ_{ψ}^+	0	$\alpha 1\rangle_0 + \beta 0\rangle_0$	X
ρ_{ψ}^-	0	$\alpha 1\rangle_0 - \beta 0\rangle_0$	Y
ρ_{ϕ}^+	0	$\alpha 0\rangle_0 + \beta 1\rangle_0$	I
ρ_{ϕ}^-	0	$\alpha 0\rangle_0 - \beta 1\rangle_0$	Z
ρ_{ψ}^+	1	$\alpha 0\rangle_0 + \beta 1\rangle_0$	I
ρ_{ψ}^-	1	$\alpha 0\rangle_0 - \beta 1\rangle_0$	Z
ρ_{ϕ}^+	1	$\alpha 1\rangle_0 + \beta 0\rangle_0$	X
ρ_{ϕ}^-	1	$\alpha 1\rangle_0 - \beta 0\rangle_0$	Y

\mathcal{F}_{gl}^H for both Alice’s measurements, ρ_{ψ}^+ and ρ_{ϕ}^+ , is given respectively as:

$$\mathcal{F}_{gl}^H = (\alpha^4 C_1^2 C_3^2 + \alpha^2 \beta^2 S_1^2 C_3^2 + \alpha^2 \beta^2 S_2^2 C_3^2 + \beta^4 C_2^2 C_3^2 + 2\alpha^2 \beta^2 C_1 C_2 C_3^2) \tag{8}$$

$$\mathcal{F}_{gl}^H = \alpha^4 C_2^2 C_3^2 + \alpha^2 \beta^2 C_3^2 (S_1^2 + S_2^2) + \beta^4 C_1^2 C_3^2 + 2\alpha^2 \beta^2 C_1 C_2 C_3^2 \tag{9}$$

Fig. 4 shows the behavior of transmission fidelity in the case of using GHZ-like state as a quantum channel. It is clear from Figs. 3 and 4 that the performance of the transmission fidelity is identical, to some extent, in both cases using GHZ or GHZ-like states.

Toward a deeper insight, Fig. 5 shows a comparison of transmission fidelity behaviours of the teleported information, which is coded in the qubit given in (4.2), where we assume that the users are accelerated with the same acceleration, namely, $r_a = r_b = r_c = r$, and Alice’s measurement is ρ_{ψ}^+ . It is clear that the fidelities are maximum when all qubits are in rest. However, the fidelities begin to decrease gradually until they reach their minimum bounds when the acceleration r_i of qubits reaches 0.8. In addition, the upper bound of transmission fidelity using the accelerated GHZ-state is larger than the upper bound shown when the users share the accelerated GHZ-like state. Therefore, we can conclude that the efficiency of the controlled quantum teleportation scheme is much better when the partners use GHZ-state as the quantum channel.

5.2. Case of a dishonest controller

In this case, we are doubtful about the authentication of the controller Charlie. In other words, Charlie is dishonest and, thereby, sends an incorrect measurement to Bob. Consequently, Bob ends the protocol by applying an adequate operation given in Table 1 according to Charlie’s measurement. Here, we consider that the users share the accelerated GHZ-state, which is given in Eq. (4.1), and Alice measures ρ_{ψ}^+ , whereas Charlie’s measurement is x_- . Then, the transmission fidelity of the teleported information in the case of a dishonest controller \mathcal{F}_{GHZ}^{DH} is given as:

$$\mathcal{F}_{GHZ}^{DH} = (\alpha^4 S_1^2 S_2^2 (C_3^2 + S_3^2) + \alpha^2 \beta^2 C_1^2 S_2^2 (C_3^2 + S_3^2) - 2\alpha^2 \beta^2 C_1 C_2 C_3 + \alpha^2 \beta^2 S_1^2 C_2^2 (C_3^2 + S_3^2) + \beta^4 C_1^2 C_2^2 (C_3^2 + S_3^2) + \alpha^4) \tag{10}$$

On the other hand, if the users share the accelerated GHZ-like state, which is given in Eq. (4.1), and Charlie plays the role of a dishonest controller, then Bob will get the coded information with a transmission fidelity depending on both Alice’s and Charlie’s measurements. For example, if Alice measures ρ_{ψ}^+ and Charlie measures 1, then the transmission fidelity of the teleported information in the case of a dishonest controller \mathcal{F}_{gl}^{DH} is given as:

$$\mathcal{F}_{gl}^{DH} = A^4 C_2^2 (S_1^2 + S_3^2) + A^2 B^2 C_1^2 C_2^2 + A^2 B^2 (S_1^2 S_2^2 + S_1^2 S_3^2 + S_2^2 S_3^2 + 1) + B^4 C_1^2 (S_2^2 + S_3^2) + 2A^2 B^2 C_1 C_2 S_2^2 + 2A^2 B^2 C_1 C_2 \tag{11}$$

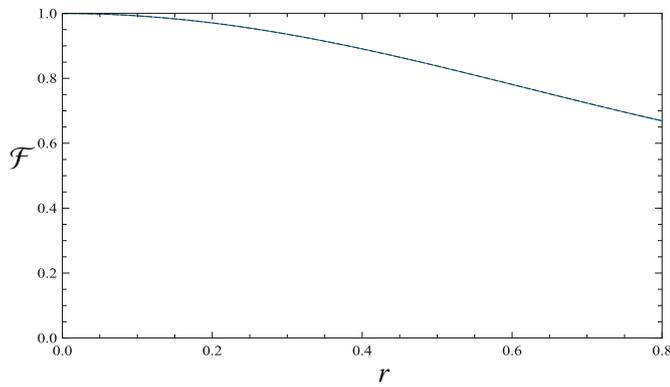


Fig. 3. The transmission fidelity of information $|+\rangle$, in the case of an honest controller using GHZ state, when Alice measures ρ_{ψ}^+ (solid line), and when Alice measures ρ_{ϕ}^+ (dashed line), where $\alpha^2 = \beta^2 = 0.5$.

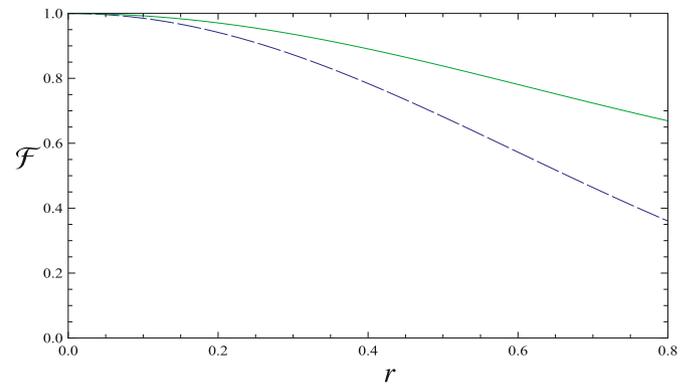


Fig. 5. The transmission fidelity of information $|+\rangle$, in the case of an honest controller using GHZ state (solid line) and GHZ-like state (dashed line), where $\alpha^2 = \beta^2 = 0.5$.

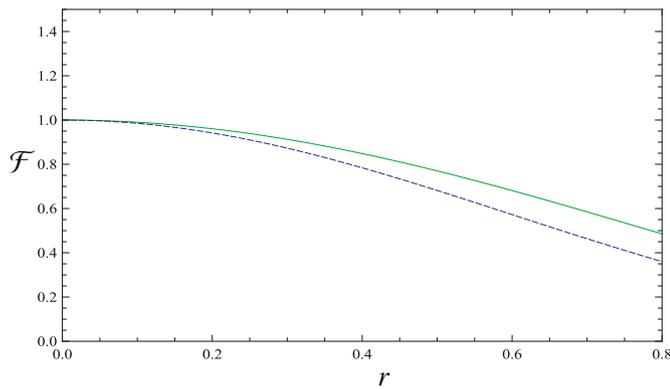


Fig. 4. The transmission fidelity of information $|+\rangle$, in the case of an honest controller using GHZ-like state, when Alice measures ρ_{ψ}^+ (solid line), and when Alice measures ρ_{ϕ}^+ (dashed line), where $\alpha^2 = \beta^2 = 0.5$.

The fidelity behaviors of the teleported state given in Eq. (10) for GHZ state and Eq. (11) for GHZ-like state are shown in Fig. 6. In the case of GHZ state, it is clear that at acceleration $r_i = 0$, the transmission fidelity $\mathcal{F}_{GHZ}^{DH} = 0$, which means that there is no information received at Bob's side. Then, the transmission fidelity increases as acceleration r_i increases gradually till it reaches its maximum bound at $r_i = 0.8$. In contrast, in the case of GHZ-like state, the transmission fidelity $\mathcal{F}_{gl}^{DH} = 1$ when all particles are inactivated, i.e., non-accelerated ($r_i = 0$). However, as r_i increases, the transmission fidelity \mathcal{F}_{gl}^{DH} decreases gradually till it reaches its minimum bound at $r_i = 0.8$.

According to Figs. 5 and 6, it is clear that using the accelerated GHZ state as a quantum channel to achieve quantum teleportation is much better than using the accelerated GHZ-like state when we are confirmed that the controller or the third user is honest. This may coincide with most contributions in literature, which shows that the standard GHZ state is optimum for CQT. However, GHZ's behavior changes dramatically when there is a doubt about security, i.e., when the controller is dishonest or non-authenticated. The proposed scheme here shows that GHZ-like state is more robust than the standard GHZ state against the dishonesty or authenticity of the controller.

It is worth to mention that the above comparison between GHZ and GHZ-like states when the controller Charlie is dishonest assumes that Charlie has the same acceleration value as both Alice (r_a) and Bob's (r_b) have, as depicted in Fig. 7. Here, Fig. 7(a) describes the behavior of \mathcal{F}_{GHZ}^{DH}

where the three partners use the accelerated GHZ-state as a quantum channel. It is clear that the transmission fidelity increases as the acceleration of the controller (r_c) increases. However, when the three qubits are accelerated with the same acceleration (i.e., $r_a = r_b = r_c = r$), the performance is finally improved (after $r = 0.5$).

For the case that GHZ-like state is used as a quantum channel, and the controller is still dishonest, the behavior is different. It is clear that as r_c increases, the transmission fidelity \mathcal{F}_{gl}^{DH} decreases for smaller values of $r_a = r_b = r$. However, for larger values (i.e., 0.1, and then 0.3) of the sender's and the receiver's acceleration, the performance can be improved by decreasing the acceleration of the dishonest controller.

6. Discussion and conclusion

It is widely agreed that quantum teleportation is a cornerstone in a variety of quantum-based technologies, such as quantum networks, quantum communication, and quantum computing. It is generalized into a controlled quantum teleportation scheme in which a third user, namely the controller, supervises the information transmission between the sender and the receiver. Most of the contributions in the literature adopted the standard GHZ state as a quantum channel and assumed that the controller should be honest and cooperate with other users in order to achieve information transmission protocol. In addition, they assumed that the three users are inactive, i.e., non-accelerated.

This paper presents a new scheme that can perform the controlled quantum teleportation using both GHZ and GHZ-like states as quantum channels. Using the fidelity transmission, we confirm the result

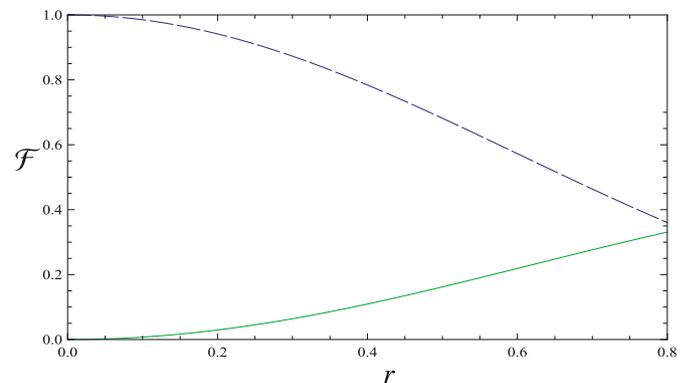


Fig. 6. The transmission fidelity of information $|+\rangle$, in the case of a dishonest controller using the GHZ state (solid line) and GHZ-like state (dashed line), where $\alpha^2 = \beta^2 = 0.5$.

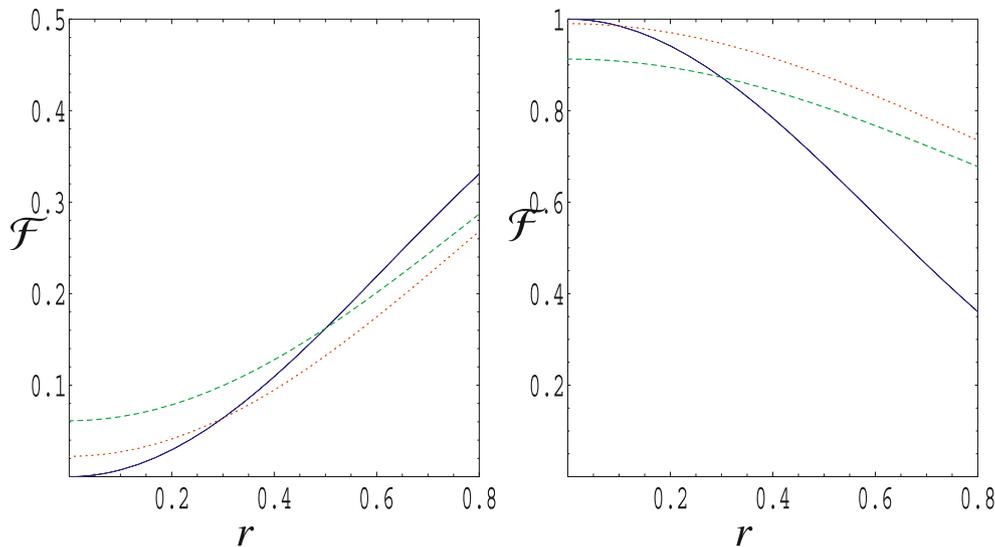


Fig. 7. The transmission fidelity of information $|+\rangle$, where it is assumed that the controller is dishonest: (a) For GHZ state and (b) for GHZ-like state. The solid, dot and dash curves are for $r_c = r, 0.1$ and 0.3 , respectively.

accomplished by most contributions in the literature, that is, GHZ state is the best quantum channel when the network users cooperate to transmit the information from the sender to the receiver. In this case, the fidelity of the teleported information decreases as the acceleration of the three users increases according to the type of the channel used. If the channel used is the accelerated GHZ-like state, the decay rate of the fidelity is greater than that when the channel is GHZ state.

The most important contribution of this paper is that it focuses on the situation where there is no evidence about the honesty of the controller or the third user. We show that in such a case, the GHZ-like state is the best quantum channel that can be used. Compared with the standard GHZ network, the fidelity transmission via the accelerated GHZ-like network is higher than that of the accelerated GHZ network. That is to say, under zero acceleration, the fidelity transmission via GHZ-like state is maximum, whereas it is zero via GHZ state. As the acceleration increases, the fidelity increases gradually when the accelerated GHZ state is used and decreases for the GHZ-like state.

Overall, we show here that the minimum bound of the fidelity of the accelerated GHZ-like state is still greater than the upper bound that depicted for the accelerated GHZ state, which gives the makes the previous state more advantageous. Furthermore, there is a possibility to improve the fidelity of the teleported state by decreasing the acceleration of the controller while increasing the acceleration of the sender and the receiver.

The impact of the proposed scheme is that it can be utilized to construct secure controlled quantum channels, which will be useful to future quantum computers. The efficiency of the proposed teleportation scheme is quantified by evaluating the fidelity of the teleported information. Since information security is concerned in this paper, it is worth mentioning that the different quantitative models starting from decision, control, and game theories address various information security problems [40].

With recent achievements in quantum computing and quantum information theories, it is known that quantum game theory may be useful in studying quantum communication to maximize the effective communication. Thus, we are planning to use quantum game theory to improve the network security of the proposed protocol. Namely, we will investigate the security of quantum games to prevent cheating. Next, we are planning to extend the model to wider and more complex quantum networks.

Declaration of competing interest

The authors declare that they have no conflict of interest or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors thank Prof. Nasser Metwally, College of Science at Bahrain University, for his valuable discussion and comments during the research of this study.

References

- [1] F. Wang, Z. Lei, X. Yin, Z. Li, Z. Cao, Y. Wang, Information security in the smart grid: survey and challenges, in: *Geo-Spatial Knowledge and Intelligence*, Springer Singapore, Singapore, 2018, pp. 55–66.
- [2] G.O. Zkik, Karim, S.E. Hajji, Secure mobile multi cloud architecture for authentication and data storage, in: *International Journal of Cloud Applications and Computing, IJCAC*, 2017, pp. 62–76.
- [3] A. D. Dakhnovich, D. A. Moskvina, D. P. Zegzhda, Analysis of the information security threats in the digital production networks, *Automat. Contr. Comput. Sci.* 52 (8).
- [4] T. A. M. Almiani, A. Razaque, A. Al-Dmour, Context-aware latency reduction protocol for secure encryption and decryption, *Int. J. High Perform. Comput. Netw.* 12 (3).
- [5] B. Gupta, D.P. Agrawal, S. Yamaguchi, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, first ed., IGI Global, USA, 2016.
- [6] R. Renner, Information security in a quantum world, in: Z. Kotásek, J. Bouda, I. Černá, L. Sekanina, T. Vojnar, D. Antoš (Eds.), *Mathematical and Engineering Methods in Computer Science*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 57–62.
- [7] R.V. Meter, Quantum networking and internetworking, *IEEE Network* 26 (4) (2012) 59–64.
- [8] P. Wallden, E. Kashefi, Cyber security in the quantum era, *Commun. ACM* 62 (4) (2019) 120–129.
- [9] H.J. Kimble, The quantum internet, *Nature* 453 (2008) 1023–1030.
- [10] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Experimental quantum teleportation, *Nature* 390 (1997) 575–579.
- [11] N. Gisin, Quantum-teleportation experiments turn 20, *Nature* 552 (2017) 42–43.
- [12] Ji-Gang Ren, et al., Ground-to-satellite quantum teleportation, *Nature* 549 (2017) 70–73.
- [13] N. Gisin, R. Thew, Quantum communication, *Nat. Photon.* 1 (2007) 165–171.
- [14] N.M.M.B.S. Aris, A. Messai, A. Kinan, A novel analysis approach of quantum transmission algorithm with blind detection method, *Int. J. Innovat. Comput. Appl.* 12 (2016) 307–320.
- [15] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, *Phys. Rev. Lett.* 70 (1993) 1895–1899.

- [16] X.-B. Chen, N. Zhang, S. Lin, Q.-Y. Wen, F.-C. Zhu, Quantum circuits for controlled teleportation of two-particle entanglement via a w state, *Optic Commun.* 281 (8) (2008) 2331–2335.
- [17] X.-W. Zha, K.F. Ren, General relation between the transformation operator and an invariant under stochastic local operations and classical communication in quantum teleportation, *Phys. Rev.* 77 (2008), 014306.
- [18] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, N. Gisin, Long-distance teleportation of qubits at telecommunication wavelengths, *Nature* 421 (2003) 509–513.
- [19] W. Pfaff, B.J. Hensen, H. Bernien, S.B. van Dam, M.S. Blok, T.H. Taminiau, M.J. Tiggelman, R.N. Schouten, M. Markham, D.J. Twitchen, R. Hanson, Unconditional quantum teleportation between distant solid-state quantum bits, *Science* 345 (6196) (2014) 532–535.
- [20] A. Karlsson, M. Bourennane, Quantum teleportation using three-particle entanglement, *Phys. Rev.* 58 (1998) 4394–4400.
- [21] M. Zak, Quantum-inspired teleportation, *chaos, Solit. Fractals* 42 (1) (2009) 306–315.
- [22] C. Na, Q. Dongxiao, Y. Hong, P. Changxing, Perfect quantum controlled teleportation via a novel three-particle partially entangled channel, *J. China Univ. Posts Telecommun.* 22 (6) (2015) 45–50.
- [23] X. Li, F. Deng, Controlled teleportation, *Front. Comput. Sci. China* 2 (2) (2008) 147–160.
- [24] F. Yan, D. Wang, Probabilistic and controlled teleportation of unknown quantum states, *Phys. Lett.* 316 (5) (2003) 297–303.
- [25] S. Lee, J. Joo, J. Kim, Entanglement of three-qubit pure states in terms of teleportation capability, *Phys. Rev.* 72 (2005), 024302.
- [26] H. Prakash, A.K. Maurya, Quantum teleportation using entangled 3-qubit states and the ‘magic bases, *Optic Commun.* 284 (20) (2011) 5024–5030.
- [27] G. Brassard, S.L. Braunstein, R. Cleve, Teleportation as a quantum computation, *Phys. Nonlinear Phenom.* 120 (1) (1998) 43–47 (proceedings of the Fourth Workshop on Physics and Consumption).
- [28] J. Bae, J. Jin, J. Kim, C. Yoon, Y. Kwon, Three-party quantum teleportation with asymmetric states, *Chaos, Solit. Fractals* 24 (4) (2005) 1047–1052.
- [29] Z.-J. Zhang, Z.-X. Man, Many-agent controlled teleportation of multi-qubit quantum information, *Phys. Lett.* 341 (1) (2005) 55–59.
- [30] X. Tan, L. Jiang, Q. Zhang, Controlled quantum teleportation with identity authentication, in: 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013, pp. 350–355.
- [31] S. Imre, L. Gyongyosi, *Advanced Quantum Communications: an Engineering Approach*, Wiley-IEEE Press, 2013.
- [32] P.M. Alsing, D. McMahon, G.J. Milburn, Teleportation in a non-inertial frame, *J. Opt. B Quantum Semiclassical Opt.* 6 (8) (2004) S834–S843.
- [33] Q. Pan, J. Jing, Degradation of nonmaximal entanglement of scalar and Dirac fields in noninertial frames, *Phys. Rev.* 77 (2008), 024302.
- [34] N. Metwally, Usefulness classes of travelling entangled channels in non inertial frames, *Int. J. Mod. Phys. B* 27 (28) (2013), 1350155.
- [35] A. Sagheer, H. Hamdoun, N. Metwally, Teleportation with multiple accelerated partners, *Commun. Theor. Phys.* 64 (3) (2015) 287–294.
- [36] F.-G. Deng, C.-Y. Li, Y.-S. Li, H.-Y. Zhou, Y. Wang, Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement, *Phys. Rev.* 72 (2005), 022338.
- [37] E. Martín-Martínez, J. León, Fermionic entanglement that survives a black hole, *Phys. Rev.* 80 (2009), 042318.
- [38] N. Metwally, A. Sagheer, Quantum coding in non-inertial frames, *Quant. Inf. Process.* 13.
- [39] A. Sagheer, H. Hamdoun, Dynamics of multi-qubit states in non-inertial frames for quantum communication applications, *Quantum Info, Comput. Times* 14 (3–4) (2014) 255–264.
- [40] B. Gupta, *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*, Taylor Francis Group, 2018.