ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

A New Proposal for QKD Relay Networks

Jisna V. A[1], Sobha Xavier P[2], Aneesh Chandran[3]

Assistant Professor, Computer Science Engineering, JECC, Cheruthuruthy, India[1,2,3]

Abstract: A simple technique to secure quantum key distribution relay networks is presented here. The paper introduces the concept of logical channels that uses a random dropout scheme. The paper also presents an enhanced protocol for key distribution in the relay networks. Previous techniques relied on creating distinct physical paths to create shares. Hence the compromise of one relay must compromise the entire channel. The concept of logical channel ensures that an attacker must compromise all the relays in order to access the key.

Keywords: Quantum cryptography, Quantum Key Distribution, Relay networks, Random dropout

I. INTRODUCTION

Quantum cryptography is an emerging technology in which two parties can secure network communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. The quantum cryptography relies on two important elements of quantum mechanics - the Heisenberg Uncertainty principle and the principle of photon polarization [1]. The Heisenberg uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits. Key distribution in quantum cryptography is referred to as quantum key distribution.

Quantum Key Distribution (QKD) is an application based on quantum cryptography. Quantum key distribution is now a commercially available technology that is currently undergoing trials in a number of locations. The technology offers a way of establishing a random sequence of binary digits between two end users in such a way that the secrecy of the established bit strings can be guaranteed [2]. This bit string can then be used as a key in cryptographic applications.

One of the biggest obstacles to the widespread introduction of QKD techniques is the distance limitation in optical fiber which restricts current applications to a few tens of kilometres. The distance can be extended by using relays. The relay is basically performing the well-known intercept/resend eavesdropping strategy, but is cooperating with sender and receiver. The quantum relay [3], which when trusted can be used as a basic building block in forming a network. A quantum relay is introduced to enable quantum key distribution links to form the basic legs in a quantum key distribution network. The idea is based on the well-known intercept/resend eavesdropping. The major difficulty with relays from a security perspective is that they must be trusted; compromise of one relay will compromise the entire channel. Secret sharing schemes have been proposed to overcome this difficulty [2]. The technique shows how a relay-based QKD network can be secured such that an attacker has to compromise all of the relays on the channel in order to access the information about the key. The basic principle is to create redundancy on the channel by using more relays than are strictly necessary for overcoming the distance limitation. Distinct logical channels necessary for implementing the technique can be created by utilizing this redundancy. The paper also introduces an enhanced protocol for key distribution over quantum key distribution relay networks [4], which seems to be more secure.

This paper is organized as follows: section II outlines the related works on this field. Section III gives the basic scheme and the enhanced protocol. Section IV discusses the scope and future work. Finally Section V concludes the work presented here following which references are given.

II. RELATED WORKS

Previous works in the field of quantum relaying networks relied on creating distinct physical paths for creating the shares. They use exact number of relays needed for the operation. In that case all relays are involved in communication at a time. Hence compromise of one relay must compromise the entire channel.

A popular QKD relaying method is proposed by H. Bechmann-Pasquinucciand A. Pasquinucci, based on trusted model [3]. The critical drawback of this method is that relaying nodes are assumed perfectly secured. Such an assumption is vulnerable to passive attacks that are difficult to be detected. Therefore, one wants to limit the number of trusted nodes in a QKD network.

C. Le Quoc and P. Bellot propose a QKD Relaying model based on quantum quasi-trusted bridge protocol [4]. This protocol can be applied in realistic scenarios, but this is a three party communication protocol. It cannot be applied in case of more than one relay.

Entanglement based QKD relaying model proposed by D. Collins, N. Gisin, and H. De Riedmatten [5] is theoretically the stronger QKD relaying model. This model allows achieving an arbitrarily long distance QKD. However, working on entangled photons is not easy in practice. Since the range of QKD is limited, QKD relaying methods are indispensable. This becomes more important while building QKD networks. All QKD relaying methods

DOI 10.17148/IJARCCE.2015.42107

so far introduced have some own undesirable drawback. This encourages looking for new approaches that can be applied in the case of more number of relays. The paper proposes an enhanced protocol that can be applied in case of more relays.

III.KEY DISTRIBUTION PROTOCOL

A. Basic Scheme

The concept of logical channels is used for implementing QKD relay networks. Two techniques for creating the logical channels are: redundancy and random drop-out scheme. To illustrate the technique, consider the figure 3.1shown below consisting of the transmitter (Alice), the receiver (Bob), and 3 intermediate relays Rj such that only one of the relays is actually needed to provide the requisite distance extension. Rest of the relays is added to create redundancy [2].

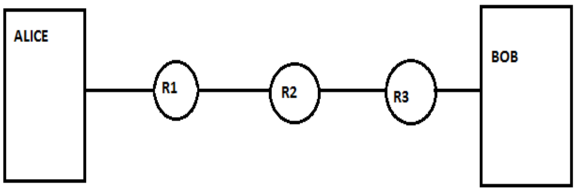

Figure 3.1: A QKD channel between Alice and Bob with 3 Relays

Consider the channel in Figure 3.1; if all of the relays are involved in the communication, then it is vulnerable to the compromise of just one of the relays. All of the relays, in this case, have to be trusted devices. One way to mitigate this is to drop out the relays at random for each time slot [2]. By drop out here it means that the relay is switched off in such a way as to be completely transparent to the channel. Thus in any given time slot 1, 2, 3, or none of the relays are operating.

Now it is straightforward to see that compromise of only one relay in this instance reduces the information available to the eavesdropper. Here keys are divided into shares and each time these shares are sending through the network. A share may not contain all the information about the secret key used. With compromise of one relay the eavesdropper is able to access 4/7 of the information about the key for the channel of Figure 3.1. And even with the compromise of two relays; the attacker would not construct the entire key. This is still too much to allow a successful quantum key distribution. The facility to drop out the relays at random, however, allows a more sophisticated approach.

Table I: The possible logical channels created using the random drop-out of Relays

Alice	R1	R2	R3	Bob	Key
ON	OFF	OFF	OFF	ON	----
ON	ON	OFF	OFF	ON	K_1
ON	OFF	ON	OFF	ON	K_2
ON	OFF	OFF	ON	ON	K_3
ON	ON	ON	OFF	ON	K_{12}
ON	OFF	ON	ON	ON	K_{23}
ON	ON	OFF	ON	ON	K_{13}
ON	ON	ON	ON	ON	K_{123}

Table I lists the possible logical channels created by the simple expedient of having the relays on or off at random. Each of these channels represents a unique quantum key distribution. Only Alice and Bob have access to all of these logical channels. Alice and Bob now consider each of these keys as shares in a secret sharing scheme and form a final key by taking the OR operation of these. The shares are kept as such and the remaining bits are set as zero for transmission. The final quantum key is therefore,

$$K = K_1 \text{ OR } K_2 \text{ OR } K_3 \text{ OR } K_{12} \text{ OR } K_{23} \text{ OR } K_{13} \text{ OR } K_{123}.$$

B. Enhanced Key Distribution Protocol

The enhanced key distribution protocol described here can be applied for key distribution in the logical channels. The key distribution protocol [4] is enhanced in such a way that it can be applied in the case of more than one relay. The protocol really helps Alice and Bob to securely establish the shared key K through the Relay. A two-qubit controlled-NOT (C-NOT) gate, also called the XOR gate,is used at each node in our network.

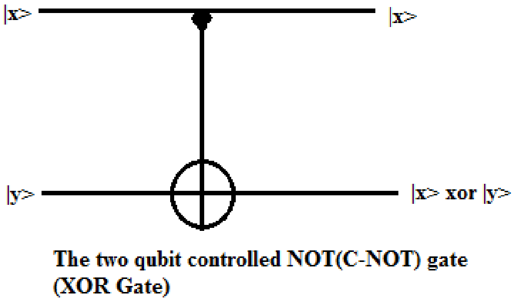

Figure 3.2: A C-NOT Gate, also called XOR Gate

1. Controlled-NOT (C-NOT) gate

The gate is one of the most popular two-qubit quantum gates. The gate can operate in two basis: rectilinear and diagonal. The C-NOT gate operates in basis rectilinear with two corresponding orthogonal basis states 0 and 1. The basis diagonal with the two orthogonal basis states is also considered. The two basis rectilinear and diagonal are maximally conjugate. By definition, this gate flips the second (target) qubit if the first (control) qubit is 1 and does nothing if the control qubit is 0.

Proposition 1: If two input qubits are basis states of one sole basis, then:

1) For the case of the input basis being rectilinear the XOR of two input qubits appears at the second output.

2) For the case of the input basis being diagonal, the XOR of two input qubits appears at the first output.

Proposition 2: If the two input qubits of the C-NOT gate are basis states in the different basis, then

1) If the first and second qubits are basis states in basis diagonal and rectilinear, respectively, then the output is an entanglement.

2) If the first and second qubits are basis states in basis rectilinear and diagonal, respectively, then the C-NOT gate does nothing.

In fact, the proposed protocol need to use a quantum circuit as described in Fig 3.2. It consists of two inputs and two outputs. Two input qubits first pass through a C-NOT gate operating in basis rectilinear, and then are measured independently by two quantum detectors that operate in different basis diagonal and rectilinear (see Fig 3.2). Two outputs are classical bits 0 or 1. From Proposition1, it is clear that this circuit does an irreversible operation. Also,

1) If two input qubits a and b are in the same basis rectilinear, then the second output is (a_L XOR b_L) and the first output is either 0 or 1 with equal probabilities, where a_L and b_L are logical values of states a and b in basis rectlinear, respectively.
2) If two input qubits a and b are in the same basis diagonal, then the first output is (a_L XOR b_L) and the second output is either 0 or 1 with equal probabilities, where a_L and b_L are logical values of states a and b in basis diagonal, respectively.
The enhanced protocol for key distribution consists of 5 main steps, which is explained below.

2. The Protocol
Step 1 : Preparing, exchanging, and measuring qubits:
1) Alice creates 2n random bits and chooses the random 2n-bit string b_A. For each bit i, she creates a state in a basis rectilinear or diagonal for $b_A[i] = 0$ or $b_A[i] = 1$, respectively. Alice sends the resulting qubits $a_1; a_2; :::; a_{2n}$ to the network.
2) Similarly, Bob creates a random 2n-bits, the random 2n-bit string b_B and the corresponding qubits $b_1; b_2; :::; b_{2n}$. Then, he sends $b_1; b_2; :::; b_{2n}$ to network.
3) Relays receive two 2n-qubit strings from Alice and Bob in a synchronousmanner. This means that it receives one by one for 2n pairs ($a_i; b_i$). For eachpair, relay firstly leads $<a_i; b_i>$ to the C-NOT gate and then measures two output qubits in two different basis: the first one in diagonal and the second one in rectlinear as described in Fig 3.2. Finally, he randomly chooses one out of two outputs to keep its measurement value and the corresponding basis and discards another one.

Step 2: Sifting:
1) Alice, Relays and Bob announce their basis.
2) If their basis are different at a position i, then they discard this position and the corresponding values.
3) The values of the remaining positions result in 2m-bit strings $a = a_1; :::; a_{2m}$; $c = c_1; :::; c_{2m}$:::; $b = b_1; :::; b_{2m}$ for Alice, Relays and Bob, respectively. In theory, these three strings hold $c_i = a_i$ XOR b_i i ranges from 1 to 2m, 2m = 2n/4.

Step 3: Checking for the presence of Eavesdropper:
1) Alice, Relays and Bob randomly agree m out of 2m positions to check thepresence of eavesdropper. This results in two m-position strings: the check-position string CP = $c_{p1}; :::; c_{pm}$ and the message-position string MP = $m_{p1}; :::; m_{pm}$.
2) Alice, Relays and Bob announce their values $a_{cpi}; b_{cpi}; c_{cpi}$ respectively, in check-positions cpi. They check if $c_{cpi} = a_{cpi}$ XOR b_{cpi} or not. If some of negative checks are there, they abort the protocol.

Step 4: Creating the pads for Alice, Relays and Bob:
1) The values in m message-positions result in m-bit pads $A = A_1; :::; A_m$; $C = C_1; :::; C_m$; ::::; $B = B_1; :::; B_m$ for Alice, Relays and Bob, respectively. These pads hold $C_i = A_i$ XOR B_i, i ranges from 1 to m, m = n/4.

Step 5: Transmitting the key K:
1) Alice creates the random m-bit key K. She adds an extra bit to indicate the number of relays. She sends K XOR A to relay.
2) The first relay receives from Alice K XOR A does an XOR operation with C, changes the extra bit and send it to second relay. Since C = A XOR B the result of the XOR operation is K XOR A XOR C = K XOR B.
3) The second relay receives from the first K XOR B, does an XOR operation with C, changes the extra bit and sends it to second relay. Since C = A XOR B the result of the XOR operation is K XOR B XOR C = K XOR A.
4) Bob receives the string and checks for the extra bit, if the bit is 1 then he computes (K XOR B) XOR B to obtain K.
if the bit is 0 then he computes (K XOR A) XOR A to obtain K. Now the Key K is obtained. The K is actually a share only. Similarly all the key shares are sent.

Simply the proposed model can be described as follows. This is a N-party communication model. Two nodes Alice and Bob want to establish a secret key. However, the distance between them exceeds the limited range of QKD. Relays act intermediate nodes that could share QKD links with Alice and Bob, which correctly follows the given protocol. However, the relay may be eavesdropped by the malicious person. Consider a channel that requires N relays to overcome the distance limitation. In order to be able to operate the sharing scheme, a redundancy is to be created. The extra relay needed is clearly just one. The final key can therefore be formed from just N + 2 key shares where N is the number of relays needed to establish the channel. An eavesdropper has to compromise all of the relays on the channel in order to obtain the entire key.

IV. DISCUSSION

Compared with other models, the enhanced model seems more reasonable in realistic scenarios. None of the relays alone is able to construct the key. Indeed, no two relays can construct the key either. An attacker would have to compromise all of the relays in the channel in order to be able to obtain the key. The protocol ensures that the check-position and message-position choices are done after arrivals of qubits. The classical information that could be eavesdropped by an eavasdropper on the relay's site now does not reveal any information of K. It can also be shown that the protocol is secure in face with attacks made by eavesdropper over channel. The price that sender and receiver have to pay for a key distribution is a lower key generation rate. This may put some practical limitations to

DOI 10.17148/IJARCCE.2015.42107

how many relays a network can contain. On the other hand, due to the simple working structure of the quantum relay [3], it is easy to implement different parts of a network with different quantum key distribution platforms. This means that some parts of the network can be carried out by fiber implementations, for example within cites, whereas the connection between cities could be carried out by, for example, free-space implementation either by line of sight or even ground to satellite.

Compared with the trusted model [3] that was applied in the two famous QKD networks the model seems more reasonable in realistic scenarios. But this model cannot deal with relay compromise. If the relay can act as active attackers, then it does not use the C-NOT (XOR) circuit. Instead, it measures independently <a_i; b_i >, then announces the result <a_i; b_i > as she had strictly followed the protocol. Sender and receiver cannot realize that relay cheats in this case. The model suffers from implementation problems. The first one is the problem of synchronizing the qubit arrivals from sender and receiver at the relay's site. Besides, the implementation of the two-qubit C-NOT gate [4] is also critical.

As of today, QKD is limited to a range of about 100km; the main limiting factor is due to losses. The losses of the detector are independent of the distance between sender and receiver, whereas the losses in the fibers are the real limiting factor on the distance. Since QKD uses single photons, once a photon is absorbed by the fiber there could not be any kind of repeater which can recreate it. Thus quantum repeaters which work in a similar way as the classical ones do not exist. If the presence of an eavesdropper is suspected then sender and receiver may choose to suspend the transmission. However, if the analysis shows that one of the relays is compromised then sender and receiver can choose channels in which this relay does not play a part.

V. Conclusion

A simple enhanced scheme for securing quantum key distribution relay networks that requires relays for its operation is presented here. It is found that an attacker has to compromise all of the relays on the channel in order to obtain the key. Furthermore, it is shown that only a single extra relay is needed to ensure this security. This is an important result that could have a large impact upon the design and operation of quantum key distribution networks. One big advantage is that the proposed quantum relay can be implemented with today’s technologies, and hence would make it possible to form small networks for quantum key distribution. Another advantage is that the nature of the relay is simple that it allows mixing different quantum key distribution platforms. Also the protocol is enhanced here in such a way that it can be applied in the case of more than one relay.

REFERENCES

[1] C. Bennett, G. Brassard et al., “Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175. Bangalore, India, 1984.

[2] S. Barnett and S. Phoenix, “Securing a quantum key distribution relay network using secret sharing," in GCC Conference and Exhibition (GCC). IEEE.

[3] H. Bechmann-Pasquinucci and A. Pasquinucci, “Quantum key distribution with trusted quantum relay," Arxiv preprint quant-ph/0505089, 2005.

[4] C. Le Quoc and P. Bellot,” A new proposal for qkd relaying models," in Proceedings of 17th International Conference on Computer Communications and Networks, 2008.ICCCN'08, IEEE, pp. 1-6.

[5] D. Collins, N. Gisin, and H. De Riedmatten, “Quantum relays for long distance quantum cryptography," Arxiv preprint quant-ph/0311101, 2003.

DOI 10.17148/IJARCCE.2015.42107