Quantum Cryptography Over Multi-Sites Networks

Hossam Abdel Rahman
Computer & Systems Engineering Dept.
Ain Shams University
Cairo, Egypt
hossam.abdelrahman@gmail.com

Mohamed A. Sobh
Computer & Systems Engineering Dept.
Ain Shams University
Cairo, Egypt
mohamed.sobh@eng.asu.edu.eg

Khaled Kirah
Computer and Systems Engineering Dept.
Ain Shams University
Cairo, Egypt
khaled.kirah@eng.asu.edu.eg

Ayman M. Bahaa-Eldin
Misr International University
On leave from Ain Shams University
ayman.bahaa@eng.asu.edu.eg

***Abstract*—While most of the researches on channel security have focused on point to point communication, little attention was given to multi nodes networks. In this study, the possibilities of loopholes in multi-sites networks using quantum secure direct communication encryption protocols are analyzed. Several solutions are proposed. Depending on the installed topology (linear, ring, star and partially meshed) and on the distance between the nodes, a different solution is proposed**

I. Introduction

Nowadays, security of information is the most important concern over all networks. Lots of efforts were deployed in different cryptography techniques to reach the unconditional secure communication between a sender (Alice) and a receiver (Bob) in the presence of an eavesdrop (Eve). This was called a point to point communication between two nodes. However, in real life situations, the two nodes may not be connected directly via a dark fibre or at least the distance between them is too long to apply a security scheme with an accepted performance. Also, the sites (aggregate/trunk sites) connecting the two nodes may be untrusted ones. Consequently, if the encryption is done hop by hop, this will introduce a loophole over the security of the whole link.

Classical cryptography cannot guarantee the security of the ciphertext. In the 80's of the last century, a practical quantum encryption method, namely the quantum key distribution (QKD) was proposed with the objective of securing an unbreakable encryption protocol [1]. The advantages of quantum encryption versus the classical one are due to its dependence on the laws of quantum mechanics such as no-cloning theorem, uncertainty principle, correlation of entangled particles and non-locality [2]. Although QKD has been developed over years, it has a major drawback. The efficiency of communication is reduced because of the major loss of qubits that results on the creation of a shared private key between the two legitimated users that will then be used in order to encrypt the transmitted message [3] [4] . In order to overcome the vulnerabilities of sending initializing data over classical channels, quantum secure direct communication (QSDC) was proposed in the last decade [5] [6] [7].

In QSDC, the message is sent directly without a priori key for encryption. Consequently, the overhead latency is decreased. Moreover, the potential security loophole of key managing and ciphers text is vanished [8], [26], [27] and [28].

II. QSDC Protocol

QSDC as an idea has evolved through different suggestions such as using the properties of Bell states and block transmission technique. However, in the early stages, security issues in noisy channel were demonstrated [9] [10]. Lately, many research groups started to find solutions to optimize the protocol using hyper-entanglement, Shor error coding and using decoy photons [6].

Realizing QSDC protocols could be done with either one of the following two methods. The first one is based on quantum entanglement where the information are encoded in the photon physical characteristics (polarization, momentum,…). Quantum protocols then control the message transfer in the time domain [11]. This is the reason why the photons are stored in quantum memory for quantum channel security checking [12]. At the receiver side, quantum state tomography (QST) is used. The second method is based on single photons devices [13]. The photons are transmitted in optical fibre and stored in a fibre coil. The information is transferred securely by frequency coding. This approach was introduced to defeat the efficiency problems in the single photon detectors and noisy channels. Instead of using the unitary operators for encoding the EPR pairs, encoding here is based on periodic sequence of operations. All four Bell states are used to encode frequencies on EPR-sequences [14]. The receiving side then uses discrete time Fourier transform to detect the encoded frequency [6].

Nowadays, intensive researches are conducted by experts everywhere to find techniques to stop Eve from jeopardizing the security of communication [15] [16]. For example, non ideal photon sources are consider by the quantum attackers as a vulnerability. Photon number splitting (PNS) attack is a theoretical powerful undetectable attack to get information without probing the main data stream [17]. Although PNS could be nearly implemented using linear optics and QND measurement with quantum memory, it is not precisely implemented like its definition [18]. In addition, QSDC protocols were proposed for ideal channels. However, noise over the channel causes losses and errors of information. Noisy channels may be a good environment for eavesdropping. Always, Eve is assumed to have full control and full capabilities on the communication channels. She has ideal channels with Alice and Bob and can monitor the communication activities between them [14]. She hides herself in the noise and performs intercept-resend attacks. Bob thinks that he got the message from Alice but with higher error rate due to the noise of the channel. Other vulnerabilities may be possible due to the imperfections in the optical components.

Using decoy state photons prevents the adversary from intercept-resend attacks. Eve has no information about the position and the initial state of the random decoy states sent by Alice. Measurements by Eve will not reveal the right measurement basis or the position of the decoy state photons. Filters to cut off all unknown wavelengths that may be introduced by the attacker are used. Moreover, using a 50:50 beam splitter assures that no multiple photons are used to sniff the message [19].

III. Applying Quantum Cryptography Over Mutli-Site Networks

Most of the quantum cryptography studies have focused on point to point communication. Security of a communication link is not limited to encrypting the message only but is extended to secure the identity of the communication parties as well. What Eve always does with any communication session is to fetch the most useful information as much as she can. She can consider the capturing of metadata as a success. Metadata may then be used to start getting in the payload of the message. According to the amount, value and type of metadata that are captured, the adversary can work with machine learning algorithms and data mining analyser to get valuable information about the communication patterns and behaviour for each party. He can then start his infiltration test according to the weak points in each party [20]. Consequently, scaling up the network to have multi node communication needs another vision regarding node identification and testing the message security strength over the intermediate sites between its generating site to its destination one.

It is therefore required to replace the way of transferring the encryption keys from the classical Diffie Hellman (DH) key exchange method to be done on a quantum channel [21]. The idea was to design scalable system based on QKD to tackle the problem of metropolitan networks (enterprise level) where the nodes are not directly connected to each other. At each site there will be a key management server that handles the key generation and sends the key using any topology of quantum key distribution among the sites [22]. Hence, secure transfer of the keys among the sites is accomplished without interfering the routing and communication protocols. Still conventional equipment at the site (routers/ switches) are used and the QKD is implement in parallel to the main network. This protocol is requesting on periodic bases for key refresh and if it is not available, the system will fall back to the DH key exchange method [21]. However, this method has two main drawbacks. First, if the distance between two consecutive nodes is too long such that a relay, which is an all optical fibre-based quantum switch which preserve entanglement while increasing the power of the photons, is used. This relay may be put in an untrusted site which will be considered as a weak point. The second disadvantage is using QKD instead of Diffie Hillmen key exchange method is good to secure the key exchange but still the encryption process is classical which may be compromised with quantum cryptanalysis.

IV. Multi-Site Quantum Secured Communication

A. Case Studies

As shown in figures (1-a) and (1-b), ground station and the trunk sites (aggregate 1 and aggregate 2) are mostly leased from a service provider. Consequently, the encryption cannot be manipulated at those sites and still the encryption must pass through them to be exchanged between Alice and Bob. Moreover, since the aggregate may work on dense-wavelength-division multiplexing networks (DWDM), nodes may combine wavelengths and introduce noise at the receiver side. Therefore, a filter is added to both Alice's and Bob's devices in order to cut off the wavelengths except the one which they use in the communication. Besides, working in a point to point manner as proposed in the literature and just focusing on sending a message from Alice to Bob will reveal a huge problem in metropolitan networks. To connect all nodes in point to point connection means a fully meshed network which needs high costs and in many cases it cannot be achieved.

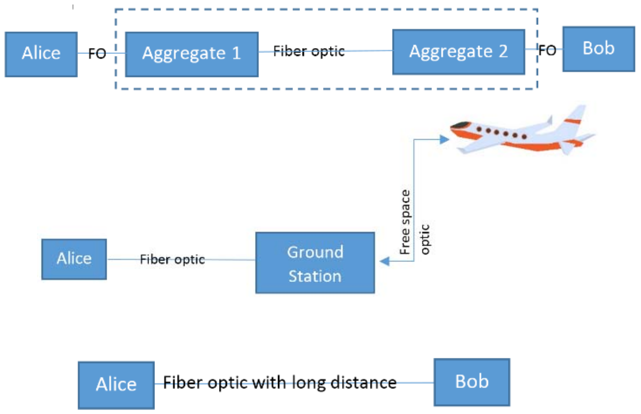

Fig. 1-a. *Two connected sites over service provider's aggregate communication nodes.* ***Fig. 1-b.*** *Connecting Alice with the private jet through free space optic to another party's ground station then backhauling over fibre optic towards Alice.* ***Fig. 1-***

c. *Two sites which are directly connected to each other over a very long dark fibre.*

In real networks, hosts are connected locally to a node and all nodes are connected in ring, star, or partially meshed topology. Accordingly, studying quantum encryption over multi-nodes in the simplest form (ring or linear) or more complex form (star - multicasting or clouding) is important for real life channels.

B. *Proposed Solution*

In the following, QSDC will be deployed to send encrypted data directly over multi-sites from Alice to Bob and possibly to Charlie with two different scenarios.

1) *First Scenario*

It is based on passing the messages among trusted sites in linear or ring topologies. If the distance between the nodes is short enough for transferring the quantum encrypted photons within an acceptable error rate, hop by hop encryption will be successful. Each node will act as two nodes attached back to back using polarization maintaining (PM) fibre to preserve the entanglement properties of the photons. Add and drop multiplexers are used such that each side can connect to another node using any QSDC protocol.

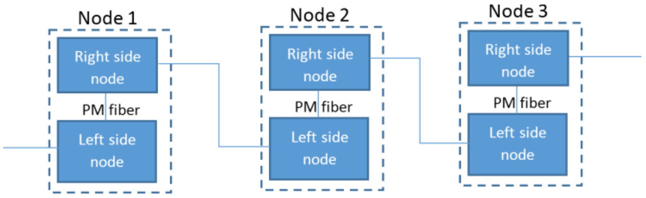

Fig. 2. *Each site consists of two nodes and each one is connected to one side from the neighbour site. Both nodes are connected with polarization maintaining fibre.*

2) *Second Scenario*

If the distance is long enough to annihilate the quantum properties, a relay is used. This is the easiest scaling up technique from two parties' communication on a direct link to multisite communication. This is usually done for star, ring and partially meshed as fully meshed is not always a practical solution. The concern in relays is that they may be added in an untrusted site which introduces the loop hole. To overcome this problem, there are two proposals according to the QSDC protocol that will be used in the encryption process.

The first one is used in the two-step entanglement based protocol. An XOR function which is known to Alice and Bob only is used on the raw data with a fixed pattern (scrambling technique). This fixed pattern is stored at both sides in quantum memories while they are manufactured. This achieves the concept of end-to-end communication, which is the same concept as quantum one-time pad. Now, Eve can hide herself in the error introduced by the relay and starts to attack. Since she cannot get the raw message, she will monitor the flow of the data only. A look up table array may be stored at each node, so that the scrambling code between each two of the three parties Alice, Bob and Charlie is different. Accordingly, if one connection is compromised, the other connections still have some sort of security.

In the second one, a frequency coding scheme single photon is used. The randomness of the used frequency allows the protocol to be robust against noisy channels and prevents the adversary from hiding inside it. Eve has to get enough amount of EPR pairs to start learning about Alice's frequencies. This is not the same as the original attack scheme where she simply intercepts the photons and resend them to the other side (intercept-resend attack) because the other side cannot accept different frequency encoding schemes for different sequences. Note that, if Eve is capable of doing continuous monitoring, she may capture the photons on long time span which allows her to get the encoding period. Therefore, more checking bits shall be used up to 50% in addition to making error density check in different positions [14]. If there is a great discrepancy in the error densities among the sequence, it means that there is a continuous monitoring and the communication will be aborted. So the only way for the adversary is to capture random photons not continuous which is useless in frequency coding scheme.

The same approach can be used on the star connection and multicasting communication using the previous scenarios. Figure (3) shows the way of connection between the master node and the remote sites. Here if node 1 wants to send message to node 2, then it should pass the message with the encryption procedure that is agreed between node1 and the master node-a. Then the master node-a transfer the message over PM fibre to master node-b, which will encode the message again with the quantum credentials established between it and node 2. So the message will be clear from the encryption over the PM link fibre between master node–a and master node-b which are located in the trusted site.

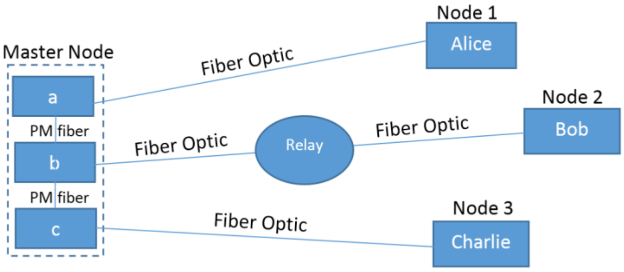

Fig. 3*.Star connection for multi-sites through the master node, each one is secured on a quantum channel and the clear connection will be in the main site only, assuming that node 2 is far away therefore a relay was added in its path.*

C. *Additional security elements (Authentication)*

QSDC scheme lacks in authentication information. So Bob cannot confirm that the received quantum state is from Alice or not. From here, "man in the middle attack" can take place [23]. The adversary has the capabilities of intercepting, storing, modifying, generating, sending and deleting quantum messages [24]. Since, the network, is not closed on two hosts point to point communication, then more authorization shall be applied to be assured of the communicating parties.

a- *Short-term public cryptography*: It can be used initially to authenticate between different nodes, then the QSDC security check takes the hand for checking the communication channel between them.

b- *Post-quantum cryptography*: This is a form of public-key algorithms capable of defeating the attacks by quantum computers. This may be used in the same way as in point (a) [25].

V. Conclusion

Depending on the topology of the connections and on the distance between the nodes, different solutions to overcome the loopholes on multi node networks using quantum secure direct communication are presented. These solutions are easy to be installed and introduce more approaching step towards the realization of quantum encryption over real networks.

VI. References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *IEEE, International Conference on Computer System and Signal Processing*, 1984, pp. 175-179.

[2] B. Schumacher and M. Westmoreland, *Quantum Processes, Systems, and Information*. Cambridge: Cambridge University Press, 2010.

[3] L. Gui-lu, D. Fu-guo, W. Chuan, L. Xi-han, W. Kai, W. Wan-ying , "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers of Physics in China*, vol. 2, no. 3, pp. 251-272, 2007.

[4] D. Huang, Z. Chen, J. Xie, Y. Guo, "Bidirectional Quantum Secure Direct Communication Based on Entanglement," in *International Conference on Security Technology*, 2008, pp. 40-49.

[5] B. Gu, Y. Huang, X. Fang, Y. Chen, "Robust Quantum Secure Communication with Spatial Quantum States of Single Photons," *International Journal of Theoretical Physics*, vol. 52, no. 12, pp. 4461–4469, 2013.

[6] J.-Y. Hu, B. Yu, M-Y. Jing, L-T Xiao, S.-T. Jia, G.-Q. Qin & G.-L. Long, "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 5, p. e16144, 2016.

[7] L. Xi-Han, "Quantum secure direct communication," *Acta Physica Sinica*, vol. 64, no. 16, p. 0160307, 2015.

[8] Z-H. Liu, H-W. Chen, "Analysis and Improvement of Large Payload Bidirectional Quantum Secure Direct Communication Without Information Leakage," *International Journal of Theoretical Physics*, vol. 57, no. 2, pp. 311–321, 2018.

[9] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," *Physical Review Letters*, vol. 89, p. 187902, 2002.

[10] A. Wójcik, "Eavesdropping on the "Ping-Pong" Quantum Communication Protocol," *Physical Review Letters*, vol. 90, p. 157901, 2003.

[11] Q-N. Zhang, Ci-Cui Li, Yuan-hua Li Yi-you Nie, "Quantum secure direct communication based on four-qubit cluster states," *International Journal of Theoretical Physics*, vol. 52, no. 1, pp. 22-27, 2013.

[12] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Physical Review Letters* , vol. 118, p. 220501, 2017.

[13] F. Zhua, W. Zhanga, Y. Shengb, Y. Huanga, "Experimental long-distance quantum secure direct communication," *Science Bulletin*, vol. 62, no. 22, pp. 1519-1524, 2017.

[14] X.-L. Zhao, J.-L. Li, P.-H. Niu, H.-Y. Ma, D. Ruan, "Two-step quantum secure direct communication scheme with frequency coding," *Chinese Physics B*, vol. 26, no. 3, p. 030302, 2017.

[15] P. Zawadzki, "Eavesdropping on quantum secure direct communication in quantum channels with arbitrarily low loss rate," *Quantum Information Processing*, vol. 15, no. 4, 2016.

[16] S. Sajeed, C. Minshull, N. Jain and V. Makarov , "Invisible Trojan-horse attack," *Scientific Reports* , vol. 7, 2017.

[17] A. A. Gaidash, V. I. Egorov, A. V. Gleim , "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices ," *Journal of Physics: Conference Series 735 (2016)* , vol. 735, p. 012072, 2016.

[18] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin, G. B. Baumgartner, "Using Modeling and Simulation to Study Photon Number Splitting Attacks," *IEEE Access*, vol. 4, pp. 2188 - 2197, 2016.

[19] L. Wang, W. Ma, M. Wang, D. Shen, "Three-party Quantum Secure Direct Communication with Single Photons in both Polarization and Spatial-mode Degrees of Freedom," *International Journal of Theoretical Physics*, vol. 55, no. 5, pp. 2490–2499, 2016.

[20] S. Sun, E. Waks, "Secure quantum routing," *arXiv:1607.03163* , 2017.

[21] P. K. Tysowski, X. Ling, N. Lütkenhaus and M. Mosca, "The Engineering of a Scalable Multi-Site Communications System Utilizing Quantum Key Distribution (QKD)," *Quantum Science and Technology*, vol. 3, no. 2, 2018.

[22] M. Sasaki, "Quantum networks: where should we be heading ?," *Quantum Science and Technology*, vol. 2, no. 2, 2017.

[23] Y.-Y. Fei, X.-D. Meng, M. Gao, H. Wang and Z. Ma , "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," *Scientific Reports* , vol. 8, 2018.

[24] X. Zou, D. Qiu, "Attacks and Improvements of QSDC Schemes Based on CSS Codes," in *Bio-Inspired Computing and Applications, ICIC*, Zhengzhou, China, 2011, pp. 239-246.

[25] D. J. Bernstein, , J. Buchmann, E. Dahmen, *Post-Quantum Cryptography.*: Springer-Verlag Berlin Heidelberg, 2009.

[26] Israa Hammouda, Hazem Saied, Ayman M. Bahaa-Eldin, "Quantum Databases: Trends and Challenges", 2016 11th International Conference on Computer Engineering & Systems (ICCES), 275-280, 2016, IEEE

[27] Israa Hammouda, Hazem Saied, Ayman M. Bahaa-Eldin, "A Generalized Grover's Algorithm with Access Control to Quantum Databases", 2016 11th International Conference on Computer Engineering & Systems (ICCES), 281-285, 2016, IEEE

[28] Ayman Mohsen, Mohmed Sobh, Ayman M. Bahaa-Eldin, "Lattice-Based Cryptography", 2017 12th International Conference on Computer Engineering and Systems (ICCES), 462-467, 2018, IEEE