35

OPTICAL NETWORK MODELS FOR QUANTUM CRYPTOGRAPHY

Sufyan T. Faraj[1], Prof. Fawzi Al-Naima[2], and Siddeeq Y. Ameen[3]

Abstract The paper presents some secure optical network models. The security of the models is achieved using quantum cryptographic-key distribution. Both point-to-point and multiple-access broadcast networks are considered. In the modeling of these networks, the simplicity, generality and flexibility are highly maintained. This enables the efficient use of these models for software simulation purposes. Each secure optical communication network model is assumed to be composed of N communication nodes (stations) that are connected by fiber-optic links. Some hardware requirements are briefly explained. Also, samples of simulation results for these network models are presented.

1. INTRODUCTION

Communication Networks can be divided according to the transmission technology into two types: broadcast and point-to-point networks. *Broadcast networks* have a single communication channel that is shared by all the stations on the network. On the other hand, *point-to-point* networks consist of many connections between individual pairs of stations [1].

Some basic network security threats include; masquerade, replay, interception of data, manipulation of messages, and repudiation. Thus, networks need to be protected against various kinds of threats. This can be achieved by designing a cryptographic system that provides the following basic security services; authentication, secrecy, integrity, and nonrepudation

[1] *Department of Computer Eng., College of Engineering, University of Baghdad, Baghdad, Iraq.*
[2] *Department of Computer Eng., College of Engineering, Sadam University, Baghdad, Iraq.*
[3] *Department of Electrical Eng., Military College of Engineering, Baghdad, Iraq.*

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

[2]. In quantum cryptography, physically secure quantum key distribution is combined with the mathematical security of the *Vernam* cipher (the one-time pad) to produce a fully secure system [3].

There are two distinct methods for achieving key security using quantum cryptography. The first scheme relies on the uncertainty principle of quantum mechanics to achieve secure key distribution on a single-quantum channel. While, the second scheme relies on the violation of the Bell inequalities to provide the required security on correlated quantum channels.

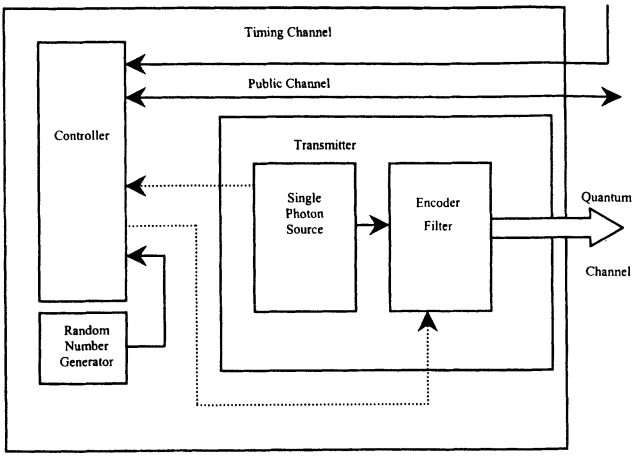
The presented work is related to single-channel quantum cryptography. In this system, a quantum key distribution scheme works according to the *Bennett-Brassard (BB)* protocol [4], where the principals *Alice* and *Bob* have access to two channels, one quantum and one classical public. Individual polarized photons are sent on the quantum channel. *Eve* may try to intercept these photons. On the other hand the public channel has a perfect authenticity and can transmit information accurately. These transmissions on the public channel cannot be modified or suppressed by Eve; however, their entire content becomes known to her. If message authenticity not enforced by the physical properties of the channel, it can be provided by the *Wegman-Carter* unconditionally secure authentication scheme.

After exchanging appropriate quantum systems (polarized photons), Alice and Bob will share a random bit string, which is often called *raw quantum transmission* (RQT). Then they can implement error elimination and privacy amplification protocols. However, these protocols will be done at the expense of reducing the RQT. Nevertheless, it is worth it because Eve's expected information about the final key would be reduced to an exponentially small fraction of one bit [3,4]. Our simulation procedure for the BB protocol is described elsewhere [5,6].

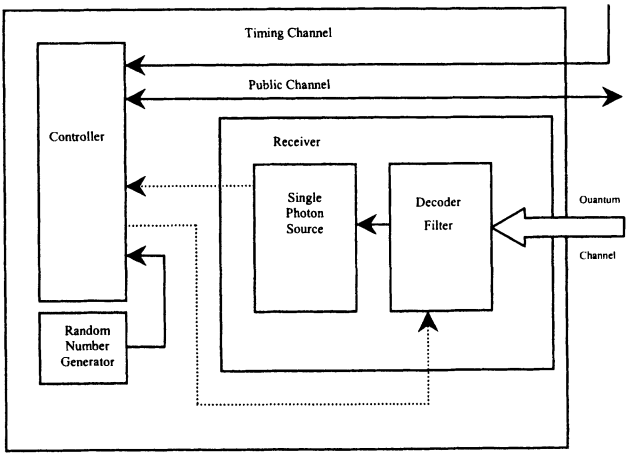
2. COMMUNICATION NODE CONFIGURATIONS

In this work, it is assumed that there are three basic configurations for communication nodes in a network for quantum key distribution. These configurations are *quantum transmission* (*QT*), *quantum reception* (*QR*), and *quantum transmission/reception* (*QTR*) nodes, as shown in Fig.1. Each node configuration contains a controller that comprises a microprocessor, memory, and controller interface. The control commands of the controller are synchronized by clock pulses from a global clock, which is connected to

each communication node via the timing channel. The controller of each node is also connected to the authenticated public channel.



(a). QT node configuration.



(b). QR node configuration.

Figure 1. Basic configurations for communications nodes.

The QT node configuration contains an apparatus for transmitting individual quantum systems. To maintain generality and simplicity of modeling, single photon systems are assumed to be used in this work. Thus, a single photon source is incorporated in the transmission apparatus. The output of the single photon source is sent to an encoder filter. The encoder filter preferably uses an electro-optic polarization modulator to alter the states of polarization of single photons.

The QR node configuration incorporates an apparatus for receiving encoded single-photons from the quantum channel. The receiver employs a

complementary architecture with the incoming optical signal being received via the decoder filter at a photon detector. The decoder filter may be formed from an electro optic polarization modulator, similar to that used in the transmitter. The photon detector is preferably be an APD based on Germanium technology.

The QTR node configuration contains an apparatus for both transmission and reception of single photons. In fact, such a node configuration may contain more than one transmitter and/or more than one receiver of single photons, according to the type of application.

The choice of polarization states at the transmitter, and choice of reading basis at the receiver, have to be made randomly (not pseudorandomly). Also, many random bits are needed during error elimination and privacy amplification phases. Thus, a random number generator (RNG) is incorporated in each node configuration.

In all node configurations, the encoder and decoder filters are managed by their respective controllers to encode or decode photons in different rectilinear or diagonal polarization states. Each photon can be identified by the clock period in which it is transmitted (or measured). This information is exchanged via the public channel. It is obvious that all node configurations must contain additional transmission and receiving equipment, which are required for exchanging *classical* messages on the public channel.

3. SECURE OPTICAL POINT-TO-POINT NETWORKS

In designing point-to-point networks for handling secure quantum transmission, it is important to note that it is not possible to use intermediate switching systems (routers). So, store-and-forward routing algorithms cannot be used. This is because that, at present, photons cannot be stored and kept correlated longer than a small fraction of a second, so they are not a good medium for information storage [3].

3.1 Decentralized Design Concept

In decentralized point-to-point networks, all communication nodes have almost the same capabilities. The most important network topology to be considered, may be the fully-connected point-to-point network, as shown in Fig.2. In this network, there are two bidirectional connections between each pair of nodes, one for quantum transmission and another for

exchanging authenticated public messages. Each node has a QTR node configuration.

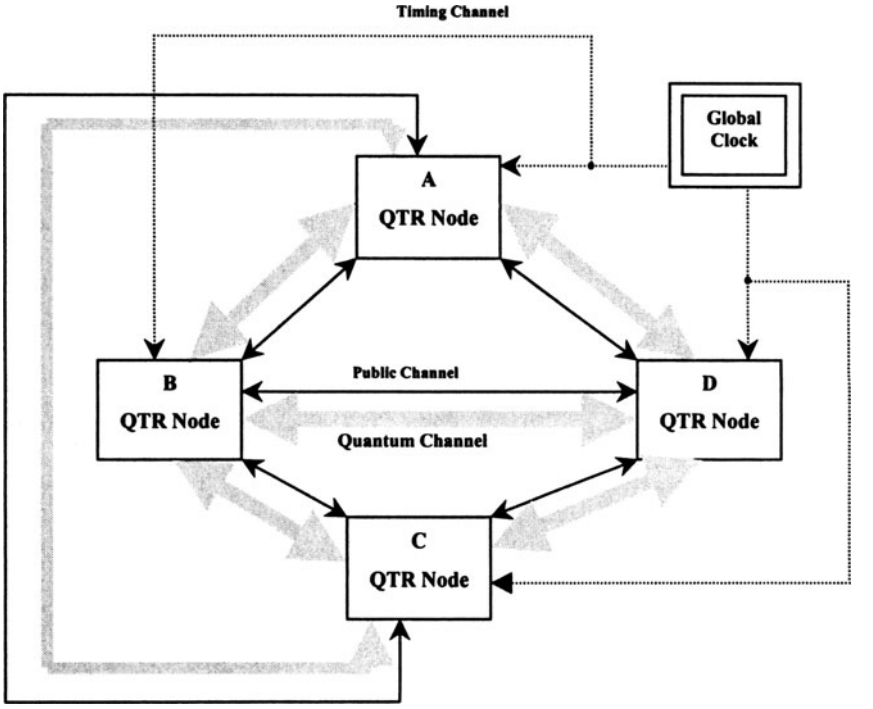


Figure 2. An example of a secure decentralized fully connected point-to-point network.

The connection of each node to quantum channels is achieved using electro-optic switches. One or more of lithium-niobate Y-junction devices can be used for implementing the required electro-optic switch. Two electro-optic switches are used for each communication node, one for the transmission quantum channel and the other for the reception quantum channel. Control signals from each node is used to set the required configuration for the transmission and reception electro-optic switches, and hence choosing the appropriate quantum channel for transmitting and receiving single photons, respectively.

3.2 Centralized Design Concept

Secure centralized point-to-point networks incorporate one or more central nodes and many terminal nodes. Central nodes act as secure interpreters for handling communication between different terminal stations. In this context, two basic network configurations are to be considered: star and tree networks.

In the star network topology, one central node is used with many terminal nodes are connected to it, as shown in Fig.3. In this network, one central QT node can perform a quantum cryptography protocol with each one of the four terminal QR nodes. It is obvious that the number of terminal nodes can be in the order of several tens of nodes or even more. The central node controls an electro-optic switch so that only the required output branch can be enabled to send quantum signals.

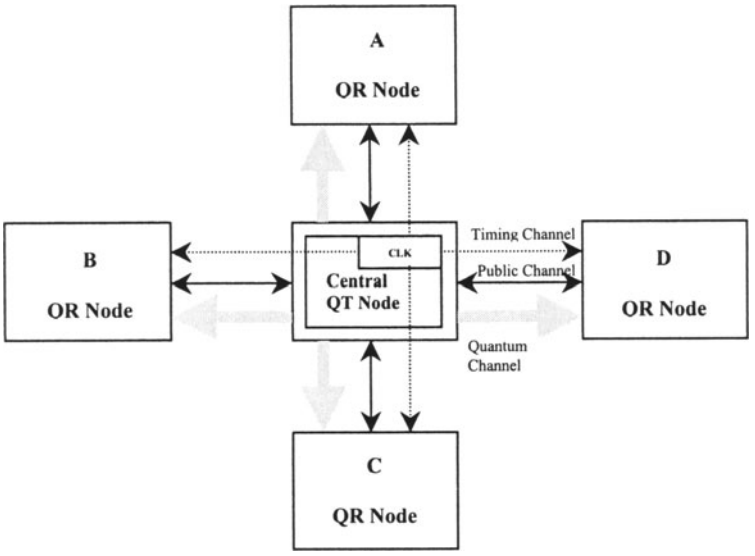


Figure 3. A secure point-to-point network with star topology.

Assuming equal priority terminal nodes, if the central node is busy in doing a quantum cryptography protocol with some terminal node, all other terminal nodes have to wait until the central node becomes idle. Since terminal nodes have no ability for transmitting quantum signals, they must request (on the public channel) from the central node to start a quantum cryptography protocol.

The secure point-to-point tree network comprises two or more central nodes, with many terminal nodes connected to them, as shown in Fig.4. The main central node is a QT node. While, other central nodes are QTR nodes. All terminal nodes are QR nodes. Quantum signals always are sent from a higher level node to a lower level node. Similarly, in each central node, electro-optic switches are used to choose the required output branch for sending quantum signals.

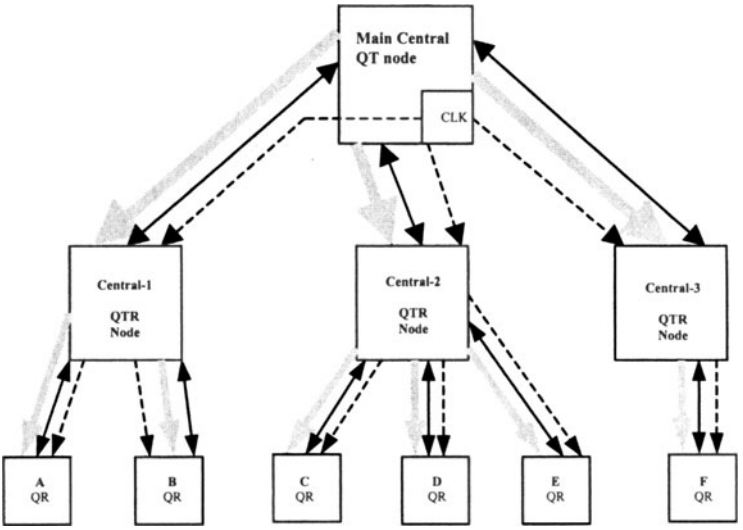


Figure 4. A secure point-to-point network with tree topology.

4. SECURE OPTICAL BROADCAST NETWORKS

Multiple-access broadcast optical networks are on the face of it unsuitable for quantum cryptography applications. However, it was realized that the non-classical behavior of a single-photon signal on such a network could be used to advantage to allow a different key to be established between the transmitting node and each one of the receiving nodes. Such behavior is very suitable to be used in Passive Optical Networks (PONs) [7,8].

4.1 Probabilistic Multiple-Access (PMA) Network

This network contains a central node (which is a QT node) and many terminal nodes (which are QR nodes). It is possible to consider different network topologies that are suitable for the application of this protocol, such as star, tree, and bus topologies. Here, the star network of Fig.5 is considered. In this network, the star connection of the quantum channel is implemented using the *passive star* configuration, which is a 1-to-N fiber coupler, where N is the number of the terminal nodes in the network. While, in the tree topology, several 1-to-M couplers (where M<N) can be used for achieving quantum channel connections.

The reason for calling this protocol as a probabilistic multiple-access (PMA) protocol is the probabilistic arrival of photons at receivers. When the central node transmit single photon pulses to the quantum channel, the quantum mechanical properties of single photons ensure that a given photon will either be detected by one of the terminal nodes or will be lost from the system.

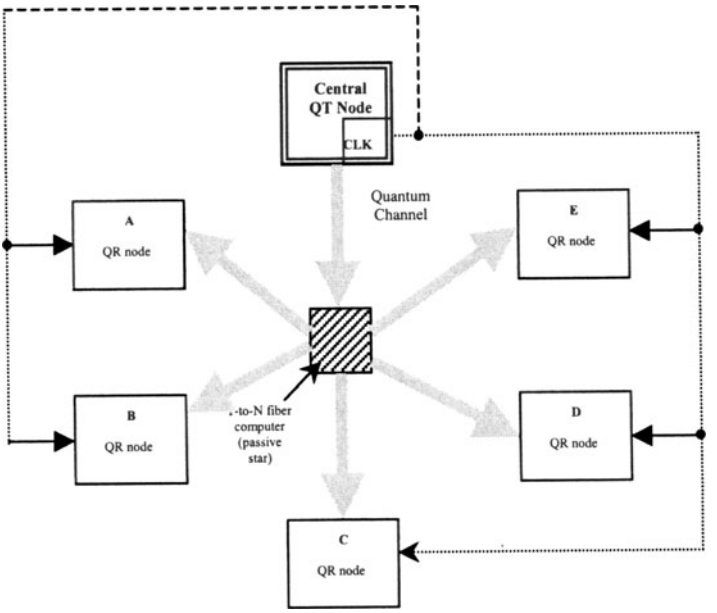


Figure 5. Quantum channel configuration for the PMA star network.

Indeed, this process occurs in a totally random and unpredictable way. Thus, all terminals make photon measurements, with appropriate detecting gate width, at the clock rate. For each successful detection of a photon, they record the basis used for measurement, the actual result of measurement, and the time slot in which the photon arrived.

When this PMA protocol is completely implemented the central node is in possession of N secret keys, each one is shared with a specific terminal node on the network. Also, each terminal has no knowledge of any other key apart from its own. Hence, this protocol is suitable for use in static channel allocation multiple access networks.

4.2 Controlled Multiple-Access Bus (CMAB)

This network can achieve dynamic channel allocation and hence multicasting operations. It comprises a central node and N terminal nodes. The central node (which is a QT node) sends single-photon pulses onto the *quantum bus* channel to which terminal nodes (which are QR nodes) are connected, as shown in Fig.6. Each terminal station is connected into the quantum bus via an electro-optic interface, which can be in one of three states, depending on a switch control signal from terminal station. These states are:

i. Opened-Bus Opened-Terminal (OBOT) State.
ii. Opened-Bus Closed-Terminal (OBCT) State.
iii. Closed-Bus Opened-Terminal (CBOT) State.

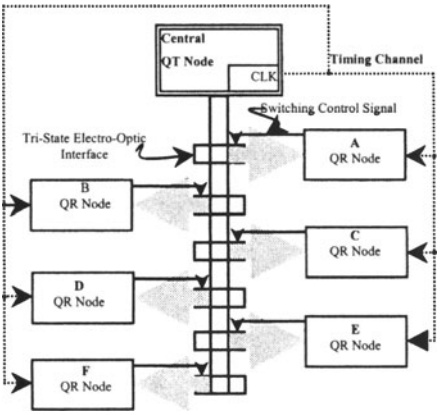


Figure 6. Quantum channel configuration for the CMAB network.

When the central node is broadcasting single-photons to all N terminal nodes, all electro-optic interfaces will act as simple passive 1-to-2 splitters (OBOT State). In this case, the system will be very similar to the PMA network. When the central node performs a multicasting process, only some of terminal stations are incorporated in the quantum key distribution protocol. In this case, the tri-state electro-optic interfaces have to be reconfigured in such a way that only the required nodes receive quantum signals.

4.3 Distributed Access Ring (DAR)

The distributed access ring can be used for quantum key distribution in both broadcasting and multicasting modes with no need for using a central node in the network, as shown in Fig.7. Communication nodes on this network need to be QTR nodes.

Single-photon pulses can move only in one direction down the ring. Each station is connected to the quantum channel ring via a *ring interface*. This interface is used for transmitting and/or receiving single photons from that quantum channel ring. The station reception quantum channel is connected to the ring via an electro-optic switch (which is a tri-state electro-optic switch similar to that used in the CMAB).

This switch is controlled by station commands. The transmission quantum channel of the station is connected to the ring via a passive fiber coupler. The reception electro-optic switch can be in either one of three states, which are:

i. Opened-Ring Opened-Station (OROS) State
ii. Opened-Ring Closed-Station (ORCS) State.
iii. Closed-Ring Opened-Station (CROS) State.

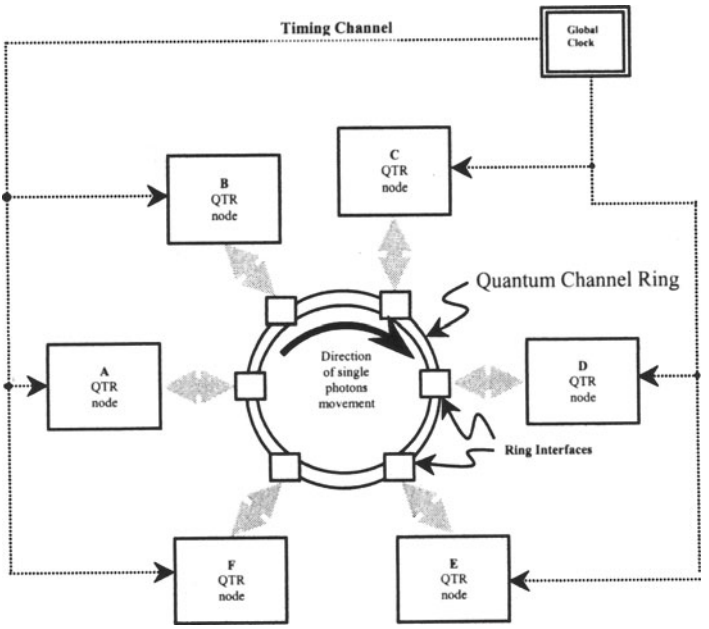


Fig.7. Quantum channel configuration for the DAR network.

When one station is transmitting single photons to some other station(s), all stations that are not incorporated in this multicasting process will turn their reception switches to be in the ORCS State. Thus, they are blocked. Stations that are required to receive single photons will turn their tri-state reception switches to be in OROS State. While, the node that is transmitting single photons will turn its switch to be in CROS State. Hence, photons that are not received by other stations are directed back to the original node, and they are prevented from recycling around the ring again. In fact these photons that are received at the same node which they are transmitted from can be measured to check for the presence of an eavesdropper.

5. COMPUTER SIMULATION RESULTS AND DISCUSSION

In this section, samples of simulation results are presented and some important performance aspects of these networks are briefly discussed. In all of these results, system losses (other than those due to eavesdropping) are neglected.

A. Point-to-Point Networks Results

This part of the results has been taken with initial number of transmitted photons equals 25000, and the value of the safety parameter (s) used in the privacy amplification stage equals 250.

Firstly, sample results obtained from test runs for the simulation of the secure fully-connected network model are presented in Tables 1 and 2. They represent six individual point-to-point quantum cryptography protocols that are implemented between each pair of communication nodes on the network. The number of RQT bits obtained at each individual protocol is around its average value of half the number of transmitted photons, given that system losses are neglected. The small deviations from the average value are due to the independent random processes of polarization bases choice between transmitting and receiving nodes.

Table 1 illustrates simulation results obtained with a constant eavesdropping action on the whole network. This eavesdropping gives about 5% expected error rate, at each individual protocol. Thus, close numbers of individual final strings (secret keys) bits are obtained at each protocol. Eve knowledge about final strings is reduced to arbitrary small values.

Table 2 illustrates simulation results that are obtained with different levels of eavesdropping on each quantum channel. This situation results in different values of expected error rate at each individual protocol. Hence, lengths of individual final strings (secret keys) differ, as the expected error rates are different. As the RQT error rate increases, the final string length will decrease. This implies that a node pair, whose quantum transmission has a higher number of eavesdropping errors, might need to implement an additional quantum cryptography protocol to increase the number of secret key bits. Eve knowledge about final strings is also reduced to arbitrary small values.

Similarly, test results for the simulation of the secure star point-to-point network are shown in Tables 3 and 4. These results represent individual quantum cryptography protocols implemented between the central node and each one of the four other nodes on the network. Table 3 illustrates test results with a constant eavesdropping action, which causes an expected error rate of about 7.5%. While, Table 4 illustrates the results with variable eavesdropping action on each individual quantum link.

Table 1. Simulation results for the secure fully-connected point-to-point network with a constant eavesdropping action:

Node Pair	(A, B)	(A, C)	(A, D)	(B, C)	(B, D)	(C, D)
RQT length (bit)	12573	12591	12503	12423	12447	12342
Expected error rate %	5	5	5	5	5	5
Final string length (bit)	5659	5506	5463	5408	5348	5440
Actual Eve information on the final string (bit)	$< 4.304 \times 10^{-154}$	$< 3.029 \times 10^{-140}$	$< 3.526 \times 10^{-150}$	$< 5.456 \times 10^{-124}$	$< 5.081 \times 10^{-133}$	$< 9.465 \times 10^{-142}$

Table 2. Simulation results for the secure fully connected point-to-point network with a variable eavesdropping action:

Node Pair	(A, B)	(A, C)	(A, D)	(B, C)	(B, D)	(C, D)
RQT length (bit)	12580	12529	12593	12428	12448	12501
Expected error rate %	1.25	2.5	6.25	7.5	8.75	10
Final string length (bit)	10127	8259	4150	3011	1752	911
Actual Eve information on the final string (bit)	< 8.939 × 10-120	< 5.328 × 10-127	< 1.551 × 10-137	< 3.443 × 10-153	< 1.763 × 10-150	< 1.444 × 10-146

Other test runs have been done on the simulation of the secure tree point-to-point network model. Test results with constant and variable eavesdropping actions are presented in Tables 5 and 6, respectively. Individual quantum cryptography protocols are implemented on each subsequent quantum channel of the network. As Table 6 illustrates, when Eve actions on a certain quantum channel increase, expected error rate increases. Hence, the obtained cryptographic key length decreases.

B. Broadcast Networks Results

In the application of quantum cryptography on multiple access broadcast networks, usually the number of messages required to be exchanged in the initialization stage of the protocol is larger than the case of point-to-point networks. This is because there are many users (communication nodes) who share communication resources. Thus, the broadcast system configuration and the channel allocation must be determined prior to any quantum transmission. This part of the results has been taken with initial number of

transmitted photons equals 32000, and the value of the safety parameter (s) used in the privacy amplification stage equals 100.

Table 3. Simulation results for the secure star point-to-point network with a constant eavesdropping action:

Node Pair	(Central, A)	(Central, B)	(Central, C)	(Central, D)
RQT length (bit)	12496	12479	12493	12464
Expected error rate %	7.5	7.5	7.5	7.5
Final string length (bit)	2949	3039	3177	3032
Actual Eve information on the final string (bit)	$< 6.984 \times 10^{-122}$	$< 1.920 \times 10^{-110}$	$< 4.846 \times 10^{-139}$	$< 3.363 \times 10^{-156}$

Table 4. Simulation results for the secure star point-to-point network with a variable eavesdropping action:

Node Pair	(Central, A)	(Central, B)	(Central, C)	(Central, D)
RQT length (bit)	12539	12523	12527	12682
Expected error rate %	1.25	3.75	5	10
Final string length (bit)	10093	7004	5485	977
Actual Eve information on the final string (bit)	$< 9.598 \times 10^{-111}$	$< 9.243 \times 10^{-145}$	$< 4.799 \times 10^{-111}$	$< 4.263 \times 10^{-126}$

Table 5. Simulation results for the secure tree point-to-point network with a constant eavesdropping action:

Node Pair	Main, Central -1	Main, Central -2	Main, Central -3	Central -1 , A	Central -1 , B	Central -2 , C	Central -2 , D	Central -2 , E	Central -3 , F
RQT length (bit)	12551	12528	12447	12381	12448	12437	12620	12579	12522
Expected error rate %	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5
Final string length (bit)	8473	8360	8382	8286	8324	8253	8487	8266	8361
Actual Eve information on the final string (bit)	$< 5.203 \times 10^{-130}$	$< 2.793 \times 10^{-121}$	$< 8.325 \times 10^{-129}$	$< 2.343 \times 10^{-114}$	$< 5.081 \times 10^{-133}$	$< 2.728 \times 10^{-124}$	$< 1.705 \times 10^{-125}$	$< 6.984 \times 10^{-122}$	$< 2.033 \times 10^{-132}$

Samples of test results, obtained from the simulation of the secure star PMA network are presented in Tables 7 and 8. Usually, the passive star configuration, used for constructing this network, results in almost equal transmission coefficients for different network paths. Hence, neglecting the effect of system losses, each terminal node path of the network can be assumed to have a transmission coefficient of 0.2 (*1/N*, in general).

Table 6. Simulation results for the secure tree point-to-point network with a variable eavesdropping action:

Node Pair	Main, Central -1	Main, Central -2	Main, Central -3	Central -1, A	Central -1, B	Central -2, C	Central -2, D	Central -2, E	Central -3, F
RQT length (bit)	12481	12418	12506	12523	12418	12550	12615	12351	12553
Expected error rate %	1.25	3.75	5	5	6.25	7.5	8.75	10	10
Final string length (bit)	9900	6717	5504	5524	4047	3055	1993	755	808
Actual Eve information on the final string (bit)	$< 5.858 \times 10^{-115}$	$< 2.131 \times 10^{-126}$	$< 1.479 \times 10^{-143}$	$< 8.815 \times 10^{-151}$	$< 8.525 \times 10^{-126}$	$< 2.152 \times 10^{-154}$	$< 6.352 \times 10^{-134}$	$< 2.664 \times 10^{-127}$	$< 1.722 \times 10^{-153}$

Thus, almost similar numbers of RQT bits are obtained at each terminal node. In the case of a constant eavesdropping action on the entire network, close values of final strings (cryptographic keys) lengths are obtained at each terminal node. This situation is represented by the test results illustrated in Table 7, where eavesdropping causes an expected error rate of about 8% at each terminal node.

Table 7. Simulation results for the secure star PMA network with a constant eavesdropping action:

Node	A	B	C	D	E
Transmission coefficient	0.2	0.2	0.2	0.2	0.2
RQT length (bit)	3194	3185	3134	3241	3153
Expected error rate %	8	8	8	8	8
Final string length (bit)	519	557	538	499	474
Actual Eve information on the final string (bit)	$< 1.246 \times 10^{-77}$	$< 1.450 \times 10^{-87}$	$< 6.230 \times 10^{-78}$	$< 6.380 \times 10^{-75}$	$< 7.605 \times 10^{-82}$

It is not so probable that Eve can eavesdrop on more than one point on an optical network. However, such eavesdropping action, if occurs, might cause different RQT error rates to be obtained at each terminal node. In this case, different numbers of final strings lengths will be obtained by each node. Terminal node, whose RQT has more errors, will get a smaller number of secret key bits, as shown in Table 8.

Table 8. Simulation results for the secure star PMA network with a variable eavesdropping action:

Node	A	B	C	D	E
Transmission coefficient	0.2	0.2	0.2	0.2	0.2
RQT length (bit)	3220	3160	3237	3179	3225
Expected error rate %	1	2	5	7	10
Final string length (bit)	2572	2254	1327	747	65
Actual Eve information on the final string (bit)	$< 9.414 \times 10^{-55}$	$< 5.746 \times 10^{-59}$	$< 3.713 \times 10^{-85}$	$< 3.987 \times 10^{-76}$	$< 5.941 \times 10^{-84}$

Terminal nodes paths of the secure CMAB network usually have different transmission coefficients. Thus, optical attenuation can be used for equalizing the values of transmission coefficients to the value of the lowest path transmission coefficient.

Table 9. Simulation results for the secure CMAB network with equalized transmission coefficients and a variable eavesdropping action:

Node	A	B	E	F
Transmission coefficient	0.15	0.15	0.15	0.15
RQT length (bit)	2416	2347	2404	2450
Expected error rate %	2	4	6	8
Final string length (bit)	1648	1073	696	343
Actual Eve information on the final string (bit)	$< 7.355 \times 10^{-57}$	$< 2.492 \times 10^{-77}$	$< 5.480 \times 10^{-65}$	$< 1.276 \times 10^{-74}$

Assuming ideal electro-optic switches, terminal nodes that are not incorporated in multicasting would have zero transmission coefficients, since their optical switches are configured in the OBCT state. Thus, the use of electro-optic switches would result in an improvement in the values of transmission coefficients of multicasting nodes. Off course, the improvement in performance of the network would be less if real electro-optic switches were considered.

A sample of test results for simulation of the secure CMAB network is shown in Tables 9. This table represents data obtained from a multicasting process with terminal nodes A, B, E, and F, with equalized transmission coefficients and a variable eavesdropping action. Although close numbers of RQT bits are obtained at each terminal, the final numbers of secret bits differ from terminal to another. This is due to the difference of RQT error rates caused by Eve action on more than one point on the network.

A sample of test results for the simulation of the secure DAR network is presented in Table 10. This table represents a situation of a multicasting process in which node A is transmitting quantum signals and nodes C, D, and F are receiving them. Thus, three individual secret keys are obtained between node A and each one of nodes C, D, and F. Also, equalized transmission coefficients and ideal electro-optic switches are assumed. Table 10 illustrates the situation when a constant eavesdropping action has been occurred. Thus, close numbers of final secret bits are obtained at each node. However, when Eve has the ability to perform a variable eavesdropping on the network, the lengths of the final secret keys would be different.

Table 10. Simulation results for the secure DAR network with equalized transmission coefficients and a constant eavesdropping action:

Node	C	D	F
Transmission coefficient	0.177	0.177	0.177
RQT length (bit)	2809	2819	2846
Expected error rate %	5	5	5
Final string length (bit)	1107	1125	1099
Actual Eve information on the final string (bit)	$< 3.345 \times 10^{-69}$	$< 2.090 \times 10^{-70}$	$< 5.884 \times 10^{-78}$

As all the previous tables indicate, it is possible that certain eavesdropping actions reduce lengths of the secret keys. However, Eve information about these keys can always be reduced to arbitrary small values.

6. CONCLUSIONS

In this work, different strategies in which many correspondents are exchanging individual quantum systems to build many identical pairs of secret keys have been considered. Hence, we believe that quantum cryptographic security services can be very helpful in network application.

Software simulation is an important tool for developing and studying real systems. However, in order to achieve an efficient and constructive simulation, some models with certain specifications have to be developed at first. We believe that our proposed modeling approach is very helpful in this field. Modeling simplicity, generality, and flexibility are obvious benefits of the applied procedure.

The communication protocols, used for different secure point-to-point and broadcast network configurations, have been simulated and tested. The results clearly verify the entire objective required by the model.

REFERENCES

[1] A. S. Tanenbaum, *Computer Networks*, Third Edition, Prentice-Hall International, Inc., USA, 1996.

[2] J. Nechvatal, *Computer Security; Public-Key Cryptography*, National Institute of Standards and Technology Special Publication 800-2, USA, 1991.

[3] T. P. Spiller, "Quantum Information Processing: Cryptography, Computation, and Teleportation," IEEE Proceedings, Vol. 84, No. 12, pp.1717-1746, December 1996.

[4] C. H. Bennett *et al.* "Experimental Quantum Cryptography," Journal of Cryptology, Vol. 5, No.3, pp.3-28, 1992.

[5] S. T. Faraj *et al.* "Simulation of a Quantum Cryptographic Protocol," Proceeding of Al-Hadba' Conference on Informatics and Software Engineering, Mousel, Iraq, 2000.

[6] S. T. Faraj *et al.* "Quantum Cryptographic Key Distribution in Multiple-Access Networks," Proceeding of 16th IFIP World Computer Congress, China, 2000.

[7] P. D. Townsend and D. W. Smith, "Key distribution in a multiple access network using quantum cryptography," US Patent No. 5, 768, 378, June 1998.

[8] S. J. D. Phoenix and S. M. Barnett, "Quantum Cryptography Using Discarded Data", British Telecomm. PLC., Int. Pat. Pub. No. 94/08409, April 1994.

[9] C. H. Bennett, IBM Corp., "Interferometric Quantum Cryptographic Key Distribution System," US Patent No. 5, 307, 410, April 1994.