Secure Message Relay over Networks with QKD-Links

Stefan Rass† and Mohammed Ali Sfaxi+ and Solange Ghernaouti-Hélie* and Kyandoghere Kyamakya†
† Institute for Smart-System Technologies, Klagenfurt University, Austria
+ ADHOC PES AG 4123 Allschwil Switzerland
* ISI - University of Lausanne 1015 Switzerland
{stefan.rass, kyandoghere.kyamakya}@uni-klu.ac.at, mohamed-ali.sfaxi@adhoc.ag, sgh@unil.ch

***Abstract*—This paper presents extensions to the classical point-to-point protocol PPP [RFC1661] and IPSEC [RFC 2401] in order to build networks that can do unconditionally secure message relay. Our work addresses the problem of how to integrate quantum key distribution (QKD) in networks such that little effort needs to be put on protocol engine adaption and network topology design. This article demonstrates how to ensure correct routing and secure authentication between adjacent QKD-capable nodes, in particular, it is demonstrated how a person-in-the-middle attack can be countered using universal hash functions.**

I. INTRODUCTION

The last two decades have witnessed the rise of a new technology of secure message transmission, which is called *quantum cryptography* or *quantum cryptographic key distribution* (QKD). The first such protocol BB84, given in 1984 by Charles Bennett and Gilles Brassard can be proven to be unconditionally secure (see, for instance, [Shor and Preskill, 2000]), however, by definition, this approach can only realize key establishment between directly connected nodes. Due to physical reasons, the distance over which photons can successfully be transmitted is way too much limited to have it applicable between cities or across the ocean. It is technically no problem to define networks which perform packet-forwarding over QKD-secured links, however, the plaintext necessarily shows up at each intermediate node along the message-path. Another problem is related to the authentication, since QKD itself cannot ensure the identity of the other party.

This paper aims at addressing the following problems, while proposing solutions which can be implemented by nowadays available technological means. Moreover, we explicitly do not consider nor confine ourselves to any specific form of QKD (several of which exist). We explicitly treat QKD as a *primitive*, which lets us secure links in an information-theoretically secure manner, and we demonstrate how to create networks inheriting the capability of unconditionally secure message relay from their links. In detail, we shall give ideas on how to solve the following issues that naturally arise when building a practical QKD-based network:

1) How to perform key distribution over multi-hop connections?
2) How to secure the corresponding routing process?
3) How to authenticate adjacent nodes in an unconditionally secure manner?

The advantage of our approach is twofold: First, it relies on QKD-extended versions of existing protocols. It has been demonstrated how to create advanced point-to-point protocols using QKD and how to extend the capabilities of IPSEC in order to benefit from the new technology. The wide acceptance and implementation of these protocols make them natural candidates for augmentation with QKD, and thus for being building blocks of future unconditionally secure networks. Second, we explicitly aim at using the simplest possible form of QKD to achieve maximum security. We consider QKD itself as a black box without relying on specific features of a certain QKD method. Our protocols thus work with BB84 equally well as with more complicated (and thus more expensive) forms of QKD, which may be still in the experimental stage.

This paper is organized as follows: Section II motivates the need for securing transmission within the link layer (layer 2) of the Open Systems Interconnection (OSI) reference model[1], and sections II-A and II-B summarize the extensions to PPP and IPSec based on QKD. Section III contains our results concerning the construction of suitable networks and the protocols for multi-hop secret distribution. Secure routing algorithms and authentication schemes are sketched in that context. The paper closes with a discussion of related work.

II. INTEGRATING QKD IN OSI LAYER 2 PROTOCOLS

Securing layer 2 transmission is fundamental because this service is common and necessary to all kinds of nodes' connections. The security processing is done transparently to the users and to the other protocols. Securing the link layer is more optimized than securing the upper OSI layers since neither additional encapsulation nor header is required in level 2.

The Point to Point Protocol [RFC1661] is a link layer protocol, widely used to connect adjacent nodes. The service of data confidentiality during transmission is not offered by the original protocol, but it has been introduced later by supporting the Encryption Control Protocol [RFC1968]. This protocol uses the classical cryptography (algorithms such as

[1]ISO International standard IS 7498 and X.200 ITU Recommendation

0-7695-3085-0/08 $25.00 © 2008 IEEE
DOI 10.1109/ICQNM.2008.14

DES or 3DES). Since traditional cryptography is not based on "unconditional" evidence of security in term of information theory, but on unproven mathematical conjectures, it rests thus on what one calls *computational intractability assumptions*, i.e. on the assumption that certain problems are difficult to solve and that one can control the lower limit of time necessary for the resolution of these problems [Alléaume, 2004]. In this context, security cannot be guaranteed. It is a crucial problem for an effective protection of sensitive data, critical infrastructures and services. Using quantum cryptography concepts, the sender and the receiver could exchange secret keys. This exchange is proven to be unconditionally secure. Quantum key distribution with the One Time Pad [Shannon, 1949] brings an unconditional security aspect to the communication upon the layer 2.

A. THE USE OF QKD TO SECURE PPP (Q3P)

As we have seen previously, the key exchange is not considered in the common use of the encryption algorithms. This fact leads to a misuse of cryptography in PPP. The Quantum Key Distribution is scientifically proven to be an unconditional secure way to share keys. That is why QKD has been proposed to exchange the secret key between two nodes [Ghernaouti-Hélie and Sfaxi, 2005].

Q3P Requirements Some requirements must be satisfied to integrate quantum cryptography within PPP.
Firstly, an optical channel: The optical channel is the physical link between two adjacent nodes. Nowadays, there are two means, which are able to carry a quantum cryptography transmission: the optical fibre or the free space (the air) [Hughes et al., 2002]. As quantum cryptography uses photons to encode the information, no other channel could be used up to now. However, quantum physicists are experimenting on the use of atoms and electrons as a quantum particle [Tonomura, 2005], [Knight, 2005]; maybe other kinds of channel could be used in the future.
Secondly, a Q3P modem is required: This modem has to polarize, send and detect photons; it has to include a photon detector and a laser with a single photon emitter and photon polarizer. The source and the detector are widely commercialized and many techniques are employed[2]. However, these devices are used to exchange the quantum key. The modem in this case is a simple optical fiber modem.
Thirdly, in order to establish an unconditional secure key, a quantum key distribution protocol is needed. This protocol must be implemented in the Q3P modem. The protocol will deliver a secure key after distilling the key and error correction [Gisin et al., 2002]. The key is stored in a flash buffer memory and used for enciphering the data. The QKD protocols BB84 and B92 [Bennett and Brassard, 1984], [Bennett, 1992] are nowadays the quantum cryptographic protocols widely used. These protocols have been proven secure and are largely experimented [Guenther, 2003].

[2]Idquantique : www.idquantique.com
magiQ www.magiqtech.com
CNRS France : http://www2.cnrs.fr/presse/journal/1979.htm

In some cases, the two nodes (Alice and Bob) are not directly connected. For this reason, the use of OSI layer 3 protocols (network layer) to carry out cryptographic tasks is a necessity. IPSec could be used in order to exchange secure data between 2 points over a network. The following section presents the use of QKD in IPSec to obtain an unconditional secure data exchange.

B. INTEGRATING QKD IN IPSEC TO SECURE A NETWORK

IPSec [RFC 2401] is a collection of protocols and algorithms and is a flexible framework that allows vendors who use IPSec in their products to select the algorithms, keys, and authentication methods they want to use. IPSec provides two basic security services: Authentication and Confidentiality.

IKE (Internet Key Exchange) is a system developed specially for IPSec to give authentication mechanisms and exchanging keys within the possible situations over the Internet. It is composed of many elements: ISAKMP [RFC 2408] and a part of Oakley [RFC 2412] and SKEME [Labouret, 2002].

Limits of IPSec and the benefits of using Quantum cryptography The vulnerability with Internet Key Exchange (IKE) [RFC2409] of IPSec is the risk of compromising the first key exchange. In fact, the point is only secured either by a pre-shared secret or by Diffie-Hellman key establishment. Classical cryptography is usually not unconditional secure. That is why a substitution with quantum cryptography can provide an efficient and unconditionally secure solution of this issue (see also [Paterson, K.G. and Piper, F. and Schack, R., 2004]).

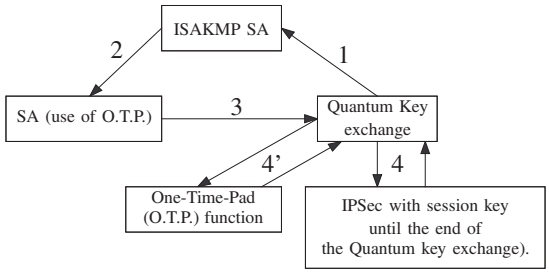

Fig. 1. Functioning of IPSec with Quantum Cryptography

SEQKEIP Operating Mode: As IPSec uses classical cryptography to secure communication, in this paragraph, the use quantum cryptography to replace the classical cryptographic protocols used for symmetric key-distribution is proposed. We assume in the following that it is possible to share a quantum key over the network. This exchange is studied in the next section. A QKD solution for IPSec is called SEQKEIP [Ghernaouti-Hélie et al., 2005], which is not based on IKE but on ISAKMP. Using this method, we avoid the problem of compatibility between IKE and QKD [Elliott, 2002], [Elliott et al., 2003]. SeQKEIP runs nearly like the IKE [RFC2409]. It includes 3 phases: phase 1 for the negotiation of the ISAKMP SA, phase 2 for the negotiation of

SA and we add a phase called "phase 0" in which Alice and Bob will share the first secret key. In the beginning (Figure 1), phase 0 and phase 1 start (1&2). After these two phases, the parameters of the protocol (such as the encryption algorithm, hash function,...) are fixed [Ghernaouti-Hélie et al., 2005]. In phase (3), the key exchanged (thanks to quantum cryptography) is used. This key will be used either as a session key (4) or in the one-time-pad function (4').

In (4), traditional symmetric cryptography algorithms to exchange data are employed. The IPSec packets are the same as without the use of quantum cryptography. The session key, therefore, is exchanged using quantum key exchange. The lifetime of the session key is very short and it is equal to the time needed to exchange the secret key using quantum cryptography. This solution is the transition (4') (cf. fig. II-B). In (4'), we use quantum cryptography concepts totally. The secrecy is completely shifted to the unconditionally secure functions, i.e. quantum key exchange and one-time-pad function.

As mentioned above, the quantum key exchange is assumed possible between any two nodes over a quantum network (a network over which QKD is possible between two adjacent nodes). The following section presents a method for establishing secrets between any two nodes within the network.

III. QKD OVER MULTI-HOP CONNECTIONS

A. Network Topology and Security

By definition, quantum key distribution can only be done between adjacent nodes, which naturally limits the maximum range of such protocols. Furthermore, an intermediate relaying node has to be trustworthy [Alleaume et al., 2007] in order to avoid leakage of secrets. The security of the entire system is hence vitally dependent on the trustworthiness of the relaying nodes, and in turn of the technical measures to ensure this. To the best of our knowledge, the only previous attempt to relax this requirement is based on a secret-sharing-like approach and the creation of a suitable network topology in order to guarantee the existence of several non-intersecting paths between any two nodes [Rass et al., 2006]. However, unconditional secrecy up to a threshold of n compromised nodes is bought at the price of an n-times higher transmission effort due to the secret sharing technique. This paper aims at achieving the same security level, but with a constant amount of $2 \cdot \text{length}(M)$ bits for a message M (neglecting protocol-induced packet overhead).

The main idea of exploiting QKD over multi-hop connections is to refrain from exchanging a key over a long distance, but to use QKD on each intermediate link to hamper an adversary eavesdropping a fixed number of nodes. More specifically, we first let Bob choose a key k, split it into several shares and send each share over a unique path to Alice. Upon reconstructing the key, she can send the entire one-time-pad encrypted message back to Bob over a single channel.

The natural question arising from this idea is the existence of disjoint paths, which is not guaranteed in general. However, since quantum cryptography has not yet seen a world-wide implementation, networks can be built incrementally such that with little additional effort, any node-connectedness number can be achieved. The key-results to this derive from classical results of graph theory and can be stated as follows: We call a graph $G = (V,E)$ t-connected, if any subset $U \subseteq V$ with $|V| - |U| \leq t$ is connected, i.e. by removing up to t nodes, we cannot disconnect the graph. A theorem due to Hassler Whitney [Chartrand, 2005], then states that a graph G is t-connected if and only if at least t node-disjoint paths exist between any two nodes in the network. This fact is at the base of the following results (proofs of which can be found in [Rass, 2005]):

Proposition III.1. *The complete graph K_{t+1} (with $t+1$ nodes) is the smallest graph being t-connected, i.e. no subgraph of K_{t+1} is t-connected.*

Proposition III.2. *Let $G_1 = (V,E)$ be a t-connected graph, and let $v \notin V$ be a node. Then for any subset $U \subseteq V$ with $|U| \geq t$, the graph $H = (V \cup \{u\}, E \cup \{(u,v) | u \in U\})$ is t-connected.*

Proposition III.3. *Let $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ be t-connected graphs. Select two sets $W_1 = \{v_1,\ldots,v_t\} \subseteq V_1, W_2 = \{w_1,\ldots,w_t\} \subseteq V_2$ and create the graph $H = (V_1 \cup V_2, E_1 \cup E_2 \cup \{(v_i,w_i) | v_i \in W_1, w_i \in W_2, i = 1,\ldots,t\})$ Then H is t-connected.*

These facts easily give a method to incrementally create t-connected networks for any a-priori fixed security parameter t (threshold): Starting with the smallest possible graph which is t-connected, we first create the complete graph K_t (prop. III.1). A single node v can be merged by connecting it to at least t nodes in the network (prop. III.2). Combining propositions III.2 and III.3, we can merge two arbitrary networks into a single t-connected network by first making both t-connected, and then adding at least t links between the networks. Making an arbitrary network t-connected is easy, since prop. III.1 and III.2 tell that we can first create a t-clique and then join the remaining nodes.

B. Secure Transmission

Sending a message M of length l securely over a t-connected graph now proceeds as follows (recall that quantum channels are *solely* used for key establishment, while any other protocol message is conveyed over classical channels or networks):

1) Bob chooses a secret key k of length l and encrypts it using a symmetric cipher E with a strong avalanche effect[3] and a key k' of shorter length (standard length for the chosen symmetric scheme). He then splits the ciphertext $C = E_{k'}(k)$ into $t-2$ blocks, which are enumerated appropriately to let Alice reconstruct it later. The $(t-1)$-th block is of the form $(k', \text{checksum}(k'), \text{padding})$. This will later allow Alice to recognize this block among the others.

[3]The *avalanche effect* is a property of cryptographic algorithms, typically symmetric ciphers or hash functions, that intuitively means the following: Given two inputs x,y that differ by a single bit, call the outputs of the function (e.g. symmetric cipher or hash) x',y', respectively. Then each bit of x' will differ from its corresponding bit in y' with probability 1/2 [Webster and Tavares, 1986].

2) He then sends the blocks over $t-1$ disjoint paths to Alice. Forwarding the message at each node proceeds as if the nodes were trustworthy (cf. [Alleaume et al., 2007]), and authentication (see below) is done prior to any transmission. The technical realization of this transmission is carried out by the Q3P and SEQKEIP protocols described in the previous sections.
3) Alice checks each block she received for the special structure of the $(t-1)$-th "key"-block. Once she has identified the key, she can decrypt and re-construct Bob's initial key k.
4) She proceeds by one-time pad encrypting her message M with k and sending it back to Bob over the last (t-th) path to Bob.

C. Security Analysis

As long as an adversary does not call all shares his own, the avalanche effect will give equal probability for each bit in the final output to be zero or one unless all other bits are known. Assuming that at most $t-1$ nodes are compromised, even if the "key"-block is among the eavesdropped packets, the one (or more) missing packets will render the reconstructed key useless for an adversary. Furthermore, it is impossible to eavesdrop the sender's node itself to gain information about all packets, since QKD ensures that the links cannot be eavesdropped, and Alice uses at least t nodes for sending her information to the outside world.

To summarize, even although the employed symmetric ciphers are *not* unconditionally secure, the avalanche effect will make all message bits dependent on the packets an adversary does not possess. Since each bit of the ones the adversary can reconstruct is correct with probability $1/2$, no reliable information is gained. Hence, *unconditional* security is achieved upon assuming that at most $t-1$ nodes are compromised, intermediate channels are QKD secured and the avalanche effect of the symmetric cipher.

The resulting message overhead is approximately $2l$ (neglecting enumeration of packets), regardless of the number of paths employed. This is an improvement upon the work of [Rass et al., 2006].

Graph topology can only ensure the possibility of sending messages unconditionally secure under the assumption that at most $t-1$ nodes are being compromised, but there are two more aspects to be considered:

1) Secure routing
2) Authentication

D. Routing

An adversary could intervene such that packets become routed all over one or a couple of compromised nodes, which may allow for a (partial) reconstruction of the message. In order to avoid such intersections between paths, [Rass et al., 2006] proposes adding the full path information to a packet before sending it, but double encrypted in the following manner: Taking two QKD-established secrets σ_1, σ_2 between two nodes u, v, the routing information R is encrypted as $E_{\sigma_1}(R) \oplus \sigma_2$, where $\oplus$ denotes the XOR-operation, and E_σ is a symmetric cipher exhibiting a strong avalanche effect. An adversary Eve now can either have compromised an entire path or multiple paths, but not more than $t-1$ nodes by our assumption. If an entire path is compromised, then Eve still lacks the information from the other paths, and thus wins nothing. On the other hand, having compromised multiple paths, but not every node on every path, there must exist at least one honest node over which the message gets passed. If Eve now wants to forge the information, she can either

- Refrain from adding her signature from the list of passed nodes,
- Intercept and forge the path information when it is passed between two honest nodes, or
- Add a faked path information.

Since there must exist at least one honest node (different from Alice's or Bob's node) on the path, a missing or faked signature on the path information will be detected by this node, since authentication should fail in the latter case. The avalanche effect on the other hand renders $E_{\sigma_1}(R)$ useless for encrypting a forged routing information R', since $E_{\sigma_1}(R')$ and $E_{\sigma_1}(R)$ differ in each bit with probability $\frac{1}{2}$ (due to the avalanche effect triggered by $R \neq R'$), so $E_{\sigma_1}(R)$ is useless for creating $E_{\sigma_1}(R')$ unless we know σ_1. But exhaustive search for σ_1 is prevented by the one-time pad with σ_2, none of which is known to Eve.

IV. Authentication

Impersonating another node is Eve's third option of having packets routed over her nodes multiple times. Her natural situation in our setting is a person-in-the-middle attack, which is the only case in which we require a secret key to be existent prior to any communication for a successful defense against this attack: To initiate a communication, Alice exchanges a key σ with a remote node X, which she believes to be Bob. Bob does the same, i.e. exchanges a key $\overline{\sigma}$ with a remote node Y, which pretends to be Alice. In other words, with no adversary in the middle, we have $X = \text{Bob}, Y = \text{Alice}$ and $\sigma = \overline{\sigma}$. However, if Eve sits in the middle, then we have $X = Y = \text{Eve}$, so Eve shares secrets σ and $\overline{\sigma}$ with Alice and Bob. This situation is depicted in figure 3. Now, Eve can passively relay the messages from Alice to Bob and vice versa. Regardless of the protocol Alice and Bob use for authentication, Eve will not be detected. Certainly, if approaches similar to quantum cryptographic key-exchange are used, then Eve can be detected while listening on the communication channel. However, eavesdropping is not even necessary, as Eve just has to wait until Alice and Bob have successfully authenticated each other. After Alice and Bob have established mutual confidence, they start exchanging secrets by means of quantum cryptography. But, since Eve shares secrets with Alice and Bob, she can read all messages transferred between Alice and Bob only by intercepting and re-sending each message appropriately. Note that under this setup, Eve will be successful *regardless* of the authentication protocol, which Alice and Bob execute! This section shall

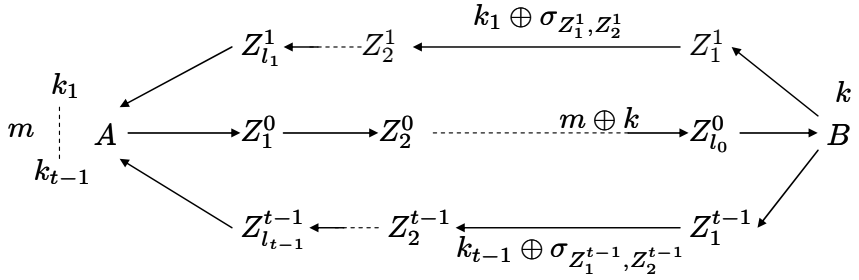

Fig. 2. Transmission of m from Alice (A) and Bob (B).

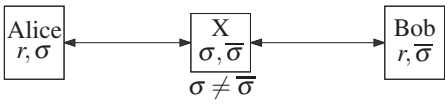

Fig. 3. An adversary sitting between Alice and Bob.

provide a method for avoiding this attack, hence realizing an information-theoretically secure authentication of Alice and Bob even in the presence of an adversary sitting in the middle.

Based on the assumption that $\sigma \neq \overline{\sigma}$ (which can be ensured by suitable privacy authentication), detection of Eve intuitively proceeds as follows: Assume that prior to any communication, Alice and Bob possess a common secret r, which is completely unknown to Eve. Such a secret could be exchanged via Smart-Cards or during manufacturing the nodes. Alice and Bob possess keys σ and $\overline{\sigma}$ being at least twice as long as r, say n bit, i.e. $2n = \text{length}(\sigma) = \text{length}(\overline{\sigma}) = 2\text{length}(r)$. The parameter n is publicly known to all parties. Fixing n as a system-wide parameter also avoids re-blocking problems arising from users using parameters of different length. For Alice and Bob to authenticate each other, Alice takes the first n bits k of σ, attaches a suitable MAC $z = s(k,r)$ using her private shared secret r and sends the message (k,z) to Bob. Two cases can be distinguished:

1) There is no adversary in the middle. Then Bob successfully verifies $z' = \overline{z}$, where z' is the value he received from "Alice" and $\overline{z}$ is the MAC he calculated from the first n bit of his key $\overline{\sigma}$. If this verification succeeds, Bob takes the second n bits from $\overline{\sigma}$ and uses them for proving his identity to Alice. If she accepts, then both can establish new secrets by means of QKD.
2) Eve sits in the middle and possesses mutual secrets shared with Alice and Bob. In this case, Eve should not be able to choose the bits of σ and $\overline{\sigma}$ freely, so we will have $\sigma \neq \overline{\sigma}$. Forging the message (k,z) such that $(\overline{k},\overline{z})$ is received and accepted by Bob, should not work because of the MAC z which is dependent on r, which in turn is unknown to Eve. Hence, for an "information-theoretically secure" MAC z, Eve will always be detected.

Any of the well-known (strongly) universal$_2$ classes of Hash-functions (or families constructed from these) may be applied to implement this protocol. (cf. [Stinson, 1992] or [Nevelsteen and Preneel, 1999] for an overview). A more recent account for the authentication problem in QKD settings is given by [Peev et al., 2005].

There are several other benefits we gain from general t-connectedness of a network (for $t \geq 2$): Safety increases, as failure of at most $t-1$ nodes will not make the network go down. Unconditional security can be provided for several concurrent connections. If the protocol above is adopted for secret relaying, then $\lfloor \frac{t}{2} \rfloor$ connections can run concurrently and securely in a t-connected network. Finally, we get better security for single connections, as higher connectivity in connection with the generalized message-relay.

V. RELATED WORK

The problem of an adversary redirecting packets is addressed in a work of [Sanzgiri et al., 2002]. This approach prevents redirecting packets using a certificate-based routing method, which we avoid as we protect our routing information by double-encryption rather than signatures to achieve information-theoretic security which is impossible for schemes based on public-key cryptography. Similarly, the security of the scheme proposed in [Castro et al., 2002] relies on (computationally secure) certificates, which we explicitly avoid by using shared secrets based on quantum cryptography.

Work on secure routing often focuses on *Byzantine attacks*, where multiple active adversaries are allowed inside a network [Hu et al., 2002]. Like for these attacks, our scheme too can handle corruption of up to t nodes, while still retaining information-theoretic security of our messages. Similar assumptions as ours were adopted by [Awerbuch et al., 2003] (assuming no trusted third party services and mutually authenticated nodes, as well as active adversarial nodes), but this work focuses on how to deliver the package over the network. On the contrary, our proposal keeps the delivery secure by perfectly concealing the routing information, such that misrouting is either impossible or detectable. [Awerbuch et al., 2004] allows an adversary to mount almost arbitrary attacks, which are repelled using a swarm-intelligence based routing strategy. In contrast, our approach is capable of preventing misrouting at negligible computational cost as well as preventing any

modification on the communications paths by using one-time pad for encryption. Active modifications by adversarial nodes having the information flowing through them will be detected as described previously.

VI. CONCLUSION

Upon the work of [Ghernaouti-Hélie et al., 2005] and [Ghernaouti-Hélie and Sfaxi, 2005] we have built a framework for delivering messages over networks in which adjacent nodes are able to establish symmetrical secrets by means of quantum cryptography. On the contrary to classical approaches which are based on unproven intractability assumptions, we propose a solution that can be shown to be information-theoretically secure. The importance of securing data transmission inside OSI layers has been argued in [Ghernaouti-Hélie et al., 2005] and [Ghernaouti-Hélie and Sfaxi, 2005] and this article extends this framework to routing issues layer 3.

Our proposed protocols are easy to implement, efficient in terms of overhead and require only particular topological properties of the underlying network. These properties can be achieved efficiently by applying procedures given in this paper. The formal correctness of the procedures has been established.

The approach does not rely on any particular form of quantum encoding or on quantum computers, so it is implementable using technology which is commercially available (IdQuantique has a commercial product available which such networks can be built upon. See `www.idquantique.com`) As a side-effect, we gain safety in terms of node-failure, thus cover many issues being considered in the context of secure routing.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewer(s) for their helpful comments on the presentation of the results and for pointing out typos and sections which require further clarification. The authors further acknowledge the support given by some SECOQC project members regarding important preliminary work on the presented solutions (www.secoqc.net).

REFERENCES

[Alléaume, 2004] Alléaume, R. (2004). Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique. Technical report, SECOQC partner.

[Alleaume et al., 2007] Alleaume, R., Bouda, J., Branciard, C., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Langer, T., Leverrier, A., Lutkenhaus, N., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H., and Zeilinger, A. (2007). Secoqc white paper on quantum key distribution and cryptography.

[Awerbuch et al., 2003] Awerbuch, B., Holmer, D., and Rubens, H. (2003). Provably secure competitive routing against proactive byzantine adversaries via reinforcement learning. Technical Report 2, Department of Computer Science at Johns Hopkins University, Baltimore, MD.

[Awerbuch et al., 2004] Awerbuch, B., Holmer, D., and Rubens, H. (2004). Swarm intelligence routing resilient to byzantine adversaries.

[Bennett, 1992] Bennett, C. (1992). Quantum cryptography: Uncertainty in the service of privacy. In *Science 257*.

[Bennett and Brassard, 1984] Bennett, C. and Brassard, G. (1984). Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems, and Signal Processing.*, LOS ALAMITOS. IEEE Press.

[Castro et al., 2002] Castro, M., Druschel, P., Ganesh, A., Rowstron, A., and Wallach, D. S. (2002). Secure routing for structured peer-to-peer overlay networks. *SIGOPS Oper. Syst. Rev.*, 36(SI):299–314.

[Chartrand, 2005] Chartrand, G. (2005). *Introduction to graph theory*. Higher education. McGraw-Hill, Boston.

[Elliott, 2002] Elliott, C. (2002). Building the quantum network. *New Journal of Physics*, (4 (46.1-46.12)).

[Elliott et al., 2003] Elliott, C., Pearson, D., and Troxel, G. (2003). Quantum cryptography in practice.

[Ghernaouti-Hélie and Sfaxi, 2005] Ghernaouti-Hélie, S. and Sfaxi, M. A. (2005). Upgrading PPP security by quantum key distribution. In *NetCon 2005 conference*.

[Ghernaouti-Hélie et al., 2005] Ghernaouti-Hélie, S., Sfaxi, M. A., Ribordy, G., and Gay, O. (2005). Using quantum key distribution within IPSEC to secure MAN communications. In *MAN 2005 conference*.

[Gisin et al., 2002] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, (74).

[Guenther, 2003] Guenther, C. (2003). The relevance of quantum cryptography in modern cryptographic systems. GSEC Partical Requirements (v1.4b).

[Hu et al., 2002] Hu, Y.-C., Perrig, A., and Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proc. of the 8th Annual International Conference on Mobile Computing and Networking* (MobiCom 2002), pages 12–23.

[Hughes et al., 2002] Hughes, R., Nordholt, J., Derkacs, D., and Peterson, C. (2002). Practical free-space quantum key distribution over 10km in daylight and at night. *New Journal of physics*, 4.

[Knight, 2005] Knight, P. (2005). Manipulating cold atoms for quantum information processing. In *QUPON conference Vienna*.

[Labouret, 2002] Labouret, G. (2002). IPSEC: présentation technique. Hervé Schauer Consultants (HSC).

[Nevelsteen and Preneel, 1999] Nevelsteen, W. and Preneel, B. (1999). Software performance of universal hash functions. In *EUROCRYPT*, pages 24–41.

[Paterson, K.G. and Piper, F. and Schack, R., 2004] Paterson, K.G. and Piper, F. and Schack, R. (2004). Why Quantum Cryptography? http://eprint.iacr.org/2004/156.pdf.

[Peev et al., 2005] Peev, M., Nlle, M., Maurhardt, O., Lornser, T., Suda, M., Poppe, A., Ursin, R., Fedrizzi, A., and Zeilinger, A. (2005). A novel protocol-authentication algorithm ruling out a man-in-the-middle attack in quantum cryptography. *Int.J.Quantum Inform.*, 3:225–232.

[Rass, 2005] Rass, S. (2005). How to send messages over quantum networks in an unconditionally secure manner. Technical Report TR-syssec-05-05, University of Klagenfurt, Computer Science, System Security, Klagenfurt.

[Rass et al., 2006] Rass, S., Sfaxi, M. A., and Ghernaouti-Helie, S. (2006). Achieving unconditional security in existing networks using quantum cryptography. In *SECRYPT*, pages 207–210.

[Sanzgiri et al., 2002] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. In *ICNP '02: Proc. of the 10th IEEE International Conference on Network Protocols*, pages 78–89, Washington, DC, USA. IEEE Computer Society.

[Shannon, 1949] Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715.

[Shor and Preskill, 2000] Shor, P. W. and Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444.

[Stinson, 1992] Stinson, D. R. (1992). Universal hashing and authentication codes. In *CRYPTO '91: Proc. of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 74–85, London, UK. Springer-Verlag.

[Tonomura, 2005] Tonomura, A. (2005). Quantum phenomena observed using electrons. In *QUPON conference Vienna*.

[Webster and Tavares, 1986] Webster, A. and Tavares, S. (1986). On the design of S-boxes. In *Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85*, pages 523–534, New York, NY, USA. Springer-Verlag New York, Inc.