Quantum Cryptography
For Secure Optical Networks

Stamatios V. Kartalopoulos
Williams Professor in Telecommunications Networking
The University of Oklahoma
4502 E. 41st Street, Tulsa, OK 74135, USA

Abstract- Dense Wavelength Division Multiplexing optical networks transport a huge aggregate traffic exceeding Tbps per single fiber, and passive optical network technology has been extended to include the residential and enterprise network layer with Fiber-to-the Premises. Because this network allows for multimedia and extremely high data rates to end-users, optical communications security is important not only on the client and the node management layers, but also on the physical layer. Thus, cyber-security becomes also important in optical networks, including unbreakable cipher keys, cipher key distribution, identification of malicious actors, source authentication, physical link signature, and countermeasure strategies. In this paper we overview the security of the WDM optical network. We discuss advanced cryptographic methods that stem from quantum mechanics, known as quantum cryptography, and we identify specific vulnerabilities. We also look into the security of the next-generation optical network.

I. INTRODUCTION

Optical communications and cryptography have entered the realm of science and mathematics, especially during the World War II. The main reason was the advent of electromagnetic wave transmission that would reach both friendly and foe antennas. The last two decades the exponential spread of the Internet, which was not designed with robust security features in mind, opened the appetite of bad actors for invading the data network with destructive results. We list only a couple to make the point:

- The post 9/11/2001 cyber attack that is known as “Code Red” infected 150,000 computers in just 14 hours and two months later the attack “NIMDA” infected 86,000 computers.
- The Congressional Research Service Report to Congress (April 2004) reported that “Estimates of total world-wide losses attributable to attacks in 2003 range from $13 billion due to viruses and worms only to $226 billion for all forms of overt attacks”.

These reports and others have raised a serious concern by government and industry that have placed network security on high national priority and an Internet Security Alliance was formed.

In this paper overview data security and we present the conditions for optical networks security and countermeasures. We discuss advanced cryptographic methods, or quantum cryptography, that stem from quantum mechanics, and we identify vulnerabilities. We finally take a closer look in the security of the next generation optical network.

2. CRYPTOGRAPHY IN COMMUNICATIONS

A. Cipher-Text Generation

In digital cryptography the cipher key changes the form of the original data so that it is unintelligible but to the intended receiver. This is the encoding phase that transforms data to cipher-text. A cipher-key is a random string of binary bits. Thus, if the text is 800 bits long, then the key should be 800-bit long and by Exclusive-Or’ing the two bit by bit the cipher-text is generated:

Text: 0 0 1 1 1 0 0 | 1 1 0 0 1 1 0 | 0 1 1 0 1
1 1 0 | 0 0 0 1 1 1 1 | …

Cipher-key: 1 1 1 0 0 1 0 | 1 0 0 0 1 0 1 | 1 0 0 0 0 1
0 1 1 | 0 1 1 1 0 1 1 | …

Cipher-text: 1 1 0 1 1 0 | 0 1 0 0 0 1 0 | 0 0 1 0 1
1 0 1 | 0 1 0 0 1 0 0 | …

The original text is recovered from the cipher-text using the modulo-two property, if C=A⊙B then A=B⊙C:

Text: 0 0 1 1 0 0 | 1 1 0 1 1 0 | 0 1 1 0 1
1 1 0 | 0 0 0 1 1 1 | …

Ciphertext: 1 1 0 0 1 0 | 0 1 0 0 0 1 | 0 0 1 0 1
1 0 1 | 0 1 0 0 1 0 0 | …

Offset Cipher-key: 0 1 1 0 0 1 | 0 1 0 0 0 1 | 1 0 1 0 0 0 1 | 1 0 1 1 1 1 1 | …

Recovered false Text: 1 0 1 0 1 1 | 0 0 0 0 0 0 | 1 1 0 0 1 0 0 1 | 1 1 0 1 1 0 0 1 | …
B. Cipher-key distribution

There are two encoding methods, asymmetric key and symmetric key. The asymmetric uses different keys for ciphering and for deciphering. The symmetric uses the same key for ciphering and for deciphering. Asymmetric key is more applicable where the transmitter does not communicate with the recipient of the cipher-text. However, this method has a weaker key and thus it is more probable to be broken. The symmetric key is more difficult to break but it requires a secure key distribution method, because it presents an opportunity to eavesdroppers.

Symmetric encryption methods are classified in two major classes. Those that transport the encryption key (stored in a secured memory device) by a courier and those that transport the encryption key over a separate network path. Methods of the first class have been used since recorded history. Recently, methods of the second class are in favor because they eliminate the human factor and they allow the encryption key to change frequently. In addition, certain precautionary practices are recommended, such as “restrict access of information on a need to know basis”, “use unique IDs to each person for access”, “test security regularly”, and “restrict the physical access to information”.

III. SECURITY IN OPTICAL NETWORKS

Optical networks based on the Wavelength Division Multiplexing (WDM) technology transport a humongous aggregate traffic that exceeds Tbps per single fiber. This traffic consists of tributaries that contain classified, private and sensitive information from clients in the government and finance sector. This type of information presents an opportunity to sophisticated eavesdroppers; even a small success in reading data brings large rewards. Eavesdropper are intrigued by the notion that credit card information, bank accounts, health and personal records, and sensitive documents can be harvested even if they are ciphered. This possibility that a third party may be able to harvest or inject misrepresenting data in the network has generated a growing concern to industry and government alike.

Traditionally, the security of optical networks is separated into three areas:

Network administration security relies on access identification codewords, passwords and firewalls to access the control function of a node for OA&M (operations, administration and management), node provisioning, and so on. Access is granted to personnel only via the network management port; there is no access to customer traffic which enters and exits the node through data ports. However, a malicious person having the access codes may access the node.

Network access security is predominantly used in wireless and in asynchronous packet networks as part of the connectivity protocol during user authentication. In optical networks, the node is secured as in #1, whereas the transport medium has not been adequately addressed.

Data security or cryptography is typically left to end users. Cryptography uses sophisticated hidden methods within a text, scrambled ASCII characters, text watermarking, and other scrambling methods.

Because of the imminent danger, the activity in encryption algorithms has recently risen exponentially. However, the security of distributing the secret key is as critical as is the security of the physical transporting medium. Therefore, we propose that one more level should be included, the link path security:

Link and path security. Data security must extend beyond developing strong encryption algorithms, distributing the cipher key securely, and authenticating the source. It must include mechanisms for detecting malicious intruders, monitoring the physical link signature for integrity, developing countermeasures to protect the physical optical channel from tapping, and developing anti-masquerading methods to outsmart and confuse the intruder.

In optical communications, it is natural that the properties of photons are employed to create the key, the cipher-text and also distribute the key over fiber. Recently, a major research activity in the photonic regime explores the potential of quantum properties of photons and thus is dubbed quantum cryptography, as we describe in the next section.

VI. QUANTUM CRYPTOGRAPHY

No matter how smart an algorithm is, soon or later someone will outsmart it and break it. In fact, a new research effort known as steganalysis is doing just that: using sophisticated methods with advanced filtering methods, it examines encrypted methods and retrieves hidden messages in them. Thus, it is no surprise that researchers refocus on unconventional methods in search of the “holy grail” of cryptography, an algorithm with origins in quantum mechanics that produces an unbreakable key.

In classical theory, a binary system is in one of two states, logic “1” or logic “0”. However, quantum mechanic theory predicts that a system may be in a superposition of both states; that is, at logic “1”, logic “0” and also between the two states (the superposition of the two) as a result of uncertainty in the system. Based on this, quantum bit that defines not only the two binary eigenstates “0” and “1” but also the superposition of the two is known as a “qubit”. Qubits may represent the two spin eigenstates of electrons, +1/2 and -1/2, or the polarization states or any other quantized property of photons. Two eigenstates that are associated with the binary logic values “1” and “0” are mathematically denoted as:
Quantum computation [1, 2] is a method based on the quantum mechanical definition of the qubit, with applicability in a relatively new encryption method known as “quantum cryptography” [3]. The two-word term “quantum cryptography” does not mean that cryptography is quantized or that quantized quantities are cryptographic; it merely describes a technology that uses quantized properties, such as photon polarization, and hence “quantum”, and a sophisticated scheme to transmit a secret code using a sequence of randomly polarized photons from which an encryption key is constructed, hence “cryptography”. In quantum cryptography, the ciphered text generated by the quantum key is then known as “quantum cipher-text”.

Assume an optical link between two points A and B, where A (or Alice) transmits to B (or Bob). The question is, how can Alice create a quantum key that she only knows, and distribute it to Bob who will not know its details but who can use it to decipher the received text? The method that addresses this question generates a quantum key and distributes it to Bob, is known as “quantum key distribution” (QKD).

Many quantum cryptographic methods, and particularly QKD, use polarized photons. According to it, a subset of photon polarization states corresponds to logic “0”, whereas another subset of states corresponds to logic “1”; this becomes evident if one consults all polarization states on a Poincaré sphere [4, Chapter 1].

The polarization states and their logic correspondence are initially known to Alice and through a process explained below, Alice defines the encryption or quantum key and makes it (partially) known to Bob. Thus, the secrecy of this method and the encryption algorithm promises a secure communications channel.

A. Generation of quantum key and QKD

Consider that the quantum quantity used in an optical cryptographic system is the polarization states of the photons. On the Poincaré sphere, SoPs on one half of the hemisphere may be associated with logic “1” and on the other half with logic “0”, Figure 1.

Thus, if randomly polarized single photons are transmitted by Alice and received by Bob, then a secret key can be defined, a concept first described in 1989 by Charles Bennett, John A. Smolin and Gilles Brassard of IBM Thomas J. Watson Research Laboratory. However, this idea is based on the assumption that the optical transmission medium has no substantial loss over long lengths and no birefringence; that is, the medium is perfect. It is well known that practical fiber has an attenuation constant and birefringence, \( B = k|n_2-n_1| \), where \( k \) is a constant and \( n_1, n_2 \) are the refractive indices along the X-Y axes. In addition, it is very difficult to cost-efficiently generate single photons in a controllable manner and couple them onto the core of single mode fiber. What can be generated is a pulse of a few photons, in which case not all have exactly the same wavelength. Thus, photons experience chromatic dispersion in addition to polarization mode dispersion.

The various steps of the quantum key generation and QKD in quantum cryptography is explained with the addition of a bad actor between Alice and Bob who would like to eavesdrop, known as Evan. Thus, the task is to generate an encryption key that Alice only knows, that Bob can use (but he does not know its details) and that Evan cannot copy. For the QKD, the method considers two separate connecting paths between Alice and Bob. One is an optical fiber and the other a separate public channel, such as the Internet or the public wireless network, Figure 2. This type of public-key cryptography was first introduced by W. Diffie and M. Hellman in 1976 [3], who defined a pair of keys, \( e \) and \( d \), where \( e \) is a publicly available key and \( d \) is a private key. Although several protocols to accomplish this have been devised, we describe a straightforward one with the following logical steps:

1. Alice passes a sequence of binary bits, say 100110111011, through a random polarization filter. This sequence is transformed in a sequence of polarization states. A subset of polarization states is associated with logic “1” and another subset with logic “0”; the two subsets may be visualized as two regions on the Poincaré sphere. The association of polarization states with logic “1” and “0” are known to Alice only and unknown to anyone else, including Bob.

2. Bob receives the sequence of polarized photons which he passes through his independently randomly varying polarization filter, but Bob does not know...
the association between logic value and polarization state.

3. The random polarization states of his filter pass or reject the received randomly polarized photons. That is, a new sequence of logic “1s” and “0s” is generated in which some bits (statistically speaking and over a long string of bits) have the correct logic value that Alice sent but not all.

4. Assume that Bob’s randomly varying polarization filter generates the sequence 010110101001 from the sequence received from Alice. Although this sequence is not what Alice transmitted, the common bits between the two sequences are important here. However, up to this step, neither Alice nor Bob know which bits are common.

5. Bob communicates with Alice over the public unsecured channel and he tells Alice the polarization sequence that he used while receiving Alice’s polarized photons. However, Bob does not reveal the logic sequence that he generated.

6. Based on Bob’s response, Alice performs an experiment. She passes the logic sequence that she sent to Bob through Bob’s polarization sequence. Then, Alice compares the initial bit string with the one generated from the experiment and she identifies the bits that are common in the two bit strings.

7. Alice tells Bob which of his filter polarization states in the sequence were used correctly, but without telling him their association with logic “1” and “0”. The polarization states that were used correctly constitute the quantum key.

8. When all this is done, Alice encrypts her message with the established key using a modulo-2 operation bit-by-bit, Figure 3) and transmits the encrypted message to Bob, who deciphers it using the same encryption key.

B. Vulnerabilities and weaknesses of quantum cryptography

To date, several quantum cryptographic algorithms have been developed such as the Greenberger-Horne-Zeilinger [6], Bostroem and Felbinger [7] and Cai [8] which have been examined and found to have vulnerabilities to eavesdropping [9]. In addition, a few testbed networks have been established such as the one in Boston, USA, and the other in Vienna, Austria that consist of single mode fiber of a few kilometers long and thus the vulnerability issue is overlooked for the time being [10]. However, vulnerabilities may be used as a means to validate or invalidate a network security method and therefore it should be carefully examined before a method is more generally deployed. Some vulnerabilities of the QC method are:

* There are no simple off-the-shelf optical sources with controllable single photon rate generation and controllable photon polarization.
* Optical fiber must maintain the polarization state of photons: manufactured fiber must comply with tight physical, optical and mechanical specifications. However, variability of these specifications is real and so is attenuation, birefringence, dispersion, and other nonlinearities that affect the properties of propagating photons in the fiber.
* As photons propagate in birefringent single mode fiber, the polarization state of photons does not remain constant.
* The fiber link in point-to-point links should remain intact and uniform without splices, connectors and other optical components that may change the polarization state.
* A not-perfectly coupled single photon source onto optical fiber: typical photonic power coupled onto fiber suffers from attenuation. There is no reason to believe...
that coupling a single photon source onto fiber will not suffer from loss which may result in photon loss and thus increased quBit Error Rate (qBER).
* Optical fiber has absorption or scattering centers: at about 1400 nm, absorption peaks due to OH-, below 1300 nm and above 1620 nm increases due to absorption and Raleigh scattering. Currently, there is no zero-loss fiber in any part of the useful spectrum. In fact, to overcome this, researchers are thinking of quantum repeaters; that is, subsystems that will receive the polarized signal, restore its strength, and retransmit it. This of course may defeat the purpose of QKD because Evan can also have the same subsystem which with minor modifications can receive the signal, copy the polarized key, restore the polarization state of photons and retransmit it to Bob.
* A very long random bit sequence is required to warrant a good encryption key. Because the two filters at each end of the fiber are randomly and independently polarized, the number of bits from Alice’s sequence that will pass through Bob’s filter are fewer; it is those bits that constitute the encryption key. Thus, in order to warrant a relatively long encryption key (few hundred bits), very long sequences must be used.
* No acknowledgment by Bob that the negotiated encryption key works reliably or correctly. Bob must know if his polarizing filter behaves as prescribed by Alice from the first arriving photon in the encrypted message. Deciding when the first photon arrives is a task of its own.
* There is no mechanism to confirm that the key has been correctly constructed and that the encrypted message has been correctly received and decrypted. This identifies a potentially serious issue with QC robustness and a lack of verification. What if a malicious attacker affects one or the other polarizing filter? What if a malicious attacker adds propagation delay on the line so that filter synchronization is shifted by a bit period? Will Bob recognize it and reconstruct the message?
* To date, only dedicated point-to-point QC and QKD solutions are contemplated thus underutilizing the full bandwidth capacity of WDM. Only one experimental network contemplates a combined QKD (at 1310 nm) and a channel in the DWDM C-band, thus not utilizing the complete potential of DWDM spectrum.
* An eavesdropper may easily attack the transmitted polarization states on purpose. So far, the focus in QKD has been to prevent eavesdropping. However, it is equally important to prevent or countermeasure attacks. An attacker may tap the medium and maliciously destroy the QKD process and thus hamper transmission of the encrypted message. In such a case, an eavesdropper is not only a person that needs to “listen” but also one that hinders and deters successful communication between point A and point B; jamming is a well known form of communications deterrence.

* If multiphoton bit transmission is contemplated, then a small part of the photonic pulse may be extracted from the fiber (by sophisticated tapping) and thus break the encrypted message (assuming that the sophisticated eavesdropper can also “listen” to the conversation between Adam and Bob).

C. Photon entanglement

Another principle that is used in quantum cryptography is known as entanglement. In optical cryptographic systems, photon entanglement uses the two orthogonal states of a photon in the following manner. Consider a photon that is passed through a strongly birefringent crystal that creates two strongly orthogonal polarized states (also known as ordinary and extraordinary). Now, if the two states are combined so that they propagate together, then they are known as entangled states. Similarly, a photon of high energy (e.g., 800 nm) may be passed through a highly non-linear material such as barium-borate, which through photon-matter interaction may create two photons at half the energy each (400 nm). If these two photons are generated with orthogonal polarizations, then the two-photon system is called entangled photons. The entangled states constitute a secure system because, if one of the two entangled states is tapped, it affects the properties of the entangled photon system, which is monitored and detected at the receiver. However, as the entangled pair is coupled onto a standard single mode fiber, fiber non-linearity and birefringence will eventually separate the entangled states because of the polarization mode dispersion. Currently, laboratory experiments use an argon-ion laser single-photon source.

V. NETWORK VULNERABILITIES AND EVAN AT WORK

Consider Evan, a sophisticated malicious actor, who may not only want to eavesdrop, but who may want to mimic the source, that is, distribute encrypted false messages, or who may want to incapacitate communications security without cutting the fiber, which can be easily detected and repaired. The latter is a particularly unexplored area and very probable during network attacks. In such case, the tools to accomplish this are very simple; a small box of paperclips becomes a powerful anti-QKD weapon. Imagine that the malevolent attacker clamps paperclips on the fiber that carries quantum encrypted messages. The pinching pressure exerted on the fiber by the paperclips will:
* Change the propagation and polarization properties of photons in the fiber such that the polarization states transmitted by Alice arrive at Bob altered.
* Bob sends back to Alice an entirely inconsistent polarization pattern.
Alice, not knowing what is going on with Evan and his paperclips, tests the received pattern that Bob sent to her, finds the (erroneous) commonality, and she sends to Bob the encrypted message using a wrong quantum-key.

Bob receives a message that he cannot decipher.

Eventually, Alice and Bob will realize that the security of the quantum channel has been compromised. To continue communicating securely, Alice and Bob must try another fiber, which also may have been compromised. Thus, few paperclips make the quantum key distribution process useless, secret documents and sensitive information cannot be transported over fiber successfully, and in critical times they may cause mass confusion.

Although the aforementioned may seem hypothetical, it is a simple, inexpensive and reasonable scenario. In a simple experiment, we have confirmed how easily the state of polarization changes using paperclips and also very small tensile or bending force exerted on fiber.

VI. SECURITY IN OPTICAL NETWORKS

The next generation SONET/SDH network has been enhanced with protocols that will encapsulate many protocols including Internet, Fiber Channel, FICON, and more over the SONET/SDH over WDM [11]. Thus, it is possible that some data payloads encapsulated in it, such as internet, may contain sophisticated viruses. The fiber optic transmission medium and the all-optical network do not provide an opportunity to hidden viruses. The opportunity appears when hidden viruses are electronically buffered. However, as the sophistication of the network increases, so is the sophistication of the malicious attacker. Thus, it is more likely that an intruder would not attack via the payload space but via control messages if they are in long packets; control messages contain executables and perhaps text-like messages. Research in this area is in progress.

Another area of opportunity is the fiber-to-the premises (FTTP). Fiber in the enterprise and to the home may entice eavesdroppers as the average residential user may not have sophisticated encryption algorithms, and thus present easier opportunity for eavesdropping. Research in this area is also in progress.

VII. CONCLUSION

Security in communication networks is of extreme importance as it impacts the privacy of client data as well as national security. It has become apparent that, in addition to end-to-end encryption algorithms and network management security, it is necessary to secure optical links between nodes so that eavesdroppers tapping the light stream from a fiber are unable to decipher or to mimic information signals. In this paper we reviewed the security of optical networks, of quantum cryptography and we identified vulnerabilities. We also identified a simple and possible way of attacking quantum cryptography, and we took a brief look into the next generation optical network security. Research on cryptography and authentication continues and more advancements are expected to be announced in the near future.

REFERENCES