Security in Photonic Networks: Threats and Security Enhancement

Ken-Ichi Kitayama, *Fellow, IEEE*, Masahide Sasaki, Soichiro Araki, *Member, IEEE*, Makoto Tsubokawa, Akihisa Tomita, *Member, OSA*, Kyo Inoue, Katsuyoshi Harasawa, Yuki Nagasako, and Atsushi Takada, *Member, IEEE*

***Abstract*—We address emerging threats to the security of photonic networks as these networks become heterogeneous being opened to the upper layers, other operators, and end users. We review the potential threats, mainly loss of the confidentiality of user data transmitted through optical fibers and disturbances of network control, both of which could seriously damage the entire network. We then propose a novel conceptual model of a secure photonic network by introducing a quantum key distribution (QKD) network to its legacy structure. Secure keys generated by the QKD network are managed by key management agents (KMAs) and used to encrypt not only user data but also control signals. The KMAs cooperate with the generalized multiprotocol label-switching controller for secure path provisioning and drive photonic and modern crypto engines in appropriate combinations. Finally, we present a roadmap of a deployment scenario, starting from niche applications such as mission critical and business applications and the next. Digital cinema distribution through a photonic network is presented as an example of a niche application.**

***Index Terms*—Network architecture, optical fiber communications, photonic network, quantum key distribution (QKD), security.**

Manuscript received January 23, 2011; revised August 22, 2011; accepted August 22, 2011. Date of publication August 30, 2011; date of current version October 19, 2011.

K.-I. Kitayama is with the Department of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University, Osaka 565-0871, Japan (e-mail: kitayama@comm.eng.osaka-u.ac.jp).

M. Sasaki is with the National Institute of Information and Communications Technology, Tokyo 184-8795, Japan (e-mail: psasaki@nict.go.jp).

S. Araki is with the System Platforms Research Laboratories, NEC Corporation, Tokyo 108-8001, Japan (e-mail: s-araki@cj.jp.nec.com).

M. Tsubokawa was with Access Network Service System Laboratory, Nippon Telegraph and Telephone Corporation, Tokyo 180-8585, Japan. He is now with Waseda University, Tokyo 169-8050, Japan (e-mail: tsubokawa.m@aoni.waseda.jp).

A. Tomita is with the Graduate School of Information Science and Technology, Hokkaido University, Hokkaido 088-1113, Japan (e-mail: tomita@ist.hokudai.ac.jp).

K. Inoue is with Osaka University, Osaka 560-0043, Japan (e-mail: kyo@comm.eng.osaka-u.ac.jp).

K. Harasawa is with Hitachi information & Communication Engineering, Ltd., Karagawa 259-0157, Japan (e-mail: katsuyoshi.harasawa.vy@hitachi.com).

Y. Nagasako was with Internet Research Institute, Inc., Tokyo 164-0011, Japan. He is now with Information Sharing Laboratory Group, Nippon Telegraph and Telephone Corporation, Tokyo 180-8585, Japan (e-mail: nagasako.yuki@lab.ntt.co.jp).

A. Takada was with Network Innovation Laboratory, Nippon Telegraph and Telephone Corporation, Tokyo 180-8585, Japan. He is now with the Institute of Technology and Science, The University of Tokushima, Tokushima 770-8506, Japan (e-mail: takada@ee.tokushima-u.ac.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2011.2166248

I. Introduction

THE data transfer of even sensitive information, such as financial transactions, medical records, and confidential intellectual property, has currently been relying on the Internet via high-speed, large-capacity optical networks, thanks to the cost effectiveness of IP networks. A loss of data confidentiality on the Internet would have a tremendous impact on society as a whole, and hence, the security of information and communication systems has currently become our primarily concern. The main objective is the protection of confidentiality, integrity, and availability (CIA) [1] (known as the CIA triad). According to the International Standards Organization (ISO) definition of CIA, confidentiality denotes which information is not made available or disclosed to unauthorized individuals, entities, or processes; integrity denotes which data have not been altered or destroyed in an unauthorized manner; and availability denotes being accessible and useable upon demand by an authorized entity.

Various security mechanisms are used on the Internet to protect the CIA triad. Internet Protocol security (IPsec) is a common and standards-based security protocol in layer 3 (network layer). Transport layer security (or secure sockets layer) can tunnel an entire network's traffic, working at the boundary between layers 4 (transport layer) and 5 (session layer). Layer 2, the virtual private network, uses a combination of Ethernet and generalized multiprotocol label switching (GMPLS). All these secure protocols are supported by modern cryptographies such as secure Hash algorithm 1 for integrity protection and authenticity and advanced encryption standard (AES) for confidentiality.

In contrast to security technologies for layer 2 and the aforementioned layers, security protection in layer 1 has not been attracting much attention. In fact, physical protection of routers, interface cards, and optical fibers has been outside the scope of cryptographic research. The importance of layer 1 security should be stressed because once a security breakdown occurs, a quick stopgap measure will not be easily implemented, but it takes a painfully long time to remedy a physically damaged photonic layer. This is in sharp contrast to the vulnerability in which the upper layers can be restored in a relatively short time by patching software or releasing new codes online. It should be noted that the security is said to be a chain of trust, and the weakest part is the security level of the whole system. There have been studies on photonic network security. Medard *et al.* raised early on that security issues of the physical layer, suggesting possible attacks such as crosstalk attacks at optical nodes and fiber tapping [2]. This was followed by studies on

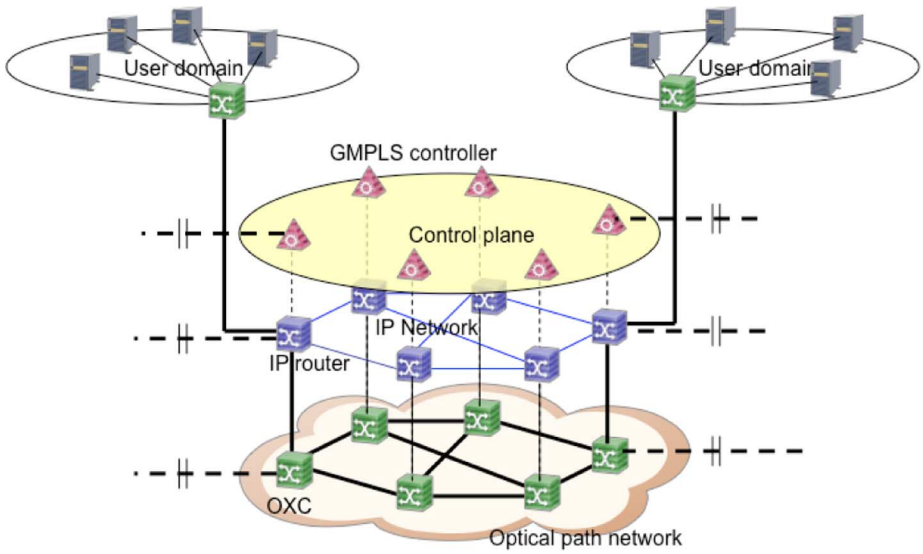


Fig. 1. IP over WDM network.

monitoring and localization techniques of crosstalk attacks [3], [4], quality of service (QoS) degrading/disruptive attacks, such as optical amplifier gain competition attacks [5], and low-power QoS attacks [6]. Attack-aware routing and wavelength assignment of optical path networks have recently gained attention [7]–[9]. Kartalopoulos suggested a possible method of implementing quantum cryptography in optical networks [10]. However, a comprehensive study taking into account cross-layer security issues in photonic network remains to be studied.

One may simply assume that network facilities and outside plants can be physically isolated from adversaries. However, optical fiber cables are exposed to physical attacks in customer premises owing to the wide use of fiber-to-the-home systems, and tapping of the optical signal from a fiber could be easily done by using inexpensive equipment [11]. Recently, risk of information leakage occurring in a fiber cable has been pointed out [12]. A small fraction of optical signals, even in a coated fiber, often leaks into adjacent fibers in a cable at the bending points. The amount of light leakage is small but detectable with a photon counting detector. Although, the optical signal in fibers may be encrypted using modern cryptography in the upper layers, its security is not entirely free from constant threats. For example, it was reported that the 768-bit Rivest, Shamir, and Adleman (RSA) cryptosystem was broken by collaborating computing by an international team of Japanese, French, and German researchers in December 2009 [13].

New threats are also emerging as the photonic network becomes multidomain, being opened to the upper layers, other operators, and end users. Fig. 1 depicts the typical architecture of a photonic network, including the IP over wavelength division multiplexing (WDM) network, consisting of the optical path network, IP network, and the control plane. The IP and optical path networks are tightly integrated with the WDM interfaces of the optical cross connects (OXCs), which are directly connected to IP routers to set up a desired optical path by wavelength switching. Routing, signaling, and link management are supported by GMPLS in the control plane. Today, confidential control signals are carried through out-of-band channels in optical fibers, or sometimes over a dedicated control network. Hackers may have the opportunity to easily access them and maliciously control the network with the control information, which could seriously damage the entire photonic network.

Recently, progress has been made in security technologies for layer 1, especially for the photonic layer. Such technologies include secure communications using optical chaos (SCOC), optical code division multiplexing (OCDM), a quantum noise randomized cipher (QNRC), and quantum key distribution (QKD). All rely on direct control of physical properties of light and, hence, are implemented in the photonic domain. They may be referred to as the photonic layer 1 security technology (PL1sec). They can be useful for protecting confidential data of photonic networks. We believe that QKD can play a key role in developing secure photonic networks. QKD can generate secure keys between distant nodes. The key can be used for one-time pad (OTP) encryption or the Vernam cipher, called as QKD-OTP, which requires the same length of the key as the message bit. OTP encryption is the only one that has been mathematically proved to be completely secure.

In this paper, we address emerging potential threats to the PL1sec as networks become heterogeneous, being opened to the upper layers, other operators, and end users. We review potential threats, mainly loss of the confidentiality of user data in optical fibers and disturbances of network control, both of which could seriously damage an entire network. Service denial induced in IP networks is not within the scope of this paper. We then propose a novel conceptual model of a secure photonic network, introducing a QKD network to its legacy structure. Secure keys generated by the QKD network are managed by key management agents (KMAs) and used to encrypt not only user data but also control signals. The KMAs cooperate with the GMPLS controller for secure path provisioning and drive photonic and modern crypto engines in appropriate combinations. Finally, we present a roadmap of a deployment scenario, starting from niche applications such as mission critical and business applications

and the next. Digital cinema distribution through a photonic network is presented as an example of a niche network.

This paper is organized as follows. Potential threats to security in IP over optical path networks are discussed in Section II, followed by a discussion on the security enhancement of photonic networks in Section III. In Section IV, a roadmap of the deployment scenario is presented, followed by concluding remarks in Section V.

II. Potential Threats to Security in Photonic Networks

Threats to security in photonic networks will be of a huge variety and extension in the near future. Cyber attacks are the most common and urgent issues. They are, however, not specific to photonic networks and may not be within the scope of this context. A straightforward protection against physical destruction of systems and devices is to isolate them from malicious parties. This is also not within the scope of this paper. Attacks on electrical devices are somewhat nontrivial cases. There are many techniques for tapping the signal from electrical devices, even leaving them physically unchanged. Most of these techniques can be categorized as side channel attacks via electrical and electromagnetic signals. They have already been extensively studied in the security field. In spite of their importance, we do not touch upon them here. Our concern is new threats, those that have recently occurred or will likely take place in the near future.

A. Control Plane

Automatic switched optical network/GMPLS control plane technology for automated path control of a photonic network was developed in the past decade. In the past few years, it has been deployed in service provider commercial networks. This control plane technology provides network operators *with* advanced network functions such as multilayer network operation and user control. The control plane technology can change the traditional closed network operation to an open-controlled network, as shown in Fig. 2. This change is beneficial for saving both operation expenditure (OPEX) and capital expenditure (CAPEX) of networks as well as for creating new services.

This technology also introduces new threats to the security of photonic network operation [14]. In the IP layer, multiprotocol label switching (MPLS) is used as a control plane in various network service provider networks. The MPLS packets use interfaces identified by their IP addresses, and the MPLS control packets use the same interfaces and addresses. Some malicious users may access the devices and channels in these lower layers and may pretend to be a network operator and flow incorrect network information to confuse the IP network through the MPLS control plane. However, in the traditional control plane configuration, photonic networks cannot be disturbed by a malicious user from the IP layer because it is controlled by the isolated control plane from the IP layer's control plane, as shown in Fig. 3(a).

The introduction of the GMPLS control plane exposes devices in a photonic network to a malicious user in the IP layer because the GMPLS control plane can be configured as an integrated control plane from layers 1 to 3, which is shown in Fig. 3(b). A potential serious problem in this architecture is that a malicious user can change and confuse a carrier's database of the network configuration through the IP layer. Hacking and hijacking a photonic network in this way would be a likely threat. This can be partially prevented by IPsec; however, the protocols used are always threatened by advances in mathematics and computer technologies, or may have already been cracked. Hence, it is not a perfect solution.

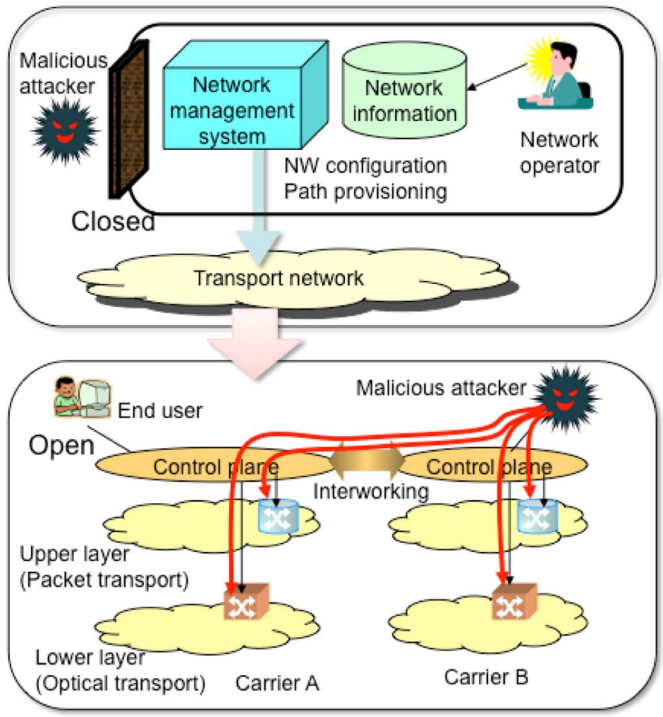


Fig. 2. Evolution of network operations.

B. Optical Path Network

Possible targets of attacks on an optical path network include devices such as optical fibers, OXC, and reconfigurable optical add–drop multiplexers (ROADMs). Access networks will be an easy target for attacks since the optical signals are at a relatively low bit rate and most of the facilities, such as optical fiber cables, are installed in the open outside plant. Moreover, passive optical network (PON) systems, in which an optical fiber is shared by typically up to 32 users, have been widely deployed in access networks, as shown in Fig. 4(a). This point-to-multipoint network topology is inherently prone to security threats, for example, tapping by detecting the leakage of light signal at the bent portion and spoofing by connecting an unauthorized optical network unit (ONU). To prevent such attacks, encryption, such as AES for payload data and authentication for individual ID of the ONU, is generally used for communication between the optical line terminal (OLT) and each ONU. Thus, PON systems provide reasonable security using currently available techniques. However, it seems worth pursuing newly emerging PL1sec technologies in the long run. Jamming by injecting high-power light from the optical fiber is another possible attack, which would paralyze the PON with the breakdown of the receiver, leading to service denial, as shown in Fig. 4(a). This can be prevented by isolating

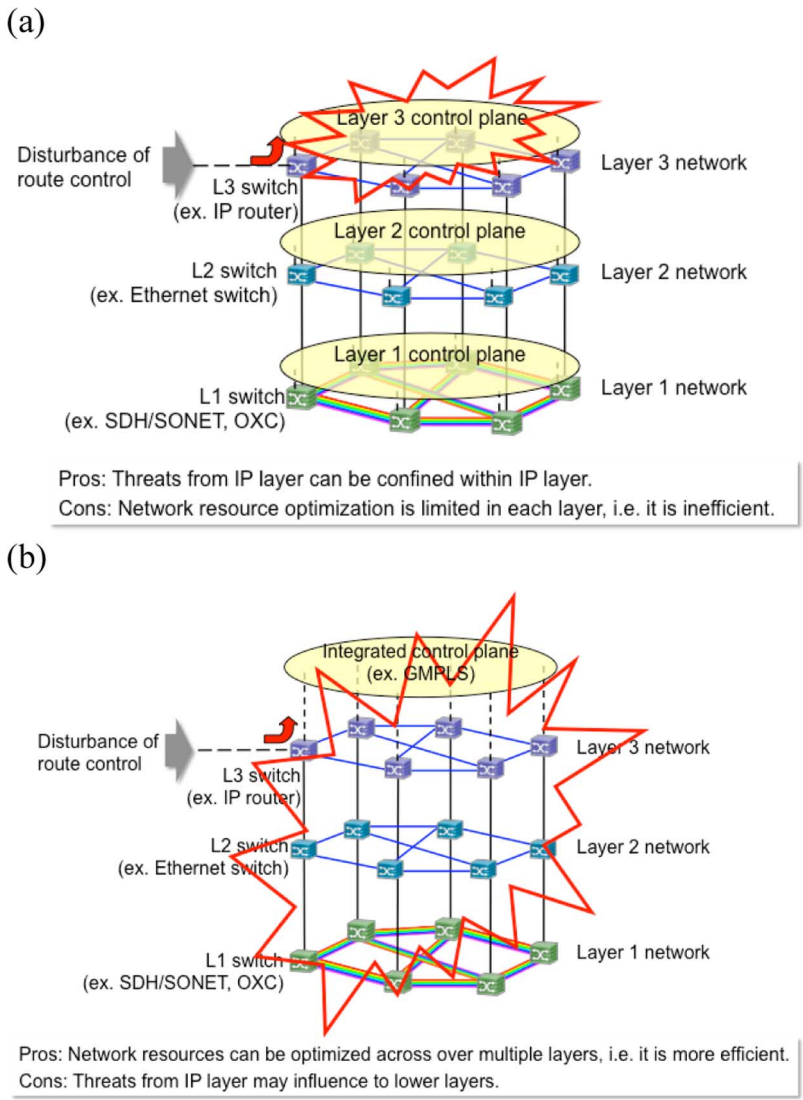


Fig. 3. Comparison of potentially threatened layers between individual and integrated types of network control technologies. (a) Individual control plane. (b) Integrated control plane.

the drop fiber from the optical splitter. For example, jamming light can be shut out by attaching an optical gate, controlled by a photovoltaic module to the fiber [15].

Another target of attack may be network nodes. As Medard *et al.* suggested [2], crosstalk attack is possible, which occurs in the optical switch at the node, as illustrated in Fig. 4(b). When an attacker injects high-power light on the same wavelength as the signal from an input port of the switch, its leaked light energy can significantly affect the normal connections passing through the same switch and can propagate to the next node.

III. Security Enhancement of Photonic Networks

There are mainly two types of security enhancements; 1) protecting the confidentiality of user data; and 2) preventing disturbances of network control and management. The former mainly relies on secure optical communications by using PL1sec technologies such as SCOC, optical code division multiple access (OCDMA), a QNRC, and QKD-OTP. The latter includes protecting the control plane and monitoring the network for detecting any malicious attempts to distribute the route control. In the following sections, we first propose a conceptual model of a secure photonic network. We then review the main features and issues for the deployment of QKD, SCOC, OCDM, and a QNRC.

A. Conceptual Model of Secure Photonic Networks

We propose a novel architecture of a secure photonic network in Fig. 5. The main features are summarized in three points. First, a QKD network is introduced on the top of the control plane. It should be noted that optical fibers do not always have to be installed for this network. Wavelength bands in existing fibers might be used for the QKD network [16]. Each KMA stores and controls the secure key under the supervision of a key management center (KMC). Both the KMC and the KMAs are assumed to be tightly protected and secure because we assume the key relay is via trusted nodes to expand the QKD distance in the prototype of a secure photonic network. Although each KMA should ideally be colocated at the same site of each OXC and IP router, one may allow that the KMAs are located at different sites for tight protection and are connected to OXCs and

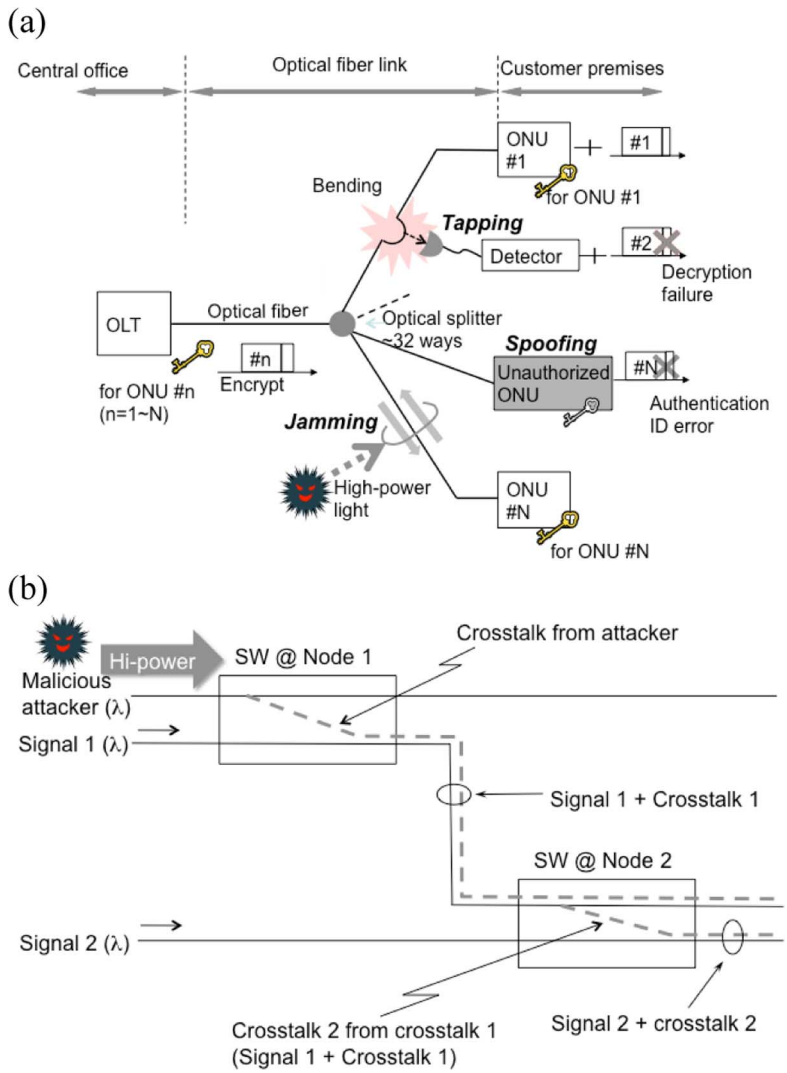


Fig. 4. Security threats (a) in PON system and (b) at network node [3].

IP routers via authenticated classical channels. The reason the QKD network in Fig. 5 is described separately from the other layers is that the KMC and the KMAs are not opened to unauthorized parties, unlike OXCs, GMPLS controllers, and IP routers, for the purpose of secure management of the keys. Second, the KMC and KMAs cooperate with the GMPLS controllers in the control plane, which is generally an open network, to encrypt the control signals and achieve secure path provisioning. Finally, crypto engines of SCOC, OCDMA, the QNRC, and QKD-OTP are implemented in the optical path network to protect confidential data from the physical layer.

In a QKD network, secure keys are generated in various pairs of QKD devices via point-to-point links. These links may be formed for any pair of nodes that can be connected by a transparent optical path via OXCs, as demonstrated by Chapuran *et al.* using cutting-edge photonic devices [16]. The generated secure keys are pushed up from the QKD devices to the KMAs. Note that in Fig. 5, the QKD devices and KMAs are not separately described, but represented as thick red disks. Each KMA stores the key and sends the bit error rates (BERs) of the quantum links, the amount of the stored key, the key generation rate, and other necessary information for key management, to the KMC. To expand the QKD distance, not only point-to-point QKD via a transparent optical link but also the key relay via trusted KMAs should be performed in the QKD network. This is based on key encapsulation, as explained in the later part of Section III-B. The network is monitored using QKD devices, which will alarm the KMC and KMAs under threat. Once a link is hacked, the KMC quickly provides a new securely protected path, and secure communications will be maintained.

In the control plane, the control signals are encrypted using QKD-OTP. The data size of the control signals is not so large, and hence, the current level of QKD technology would suffice for this application. The secure keys for this purpose should be transported from the KMAs to GMPLS controllers through authenticated channels. GMPLS controllers cooperate with the KMAs for path provisioning and driving crypto engines upon the receipt of security requests from user domains.

The crypto engines include modern crypto systems for IPsec and novel systems of SCOC, OCDM, a QNRC, and QKD-OTP for PL1sec. KMAs would not only perform QKD-OTP in the optical path network, but also provide secure keys for refreshing the seed keys of modern crypto systems in the IP network. In

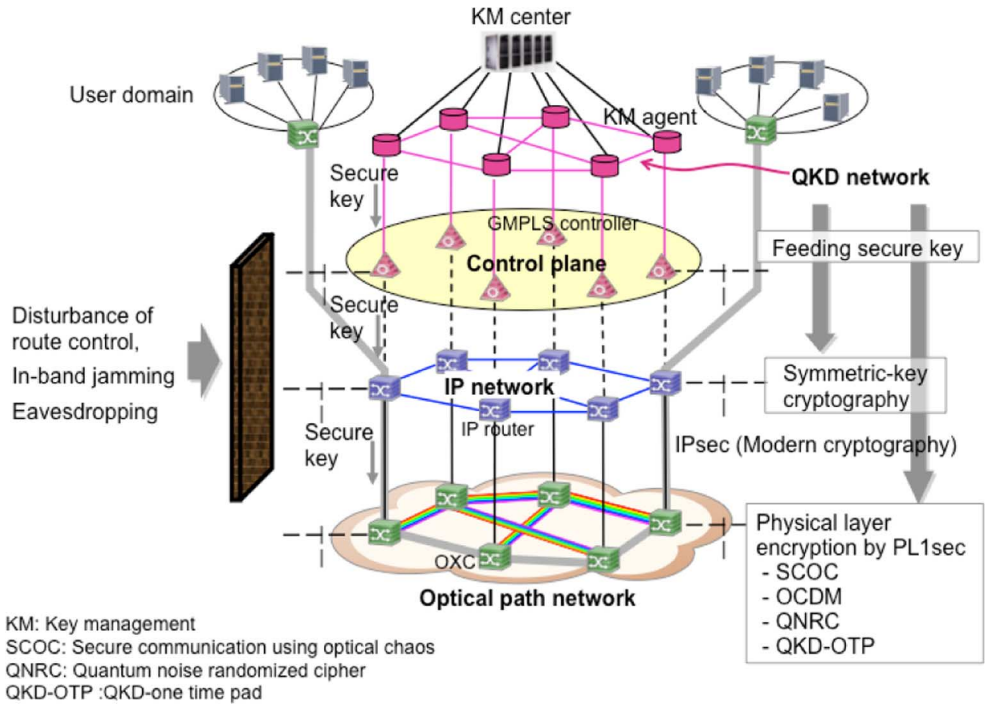


Fig. 5. Conceptual model of a secure photonic network.

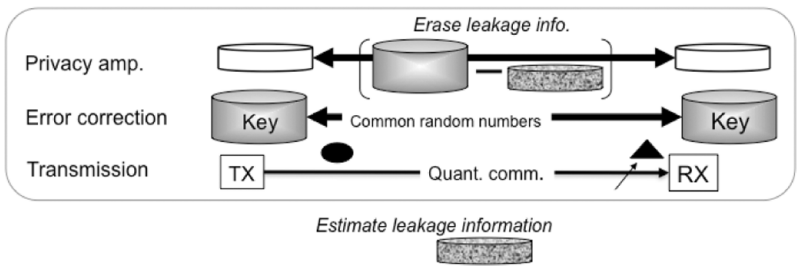


Fig. 6. QKD process.

optical path networks, user data are encrypted by appropriate schemes of PL1sec. Upon a user request, a QKD or a key relay via trusted nodes is made on demand.

The security ensured by QKD-OTP is robust against any future eavesdropping technologies. Therefore, no updating of crypto schemes is needed unlike the conventional scheme of key exchange. It would be beneficial to reduce the maintenance cost of photonic network. On the other hand, however, QKD-OTP inevitably evolves a legacy closed network to the open-controlled network, because it requires preestablished secret, i.e., shared random numbers (even small) and authentication of the parties. Use of the trusted nodes for key relay further forces to introduce secure walls in the electrical domain. In an all-optical network in the future, more flexible on-demand connectivity can be realized, relaxing the tradeoff between the openness (or the convenience) and the security in the photonic network. It is an open issue to develop a more effective architecture with the optimal tradeoff.

B. QKD

QKD, originally proposed by Bennett and Brassard in 1984 [17], can provide an effective method for distributing truly random numbers between remote parties in a theoretically secure way such that the amount of information leakage can be made arbitrarily small for eavesdropping attacks by sufficiently increasing the key length. The security of QKD is based on a NO-GO theorem that nonorthogonal quantum states cannot be perfectly discriminated nor copied without errors. Eavesdropping on quantum states will inevitably cause errors in the received bits. As summarized in Fig. 6, a sender and a receiver first share a sequence of random bits by selecting appropriate signals from transmitted signal pulses through basis matching and error correction. They estimate the upper bound of leaked information by the BER and erase the leaked information by privacy amplification. A secure key is finally generated. Many different protocols have been proposed, tested, and recently commercialized [18], [19]. They can be categorized into two types based on the detector used 1) photon-QKD; and 2) continuous variable (CV) QKD.

Photon-QKD includes protocols using single photon (or on/off) detectors. The original BB84 protocol requires a single photon source to guarantee security, but it has been shown that even a weak laser light can provide secure keys with a decoy method [20]. Other than the traditional BB84,

a nonsingle-photon-based scheme also includes B92, differential-phase-shift (DPS)-QKD, coherent-one-way (COW), SARG04, as well as entanglement QKD, such as E91 and BBM92 [18]. The unconditional security proofs were already given to BB84, B92, and SARG04. Currently, the performance of the BB84 system reaches the secure key rate of 1 Mbps over a 50 km fiber in the laboratory [21]. A design for a higher speed and stable system was also developed [22], [23]. DPS-QKD and COW have remained within the conditional security proofs. They can, however, operate at high speed over longer distance with reasonable security and easier implementation. For example, DPS-QKD [24] is basically the same as conventional optical DPSK systems, except that very weak light and single-photon detectors are used. A record high key creation speed (1.85 Mbps over 101 km) was demonstrated with DPS-QKD [25]. Not only high-speed key generation but also continuous generation of secure keys over a long time is an important task. This task relies on true random number generators operating at much higher rates.

The security of entanglement QKD is rather straightforward. Sharing a perfect entanglement between two parties means perfect isolation from an environment, automatically ensuring unconditional security. It can be used to certify the absence of side channels. Security analysis as well as physical implementation can be much more simplified compared with single-photon QKD [26]. This would be the second generation photon-QKD. To make it practical, however, entangled photon sources and photon detectors need to be greatly improved, at least an order of magnitude in operation speed. CV-QKD uses quadrature-amplitude modulation and homodyne detection, which are the same elements used in optical communications technology [27], [28]. The unconditional security proof for CV-QKD has been given at last very recently [29] as well as a proposal of a much simpler implementation [30]. These achievements will open a new phase of CV-QKD research and accelerate embedding CV-QKD into photonic networks.

QKD and optical path networks should be tightly coupled together. The first challenge is to develop quantum WDM technology to integrate QKD channels into WDM networks. Spontaneous Raman emission caused by WDM data signals contaminates photon signals for QKD. For example, 0.1 photon/ns of Raman antiStokes is generated over the spectral range of 1400–1520 nm by a 6 dBm signal at 1551 nm after 25 km long propagation in the fiber. Careful wavelength allocation and a special separation technique as well as narrow bandpass filtering and short time-gating are necessary. The noise effects and quantum WDM technology are under investigation [22], [31]–[33].

A target in the long run would be a long reach and point-to-multi-point QKD link, while, on the other hand, a short-term approach is classical relaying via trusted nodes. In each node, a classical memory (a KMA) receives and stores the secure key from the QKD device. The relay node in the middle of two connections shares two keys of which one is encapsulated with the other to guarantee safe passage from one connection to the next. A QKD network architecture based on key relay via trusted nodes was successfully demonstrated in a metropolitan network in Vienna in 2008 by the SECOQC project [34], [35].

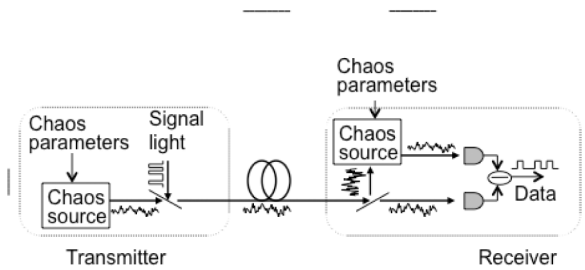


Fig. 7. Secure communication system using optical chaos.

A long-term approach is using a quantum repeater [36], [37], but we do not discuss this in detail.

C. SCOC

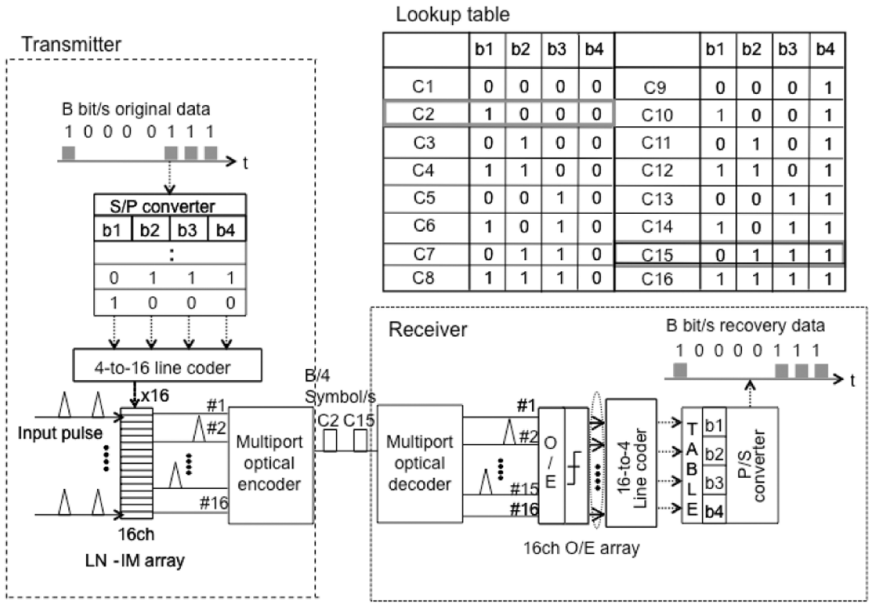
A nonlinear optical system with some feedback can emit light with randomly changing amplitude and frequency, even though the system follows a deterministic differential equation. Such a phenomenon is called "optical chaos," whose behavior is determined by system parameters such as the operating point of a nonlinear device in the system, the feedback gain, and the delay time. Optical chaos has been studied for secure communications by masking transmitted data from third parties, where system parameters determining chaotic behavior function as a secret key [38]. Fig. 7 illustrates the setup of an SCOC system. A transmitter sends signal light together with chaos light such that the signal is completely masked by the chaos waveform, and a receiver demodulates the signal by recovering the chaos waveform and extracting it from the received light by virtue of synchronization of chaos. Currently 1 Gbps over 120 km with a BER of 10^{-7} was demonstrated.

It is worth mentioning that an SCOC using an ultralong fiber laser can also be applied to the classical approach to key distribution [39]. This optical scheme might have practical benefits by allowing simpler implementation than the unconditional security requirement of QKD.

D. OCDM

One of the well-cited benefits of OCDM or OCDMA is good data confidentiality. There is an excellent overview for better understanding OCDM and OCDMA [40], [41]. It has been theoretically examined that under *Kerckhoffs' principle*, OCDM with reasonable choices of system and encoding parameters provides considerably less data confidentiality than standard cryptography [42]. To enhance the data confidentiality of OCDM, a promising approach would be the $M\ (=\ 2^n)$-ary OCDM system, which adopts block ciphering of n-bit sequence, distinct from conventional bit-ciphered OCDMs [43], [44]. This is because bit ciphering is resistant only against ciphertext-only attacks (COAs), while block ciphering is robust against chosen-plaintext attack (CPA).

The architecture and the operation principle of an M-ary OCDM-based block-ciphering system using XOR, for example $M\ =\ 2^4\ (=\ 16)$, are depicted in Fig. 8 [45]. At the transmitter, a serial data bit stream is segmented every four bits $b_i\ (i\ =\ 1\text{–}4)$. Each four-bit block is mapped onto a different optical code out of 16 codes according to the code lookup table. Each output of this line coder generates the corresponding



	b1	b2	b3	b4		b1	b2	b3	b4
C1	0	0	0	0	C9	0	0	0	1
C2	1	0	0	0	C10	1	0	0	1
C3	0	1	0	0	C11	0	1	0	1
C4	1	1	0	0	C12	1	1	0	1
C5	0	0	1	0	C13	0	0	1	1
C6	1	0	1	0	C14	1	0	1	1
C7	0	1	1	0	C15	0	1	1	1
C8	1	1	1	0	C16	1	1	1	1

Fig. 8. Architecture and operation principle of 16-ary OCDM system using XOR logic operation.

optical code by driving the 16-channel optical gate (LN-IM) array. Only the optical pulse train passing through the optical gate is forwarded to a designated input port of the multiport optical encoder, and one of 16 optical codes is generated. For example, gates are opened to launch the optical pulses to input ports of encoders #2 and #15, respectively, to generate optical codes C2 and C15. At the receiver, the received optical codes are sent to the multiport optical decoder. The decoding process follows the reverse order of the encoding at the transmitter. This scheme was experimentally demonstrated at 2.5 Gbit/s or 622 MSymbol/s, over a 50 km single-mode fiber. The quantitative evaluation of confidentiality against both COA and CPA has been investigated [46].

E. QNRC

A QNRC can be regarded as a kind of stream cipher enhanced by quantum noise randomization. Quantum noise is inevitable random fluctuation associated with every light-field mode and imposes the ultimate limit of signal discrimination. For example, when quadrature amplitude of light is modulated into densely packed signals with limited signal power, the signal distances get closer in the *Q–I* space than a range of quantum noise fluctuations. This is a quantum-limited constellation, where the signal-to-noise ratio in detection degrades significantly. More precisely, the quantum states become nonorthogonal to each other, with finite overlaps. Such signals cannot be perfectly discriminated in principle, nor be copied without errors. A QNRC imposes this kind of situation only on an eavesdropper, Eve, by an appropriate random modulation with a shared key between legitimate users, a sender Alice, and a receiver Bob. Bob can decrypt his received cipher using only the shared key, while it acts as inevitable noise for Eve. The first protocol was proposed by Yuen in 2000 [47], which is often called Y00 protocol. There is now a family of several different implementations [48], [49].

As does modern cryptography, a QNRC can directly encrypt plain text. A sharp distinction is that cipher text of modern cryptography can be copied with no errors for attacks while cipher text of a QNRC cannot be precisely copied. Copying QNR-ciphered text must be associated with finite errors due to the uncertainty principle of quantum mechanics. This would offer a new mechanism to enhance security. These two crypto schemes can be used in a cascaded manner to enhance total security. The protocol can be implemented with bright laser light and conventional detectors of optical communications and can operate at high speed (>gigabit per second), enabling real-time high capacity secure communications. Several implementation schemes have been developed and deployed in a field environment, including phase modulation [50] and intensity modulation [51], [52]. Fig. 9 shows a simple sketch of the intensity modulation scheme of Y00 protocol. The signal amplitude of the light is divided into multiple levels, coarse enough to be quantum limited. Alice and Bob choose a pair of values among many value levels using a common key for each one-bit frame, and Alice encodes the bit of the signal.

IV. Deployment Scenario: Niche Application and the Next

A. Deployment Roadmap

It would take long for PL1sec technologies to be practically implemented on a global scale. However, the PL1sec system will enter niche markets in various sectors such as 1) government agencies; 2) public infrastructures; 3) financial and medical facilities; and followed by 4) business sectors and private homes. The roadmap we envisage is shown in Fig. 10, consisting the three stages. PL1sec will be deployed in a point-to-point link at the beginning and migrate into photonic networks. In sectors (1) and (2), cost is not a major issue but the only concern would be the high level of security. In sector (3), there would be a tradeoff between the security level and its CAPEX and OPEX.

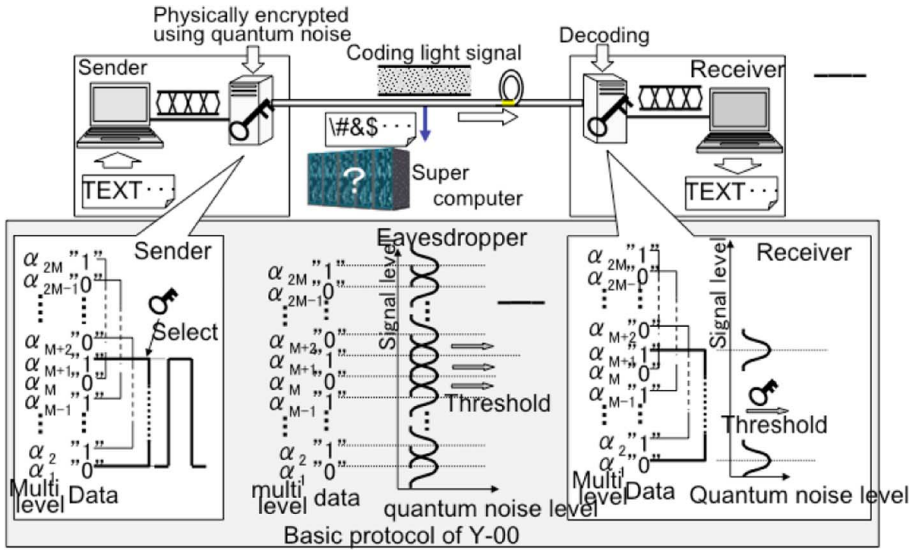


Fig. 9. Example of quantum noise-randomized encryption (QNRC), Y-00 protocol [50], [51].

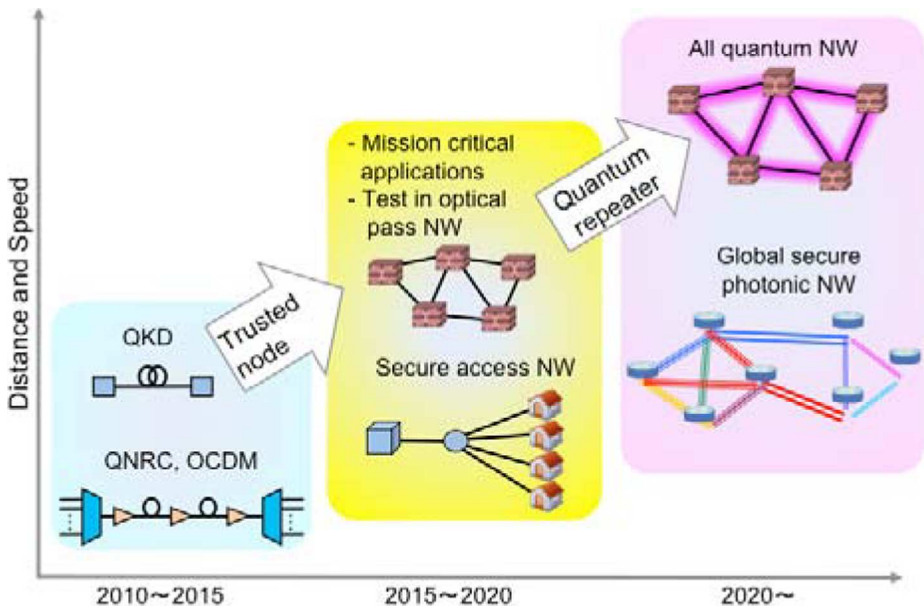


Fig. 10. Roadmap of secure photonic network.

The first major application of PL1sec will be government communication lines. A possible scenario of deployment would start with point-to-point links using QKD-OTP at around 50 km. This corresponds to the first stage around years of 2010–2015 in Fig. 10. Next, QKD will be applied to sector (2) public infrastructures such as power plants and water and gas utilities. In these public facilities, optical fibers are already installed along the electrical cables and water and gas pipelines in a duct and are used to transmit surveillance and control data. QKD-OTP is expected to show its strength in preventing hacking into such data transfer. This provides an appropriate test case of the novel control plane technologies shown in Fig. 5 in a metropolitan area. The important requirements will be fast rerouting against attacked damage, automatic restoration, and reasonable maintenance cost. These applications correspond to the second stage around 2015–2020 in Fig. 10.

In sectors (3) and (4), a prototype of a secure photonic network needs to be operated on an intercity scale. In addition to high security, for example, ultrahigh resolution medical images require small latency, large capacity, long distance of a few hundred kilometers, and low cost. Not only QKD-OTP, but also other schemes even with compromised security should be used to enhance the practical security. For example, the security level of modern cryptography will be enhanced by QKD-assisted key refresh. The QKD network will be operated using key relay via trusted nodes. A QNRC is a potential candidate for the high-speed crypto engine because it can rapidly exploit advancing technology of the multilevel modulation format for high-capacity optical transmission. QKD can also provide a secure seed key for a QNRC for improving security. Those applications in sectors (3) and (4) still are involved in the second stage in Fig. 10. Finally, extending secure photonic network into

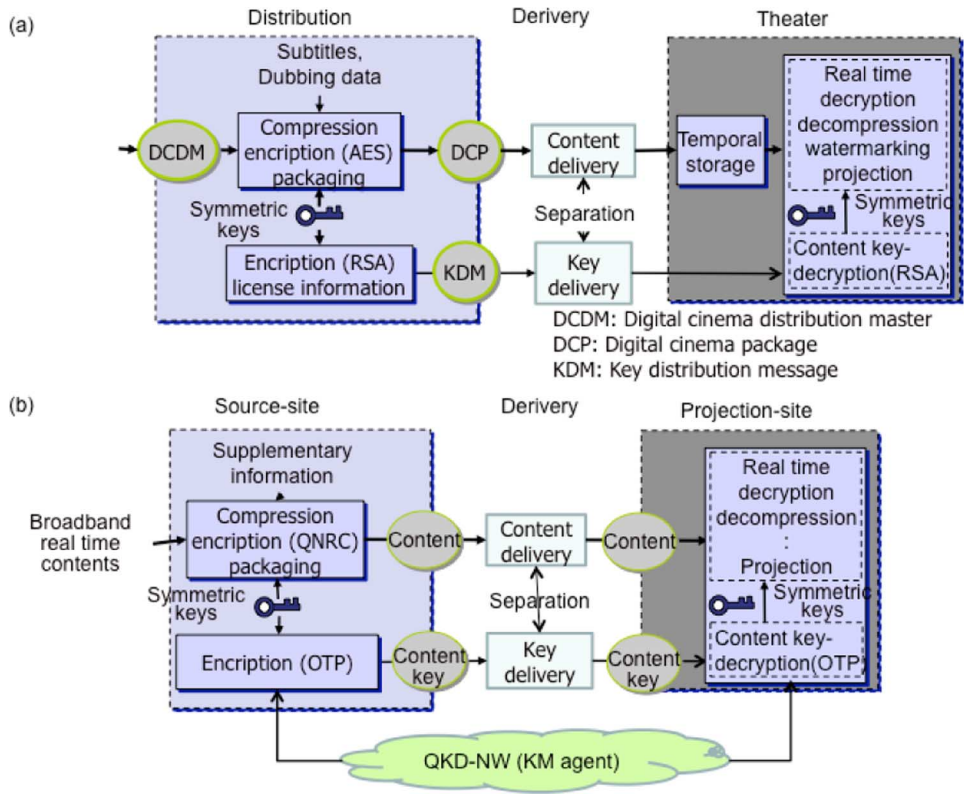


Fig. 11. Configuration of digital cinema distribution system. (a) Current scheme. (b) Proposed scheme with QNRC and QKD.

the global scale need many technological breakthrough such as quantum repeater. Its time line can be hardly predicted, but it is indeed a frontier in future network technology.

B. Niche Application: Digital Cinema Distribution Through Photonic Network

Digital cinema distribution through photonic network is presented as an example of sector (4). Compared with traditional film prints and staggered film release due to shipping, digital cinema distribution has been shown to dramatically reduce costs and make simultaneous worldwide release possible. However, a high level of security is a "must" to protect the copyright of first-run films against the attacks. It is estimated that all screens in Japan will be digitized by 2018. Digital cinema standard was developed by Digital Cinema Initiatives, LLC, issued as the digital cinema system specification on their website [53]. The specification includes the transport of packaged contents and the security requirement. The extension of requirements and techniques on data secure transport will be required for new types of business image content. For example, real-time broadcasting of sports, live concerts, remote lectures, and other digital stuff/online digital source are becoming new types of digital image distribution services. Very sensitive data such as medical movie images will soon be a target as well.

Fig. 11 shows schematic configurations of the current digital cinema distribution system and an updated scheme adopting a QNRC and QKD. As shown in Fig. 11(a), digital cinema content, including picture, sound, and other data elements, are assembled into a digital cinema distribution master (DCDM) at a production company. The DCDM added with subtitle and dubbed voice data are compressed, encrypted, and packaged into a form of digital cinema package (DCP). The DCP is encrypted by symmetric-key cryptography, 128-bit AES. The keys for this encryption are called content keys. They are further encrypted using a 2048-bit RSA public key for key distribution. This public key constitutes a key pair with the private key of the theater exhibition device. RSA-encrypted content keys and other security information such as the trusted device list are packaged into a key delivery message (KDM). The DCP and KDM are delivered to theaters separately using different networks. The delivered DCP and KDM are first stored in a playback server system in a theater. When the exhibition device is ready, a decoding device receives the DCP and KDM in the theater server system, extracts encryption keys from the KDM, decrypts and decompresses the DCP, performs other processes such as watermarking for preventing rephotographing (content theft), and simultaneously sends the projection data to the cinema projector.

In a next generation system, shown in Fig. 11(b), a QNRC may be used for content encryption with throughput faster than several tens of gigabit per second. QKD-OTP is not matured enough yet for this purpose. For encrypting content keys, on the other hand, QKD-OTP would be useful to enhance security because the required key rate is relatively slow. Secure key distribution will be done by the key relay via trusted nodes, at least for intra-continental links. For intercontinental links, one faces a challenge of developing quantum repeater technology and/or satellite-ground QKD technology; however, this will not be ready for practical use.

V. Conclusion

We have addressed emerging threats to the security of photonic networks, reviewed security technologies for protecting the photonic domain of layer 1, referred to as PL1sec, and proposed a novel conceptual model of a secure photonic network, in which a QKD network is introduced to a legacy photonic network. Secure keys generated by the QKD network are managed in the control plane by KMAs and KMC, which drive PL1sec and modern crypto engines in appropriate combinations in cooperation with path provisioning by GMPLS. Finally, we presented a roadmap of a deployment scenario, starting from a niche application in digital cinema distribution along with applications relevant to mission critical and public infrastructures.

Acknowledgment

The authors would like to thank the members of the "Secure Photonic Networks" study group organized at the Technical Research Committee of the Photonic Internet Forum of Japan (http://www.scat.or.jp/photonic/english/index.html). The authors would like to thank T. Aoyama of Keio University and T. Yamauchi and Y. Tawara of the Ministry of Internal Affairs and Communications, Japan, for initiating the study and for their invaluable comments. Finally, they will express their sincere thanks to the anonymous reviewers of the preceding manuscript submitted to this journal for their invaluable comments. This work is based on a study report entitled "Secure Photonic Networks (unpublished)," which was written by the study group of *Photonic Internet Forum* (http://www.scat.or.jp/photonic/english/index.html).

References

[1] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 74–81, Nov. 2009.

[2] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues of all-optical networks," *IEEE Netw.*, vol. 11, no. 3, pp. 42–48, May/Jun. 1997.

[3] T. Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 6, pp. 1390–1401, Dec. 2005.

[4] R. Rejeb, M. S. Leeson, and R. J. Green, "Fault and attack management in all-optical networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 79–86, Nov. 2006.

[5] T. Deng and S. Subramaniam, "Analysis of optical amplifier gain competition attack in a point-to-point WDM link," in *Proc. Int. Soc. Opt. Eng.*, Jul. 2002, vol. 4874, pp. 249–261.

[6] T. Deng and S. Subramaniam, "Covert low-power QoS attack in all-optical wavelength routed networks," in *Proc. Global Telecommun. Conf.*, 2004, vol. 3, pp. 1948–1952.

[7] G. Liu and C. Ji, "Resilience of all-optical network architectures under in-band crosstalk attacks: A probabilistic graphical model approach," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 2–17, Apr. 2007.

[8] N. Skorin-Kapov, J. Chen, and L. Wosinska, "A new approach to optical networks security: Attack aware routing and wavelength assignment," *IEEE/ACM Trans. Netw.*, vol. 18, no. 3, pp. 750–760, Jun. 2010.

[9] C. M. Machuca, I. Tomkos, and O. Tonguz, "Failure location algorithm for transparent optical networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 8, pp. 1508–1519, Aug. 2005.

[10] S. V. Kartalopolos, "Security in advanced optical communication networks," in *Proc. IEEE Int. Conf. Commun.*, 2009, pp. 1–5.

[11] The Wolf Report (in German) [Online]. Available: http://www.youtube.com/watch?v=2DvaubDDbss see also

[12] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, Photon Level Crosstalk Between Parallel Fibers Installed in Urban Area arXive:quant-ph/1008.0893 [Online]. Available: http://xxx.lanl.gov/abs/1008.0893, 2010

[13] T. Kleinjung1, K. Aoki, J. Franke, A. K. Lenstra1, E. Thomél, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, Factorization of a 768-bit RSA Modulus Cryptology ePrint Archive: Report 2010/006.

[14] A. Farrel, "Control plane resilience and security in GMPLS networks: Fact and fiction," presented at the presented at the Adrian Farrel Old Dog Consulting, U.K., Jun. 2008 [Online]. Available: http://pil.yamanaka.ics.keio.ac.jp/2008/info/pdf/iPOP2008_1-1.pdf

[15] H. Ramanitra, P. Chanclou, Z. Belfqih, M. Moignard, H. Le Bras, and D. Schumacher, "Scalable and multi-service passive optical access infrastructure using variable optical splitters," presented at the presented at the Opt. Fiber Commun., Anaheim, CA, Mar. 2006.

[16] T. E. Chapuran, P. Toliver1, N. A. Peters1, J. Jackel1, M. S. Goodman1, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, pp. 1–19, 2009, 105001.

[17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–151, 2002.

[19] Updating Quantum Cryptography Report ver. 1 The UQC Working Group, 2009 [Online]. Available: http://xxx.lanl.gov/abs/0905.4325, arXive:quant-ph/0905.4325

[20] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 057901, 2003.

[21] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," *Appl. Phys. Lett.*, vol. 96, p. 161102, 2010.

[22] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," *Opt. Exp.*, vol. 16, pp. 11354–11360, 2008.

[23] A. Tajima, A. Tanaka, S. Takahashi, K. Yoshino, and Y. Nambu, "High speed quantum key distribution system," *IEICE Trans. Fund. Electron., Commun. Comput. Sci.*, vol. E93-A, no. 5, pp. 889–896, 2010.

[24] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, p. 022317, Aug. 2003.

[25] E. Dauler, N. Spellmeyer, A. Kerman, R. Molnar, K. Berggren, J. Moores, and S. Hamilton, "High-rate quantum key distribution with superconducting nanowire single photon detectors," in *Proc. Quantum Electron. Laser Sci.*, 2010, pp. 1–2.

[26] A. K. Ekert, "Less reality, more security," *Physics World*, pp. 28–32, Sep. 2009.

[27] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, pp. 057902-1–057902-4, 2002.

[28] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A*, vol. 68, no. 4, pp. 042331-1–042331-7, 2003.

[29] R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, no. 11, pp. 110504-1–110504-4, 2009.

[30] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with direct modulation," *Phys. Rev. Lett.*, vol. 102, no. 18, pp. 180504-1–180504-4, 2009.

[31] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electron. Lett.*, vol. 33, pp. 188–190, 1997.

[32] P. Toliver, R. J. Runser, T. E. Chapuran, S. McNown, M. S. Goodman, J. L. Jackel, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. A. Dallmann, "Impact of spontaneous antiStokes Raman scattering on QKD + DWDM networking," in *Proc. 17th Annu. Meet. IEEE Lasers Elecro-Optics Soc.*, 2004, vol. 2, pp. 491–492.

[33] T. J. Xia, D. Z. Chen, G. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels," presented at the presented at the Opt. Fiber Commun. Conf., Anaheim, CA, 2006.

[34] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, pp. 075001-1–075001-37, 2009, (58 authors).

[35] *SECOQC White Paper on Quantum Key Distribution and Cryptography*, arXive:quant-ph/0701168, 2010 [Online]. Available: http://xxx.lanl.gov/abs/quant-ph/0701168, Document of SECOQC project,
[36] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, 1998.
[37] C. Simon, H. De Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, "Quantum repeaters with photon pair sources and multimode memories," *Phys. Rev. Lett.*, vol. 98, p. 190503, 2007.
[38] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. Mirasso, L. Pesquera, and K. Shore, "Chaos-based communications at high bit rates using commercial fiber-optic links," *Nature*, vol. 438, no. 17, pp. 343–346, Nov. 2006.
[39] A. Zadok, J. Scheuer, J. Sendowski, and A. Yariv, "Secure key generation using an ultra-long fiber laser: Transient analysis and experiment," *Opt. Exp.*, vol. 16, pp. 16680–16690, Oct. 2008.
[40] J. P. Heritage and A. M. Weiner, "Advances in spectral optical code-division multiple-access communications," *IEEE J. Sel. Top. Quantum Electron.*, vol. 13, no. 5, pp. 1351–1369, Sep./Oct. 2007.
[41] , P. R. Prucnal, Ed., *Optical Code Division Multiple Access: Fundamentals and Applications*. New York: Taylor & Francis, 2006.
[42] T. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.
[43] E. Narimanov and B. Wu, "Advanced coding techniques for asynchronous fiber-optical CDMA," in *Proc. IEEE Quantum Electron. Laser Sci Conf.*, May 2005, pp. 1768–1770.
[44] R. Menendez, A. Agarwal, P. Toliver, J. Jackel, and S. Etemad, "Direct optical processing of M-ary code-shift keyed spectral phase encoded OCDMA," *J. Opt. Netw.*, vol. 6, no. 5, pp. 442–450, May 2007.
[45] T. Kodama, N. Nakagawa, N. Kataoka, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, "Secure 2.5 Gbit/s, 16-Ary OCDM block-ciphering," *J. Lightw. Technol.*, vol. 28, no. 1, pp. 181–187, Jan. 2010.
[46] G. Cincotti, N. Wada, and K. Kitayama, "Secure optical bit- and block-cipher transmission using a single multiport encoder/decoder," in *Proc. Opt. Fiber Commun. Conf. Nat. Fiber Opt. Eng. Conf.*, 2008, pp. 1–3.
[47] H. P. Yuen, "A New Quantum Cryptography," Report in Northwestern University, 2000, DARPA proposed paper.
[48] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, "Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks," *Phys. Rev. A*, vol. 71, p. 062326, 2005.
[49] O. Hirota, "Optical communication network and quantum cryptography," *IEICE Trans. Commun.*, vol. J87-B, no. 4, pp. 478–486, 2004, in Japanese.
[50] G. Kantor and P. Kumar, "After quantum key distributed: Physical layer encryption aided by optical noise," in *Proc. IEEE Globcom. 2007 DESIGN & DEVELOPERS FORUM* [Online]. Available: http://www.nucrypt.net/documents/globcom_2007.pdf
[51] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, S. Akutsu, K. Hosoi, Y. Doi, K. Ohhata, T. Katayama, and T. Shimizu, "Consideration of the implementation circuit of randomization for physical cipher by Yuen 2000 protocol," *IEICE Jpn.*, vol. J91-C, pp. 399–408, 2008.
[52] Y. Doi, S. Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, K. Ohhata, and K. Yamashita, "360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network," in *Proc. Opt. Fiber Commun. Conf. Nat. Fiber Opt. Eng. Conf.*, 2010, pp. 1–3.
[53] DCI Specification, Version 1.2. March 07 2008. [Online]. Available: http://www.dcimovies.com.

Ken-Ichi Kitayama (S'75--M'76--SM'89--F'03) received the B.E., M.E., and Dr.Eng. degrees in communication engineering from Osaka University, Osaka, Japan, in 1974, 1976, and 1981, respectively.

In 1976, he joined the NTT Laboratory. From 1982 to 1983, he was with the University of California, Berkeley, as a Research Fellow. In 1995, he joined the Communications Research Laboratory (currently National Institute of Information and Communications Technology), Tokyo, Japan. Since 1999, he has been a Professor in the Department of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University, Osaka, Japan. He has published more than 250 papers in refereed journals, written two book chapters, and translated one book. He holds more than 30 patents. His research interests include photonic label switching, optical signal processing, optical code-division-multiple access systems, and radio-over-fiber communications.

Dr. Kitayama currently serves on the Editorial Boards of the *IEEE/OSA Journal of Lightwave Technology*, *IEEE/OSA Journal of Optical Communications and Networking*, *Optical Switching and Networking* as an Associate Editor. He received the 1980 Young Engineer Award from the Institute of Electronic and Communication Engineers of Japan, the 1985 Paper Award on Optics from the Japan Society of Applied Physics, and the 2004 Achievement Award from Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, 2007, and the Shida Rinzaburoh Award and Fuji Sankei Business Eye Award in 2009. He is the Fellow of the IEICE of Japan.

Masahide Sasaki received the B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Sendai, Japan, in 1986, 1988, and 1992, respectively.

From 1992 to 1996, he was involved in the development of Si-MOSFETs with Ayase Laboratory, Nippon Kokan Company, Kanagawa, Japan. In 1996, he joined the Communications Research Laboratory, Ministry of Post and Telecommunications (currently National Institute of Information and Communications Technology, Ministry of Internal Affairs and Communications). Since 1994, he has been involved in Quantum Information Theory and Quantum Optics. He is currently a Group Leader of the Quantum ICT group.

Dr. Sasaki is a member of the Japanese Society of Physics, and the Institute of Electronics, Information and Communication Engineers of Japan.

Soichiro Araki (M'03) received the B.E. and M.E. degrees in electrical engineering from Kyoto University, Kyoto, Japan, in 1987 and 1989, respectively.

In 1989, he joined Opto-Electronics Research Laboratories, NEC Corporation, Kawasaki, Japan. In 1995, he was a Visiting Researcher at NEC Research Institute, Princeton, NJ, where he contributed to the analysis of communication performance in PC clusters. He is currently a Senior Manager at the System Platforms Research Laboratories, NEC Corporation. His current research interests include wavelength division multiplexing optical network architecture and generalized multiprotocol label switching/automatic switched optical network technologies.

Mr. Araki is the Fellow of the Institute of Electronics, Information and Communication Engineers of Japan.

Makoto Tsubokawa received the B.E., M.E., and Dr.Eng. degrees in applied physics from Hokkaido University, Hokkaido, Japan, in 1981, 1984, and 1989, respectively.

In 1984, he joined the NTT Electrical Communication Laboratory, where he was involved in research on transmission characteristics of optical fiber cables and network architecture of optical subscriber loops and in-house networks. From 2007 to 2010, he was an Executive Manager of research projects on next generation access systems and future access media at NTT Electrical Communication Laboratory. Since September 2010, he has been a Professor in the Graduate School, Waseda University, Tokyo, Japan.

Dr. Tsubokawa is a member of the Institute of Electronics, Information and Communication Engineers of Japan and IEEE Comsoc.

Akihisa Tomita received the B.S. and M.S. degrees in physics and the Ph.D. degree in electronics from the University of Tokyo, Tokyo, Japan, in 1982, 1984, and 1998, respectively.

He joined NEC Corporation in 1984. From 1991 to 1992, he was at AT&T Bell Laboratories, Holmdel, NJ, as a Visiting Researcher. In April 2010, he joined as a Professor in the Graduate School of Information Science and Technology, Hokkaido University, Hokkaido, Japan. He is the Leader of the Quantum Information Experimental Group, Quantum Computation and Information Project, ERATO-SORST funded by the Japan Science and Technology. His research interests include optical devices and systems for quantum information processing and communication.

Dr. Tomita is a member of the Physical Society of Japan, Japanese Society of Applied Physics, the Institute of Electronics, Information and Communication Engineers, and the Optical Society of America.

Kyo Inoue was born in Tokyo, Japan, in 1959. He received the B.S. and M.S. degrees in applied physics and the Ph.D. degree in electrical engineering from Tokyo University, Tokyo, in 1982, 1984, and 1997, respectively.

From 1984 to 2005, he was with Nippon Telegram and Telephone Company, where he was involved in the study of optical communication and quantum communication. He is currently a Professor at Osaka University, Osaka, Japan.

Katsuyoshi Harasawa received the B.S. degree in electrical engineering from Tokyo Denki University, Tokyo, Japan, and the Ph.D. degree from Kagoshima University, Kagoshima, Japan, in 1983 and 2008, respectively.

In 1983, he joined Hitachi Information & Communication Engineering, Ltd., Kanagawa, Japan, where he is currently the General Manager of the Communication Technology Division, and has been involved in the development of high-speed optical network systems and high-secure encryption systems.

Dr. Harasawa is a member of the Institute of Electronics, Information and Communication Engineers of Japan.

Yuki Nagasako received the B.Eng. degree from Nagoya University, Nagoya, Japan, in 1986, the M.Eng. degree from Kyoto University, Kyoto, Japan, in 1988, both in nuclear engineering, and the M.Sc. degree in theoretical physics from the University of Missouri, Columbia, in 1996.

He was with the Internet Research Institute, Inc., Tokyo, Japan. He is currently with the Information Sharing Laboratory Group, Nippon Telegram and Telephone Corporation, Tokyo, Japan. He joined the Quantum Information Science Research Center, Tamagawa University, Tokyo, in April 2007 as a Ph.D. student. He joined the NTT Transmission Systems Laboratory in 1988 and Bell Labs, Lucent Technology in 1998. His research interests include quantum cryptography and quantum communication.

Atsushi Takada (M'90) received the B.E., M.S., and Ph.D. degrees in electrical engineering from Osaka University, Osaka, Japan, in 1982, 1984, and 2005, respectively.

In 1984, he joined the Yokosuka Electrical Communication Laboratory, Nippon Telephone and Telegraph Public Corporation, Yokosuka, Japan, where he was involved in research on ultrafast optical pulse generation, optical amplification, high-speed optical transmission systems, photonic transport networks, and optical burst/packet switching networks. He is currently a Professor at the Institute of Technology and Science, The University of Tokushima, Tokushima, Japan.

Dr. Takada is a member of the Institute of Electronics, Information, and Communication Engineers of Japan and the Japan Society of Applied Physics.