Physical-Layer Security in Evolving Optical Networks

Nina Skorin-Kapov, Marija Furdek, Szilard Zsigmond, and Lena Wosinska

The authors provide a comprehensive overview of potential physical-layer attack scenarios in current and future optical networks. They then propose a general security framework, outlining possible strategies for dealing with such attacks, meant to aid in the development of efficient provisioning, monitoring, protection, and restoration schemes in the context of optical-layer security.

Abstract

We are witnessing the evolution of optical networks toward highly heterogeneous, flexible networks with a widening area of application. As the bandwidth and reliability performance requirements of mission-critical applications tighten, and the amount of carried data grows, issues related to optical network security are becoming increasingly important. Optical networks are vulnerable to several types of attacks at the physical layer, typically aimed at disrupting the service or gaining unauthorized access to carried data. Such security breaches can induce financial losses to clients or loss of privacy, or cause network-wide service disruption, possibly leading to huge data and revenue losses. Awareness of system weaknesses and possible attack methods is a prerequisite for designing effective network security solutions. As optical networks evolve, new and changing vulnerabilities must be identified and dealt with efficiently. To this end, this article provides a comprehensive overview of potential physical-layer attack scenarios in current and future optical networks. It then proposes a general security framework, outlining possible strategies for dealing with such attacks, meant to aid in the development of efficient provisioning, monitoring, protection, and restoration schemes in the context of optical-layer security.

Introduction: Optical Network Evolution

Optical networks have evolved from simple point-to-point systems operating on a single wavelength at megabit per second rates over a few kilometers to ultra-long-haul multiterabit systems supporting over a 100 wavelengths per fiber and all-optical transmission schemes [1]. Due to ever increasing bandwidth demands, and new traffic requirements and models stemming primarily from the proliferation of cloud services, further developments in optical networking are pushing toward increased dynamicity and flexibility.

To support the increasing complexity associated with future dynamic optical networks, software defined networking (SDN) has been proposed as a promising solution for simplifying control and management. The SDN paradigm focuses on decoupling the control and data planes, and shifting the control logic from routers and switches to a logically centralized controller, essentially acting as a network operating system. The network can then be made programmable through software applications running on top of this operating system and interacting with underlying physical network devices [2].

To enhance flexibility for more efficient resource usage, mixed line rate (MLR) networks allow the coexistence of different channel sizes over the existing infrastructure based on the legacy fixed 50 GHz grid pattern set by the International Telecommunication Union (ITU). A *flexible grid* option based on 12.5 GHz frequency slots was adopted by the ITU in 2012 to support finer grid granularity. Further flexibility is envisioned with the *elastic optical networking* (EON) paradigm where use of a flexible grid and adaptive transceivers will allow connections to be established with variable bit rates and the spectrum allocated to demands to grow/shrink as needed [3].

The foreseen evolution of optical networks to dynamic elastic SDN-based networks will lead to new security vulnerabilities that must be addressed in order to provide a secure networking environment. In fact, there is growing interest of major telecom operators and vendors in optical-layer security, driving the development of solutions for optical fiber intrusion detection and encryption-enabled transponders. However, many aspects of determining and counteracting security breaches are yet to be addressed. Identifying vulnerabilities and possible threats in both current and future networks is a crucial prerequisite for developing secure planning approaches and effective protection and restoration strategies to support this migration. In this article, we provide an overview of physical-layer vulnerabilities and potential attack scenarios in evolving optical networks, aimed at highlighting important security issues and challenges. We then present a general security framework outlining possible methods of dealing with some of them and provide directions for future work.

Physical-Layer Attacks in Evolving Optical Networks

Physical-layer attacks have traditionally been categorized according to the type of damage they cause: service disruption or eavesdropping. Some

Nina Skorin-Kapov is with the University Centre of Defense, San Javier Air Force Base; Marija Furdek and Lena Wosinska are with KTH Royal Institute of Technology; Szilard Zsigmond is with Nokia.

0163-6804/16/$25.00 © 2016 IEEE

	Signal insertion attacks	Signal splitting attacks	Physical infrastructure attacks
Example attacks	High-power jamming attack Amplifier transient attack Mixed modulation attack	Tapping attack Low-power QoS attack	Single component attack Disaster-like attack Critical location attack
Characteristics	• Typically cause signal degradation • Can appear sporadically • May propagate • May disrupt individual or multiple connections traversing a link	• Breach privacy and/or cause signal degradation • Some attacks may propagate • Potentially difficult detection/source identification	• Typically cause channel outage • Persist until repaired • Do not propagate • Typically disrupt all connections traversing the affected nodes/links • Usually easier detection

Table 1. Physical-layer attack examples and their typical characteristics.

Signal insertion attacks reduce the quality of transmission of legitimate connections by injecting harmful signals into the network, causing service degradation (or possibly service denial). Depending on the network architecture and optical components used, signal insertion attacks may propagate through the network, causing system-wide damage, and can appear sporadically, potentially incurring multiple restorations.

of these attacks have previously been identified and described in [4, 5, references therein], primarily exploiting the transparency associated with optical-bypass-based networks. Here we extend these works with several new attack scenarios exploiting the vulnerabilities of evolving optical networks and classify them according to the attack method used, which may call for distinct protection schemes. We distinguish between three types of attacks: *signal insertion attacks*, *signal splitting attacks*, and *physical infrastructure attacks*, as shown in Table 1.

Signal Insertion Attacks

Signal insertion attacks reduce the quality of transmission of legitimate connections by injecting harmful signals into the network, causing service degradation (or possibly service denial). Depending on the network architecture and optical components used, signal insertion attacks may propagate through the network, causing system-wide damage, and can appear sporadically, potentially incurring multiple restorations. Examples of such attacks are described below.

High-Powered Jamming Attacks

High-powered jamming attacks can be realized by inserting an optical signal of excessive power (e.g., 5–10 dB above normal signals) on a legitimate channel used in the network (in-band jamming) or on a wavelength outside the signal window (out-of-band jamming) [4]. Such high-power signals, which exceed the component specifications, can degrade co-propagating user channels due to increased nonlinear effects and crosstalk in fibers and switches. Furthermore, a jamming signal out of the working range of the amplifier can cause so-called gain competition in optical amplifiers where the high-powered signal robs weaker legitimate signals of gain.

Typical point-to-point data center applications or filterless network architectures for terrestrial or submarine applications route traffic using only passive couplers with amplifiers, and cannot thwart or readjust such jamming signals. For actively switched networks, this type of attack can be especially harmful in older networks deploying fixed optical add/drop multiplexers (FOADMs) without power equalization capabilities, as a jamming signal inserted on a legitimate connection could also propagate through the network unthwarted, causing excessive damage. Since approximately 40 percent of current networks still employ this type of technology, this scenario still poses a significant threat. FOADMs are particularly dominant in Asian markets, as well as having significant presence in U.S. metro applications.

In more modern networks, which deploy reconfigurable OADMs (ROADMs) equipped with variable optical attenuators (VOAs) to regulate the output power of transiting signals, such a jamming signal would be attenuated at the first downstream node, limiting its propagation. However, it would still cause increased crosstalk to co-propagating signals on the link where it was inserted, in addition to disrupting the jammed signal itself. Additionally, even if electronic equalization in amplifiers counteracts gain competition in the steady-state, initial brief oscillations in gain (called transients) can occur. Some example effects of a high-power jamming attack are illustrated in Fig. 1a.

Amplifier Transient Attacks

Amplifier transients, arising in both erbium doped fiber amplifiers (EDFAs) and Raman amplifiers [1], occur when there is a sharp change in the input power level, causing the amplifier gain to change briefly before returning to its nominal value (steady-state). The power of the remaining channels increases or decreases as the optical amplifier attempts to maintain a constant total power level on the fiber. Besides high-power jamming, establishing and tearing down normal connections (e.g., for restoration purposes) in optical bypass networks can cause undesirable transients. Although these oscillations are short-lived, they can still cause error bursts and may even propagate, where transients on one link cause transients on successive links. These effects could be exploited by a malicious attacker by repeatedly or sporadically inserting a high- or even normal-powered jamming signal (e.g., inserting fast pulsing signals in less than a 1 ms timeframe), which would not only cause transients itself, but could incur multiple restorations of the affected legitimate signals, subsequently causing additional transients on other links.

Systems that better manage transients are evolving as a prerequisite for future dynamic networking. Consequently, the amplifiers used in the newest systems work in constant gain mode with transient suppression control. However, there are still significant deployments with constant-power-based amplifiers where transient attacks could cause significant signal deterioration. This is especially true in submarine cables where loading lines are used to maintain a constant input power in undersea amplifiers. Based on the implementation, the reaction time of such loading lines may be much slower than the transient controls

In newer generation networks, a dedicated interface will be defined to host alien wavelengths in order to tune their power levels, but there will still be no control over frequency and modulation format. Frequency control can be enabled by using additional built-in tunable filters, at the expense of increased complexity, insertion loss, and cost.

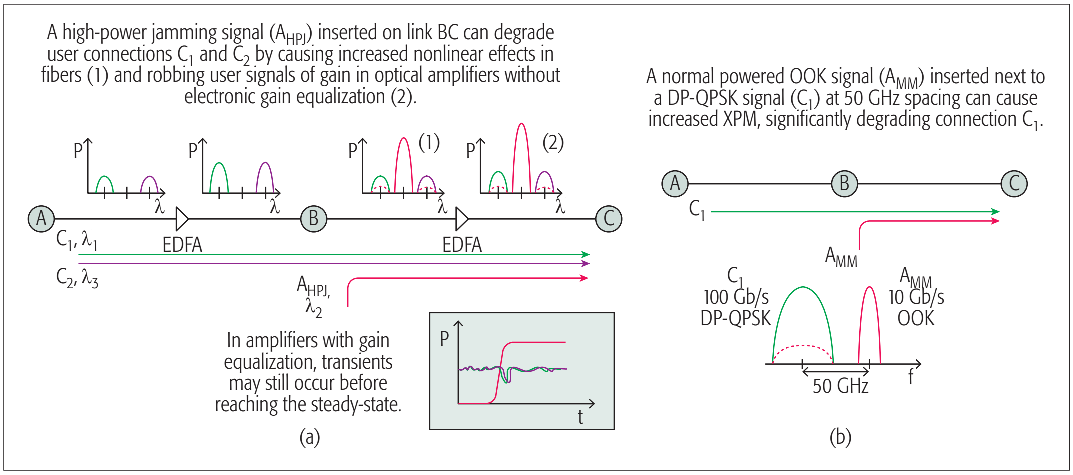

A high-power jamming signal (A_{HPJ}) inserted on link BC can degrade user connections C_1 and C_2 by causing increased nonlinear effects in fibers (1) and robbing user signals of gain in optical amplifiers without electronic gain equalization (2).
P
λ
(1)
(2)
A
B
C
EDFA
EDFA
C_1, λ_1
C_2, λ_3
A_{HPJ}, λ_2
In amplifiers with gain equalization, transients may still occur before reaching the steady-state.
t
(a)
A normal powered OOK signal (A_{MM}) inserted next to a DP-QPSK signal (C_1) at 50 GHz spacing can cause increased XPM, significantly degrading connection C_1.
C_1
A_{MM}
C_1 100 Gb/s DP-QPSK
A_{MM} 10 Gb/s OOK
50 GHz
f
(b)

Figure 1. Example effects of a) a high-power jamming attack; b) a mixed modulation attack.

implemented in terrestrial amplifiers, making them more vulnerable to transient-based attacks.

Mixed Modulation Attacks

In mixed line-rate (MLR) and future elastic optical networks (EONs), a key security vulnerability stems from the nonlinear effects arising between line rates using different modulation formats. Typically, on-off keying (OOK) is used for 10 Gb/s rates, binary phase shift keying (BPSK) or quadrature phase shift keying (QPSK) for 40 Gb/s rates, and dual-polarization QPSK (DP-QPSK) for 100 Gb/s rates. OOK 10G channels strongly deteriorate the quality of the higher-bit-rate phase modulated channels due to cross phase modulation (XPM). Although it is technically possible to have 10G and 40/100/200G channels at 50 GHz spacing, larger guardbands should be employed to reduce the nonlinear penalty imposed on the higher line rate channels to an acceptable level. This is especially critical in more nonlinear G655 fiber types.

A possible attack causing signal degradation could be realized by inserting an OOK channel near a 40/100/200G channel without allowing for enough guardband, as shown in Fig. 1b, significantly deteriorating the optical signal-to-noise ratio (OSNR) of the higher-line-rate signal. If such a signal was inserted as a legitimate connection by an inside attacker, it could propagate through the network, degrading multiple co-propagating neighboring channels. As opposed to high-power jamming, such a signal would not be thwarted by power equalizing components or even be detected as malicious by power monitoring equipment.

To perform any of the aforementioned signal insertion attacks, an attacker can access the network via various entry points. An insider with node access can directly tamper with the associated lasers and patch panels to increase power or insert harmful signals. Note that depending on the nodal architecture (e.g., a ROADM in a broadcast-and-select configuration with a wideband coupler on the add side), an attacking signal may be launched into the network unfiltered. Alternatively, a harmful signal can be inserted by an external attacker with physical access to part of the fiber by removing the cladding, slightly bending the fiber and radiating light into it. Another possible way to access the channel is via monitoring ports typically present at network components, such as amplifiers, wavelength selective switches (WSSs), or (de)multiplexers, which mirror the signal with an optical splitter to allow for monitoring devices to be connected without traffic interruption. In addition to providing a means for potential eavesdropping, these ports could also be used to insert malicious signals into the network and damage live traffic.

Another entry point to the network can be realized through alien wavelengths. Namely, in order to allow for network upgrades and efficient transmission of high-capacity connections over the existing infrastructure, operators are forced to implement alien wavelengths in their networks. Such connections can traverse multiple domains without optical-electronic-optical (OEO) conversions at domain boundaries in multi-vendor environments. In simple FOADM-based networks, the network management system (NMS) has no information on the performance of the alien channels or control over their power and frequency. In more intelligent networks, the alien channels are configured as friendly wavelengths, allowing the management system to have information on signal parameters, but still no control over their values. If the nodal architecture is such that there is no WSS on the add side, such as a colorless FOADM with no WSSs on the add/drop parts or a 1 × 9 broadcast-and-select ROADM with a WSS only on the drop side and a coupler on the add side, these alien wavelengths can enter the network unfiltered, providing a point of entry for any of the aforementioned signal insertion attacks. In newer generation networks, a dedicated interface will be defined to host alien wavelengths in order to tune their power levels, but there will still be no control over frequency and modulation format. Frequency control can be enabled by using additional built-in tunable filters, at the expense of increased complexity, insertion loss, and cost.

Signal Splitting Attacks

We refer to signal splitting attacks as attacks that split and remove part of a legitimate signal carried in the network, for either eavesdropping or signal degradation purposes. Such attacks may be difficult to detect and locate due to low losses incurred at the insertion point, going undetected by the network management system and/or raising alarms only downstream of the attacking point. Two examples of such attacks are described below.

Tapping Attacks

Tapping attacks physically tap into the optical signals traversing the network in order to gain unauthorized access to confidential privileged information. In today's digital era, eavesdropping occurs on all network layers from the application to the physical layer, primarily targeting governments and the financial, energy, transport or pharmaceutical sectors. This becomes even more important with the development of cloud services and tremendous amounts of data, including mission-critical data, being stored in data centers. One way of performing such an attack at the physical layer is by directly accessing the optical channel via fiber tapping, that is, removing the fiber cladding and bending the fiber to cause part of the signal to leak out onto a photo detector [6]. Tapping devices, which can be clipped onto the fiber and cause micro-bends to leak signals, are easily accessible on the market. Furthermore, existing tapping devices can cause losses below 1 dB, which would not be detected by most commonly used NMSs unless sensitive power monitors and intrusion detection systems (IDSs), typically based on bulk power measurements, are employed. Another possible way of accessing user channels could be via component monitoring ports, as mentioned in the previous subsection.

Low-Power QoS Attacks

A low-power quality of service (QoS) attack, identified in [7], deliberately attenuates the power of a legitimate channel by inserting a splitter along the link for signal degradation purposes. Since optical amplifiers are placed such that they compensate only for the losses on the previous fiber span, the induced attenuation could significantly degrade the performance metrics of the attacked connection. Even if power monitoring is employed, the power degradation may not be significant enough to cross the alarm threshold at the attack location, but may do so on downstream links far from the attacking point, making source identification and localization more difficult. Furthermore, if nodes are equipped with fixed attenuation-based power equalization, the attack could propagate since legitimate co-propagating channels would be attenuated to ensure a flat power spectrum.

Physical Infrastructure Attacks

Physical infrastructure attacks include all attacks that physically damage or tamper with the optical network infrastructure, such as cutting a fiber, unplugging connections, or damaging optical components. These attacks typically persist until repaired and do not propagate through the network. They can often be modeled as single or multiple component faults and require efficient protection and/or restoration mechanisms. We distinguish between three types of physical infrastructure attacks as follows.

Single Component Attacks

Single component attacks refer to attacks that mimic single link or node component failures, such as deliberately cutting a fiber or damaging a switch or amplifier. Individual connections could also be unplugged at the patch panel. Such attacks are typically detected by a loss of light and rely on standard survivability techniques.

Disaster-Like Attacks

Disaster-like attacks are human-made attacks that have the effect of multiple failures in a specific geographical area, such as weapons of mass destruction (WMD) and electromagnetic pulse (EMP) attacks [8]. EMP attacks are realized by radiating a short burst of electromagnetic energy that can disrupt the electronic components needed to operate the fiber plant in a large geographical area. From a network perspective, these attacks have similar effects as natural disasters and can affect all generations of optical networks.

Critical Location Attacks

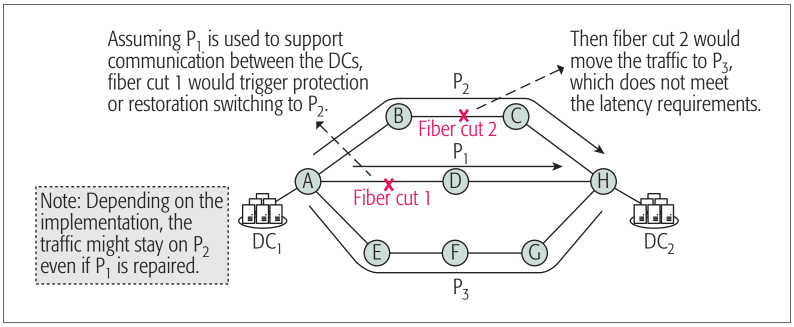
Critical location attacks are aimed at specifically attacking weak points or critical hub nodes in the network to cause system-wide damage. Although these attacks can fall under single component failures or disaster-like failures, we consider them separately since they also include coordinated multiple failures that are not geographically localized.

For example, a critical location attack could target undersea landing points. Generally, undersea landing points are highly localized due to regulatory limitations, and as a consequence are at a high risk of location-based attacks. Given the remote location and fairly sparse undersea connectivity of some islands or even continents, targeting specific undersea landing points could impact the overall reachability of such areas.

As demands for cloud services proliferate, content service providers (Amazon, Google, Facebook, Yahoo, etc.) increasingly store and replicate massive amounts of content in multiple data centers. Although storing data in multiple geographically distributed locations generally leads to increased reliability in case of localized failures, if an attacker were to acquire information regarding the sites where the content is replicated, a coordinated attack targeting all mirrored sites could cause tremendous damage. A more covert attack could target replica synchronization by exploiting network latency. Namely, synchronous replication used between data centers is very sensitive to signal latency, limiting the maximum distance suitable for synchronous replications to 100–200 km. If the topology of the network is known, a set of systematic fiber cuts or component damaging attacks could be performed to take advantage of this vulnerability by forcing the path between two data centers to be restored to a path that does not meet these requirements, as illustrated in Fig. 2. Although latency measurements are defined in optical transport network (OTN) frames, real-time latency monitoring is not implemented in most networks, which complicates the detection of such attacks.

In future SDN-based networks, network control logic will be moved to an external entity, referred to as the SDN controller, which will

As demands for cloud services proliferate, content service providers increasingly store and replicate massive amounts of content in multiple data centers. Although storing data in multiple geographically distributed locations generally leads to increased reliability in case of localized failures, if an attacker were to acquire information regarding where the content is replicated, a coordinated attack targeting all mirrored sites could cause tremendous damage.


Assuming P_1 is used to support communication between the DCs, fiber cut 1 would trigger protection or restoration switching to P_2.

Then fiber cut 2 would move the traffic to P_3, which does not meet the latency requirements.

Note: Depending on the implementation, the traffic might stay on P_2 even if P_1 is repaired.

Figure 2. Example of a critical location attack targeting latency sensitivity of synchronous replication between data centers. Paths P_1 and P_2 are assumed to satisfy the latency requirements, while P_3 does not.

serve as a network-wide operating system. This approach offers many benefits, such as simplification of network management, easier modification of control software, and increased control to carriers and enterprises. It can also provide enhancements in security by providing a centralized point of control to collect and distribute security information. However, the SDN controller will also be prone to a whole set of new security threats since a compromised controller can compromise the entire network [2]. At the physical layer, a centralized architecture for the SDN controller would make it very vulnerable to physical infrastructure attacks, presenting a single point of attack. Due to reliability and scalability issues, the SDN controller will most likely be implemented in a distributed computing environment. However, a coordinated attack could still target the multiple locations of the SDN controller, causing massive system-wide damage.

A Physical-Layer Security Framework

Operators are often faced with making complex routing and fiber infrastructure deployment decisions, which are heavily influenced by security issues and involve significant trade-offs with route length, latency, and cost. For example, networks across the Middle East could be serving traffic between Asia and Europe (approximately 7 TB exchanged every second) with the lowest latency due to the shortest physical distance. However, due to security risks and geo-political factors, most commonly alternative, longer options (e.g., SEA-ME-WE undersea cables or routes via Russia or the Pacific and Atlantic Oceans) are used.

To aid operators in making the network provisioning decisions considering physical-layer security, we present a general security framework for evolving optical networks, outlining potential approaches to mitigate, avoid, and/or reduce the damage caused by the aforementioned physical-layer attacks, as summarized in Table 2. Depending on the quality of protection and security required, we propose to differentiate between *best effort*, *standard protected*, and *gold user* connections, and define security-aware provisioning methods corresponding to each class.

Best Effort

Best effort connections would rely on efficient network planning approaches, but no specific protection resources would be allocated. Attack-aware optical network planning, originally proposed in [9], could be applied where the propagation characteristics of various attack scenarios are incorporated into the planning phase to find connection arrangements that incur the least damage in case of an attack without the need for extra resources. In such an approach, hard attack-aware constraints are not considered, but rather "safer" schemes are favored among alternatives of equal cost (in terms of resources used). Consequently, we refer to such methods as *soft attack-aware* planning schemes. *Soft attack-aware routing and wavelength assignment* (Soft AA-RWA) schemes for high-power jamming attacks have been proposed in [9, 10]. A simple example of such an approach is shown in Fig. 3. Similar methods could be applied to transient attacks and mixed modulation attacks, for example, by incorporating larger channel spacing where available in wavelength or spectrum assignment schemes to minimize the number of connections that can simultaneously be affected by a mixed modulation attack.

In future elastic optical networks, mixed modulation and jamming attacks could additionally be dealt with by taking advantage of spectrum reallocation methods proposed for dynamic defragmentation where optical corridors are shifted to alternative spectrum slots to better align the available spectrum on adjacent links. A method for hitless spectrum re-allocation has been proposed where optical corridors first grow to include new contiguous free spectral slots, and subsequently shrink to encompass only the new slots [3]. This method could be applied as a best effort attack restoration mechanism by shifting the assigned spectrum of affected connections to neighboring free spectrum (if available), away from the spectrum of the malicious signal.

To deal with eavesdropping, encryption methods implemented in optical transponders would protect the carried data. Some such encryption cards are commercially available from most vendors. Physical-layer technologies proposed for further security enhancements in protecting user data confidentiality include secure communications using optical chaos (SCOC), optical code-division multiplexing (OCDM), and quantum key distribution [5, 6, 11]. Optical monitoring solutions are also available that monitor power levels at nodes. Some vendors have implemented intrusion detection based on power monitoring to trigger alarms when the power unexpectedly drops. Such IDSs would be employed to monitor network operations and raise an alarm in case of any anomaly, but no direct action would be undertaken for best effort connections. For physical infrastructure attacks, standard best effort restoration would be employed.

Standard Protected

Standard protected connections refer to higher-priority connections that would employ shared or dedicated path protection schemes, depending on the level of protection required. As with best effort traffic, these connections would rely on general soft attack-aware planning to minimize the number of connections simultaneously affected by signal insertion attacks. The approaches would be extended to encompass survivability to ensure successful restoration of affected con-

	Signal insertion attacks	Signal splitting attacks	Physical infrastructure attacks
Best effort connections	–Soft AA-RWA/RSA schemes –Best effort spectrum reallocation	–Optical encryption –IDS for detection	–Best effort restoration
Standard protected connections	–Soft Survivable AA-RWA/RSA schemes –Spectrum reallocation with priority over best effort channels	–Optical encryption –IDS with a less sensitive reaction threshold	–Shared or dedicated path protection for single failures
Gold user connections	–Hard Survivable AA-RWA/RSA schemes –Enhanced spectrum reallocation schemes and larger guardbands	–Optical encryption – Hard AA routing schemes –Optical steganography – Route hopping –IDS with a more sensitive reaction threshold –Proactive recovery using fiber tampering detection methods	–Dedicated (1+2) path protection for single and multiple failures –Disaster- and critical location-aware survivability schemes –Proactive recovery using fiber tampering detection methods

AA-RWA/RSA: attack-aware routing and wavelength assignment/routing and spectrum assignment
IDS: Intrusion detection systems

Table 2. The proposed security framework indicating possible approaches to deal with physical-layer attacks for best effort, standard protected, and gold user connections.

The user class that we refer to as Gold users would comprise a smaller portion of customers who are willing to pay more for gold services in terms of security. Such connections would be provisioned with special dedicated 1+2 attack-aware path protection schemes. Security measures for gold users would potentially incur higher costs, but would provide enhanced protection.

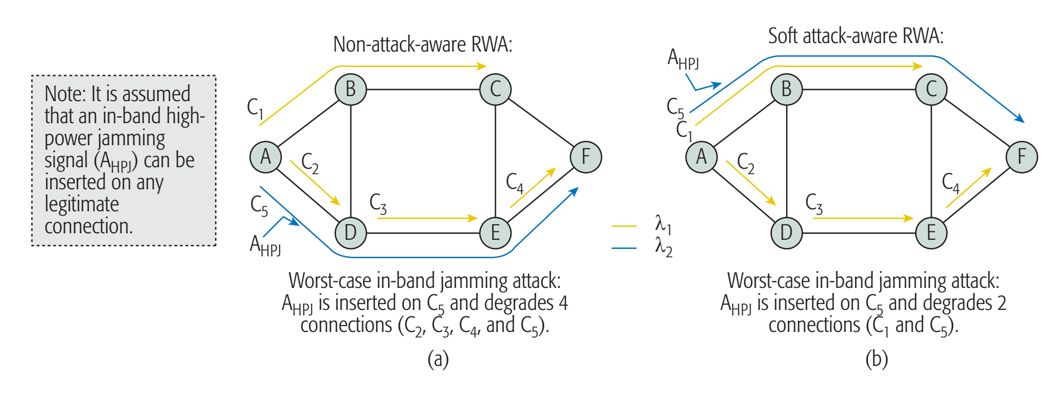

Note: It is assumed that an in-band high-power jamming signal (A_{HPJ}) can be inserted on any legitimate connection.
Non-attack-aware RWA:
A
B
C
D
E
F
C_1
C_2
C_3
C_4
C_5
A_{HPJ}
Worst-case in-band jamming attack: A_{HPJ} is inserted on C_5 and degrades 4 connections (C_2, C_3, C_4, and C_5).
(a)
λ_1
λ_2
Soft attack-aware RWA:
A_{HPJ}
C_5
C_1
C_2
C_3
C_4
Worst-case in-band jamming attack: A_{HPJ} is inserted on C_5 and degrades 2 connections (C_1 and C_5).
(b)

Figure 3. An example of: a) a non-attack-aware; b) a soft attack-aware RWA scheme for in-band jamming attacks in FOADM-based networks. While both schemes use equal resources in terms of wavelength links, the soft attack-aware solution faces less potential damage in the presence of in-band jamming.

nections. As an example, a survivable AA-RWA scheme that ensures that the primary path and backup path of protected connections cannot be affected by the same jamming signal was proposed in [12].

Where spectrum is scarce and larger spacing cannot be allocated to reduce the effects of mixed modulation attacks in MLR and elastic networks, interleaving higher-priority (protected) and lower-priority (best effort) connections can ensure that at most one higher-priority connection is affected by an attack on a link. Furthermore, if higher-priority connections are alternated with sets of best effort channels in elastic networks, lower-priority channels could potentially be dropped to allow for spectral reallocation of higher-priority connections in case of an attack, as illustrated in Fig. 4. Besides attack scenarios, interleaving low- and high-priority connections could also leave more space for reallocating higher-priority connections in case of standard defragmentation.

As with best effort traffic, encryption methods would be used to protect carried data from eavesdropping. As a second line of defense for tapping and other component insertion attacks, power drops detected by the IDS would incur restoration. Two alarm thresholds could be incorporated into the IDS, where only alarms corresponding to the higher threshold would trigger reaction mechanisms for standard protected users, to avoid excessive false alarms and frequent restorations.

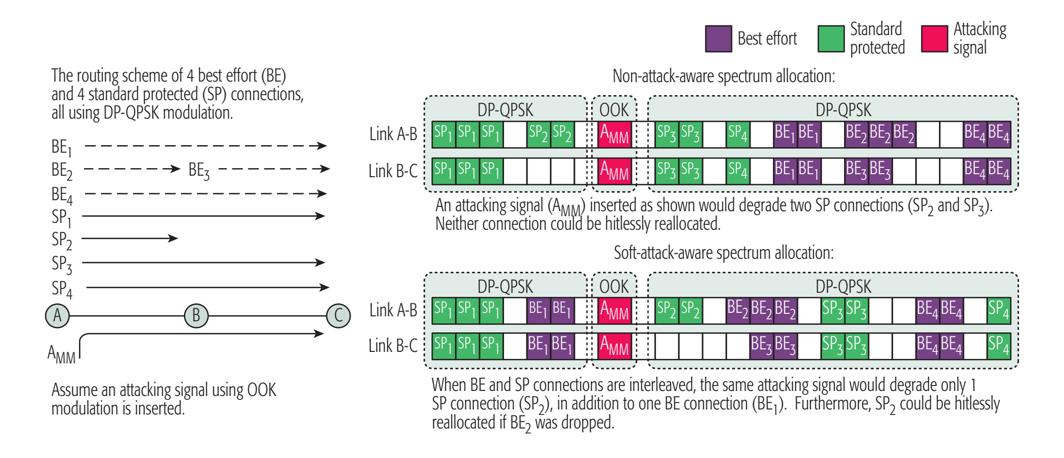
Regarding physical infrastructure attacks, regular protected users would rely on standard shared or dedicated path protection for single link and node failures. Such protection schemes typically do not consider multiple failures and disasters, and thus would not specifically deal with disaster-like and critical location attacks.

Gold Users

The user class that we refer to as *gold users* would comprise a smaller portion of customers who are willing to pay more for gold services in terms of security. Such connections would be provisioned with special dedicated 1+2 attack-aware path protection schemes. Security measures for gold users would potentially incur higher costs, but would provide enhanced protection.

As opposed to soft attack-aware planning schemes, which are not aimed at protecting individual connections, gold users would be specifically routed over "safer" paths, even if extra

Larger guardbands could be employed to ensure sufficient space for reallocation, as well as enhanced versions that allow other standard protected connections to be re-allocated and best effort connections to be torn down to make room for the necessary shift of gold users.


Best effort
Standard protected
Attacking signal
Non-attack-aware spectrum allocation:
DP-QPSK
OOK
DP-QPSK
Link A-B
SP_1 SP_1 SP_1 SP_2 SP_2 A_{MM} SP_3 SP_3 SP_4 BE_1 BE_1 BE_2 BE_2 BE_2 BE_4 BE_4
Link B-C
SP_1 SP_1 SP_1 A_{MM} SP_3 SP_3 SP_4 BE_1 BE_1 BE_3 BE_3 BE_4 BE_4
Soft-attack-aware spectrum allocation:
DP-QPSK
OOK
DP-QPSK
Link A-B
SP_1 SP_1 SP_1 BE_1 BE_1 A_{MM} SP_2 SP_2 BE_2 BE_2 BE_2 SP_3 SP_3 BE_4 BE_4 SP_4
Link B-C
SP_1 SP_1 SP_1 BE_1 BE_1 A_{MM} BE_3 BE_3 SP_3 SP_3 BE_4 BE_4 SP_4
BE_1
BE_2
BE_3
BE_4
SP_1
SP_2
SP_3
SP_4
A
B
C
A_{MM}

The routing scheme of 4 best effort (BE) and 4 standard protected (SP) connections, all using DP-QPSK modulation.

Assume an attacking signal using OOK modulation is inserted.

An attacking signal (A_{MM}) inserted as shown would degrade two SP connections (SP_2 and SP_3). Neither connection could be hitlessly reallocated.

When BE and SP connections are interleaved, the same attacking signal would degrade only 1 SP connection (SP_2), in addition to one BE connection (BE_1). Furthermore, SP_2 could be hitlessly reallocated if BE_2 was dropped.

Figure 4. An example of the effects of distinct spectrum allocation schemes in the presence of a mixed modulation attack.

resources are required. We refer to this as *hard attack-aware* (AA) planning. Hard (survivable) AA-RWA schemes for gold users could be applied in future SDN networks by incorporating data and statistics collected by the SDN controller to avoid untrustworthy links, nodes, domains, or channels. Since attacks can occur sporadically, nodes and links that have previously raised alarms or have shown suspicious behavior, such as power fluctuations indicating jamming, transients, or tapping, could be avoided. Furthermore, gold users could be routed over paths or domains that do not support alien wavelengths. They could also be routed to avoid higher-risk areas, such as locations of major military facilities or political unrest, which are more probable targets of WMD and EMP attacks. As an example, in 2012 Gulf Bridge International (GBI) integrated a terrestrial link in addition to its submarine network for Asia-Europe route diversity that avoids Egypt [13]. Routing schemes could also favor links and nodes employing better optical monitoring equipment or more advanced technology, such as amplifiers with more effective transient control or programmable transponders that can change the modulation format if the quality of transmission falls below a certain threshold.

Gold users would also take advantage of spectral reallocation in elastic networks in case of a mixed modulation or jamming attack. Larger guardbands could be employed to ensure sufficient space for reallocation, as well as enhanced versions that allow other standard protected connections to be re-allocated and best effort connections to be torn down to make room for the necessary shift of gold users.

In addition to optical encryption methods to protect against eavesdropping, another layer of privacy could be provided for gold users transmitting highly sensitive information by applying optical steganography where secret so-called stealth channels are hidden among regular public channels [6, 14]. In future dynamic networks with fast setup times, enhanced privacy for mission-critical demands could also be realized using route hopping [1]. In this approach, the route of a connection is changed rapidly to avoid eavesdropping, analogous to frequency hopping in military radio applications.

Assuming a double threshold IDS, the more sensitive reaction threshold would be applied to gold users to cease transmission on the intruded path. The proactive recovery scheme described in [15] could also be applied, where connections are preemptively restored before conventional performance monitoring detects power variations or before a failure (e.g., a fiber cut) actually occurs by detecting vibrations and other environmental variations around a fiber.

For physical infrastructure attacks, the dedicated path protection schemes designed for gold users would not only consider single component failures, but would also be designed to deal with multiple failures or attacks. A disaster-resilient protection and content placement scheme for data center networks was proposed in [8] where anycast routing is exploited to protect mission-critical demands accessing data center content by routing their protection paths to data centers in different geographical regions. Similar approaches should be investigated to deal with critical location attacks.

Main Research Challenges and Opportunities

Developing new attack-aware planning methods for both current and future networks brings forth many new research challenges and offers opportunities for novel research ideas on topics such as latency-aware and attack-aware anycast protection schemes for inter-data center networks, and enhanced survivable RSA schemes and defragmentation algorithms for elastic and flexible-grid networks. At the component level, improvements in amplifier transient control will play an important role, not only in the context of attacks, but also as a prerequisite for future dynamic networks. Furthermore, perhaps one of the biggest challenges in the context of future optical networks security will lie in the secure design of the SDN controller in future SDN-based networks. Methods to exploit the benefits of this centralized approach for secure network planning should be developed in hand with effective methods to protect the SDN controller, not only from physical infrastructure attacks, but also from unauthorized access. That is, breaching the

SDN controller and gathering intelligence on the network topology, routing, availability, and so on could be used to realize any of the aforementioned attacks. As such, secure authentication and access will pose big challenges, particularly as network management systems become accessible via mobile phone applications (and not only from secured offices). Advances in optical encryption methods can aid in the development of new authentication schemes and help protect user privacy, while effective alarm correlation and attack location algorithms for improved IDS software can further facilitate attack detection and isolation.

Conclusion

Due to increasing bandwidth and performance requirements, primarily stemming from the growth of cloud services, security issues in optical networks are of ever increasing importance. Although the dynamicity and flexibility associated with future optical networks offers many advantages, it also incurs additional security vulnerabilities, which must be identified in order to develop efficient and cost-effective countermeasures. In this article, an overview of physical-layer attacks in evolving optical networks is given, identifying various attack scenarios, their potential consequences, and possible entry points for attackers. A general security framework is then proposed, describing potential methods for dealing with such attacks for different classes of users aimed at reducing the overall network vulnerability. The proposed framework serves as a starting point for developing new and enhanced security solutions in current and future optical networks.

Due to increasing bandwidth and performance requirements, primarily stemming from the growth of cloud services, security issues in optical networks are of ever increasing importance. Although the dynamicity and flexibility associated with future optical networks offers many advantages, it also incurs additional security vulnerabilities which must be identified in order to develop efficient and cost-effective countermeasures.

Acknowledgments

This research was partially supported by Spanish grant TEC2014-53071-C3-1-P (“ONOFRE”) and European Union FP7 grant agreement no. 318137 (Collaborative Integrated Project “DISCUS”).

References

[1] J. M. Simmons, *Optical Network Design and Planning*, 2nd ed., Springer, 2014.

[2] D. Kreutz *et al*., “Software-Defined Networking: A Comprehensive Survey,” *Proc. IEEE*, vol. 103, no. 1, 2015, pp. 14-76.

[3] O. Gerstel *et al*., “Elastic Optical Networking: A New Dawn for the Optical Layer?” *IEEE Commun. Mag*., vol. 50, no. 2, Feb. 2012, pp. S12–S20.

[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, 2006, pp. 79–86.

[5] K. Kitayama *et al*., “Security in Photonic Networks: Threats and Security Enhancement,” *IEEE/OSA J. Lightwave Tech*., vol. 29, no. 21, 2011, pp. 3210–22.

[6] M. P. Fok *et al*., “Optical Layer Security in Fiber-Optic Networks,” *IEEE Trans. Info. Forensic Security*, vol. 6, no. 3, 2011, pp. 725–36.

[7] T. Deng and S. Subramaniam, “Covert Low-Power QoS Attack in All-Optical Wavelength Routed Networks,” *Proc. IEEE GLOBECOM*, 2004, vol. 3, pp. 1948–52.

[8] M. F. Habib *et al*., “Design of Disaster-Resilient Optical Datacenter Networks,” *J. Lightwave Tech.*, vol. 30, no. 16, 2012, pp. 2563–73.

[9] N. Skorin-Kapov, J. Chen, and L. Wosinska, “A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment,” *IEEE/ACM Trans. Net*., vol. 18, no. 3, 2010, pp. 750–60.

[10] K. Manousakis and G. Ellinas, “Attack-Aware Planning of Transparent Optical Networks,” *Opt. Switch. Net*., vol. 19, no. 2, 2016, pp. 97–109.

[11] M. Sasaki *et al*.,”Quantum Photonic Network: Concept, Basic Tools, and Future Issues,” *IEEE J. Sel. Topics Quantum Electron*., vol. 21, no. 3, 2015, pp. 6400313-1–13

[12] M. Furdek, N. Skorin-Kapov, and L. Wosinska, “Attack-Aware Dedicated Path Protection in Optical Networks,” *IEEE/OSA J. Lightwave Tech*., vol. 34, no.4, 2016, pp. 1050–61.

[13] A. Eid, “The Naked Truth about Submarine Cables,” Submarine Cable Wksp., Pacific Telecommunications Council, 2014.

[14] Ben Wu *et al*., “Optical Signal Processing and Stealth Transmission for Privacy,” *IEEE J. Sel. Topics Signal Processing*, vol. 9, no. 7, 2015, pp. 1185–94

[15] E. Le Rouzic, N. Brochier, and J. Pesic, “Procédé et Dispositif de Détermination d’un Risque de Coupure d’Une Fibre Optique,” European Patent EP 2 403 164 A1, Jan. 4, 2012.

Biographies

Nina Skorin-Kapov is an associate professor at the University Centre of Defense at the San Javier Air Force Base, Spain. She received her Ph.D. in telecommunications from the University of Zagreb, Croatia, in 2006 and completed a postdoctoral fellowship at Ecole Nationale Superieure des Telecommunications, Paris, France, in 2006–2007. Before joining the University Centre of Defense in 2013, she was an assistant professor (2008–2012) and associate professor (2012–2013) in the Department of Telecommunications at the Faculty of Electrical Engineering and Computing, University of Zagreb. Her main research interests include optimization and planning of communication networks, particularly in wide-area optical networks. She has co-authored over 50 papers in international conferences and journals, has served on several conference committees, such as IEEE GLOBECOM and IEEE ICC, and served on the Editorial Board of the *CIT Journal of Computing and Information Technology* from 2011 to 2015.

Marija Furdek received her Dipl.-Ing. and Ph.D. degrees in telecommunications from the Faculty of Electrical Engineering and Computing, University of Zagreb, in 2008 and 2012, respectively. Since 2013, she has been with the Optical Networks Lab (ONLab) at KTH Royal Institute of Technology, Stockholm, Sweden. She was also a visiting researcher at the Massachusetts Institute of Technology and Athens Information Technology, Greece. Her research interests include planning of optical networks and optical node architecture, physical-layer security, network survivability, reliability analysis, and optimization techniques. She has co-authored more than 40 publications in international journals and conferences. She is currently serving as a General Co-Chair of the Photonic Networks and Devices Conference, a part of the OSA Advanced Photonics Congress, and a Guest Editor of the *IEEE/OSA Journal of Optical Communications and Networking* Special Issue featuring selected papers from the conference.

Szilard Zsigmond is the principal product line manager of photonic line systems, amplifiers, and node configurations at Nokia. He is also the product line manager of Terrestrial-Subsea integration. He has extensive knowledge of optical communication systems and expertise of fiber optics communication. Prior to Nokia, he was a researcher and lecturer at Budapest University of Technology and Economics. He was also a visiting researcher at the-National Institute of Information and Communications Technology, Japan. In 2010, he joined Alcatel-Lucent, where he was responsible for transport solutions and business development in the central and northeast region of Europe. In 2012, he became the solution architect of the Asia-Pacific region and later the head of Asia-Pacific regional product line management. In 2014, he joined the core Product Line Management team as the principal product line manager of photonic line systems. He holds a Ph.D. degree from Budapest University of Technology and Economics. He has delivered a number of talks at various conferences and has published more than 40 scientific papers.

Lena Wosinska received her Ph.D. degree in photonics and Docent degree in optical networking from KTH Royal Institute of Technology, where she is currently a full professor in telecommunication at the School of Information and Communication Technology. She is the founder and leader of the Optical Networks Lab (ONLab). She has worked in several EU projects and coordinated a number of national and international research projects. Her research interests include fiber access and 5G transport networks, energy-efficient optical networks, photonics in switching, optical network control, reliability and survivability, and optical data center networks. She has been involved in many professional activities including Guest Editorship of IEEE, OSA, Elsevier, and Springer journals, serving as General Chair and Co-Chair of several IEEE, OSA, and SPIE conferences and workshops, serving on committees of many conferences, as well as being a reviewer for scientific journals and project proposals. She has been an Associate Editor of the *OSA Journal of Optical Networking* and *IEEE/OSA Journal of Optical Communications and Networking*. Currently she is serving on the Editorial Board of the *Springer Photonic Networks Communication Journal*.