M. Furdek, L. Wosinska, R. Goscien, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, J.L. Marzo
"An overview of security challenges in communication networks"
In Proc. RNDM 2016 - 8th International Workshop on Resilient Networks Design and Modeling, Sept. 13-15, 2016, Halmstad, SE, pp. 43-50
ISBN: 978-1-4673-9023-1 http://dx.doi.org/10.1109/RNDM.2016.7608266 http://ieeexplore.ieee.org/document/7608266/

An overview of security challenges in communication networks

Marija Furdek[1], Lena Wosinska[1], Róża Goścień[2], Konstantinos Manousakis[3], Michał Aibin[2], Krzysztof Walkowiak[2], Sashko Ristov[4,5], Marjan Gushev[4], José L. Marzo[6]

[1] ICT School, KTH Royal Institute of Technology, Stockholm, Sweden
[2] Wroclaw University of Science and Technology, Wroclaw, Poland
[3] KIOS Research Center, University of Cyprus, Nicosia, Cyprus
[4] Ss. Cyril and Methodius University in Skopje, Skopje, Macedonia
[5] University of Innsbruck, Innsbruck, Austria
[6] University of Girona, Girona, Spain

E-mail: *marifur@kth.se, wosinska@kth.se, roza.goscien@pwr.edu.pl, manouso@ucy.ac.cy, michal.aibin@pwr.edu.pl, krzystof.walkowiak@pwr.edu.pl, sashko.ristov@finki.ukim.mk, marjan.gushev@finki.ukim.mk, joseluis.marzo@udg.edu*

***Abstract*—The ongoing transition towards a networked society requires reliable and secure network infrastructure and services. As networks evolve from simple point to point systems towards complex, software-defined, ultra-high capacity and reach, and distributed cloud environments, new security challenges emerge. The EU-funded RECODIS project aims at coordinating and fostering research collaboration in Europe on disaster resiliency in communication networks. One of the disaster types, considered by RECODIS Working Group (WG) 4, are deliberate human-made attacks aimed at gaining unauthorized access to the network or disrupting the service. In order to develop methods for increasing network security in the presence of attacks, it is crucial to first identify the security vulnerabilities and attack methods that exploit them, as well as the capabilities and shortcomings of existing security schemes. To this end, the members of RECODIS WG4 performed a comprehensive overview of attack methods and security approaches from the literature. This overview covers the security vulnerabilities inherent to the underlying physical layer, the implications of software-defined networking to security, and security challenges in cloud networks spanning geographically distributed data centers.**

Keywords—security; attacks; protection; DDoS; optical network; SDN; cloud network.

I. INTRODUCTION

Communication networks, as the key enabler of the information society, are a desirable target for malicious attackers. Network breaches occur on all network layers and are growing in frequency, magnitude and sophistication. For example, the number of DDoS attacks grew by 85% over the previous year and the attacks reached an average peak size of 6.9 Gbit/s [1]. At the same time, the network capacity and reach grow, causing any kind of breach or failure to affect larger amount of data and, consequently, cause greater losses.

The effects of malicious attacks are typically divided into three classical aspects – confidentiality, integrity and availability. Confidentiality refers to the communication being accessed only by authorized parties. Integrity implies the wholeness and trustworthiness of received data, without accidental or intentional modifications. Availability denotes accessibility and usability of service, data and network elements upon an authorized request.

Communication networks are undergoing a transformation from simple point to point, static systems that are configured and managed as silos, towards sophisticated programmable systems with a flexible network fabric and cognitive control plane. The physical layer of the network is evolving towards ultra/high capacity long reach optical transmission with elastic spectrum division deploying multiple modulation formats supported by sliceable bandwidth variable transponders. The control plane becomes decoupled from the data plane and centralized, as Software Defined Networking (SDN) allows for opening up the network devices via programmable interfaces.

Connectivity and traffic patterns also change as the network transitions towards distributed cloud scenarios. In cloud applications, enterprises migrate their computing and storage resources to distributed datacenters and are interested in connectivity to resources under a stringent set of performance requirements, rather than connectivity to particular sites. Thus, the unicast communication between a source of a request and a specific, known destination that hosts the desired content changes into anycast communication where any one of the datacenters that host the content can be selected as the destination node of a particular request. Moreover, the virtualized services can be migrated among different physical machines located within the same or at different datacenters, giving rise to changing traffic patterns.

A plethora of malicious attack methods can be designed to target different layers of the network. Several attacks target the physical layer, exploiting the security vulnerabilities of key optical devices in order to disrupt service or analyze traffic. The centralized controller of SDN also represents a desirable target for attackers as gaining control over it would enable controlling a wide portion of the network. In cloud scenarios, new security vulnerabilities emerge due to multitenancy and service migration. Some of the attack methods have similar characteristics to failure components and can be mitigated using existing approaches, particularly approaches that consider large-scale network disasters that are in the focus of RECODIS. However, attacks

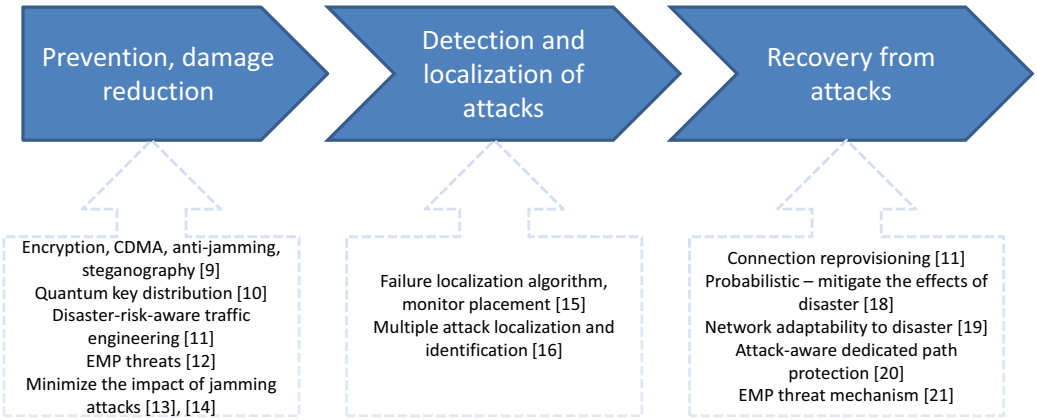

Figure 1. Physical-layer security management framework.

differ from natural disasters because they typically do not have geographical correlation, and can be designed to appear sporadically and concurrently from multiple sources, while the attackers are typically interested in avoiding detection and maximizing the damage.

In this paper, the members of RECODIS WG4 aim at providing an overview of security issues characteristic to the different layers of today's optical network. Section II focuses on the vulnerabilities of the optical layer. Section III analyzes security issues in SDN, while Section IV considers implications to network security characteristic to cloud networking. Each section presents the attack methods and attack management strategies from the literature.

II. Optical Layer Security

The high data rates employed in optical networks make them very sensitive to communication failures since large amounts of data can be affected even with failures of very short duration [3]. Optical network infrastructure is a crucial enabler of communication between cities, countries, and continents.

A. Types of Threats

Generally, large scale network failures can be classified as natural disasters (unintended components faults) and man-made attacks. The former type results or follows in the wake of a natural disaster such as earthquakes or floods. On the other hand, man-made attacks are a repercussion of malicious human activities aimed at service disruption, which prevents communication or degrades quality of service, and/or information tapping, which compromises privacy by providing unauthorized users access to data which may be used for eavesdropping or traffic analysis [1], [19].

One of the most dangerous man-made threats that can disable the network infrastructure is electromagnetic pulse (EMP) attack which is defined as a burst of electromagnetic radiation [4], [5], [6]. The burst can cause high electric currents in electronic components and render them unusable. Typically, EMP results from certain types of high-energy explosions, especially a nuclear explosion, or from a suddenly fluctuating magnetic field [6]. The EMP that follows from an explosion is especially dangerous since the corresponding explosion can not only destroy network physical elements, but directly threaten people's life and health as well. Additionally, the resulting rapidly changing electric fields and magnetic fields may couple with electrical/electronic systems to produce damaging current and voltage surges. Each EMP is characterized by a rise time and its electrical field strength. Both characteristics allow to assess the threat level of an EMP to a specific system (e.g., network) [5].

Aside from the EMP targeted at disabling electronic components in the network, several attack methods can be designed to affect the optical layer [1], [3], [19]. These attacks can exploit vulnerabilities of key optical building blocks: fibers, amplifiers and cross-connects [3]. Attacks targeting optical fiber include fiber cuts and bends. A fiber cut breaks a corresponding link, causing an interruption in data transfer, similarly to a component fault. A fiber bend causes excessive light radiation at the border of the fiber core and cladding by breaking the conditions of total internal reflection. Such leakage of light degrades the quality of signal and can also be used to tap communication, delivering the carried information straight into the hands of the attacker [1], [3].

Another important group of attacks targeting optical fibers and amplifiers is jamming by injection of harmful signals onto a fiber link. The jamming signal interferes with the co-propagating useful signals, possibly leading to service degradation or modifications of transferred data [1], [3], [19]. In optical fibers, jamming signals cause non-linear effects, leading to out-of-band crosstalk. In erbium doped fiber amplifiers (EDFA), where a pool of excited photons is distributed among the incoming signals proportionally to their power levels, high-power jamming signals can cause gain competition, depriving the weaker useful signals of gain. In optical cross-connects, high-power jamming signals can increase level of in-band crosstalk and cause unfilterable noise addition to useful signals at the same wavelength as the jamming signal.

B. Methods of risk assessment

In order to design and implement efficient protection/restoration mechanisms against repercussions of large scale disasters or attacks, it is crucial to estimate the risk of a particular threat and its potential influence on an optical network. As network attacks are extremely difficult to predict, and their consequences hard to evaluate, risk assessment relies on

developing convincing models of attacks and evaluating network vulnerability under a set of assumptions.

An approach for risk assessment on random (non-deterministic) network topologies can be found in [7], where disasters or attacks are modeled as cuts. Each cut incorporates a subset of fiber links that are broken due to the disaster. The main paper goal is to find a disaster (attack) location (or set of locations) which has the highest expected disruptive impact on the network. The impact is measured by the total capacity of failed fibers or by the total number of failed fibers. In order to find the most vulnerable location, the authors introduce a scheme to evaluate the total expected capacity of intersected (broken) links of the network under a circular disaster (attack) in a specific location. Then, they propose an approximation algorithm to evaluate the total damage of a circular disaster (attack) and find the most vulnerable network location.

The problem of identifying the network location most vulnerable to disasters and attacks under multiple simultaneous attacks is studied in [8]. The study uses a general probabilistic model for geographically correlated failures and presents efficient approximation algorithms for finding the most vulnerable network locations considering two measures: the expected number of failed components and the expected total data loss. In addition, the authors provide a set of algorithms that deal with simultaneous attacks. These approaches are then extended to networks with precomputed protection plans (e.g., dedicated path protection) and dynamic restoration capabilities.

C. *Management of attacks*

The management of attacks in optical networks comprises three main steps that take place before, during or after an attack and can, thus, be grouped together into preemption, detection and reaction approaches. An outline of these steps together with a summary of related works from the literature is shown in Fig. 1.

Preemptive approaches focus on increasing network security and robustness to attacks in the deployment phase. These approaches can focus on preventing attacks from happening by, e.g., shielding the fiber, using encryption, or applying strong authentication and authorization mechanisms. As some attacks cannot be prevented, particularly in an economically viable way, several preemptive methods are aimed at reducing the extents of damage that can be caused by an attack in case it does happen.

Detection approaches need to be activated upon occurrence of an attack, and are aimed at quickly and correctly locating the type and the source of the attack. These methods typically rely on the diagnostic information received from the monitoring devices and need to perform accurate correlation of connection statuses, reducing the influence of false alarms. In addition, the exact origin point for some of the attack methods at the optical layer may be very difficult to locate as their effect becomes more prominent on downstream links due to the compensation settings of optical amplifiers.

Once the attack is localized, the network management system needs to trigger the appropriate reaction mechanism. The source of the attack needs to be neutralized and the affected connections need to be restored. In doing so, it is important to minimize the likelihood of the backup path being affected by the same attacker that degraded the primary path. Moreover, the restoration process may be different for different classes of service and the willingness of clients to pay for sec. Preemption, detection and reaction approaches from the literature can be summarized as follows.

1) *Preventive and damage reduction approaches*

The study in [9] discusses various defenses against the security threats, including optical encryption, optical code-division multiple access (CDMA) confidentiality, self-healing survivable optical rings, anti-jamming, and optical steganography. In [9], the authors 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. Security technologies for the optical layer include secure communications using optical chaos (SCOC), optical code division multiplexing (OCDM), quantum noise randomized cipher (QNRC), and quantum key distribution (QKD). Authors also propose a novel conceptual model of a secure photonic network by introducing a QKD network to its legacy structure.

The authors in [10] developed a probabilistic model to evaluate the risk of a disaster to the network operator by analyzing the loss or penalty for a given set of possible disasters. Prevention of network disasters is addressed by a proactive disaster-risk-aware traffic engineering approach based on ILP aimed at minimizing the risk, i.e., network operator's losses in case of a disaster. For scalability reasons, a heuristic is proposed for larger network instances, based on modifying link weights according to the risk of disaster. The report [11] describes EMP threats and proposes changes to amend the Homeland Security Act of 2002 in order to secure critical infrastructure against electromagnetic threats.

A security-aware routing approach for limiting the potential propagation of high-power jamming attacks among lightpaths is proposed in [13] to address the harmful effects on links. Attack-aware wavelength assignment approaches from [14] consider the harmful effect of in-band crosstalk in switches that allows jamming attacks to spread in one or two steps. A study in [15] proposes multi-domain attach-aware routing and spectrum assignment that focuses on inter-domain connections as potential sources of jamming.

2) *Detection and localization of attacks*

A study of several types of failures and the behavior of network elements in their presence is presented in [16]. Based on this behavior, the authors define different alarming properties and propose a failure location algorithm. The alarm capabilities of optical equipment depend on the types of failures they are able to mask, causing the monitoring equipment that follows a specific channel to be unable to detect masked failures. The presented algorithm can cope with four types of failures: power, wavelength misalignment, in-band and out-band jamming. The algorithm was also extended to find the best location to place new monitoring equipment so that failures can be identified more precisely.

A Multiple Attack Localization and Identification (MALI) algorithm can be found in [17]. The MALI algorithm is distributed and relies on the Link Management Protocol. A downstream node that first notices serious performance degradation at a disturbed lightpath raises an alarm, indicating that a failure is detected on its output side. The status is compared to the input port and, if the two statuses match, the diagnostic procedure is forwarded to the next upstream node until a node with different statuses of the affected connection at the input and the output side is found and identified and the source of the attack. Thus, the localization procedure provides the Network Management System (NMS) information about locations of possible failures and attacks.

3) Recovery from attacks

Recovery from a disastrous network can take place by re-provisioning connections so as to minimize the impact of correlated cascading failures to the subset of connections affected by the original disaster [11]. Such reactive approach significantly reduces the risk and penalty, particularly when a disaster is predicted. However, as attacks and their consequences are very hard to predict, attack recovery approaches often resort to probabilistic modeling or the evaluation of worst-case scenarios.

The authors in [18] propose and evaluate an approach in probabilistic large-scale failure scenarios, which aims to increase network survivability level and mitigate the effects of disaster, i.e., connection disruption. The proposed survivability scheme allows the network control plane to receive notifications about the current impact range of disaster, estimate the probability of failure for each path, and reroute the traffic from the endangered routes to the more reliable paths prior to the failure. To this end, the method process is divided into three parts (e.g., calculation of end-to-end path failure probability, calculation of k-shortest paths failure probabilities, and pre-failure preventive rerouting) and repeated until the disaster impact is subsided.

The authors in [19] propose a survivability scheme, which improves the network performance and makes it more robust to disasters. The scheme operates in a normal network state as well as after a disaster has occurred. The proposed method aims at minimizing: *(i)* the blocking rate, *(ii)* the dropping rate, and *(iii)* the disruption rate (the rate of re-provisioning of connections) during disaster. It also aims at providing the best service possible to connections with remaining network resources by rearranging the resource allocation if needed.

In [20], the authors propose a survivability scheme considering high-power jamming attacks, i.e., attack-aware dedicated path protection (AA-DPP). The AA-DPP method aims to reduce the damaging effects of network attacks, which can be considered as large scale network disasters that can propagate. To this end, the method identifies attack groups of the working and the backup path candidates of each connection request, and searches for a common potential attacker that could simultaneously affect both the working and the backup path of each connection. The ILP and heuristic approaches of AA-DPP have the objective of minimizing the portion of such, attack-unprotected connections.

The authors in [21] present and discuss the EMP threat mechanism on electronic information system and the appropriate protection methods. EMP threats to sensitive electronic systems are presented, as well as several types of EMP threats cush as high-altitude electromagnetic pulse (HEMP), ultra-wideband (UWB) and narrow-band high power microwave (HPM). The analysis is divided into several types of systems: semiconductor elements, antennas, aperture and cable. Finally, EMP protection methods for electronic information systems are described such as screen, filter, voltage limiting, and others.

III. Security in Software-Defined Networks

The concept of Software Defined Networks (SDN) allows to decouple the control and data planes, centralize network intelligence, and abstract the underlying network infrastructure from the applications. SDN relies on deploying centralized and programmable network control and management functions thus enabling efficient orchestration of network and DC resources as well as application of various optimization techniques to control the network.

A. Challenges to security introduced by SDN

Security challenges focuses on a greatly expanded attack footprint that includes the control plane as well as the data plane [22]. SDN security needs to be built into the architecture, as well as delivered as a service to protect the availability, integrity, and privacy of all connected resources and information. For example, the SDN controllers are very attractive target for attacks. Should an adversary gain access to the network control, it could essentially hijack the network [10]. Therefore, it is crucial to define policies that will clearly indicate all possible attacks and processes/methods to prevent/defend from them. Infections in the data plane layer can in theory spread much more quickly because an SDN will be more pervasive in terms of deployment than server virtualization. It is also possible for communication difficulties and disruptions between the control plane and data plane to create vulnerable spots and open new ways for attackers to breach the network perimeter.

Network operators should use all existing facilities and services to increase the quality of security. Applications like firewalls, Intrusion Detection Systems or role-based authorization schemes (such as FortNox) will decrease the chance of being affected by malicious operations. Moreover, it is crucial to enable early malicious attack detection in SDN controller, such as checking the headers of packets to classify the traffic. These methods can provide protection from majority of threats, and provide robust and secure network operation environment.

However, although there are several tools that can be used to determine the performance, security and dependability aspects of SDN components, there is a lack of systematic and comprehensive way to measure the behavior of various SDN configurations upon internal and external changes. In order to develop a resilience benchmark, and to migrate from fault to change tolerant, it is necessary to define resilience metrics, a set of resilience changes and procedure for benchmarking. The biggest challenge is caused by network dynamics. The new control plane is changing often with new innovations, which makes it difficult to define a benchmark methodology [22].

B. *Attack methods and mitigation techniques*

Cyber attacks have become a fact of life, with data breaches of high-profile businesses and organizations making headline news practically on a daily basis. Currently, two biggest security threats in networks stem from Distributed Denial of Service (DDoS) attacks and Byzantine failures.

Byzantine failures represent the most general and the most difficult class of failures. They imply no restrictions on the failure model and encompass a wide array of failures where the failed node can either crash and stop transmission, or it can continue to generate arbitrary data, pretending to be correct, which makes fault tolerance extremely difficult. In Byzantine attacks, the adversary has full control over a number of authenticated devices and behaves arbitrarily to disrupt the network [24].

Having only one control plane in SDN structure increases the risk of Byzantine attacks on the links between controllers and the SDN switches, as well as on the controllers. Moreover, introducing more additional backup controllers cannot solve the threats of compromised controllers since they will be activated in case of primary controller's failure.

One possible solution to address this issue is to use Byzantine Fault-tolerance. In [25], the authors propose a system with a big fault-free controller, where each switch is connected to n controllers instead of communicating with only one. This will mitigate the risk of big controller's failure and the system will be resilient to up to f controller failures. Various, protocol-dependent proposals can be found for the relationship between the parameters f and n. The study indicates that even for small values of f, the number of required controllers n depends on the number of switches in the network. Therefore, in order to ensure scalability and integrity, it might be desirable to place the controllers in the cloud environment.

In a DDoS attack, the incoming traffic that floods the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address. Moreover, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

DDoS attacks become more and more sophisticated, targeting vulnerabilities of widely used protocols such as DNS and NTP. Current solutions are either highly network resource consuming or require human intervention, thus increasing the costs. A possible approach to prevent DDoS relies on exploiting network programmability enabled by SDN. The approach uses a specific implementation of the OpenFlow protocol as a means to enhance the legacy Remote Triggered Black-Hole (RTBH) routing approach, which is a mechanism for automatic propagation of rules to discard anomalous flows [26]. The key properties of this approach include dynamic RTBH configuration, matching and handling of traffic on a per-flow level, and preserving the functionality of the victim, while pushing the mitigation process upstream towards the edge of the network. The architecture proposed in [26] consists of three fully separated components: the Anomaly Detection and Identification mechanism, the RTBH trigger device, and the Anomaly Mitigation mechanism in order to prevent DDoS attacks. The architecture is shown in Fig. 2.

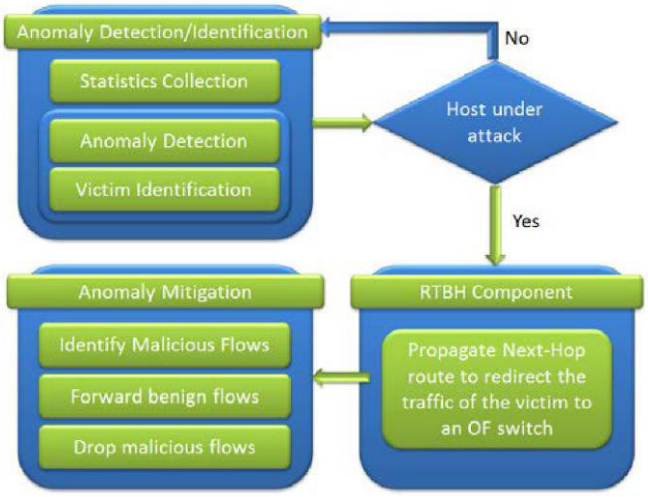

Figure 2. DDoS prevention architecture using SDN controller and RTBH component [26].

The role of the first component is to collect data, analyze it, detect anomaly and provide victim identification. If the host is under attack, the collected information is sent to the decision controller, which is the SDN controller. Once an attack is detected, the RTBH triggers device to propagate a static route for the victim's traffic, in order to mitigate the attack. Mitigation is held by Remote Triggered Black-Hole Routing Component. This approach permits traffic data that matches the destination IP address of the victim to be redirected to an OF switch and handled or inspected in a per flow manner. Redirected traffic is routed using iBGP protocol. In the last step, the Anomaly Mitigation component performs three actions. The first function includes the identification of malicious flows, based on network monitoring data exported by the OF switch. The second segregates the malicious and benign traffic flows through packet asymmetry ratio inspection, returning benign packets to their original destination. Finally, the last function is able to drop malicious traffic by instantiating appropriate flow entries to the OF switch.

Using the above-mentioned identification mechanism capable of pinpointing the victim and remotely triggering the mitigation of the offending network traffic, allows for identification of the victim of the attack and filtering the malicious sources in a short time.

IV. Cloud Networks Security

The ongoing transition from maintaining all content on proprietary, premise-confined hardware towards virtualizing services and deploying external IT resources in distributed cloud-based networks brings forth new security concerns. Cloud computing encompasses the delivery of computing and storage capacity as a service to users in three fundamental models: Infrastructure as a Service (IaaS), where users hire servers owned by a cloud provider (CP); Platform as a Service (PaaS), where users also hire the system software on the servers; and Software as a Service (Saas), where users hire the application software and databases as well [27]. In addition, SDN-based clouds enable the emergence of so-called Networking as a

Service (NaaS), where SDN technology provides control over network infrastructure while cloud computing is extended to include network centralization and virtualization [28]. Thus, cloud-based services supported by mega-scale datacenters (DCs) are becoming one of the key enablers of today's information society. These networks rely on the concept of virtualization and 'slicing' of the common physical network infrastructure to enable sharing of network and IT resources among many diverse virtual networks and connections with different service requirements.

Virtualization allows for services to be migrated among different IT resources located within the same or in distant datacenters, typically to obtain better load balancing, decrease latency by migrating the service closer to the user, or to improve fault tolerance. The relocation of services to the cloud introduces new traffic patterns and changes the perception of security perimeters, which deteriorates the effectiveness of traditional protection mechanisms.

A. *Challenges to security introduced by cloud networking and service virtualization*

The architecture and design of cloud computing bring a number of security advantages, such as security centralization, data and process segmentation, redundancy and high availability. However, new security challenges also arise in cloud scenarios, and can be related to three key aspects i.e., confidentiality, integrity and availability of data, software and hardware resources [27]. Increased number of parties, devices and applications, i.e., a higher number of access points, increase the risk of data compromise.

The security property unique to the cloud context refers to isolation that arises from multitenancy, i.e., sharing of common resources among multiple users. Although users are separated in the logical domain, they use the same hardware whose reusability must be regulated and strong isolation must be maintained among the tenants.

Another security challenge inherent to the cloud environment stems from the changes introduced in the traffic profile when virtual machines are migrated among different physical machines. These changes may either trigger false alarms by anomaly detection algorithms or they can mask actual attacks.

Integrity is another important security aspect to consider in the cloud. An entity's admittance and resource usage rights must be carefully managed in order to ensure that valuable data and services are not abused, misappropriated or stolen. A widely used assumption in network virtualization is that all the parties that share the common infrastructure are always trusted. However, in environments where there are many intelligent devices with self-adaptation and context awareness, this assumption may no longer hold, and compromised parties can exploit network virtualization to launch DDoS attacks [28].

In addition, keeping a satisfactory level of availability is crucial in order for the system to be accessible and usable upon demand by an authorized entry. Aside from maintaining network resource availability through path redundancy, the cloud providers must also make sure that the data retrieval and information processing is available [27].

B. *Attack methods and mitigation techniques*

Some attack techniques may be design so as to exploit poor isolation and multitenancy. For example, the residual representation of data that remains after it has been nominally removed, called data remanence, may be exploited by a malicious attacker who can claim large disk space and then perform sensitive data harvesting. Methods for avoiding data disclosure include limiting the point of view and support of hypervisor hardening [29].

The authors in [32] investigate the impact of virtual service migration to the anomaly detection algorithms. The study indicates that a potentially insecure number of attacks are missed, and an unusably high number of alarms under normal traffic are generated due to the changes in the traffic caused by migration. Interestingly, even when a portion of migration traffic is incorporated into the baseline scenario for anomaly detection to mark it as 'normal' traffic, the detectability of attacks does not improve. The authors identify keeping track of migrations and deducing their trails from the traffic patterns as a possible way of avoiding the generation of false alarms.

A study in [31] investigates the network performance under DDoS attacks depending on three different types of virtualization deployed in the network. In paravirtualization, no special hardware is used, but special kernels and drivers are deployed, aware that they are being virtualized. In hardware virtual machine, special hardware allows for full virtualization without the need for specialized operating system or drivers. In container virtualization, multiple secure virtual containers are created to run different applications. The first two techniques rely on using a hypervisor that communicates with the underlying hardware, while the third does not. The hypervisor improves performance isolation between guests on a hosts by acting as a gatekeeper to the underlying hardware but it can also introduce measurable overhead.

The experimental results show a rapid increase in CPU usage under DoS attack, especially for systems based on paravirtualization and hardware virtual machine. Similar performance is present for UDP, ICMP and IP traffic, indicating that high CPU usage is present whenever the hypervisor experiences a data stream that contains small packets sent at a high rate. Much of this CPU usage comes from the many extra operations that need to be performed by the hypervisor to deliver the packet to virtualized system. It is also interesting to note that the system based on container virtualization, i.e., not using the hypervisor, performs almost the same as the nonvirtualized benchmarking system, i.e., does not suffer as significant CPU degradation as the hypervisor-based systems. The memory performance degradation is also strongest in hardware virtual machine-based systems where the hypervisor is busy servicing I/O requests created by DDoS packets.

In [27], the authors propose a Trusted Third Party (TTP) framework which leverages clients from the security burden by trusting a Third Party. The Third Party then assures certain security characteristics within a distributed information system and realizes a trust mesh between involved entities, forming federations of clouds.

Such solution relies on the concept of Public Key Infrastructure (PKI) capable of providing strong authentication, authorization, data confidentiality, data integrity, and non-repudiation. Data confidentiality can be supported by implementing IPSec or SSL that enable end-to-end encryption. For server and client authentication, a key feature is to enable Single-Sign-On solution, where applications can be secured in the cloud with identities originating within the enterprise, requiring a single strong authentication process without repeating it for each service. In addition, cloud infrastructure can be organized in distinctive security domains, forming so-called federated clouds, i.e., interoperable collections of independent clouds that can exchange data and computing resources through defined interfaces.

CONCLUSION

Communication networks are vulnerable to malicious attacks at all network layers. In this paper, we collect some of the known security challenges and approaches that aim at addressing them. We first focused on security vulnerabilities and management of attacks targeting the optical layer. As all upper layer services rely on the common physical infrastructure, maintaining its secure operation is of utmost importance. We then surveyed security issues inherent to software-defined networking that enables centralized control over the whole network. Keeping the control plane and the links between SDN controller and switches secure is a key prerequisite in preventing potential hijacking of the network. Finally, we surveyed the security challenges brought by the expansion of cloud-based services that rely on multitenancy and service virtualization. As the networks play an increasingly prominent role in supporting today's society, and as attacks grow in frequency, size, and sophistication, maintaining secure network operation under changing connectivity and traffic patterns will be imperative.

ACKNOWLEDGMENT

This article is based upon work from COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures – RECODIS") supported by COST (European Cooperation in Science and Technology).

REFERENCES

[1] D. Bisson, "Report: DDoS attacks grew in number, size, and sophistication in Q4 2015," The State of Security, Mar 2016.

[2] M. Médard, D. Marquis, R. A. Barry, S. G. Finn, "Security issues in all-optical networks," IEEE Network, vol. 11, no. 3, pp. 42-48, 1997.

[3] M. Furdek and N. Skorin-Kapov, "Physical-layer attacks in all-optical WDM Networks," in Proc. MIPRO 2011, Opatija, Croatia, pp. 446-451, May 2011.

[4] Homeland Security Subcommittee on Cybersecurity, "The EMP threat: Examining the consequences," Hearing before the The Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, September 12, 2012, Serial No. 112-115.

[5] Electromagnetic Pulse Threats in 2010 by Colin R. Miller, Major, USAF Center for Strategy and Technology Air War College, Air University.

[6] V. Pereira and G. R. Kunkolienkar, "EMP (Electro-Magnetic Pulse) weapon technology along with EMP shielding & detection methodology," in Proc. of Intl. Conf. on Computing, Communications and Networking Technologies (ICCCNT), 2013, pp. 1-5.

[7] O. Gold and R. Cohen, "Coping with physical attacks on random network structures", in Proc. of IEEE ICC 2014.

[8] P. K. Agarwal, A. Efrat, S. K. Ganjugunte, D. Hay, S. Sankararaman, G. Zussman, "The resilience of WDM networks to probabilistic geographical failures", IEEE ACM T. Network., vol. 21, no. 5, 2013, pp. 1525-1538.

[9] M. Fok, Z. Wang, Y. Deng, P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE T. Information Forensics and Security, vol. 6, no. 3, pp. 725-736, Sept. 2011.

[10] K. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in photonic networks: threats and security enhancements," IEEE/OSA J. Lightwave Technol., vol. 29, no. 21, pp. 3210-3222, Nov. 2011.

[11] F. Dikbiyik, M. Tornatore, B. Mukherjee, "Minimizing the risk from disaster failures in optical backbone networks," IEEE/OSA J. Lightwave Technol., vol. 32, no. 18, pp. 3175-3183, Sept. 2014.

[12] M. McCaul, CRITICAL INFRASTRUCTURE PROTECTION ACT, AUGUST 4, 2015.—Committed to the Committee of the Whole House on the State of the Union.

[13] N. Skorin-Kapov, J. Chen, and L. Wosinska, "A new approach to optical networks security: Attack-aware routing and wavelength assignment," IEEE ACM T. Network., vol. 18, no. 3, pp. 750-760, June 2010.

[14] N. Skorin-Kapov, M. Furdek, R. Aparicio-Pardo, and P. Pavon-Mariño, "Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms", European Journal of Operational Research, vol. 222, no. 3, pp. 418-429, 2012.

[15] J. Zhu, B. Zhao, W. Liu, Z. Zhu, "Attack-aware service provisioning to enhance physical-layer security in multi-domain EONs," IEEE/OSA J. Lightwave Technol., vol. 34, no. 11, pp. 2645-2655, March 2016.

[16] C. Mas, I. Tomkos, and O. Tonguz, "Failure Location Algorithm for Transparent Optical Networks", IEEE J. Sel. Areas Commun., vol. 23, no. 8, pp. 1508–1519, 2005.

[17] 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.

[18] A. Izaddoost, S. Heydari, "Enhancing networks service survivability in large-scale failures scenario," Journal of Communications and Networking, vol. 16, no. 5, pp. 534-547, 2014.

[19] S. S. Savas, M. F. Habib, M. Tornatore, F. Dikbiyik, B. Mukherjee, "Network adaptability to disaster disruptions by exploiting degraded-service tolerance", IEEE Commun. Mag., vol. 52, no. 12, 2014, pp. 58-65

[20] M. Furdek, N. Skorin-Kapov, L. Wosinska, "Attack-aware dedicated path protection in optical networks", IEEE/OSA J. Lightwave Technol., vol. 34, no. 4, 2016, pp. 1050-1061.

[21] S. Q. Zheng, D. Y. Hou, Q. F. Liu and F. Deng, "Electromagnetic pulse threats to electronic information system and corresponding protection measures," Microwave, Antenna, Propagation, and EMC Technologies for Wireless Communications (MAPE), 2011 IEEE 4th International Symposium on, Beijing, 2011, pp. K5-K10.

[22] B. Fraser, D. Lake, C. Systems, J. Finnegan, N. Viljoen, and S. O. E. N. Etworking, "Are we ready for SDN? Implementation challenges for software-defined networks," IEEE Commun. Mag., vol. 51, no. 7, pp. 36–43, 2013.

[23] L. E. Santos, M. Curado, M. Vieira, "A research agenda for benchmarking the resilience of software defined networks," in Proc. IEEE International Symposium on Software Reliability Engineering Workshops, pp. 168-174, 2014.

[24] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, H. Rubens, "Mitigating Byzantine attacks in ad hoc wireless networks," Dept. of Computer Science, Johns Hopkins University, Technical Report, 2004.

[25] H. Li, P. Li, S. Guo and A. Nayak, "Byzantine-Resilient Secure Software-Defined Networks with Multiple Controllers in Cloud," IEEE T. Cloud Computing, vol. 2, no. 4, pp. 436-447, Oct.-Dec. 1 2014.

[26] K. Giotis, G. Androulidakis, V. Maglaris, “Leveraging SDN for efficient anomaly detection and mitigation on legacy network,” in Proc. European Workshop on Software-Defined Networking, EWSDN, 2014.

[27] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, 20 (2012), 583-592.

[28] Q. Yan, F. R. Yyu, Q. Gong, J. Li, “Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges,” IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 602-622, 1st quarter 2016.

[29] C. Kalloniatis, H. Mouratidis, M. Vassilis, S. Islam, S. Gritzalis, E. Kavakli, “Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts,” Comput. Stand. Inter., vol. 36, no. 4, pp. 759-775, June 2014.

[30] Q. Yan and F. R. Yu, “Distributed denial of service attacks in software-defined networking with cloud computing,” IEEE Commun. Mag., vol. 53, no. 4, pp. 52–59, 2015.

[31] R. Shea, J. Liu, "Performance of virtual machines under networked denial of service attacks: Experiments and analysis," IEEE Systems Journal, vol. 7, no. 2, pp- 335-345, June 2013.

[32] K. Adamova, D. Schatzmann, B. Plattner, P. Smith, “Network anomaly detection in the cloud: The challenges of virtual service migration,” in Proc. ICC 2014.