2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems

Security-Awareness in Network Virtualization: A Classified Overview

Phanvu Chau
Department of Math & Computer Science
La Salle University
Philadelphia, PA 19141
Email: chauv1@student.lasalle.edu

Yang Wang
Department of Math & Computer Science
La Salle University
Philadelphia, PA 19141
Email: wang@lasalle.edu

***Abstract*—Network virtualization is a promising solution to overcoming ossification of the current Internet. With the support of Software Defined Networking components, the Service Provider can customize the network request as a virtual network, which is agilely implemented in the physical network managed by the Infrastructure Provider. In the literature, extensive works have studied the enabling technologies of network virtualization, with a focus on the virtual network embedding (VNE) problem that allocates substrate resources to instantiate the virtual network request. Very limited work, however, has taken the security aspects of network virtualization into account. In this work, we present a comprehensive overview of the security issues in network virtualization. Under different criteria, we classify possible security attacks into various categories. For security issues that are related to the VNE process, we model and define the Security-Aware Network Embedding problem, and address it with an optimal framework. We also discuss other security issues that are independent of the VNE process.**

I. Introduction

One of the problems that is faced by the current Internet is *ossification* [1]–[8]. It refers to the network's inherent resistance to changes. The existing architecture of the Internet was proven to be difficult for Internet Service Providers (ISPs) to reach consensus on the implementation of new technological innovations. One promising solution to address this impasse is network virtualization, where the traditional ISPs are decoupled into two independent roles: the Infrastructure Provider (InP), which manages the substrate or physical networks; and the Service Provider (SP) that offers end user services by instantiating virtual networks over the resources of the former.

The SP generally expresses the demand for physical resources as a virtual network. With the support of Software Defined Networking components, the virtual network is then mapped to the substrate network via the process of Virtual Network Embedding (VNE), where virtual nodes and links are mapped as substrate nodes and path(s), respectively. This separation of virtual and physical network, as many designs in Computer Science, creates an extra layer of abstraction, and enables freedom of technologies innovations for both parties. In the literature, extensive studies have focused on the VNE problem. At the same time, however, very limited work has treated the topic of security in the context of network virtualization.

Note that security is a vital component of network virtualization, despite the difficulty and complexity in achieving security in virtualized environments. Similar to Cloud Computing, shifting the computing and/or storage functionalities towards the substrate network managed by a third party inherently poses issues of data privacy and integrity. Moreover, due to virtualization, the co-residency of virtual nodes could lead to multiple vulnerabilities that can be exploited by malicious parties. For the first time, we will present an overview of the potential attacks in network virtualization, which are classified according to multiple criteria. To overcome the possible vulnerabilities, we will discuss defense mechanisms for attacks that both can and cannot be addressed in the VNE process.

The remainder of this work is organized as follows. In section II, we review the related literature study. We classify possible security attacks in the context of network virtualization in Section III. In Section IV, we address security issues that can be incorporated into the SVNE problem. We discuss other security issues that are not considered in the SVNE problem in Section V, and conclude this work in Section VI.

II. Related Works

In the literature, extensive studies have addressed the VNE problem. Given the NP-Completeness of VNE, the approaches to solving it can be classified into three categories: *i.)* Optimal solutions based on the Integer Linear Programming (ILP) formulations (e.g., [5], [9]); *ii.)* Relaxation approaches based on the LP-relaxation of the ILP formulations (e.g., relaxation and rounding in [9]); and *iii.)* heuristic or meta-heuristic algorithms (e.g.,

978-1-4799-6036-1/14 $31.00 © 2014 IEEE
DOI 10.1109/MASS.2014.59

[10]). For a comprehensive review, one can refer to the survey paper in [1].

Security, one the other hand, has been an everlasting issue in virtualized environments since out-sourcing data computation and/or storage towards a third-party network bears inherent Confidentiality, Integrity and Availability (C.I.A) vulnerabilities. The work of [11] has comprehensively covered major possible attacks in Cloud Computing. Many of those issues similarly arise in the context of network virtualization, which will be further discussed in the next section.

Security issues in network virtualization, despite its importance, has received only limited attention, however. As pointed out in [1], the security issues in network virtualization is preferred to be integrated into the VNE process to ensure an inherent network robustness. The resulted SVNE problem has been studied in [6]–[8]. Bays et al. [6] considered security as additional constraints. To enforce security, a virtual network request can request cryptography for its virtual nodes, including: *i.) End-to-end cryptography* indicates the need for the end virtual nodes to have data encryption and decryption. *ii.) Point-to-point cryptography* requests that there be secure data transmission protocols in place for any two virtual nodes in the path a packet is traveling. Therefore, the packet will be encrypted in its entirety (i.e. both its payload and header), and decrypted when it arrives at the next node; *iii.) Non-overlapping* constraint disallows more than one virtual network to be mapped to the same set of substrate resources. Xing et al. [7] introduced the concept of Trust Value, and Security Level to virtual network embedding. A virtual link from A to B is given a trust value of a decimal from 0 to 1. The value fluctuates relative to the trustworthiness of the nodes. Liu et al. [8] adopted an economical security-aware approach by integrating functions that compute cost and revenue, which act as metrics and are used to assess the profitability of the embedding. The proposed VNE algorithm prefers virtual network requests with higher security demands and also those that enforce and request security in links and paths, as such factors generate more revenue. Along a separate line, the authors of [12] looked at a different problem: how to deduce the substrate network topology via virtual network embedding responses. According to their study, the substrate network topology can be exposed after a sufficient number of probing trials in the form of well-crafted virtual network request.

In the next section, we will integrate the literature work and present a classified overview for the security issues in network virtualization.

III. Overview Security Issues in Network Virtualization

In this section, we first discuss the network architecture of network virtualization. We then classify the security issues in network virtualization based on multiple criteria.

A. Architecture of Network Virtualization

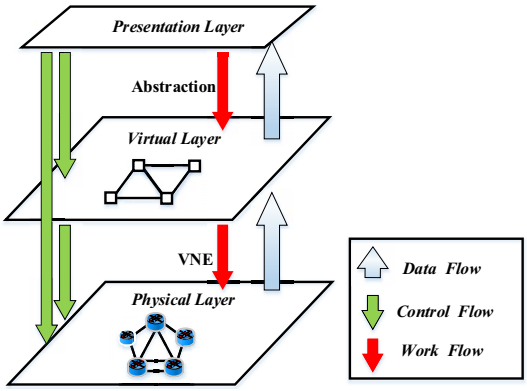

Fig. 1: Architecture

In the literature, network virtualization generally consists of a two-layer model. For the sake of security discussion, we present a three-layer model in Fig. 1 incorporating the classic virtual and physical network layers, and the extra presentation layer. The presentation layer serves the end-user with interfaces (e.g, Web, RESTful) via which the user can customize their requests. Those requests can be abstracted by the virtual layer as a virtual network, which is accommodated either by using the present network resources of the Service Provider, or by triggering further resource allocation at the substrate network via the VNE process.

B. Layer Perspective

From an architecture viewpoint, security can exist at different layers and/or the in between external channels, as summarized with representative examples in Table I. At the presentation layer, for instance, a web-based interface can be vulnerable to classic attacks such as SQL Injection, and Cross-Site Scripting. At the virtual network layer, attackers can masquerade as a service provider and probe the topology and determine the locations as well as attributes of possible victims in the substrate network. The physical network, as traditional networks or cloud networking paradigms, can be exploited by many classic attacks (e.g., Denial of Service). It is worth noting that the work flow (e.g., VNE process), control flow (e.g., remote access session), and data flow (e.g., computation results) among layers could be hijacked by attacks such as *man-in-the-middle*. In

TABLE I: Layer-centric Classification

Layer	Index	Representative Examples
Physical	1	Side-channel attacks [13], [14]
	2	Fiber optics exploitation (e.g., tapping, jamming) [15], [16]
	3	Hypervisor and shared resources vulnerabilities [11], [14]
	4	DOS attacks [17]
Virtual	5	Topology discovery [12], [13], [17]
Presentation	6	HTTP exploitation (e.g., SQL injection, Cross-Site Scripting) [11], [18]
Among Layers	7	Man-in-the-middle (e.g., impersonation, eavesdropping) [18]
	8	Availability issues (e.g., auditing, backup and migration failures) [11], [17]
	9	Assurance issues (e.g., computational integrity [19])

addition, the Infrastructure Provider may not deliver the agreed computing/bandwidth resources to the subscriber (i.e., 9 in Table I), which could be hard to verify in scenarios such as Big Data Computation. Thus a form of assurance has to be in place [19].

C. Service Perspective

We next classify the security issues in network virtualization from a service or customer viewpoint, associated with major security goals, among which we discuss the goal of *Confidentiality*, *Integrity*, *Availability* (C.I.A) and *Assurance* here. Fig. 2 illustrates the example attacks (denoted with indices from Table I) that can compromise the C.I.A goals. Note that those goals can be breached with attacks at different layers. For instance, confidentiality can be compromised with traditional HTTP exploits at the presentation layer, topology discovery at the virtual layer, as well as side-channel attacks at the physical layer. Moreover, multiple goals can possibly be violated by one type of attack. In addition, although not shown in Fig. 2, the security goal of *Assurance* (related to attack 9 in Table I), which measures whether the Infrastructure Provider or Service Provider adheres to the SLA (service level agreement) by providing claimed resources or services [19] to the Service Provider and end-users, has to be enforced in network virtualization.

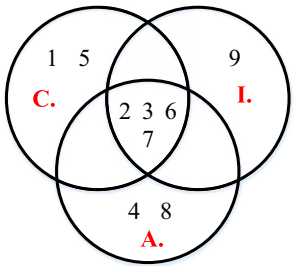

Fig. 2: Classification based on Security Goals

D. Granularity Perspective

TABLE II: Classification based on the Granularity

Granularity	Example(s) of Attack	Layer(s) Involved
Node Level	1, 3	Physical
Link Level	2	Physical
Topology Level	5	Virtual and Physical
Network Level	4	Physical

In this section, we classify the security issues from the physical or infrastructure's viewpoint depending on the granularity on the origins or targets of the attack, as summarized in Table II.

At the node level, the attackers can employ *host exploits* by taking advantage of vulnerabilities existing in the hypervisor or VM management software (i.e., attack 3 from Table I). This exploit will lead to penetration of the physical node. Since the latter has the ultimate privilege, it could in turn manipulate any other co-resident targeted VMs. Note that the attacker can exploit the target VM even without penetrating the host. This can be achieved with *cross-VM attacks* among co-resident VMs as shown in Fig. 3. The co-residency generally indicates the sharing of physical hardware, which can also serve as a common medium between the VMs. As a result, activity unique to the victim VM can be "listened to" and analyzed by the vicious VM. Side-channel attack is an example of this, where a side channel can be a shared cache or memory bus between the co-resident VMs. The vicious VM listens to such medium and observes the victim's load-based computational period, and uncover sensitive information of the target after sufficient recording.

At the link layer, the attacker can employ classic approaches to sniff the traffic from/to victim VMs (e.g., in an Ethernet-based substrate network). The recent trend of employing optical transmission technology in data center networks has also opened doors to attacks on optical fibers. For instance, in *tapping* attacks, attackers

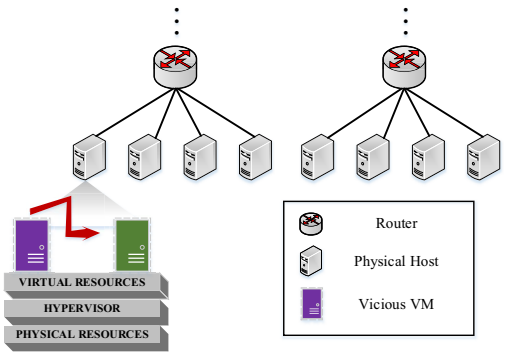

Fig. 3: Cross-VM Attacks

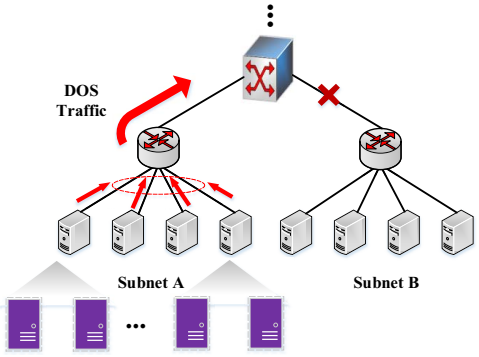

Fig. 4: DOS Attacks

can bend fibers to cause data alteration. A *jamming* attack allows the intruder to inject malicious signals, noise, or delays to the legitimate optical signals [15], [16].

The **topology level** attack can lead to topology discovery of the substrate network. In its most simplified and economic form, the attacker can probe the topology by iteratively sending requests to the InP. Each request comes with a virtual network topology with constraints on computing capacity, and bandwidth resources. After the InP responds with a binary answer–whether the request can be accommodated based on its physical resources, the attacker can decide on the topology, or proceed by issuing more inquiries to the InP. Such requests are always responded free of charge, and the attacker can figure out the topology of the InP after a certain minimal number of requests [12].

At the network scale, the attack can employ classic *DOS attacks* to overwhelm the target virtual machines. Note that one key difference in the context of network virtualization is that the source of the DOS attack is also from the same network (i.e., data center) as the target, thus it is hard to prevent with firewalls or Intrusion Detection Systems. One possible DOS attack relies on the under-provisioned nature of data centers [17]. As shown in Fig. 4, multiple vicious VMs are located on physical hosts in subnet A. When all the vicious VMs purposely transmit at the peak rate, the aggregated traffic could saturate an under-provisioned hardware or uplink, which in turn lead to a denial of service to the users of hosts in subnet B.

E. Classification based on Relation with VNE

Finally, we can classify all attacks into two categories: those that can be addressed in the VNE process, which will be further elaborated in Section V; and others that should be addressed independently of the VNE process, which will be further discussed in Section VI.

IV. Security Awareness in Virtual Network Embedding

In this section, we discuss the SVNE problem, and design a framework consisting of three phases to address it.

A. Network Model and Definition

A virtual network is modeled as an undirected weighted graph $G^V(N^V, L^V)$ in which N^V represents the set of virtual nodes, and L^V represents the set of virtual links. Each virtual node requests a certain amount of computing capacity. Each virtual link requests a certain amount of bandwidth resources. The virtual network as a whole demands a certain **security plan** to address attacks of different types, which includes per-virtual-network (i.e., data center level), per-virtual-node (i.e., physical host level), and per-virtual-link (i.e., node-pair level) security specifications. Those security plans will be further elaborated in the next subsection, which will serve as defense mechanisms to address some of above security vulnerabilities. For instance, the node-pair security specification implements the *semantic security* mechanisms, which requests the incident nodes of a virtual link to possess encryption and decryption capabilities in order to render data non-readable in case of privacy and information compromise.

Similarly, the substrate network is defined as an undirected weighted graph $G^S(N^S, L^S)$, in which N^S represents the set of substrate nodes, and L^S represents the set of substrate links. Each substrate node has **four** attributes: the available computing capacity, the encryption/decryption capability, the associated data center, and a list of currently hosted virtual nodes. Each substrate link has a certain amount of available bandwidth resources.

Finally, the Security-Aware Virtual Network Embedding (SVNE) problem can be defined as a decision problem that satisfies the *node mapping* and *link mapping* requirements [9] as well as the *security plan* constraint.

Level	Plan	Embedding Policy
Data Center (DC)	High	No DC sharing
	Medium	DC sharing only with *trusted* nodes
	None	DC sharing with *any* nodes
Physical Host (PH)	High	No PH co-residency
	Medium	PH co-residency only with *trusted* nodes
	None	PH co-residency with *any* nodes
Node-Pair	E2E Encryption	End physical hosts perform encryption/decryption
	P2P Encryption	End *and* intermediate physical hosts perform encryption/decryption
	None	No semantic security mechanisms

TABLE III: Security plans per topological levels

In the next three subsections, we employ three components/phases to address the SVNE problem including the security plan customization, admission process, and a mathematical model.

B. Security Plans Customization

In this phase, security level is customized by specifying the security plans that are summarized in Table III at the data center, the physical host, and the node-pair level. Each level provides three plans–two with security measures and one without. Note that the security plans and levels are designed to minimize the risks of attacks discussed in the last section. For example, a "Data Center" level with a high security plan seeks to host virtual nodes across "secure" data centers to reduce the probability of DOS attacks (as well as node level attacks). A "Physical Host" level accompanied by a "high" security plan does not allow virtual nodes from one virtual network to share the same physical host with existing virtual nodes. When this mapping is in place, the occurrence of node level attacks can be reduced. Similarly, on the node-pair level, End-to-End Encryption (E2E) and Point-to-Point Encryption (P2P) promise to mitigate the effects of eavesdropping and/or packet sniffing.

C. VNE Admission Process

The purpose of this phase is to filter the node assignment choices according to the capacity and security requirements.

1) In the first step, for each virtual node, we find a group of substrate nodes that satisfies the computing capacity.

2) According to the data center/node level/node-pair security plans, remove the candidate nodes that are incompatible with the data center/node level/node-pair security plans. Note that if a virtual node has any incident link with semantic security requirement, the candidate node(s) must have such capability.

3) For each virtual node, connect it to each of its resulted substrate node with an auxiliary edge, and generate the auxiliary graph.

D. Mathematical Model for SVNE

With the constructed auxiliary graph (G), we can model the SVNE problem using Integer Linear Programming models. In the following, we present a link-based model adapted from [9].

$\gamma_{(i,j)}$	the unit cost of bandwidth at substrate edge *(i, j)*;
cn_s:	the unit cost of computing resources at substrate node s;
$\beta c_{(i,j)}$	the bandwidth capacity of substrate edge *(i, j)*;
$\alpha_{i,j}^{I,J}$	the size of the flow for commodity *(I, J)* over physical edge *(i, j)*, $\alpha_{i,j}^{I,J} \geq 0$;
$E_{V,s}$	1 if virtual node *V* is embedded to substrate node *s*; 0 otherwise;
$P_{I,J}$	1 if virtual edge I-J needs P2P encryption, 0 otherwise;
X_i	1 if substrate node i supports encryption/decrption; 0 otherwise;
B	A large number;
AE	the set of auxiliary edges.

Eq. (1) states the goal, which seeks to minimize the overall cost. Eq. (2) and (3) implement the node assignment. Eq. (4) ensures that the aggregated flow does not exceed the capacity of physical edge *(i, j)*.

$$Min \sum_{(i,j)\in L^S} \sum_{(I,J)\in L^V} \alpha_{i,j}^{I,J} * \gamma_{(i,j)} + \sum_{s\in N^S} \sum_{V\in N^V} cn_s * E_{V,s} \quad (1)$$

$$\sum_{s:(V,s)\in AE} E_{V,s} = 1, \forall V \in N^V \quad (2)$$

$$\sum_{V:(V,s)\in AE} E_{V,s} \leq 1, \forall s \in N^S \quad (3)$$

$$\sum_{(I,J)\in L^V} \alpha_{i,j}^{I,J} \leq \beta c_{(i,j)} \forall (i,j) \in L^S \quad (4)$$

We omit the flow conservation constraints at the source and destination. For intermediate nodes, we have Eq. (5) and (6) to ensure flow conservation. Note that when P2P encryption plan is selected, we need to prevent the flow of a virtual edge, say (I,J) to pass substrate nodes that do not have encryption capability. This is achieved with Eq. (6). Eq. (7) ensures that flow is carried only on mapped auxiliary edges.

$$\sum_{i;(i,j)\in G} \alpha_{i,j}^{I,J} = \sum_{k;(j,k)\in G} \alpha_{j,k}^{I,J} \forall j \in N^S, (I,J) \in L^V, X_j = 1 || P_{I,J} = 0 \tag{5}$$

$$= 1$$

$$\sum_{i;(i,j)\in G} \alpha_{i,j}^{I,J} = \sum_{k;(j,k)\in G} \alpha_{j,k}^{I,J} = 0 \forall j \in N^S, (I,J) \in L^V, X_j = 0 \&\& P_{I,J} \tag{6}$$

$$\sum_{J:(I,J)\in L^V} \alpha_{I,j}^{I,J} \leq E_{I,j} * B \forall (I,j) \in AE \tag{7}$$

V. Addressing Other Security Issues in Network Virtualization

The overall security of network virtualization also relies on components that are independent of the VNE process. We briefly discuss some of those security aspects and defense strategies below.

First, the SP should prevent possible exploitations that can occur at the presentation layer (e.g., End-user web interface) as well as the communication channel between the end user and the SP.

Second, the physical security of the substrate resources should be the sole responsibilities of the InP (e.g., when attackers obtain access to the physical fiber link, they can achieve the *tapping* and *jamming* attack as discussed earlier [15]).

Third, the hosting vantage of the InP could lead to data privacy and integrity issues [11], which necessitates assurance processes that may be audited by the third party.

Finally, the InP holds the main responsibility to ensure the security of the operating system (if not bare metal deployment), hypervisor, network security of the data center as well as the interface (e.g., HTTP, remote control sessions) to other parties. Their efforts should include, for instance, hardening the host via firewall, and Intrusion Detection Systems to prevent attacks such as *Host Exploit*.

VI. Conclusion

In this paper, we have presented a classified overview of the security issues in network virtualization. We have also designed defense mechanisms, which are embedded in the Security-Aware Virtual Network Embedding (SVNE) problem, to address these attacks. In addition, we have presented a security framework that employs three major processes that can optimally address the SVNE problem. In the future, we plan to evaluate the performance of the proposed framework, and develop alternative models for comparison.

References

[1] A. Fischer, J. F. Botero, M. T. Beck, H. de Meer, and X. Hesselbach, "Virtual network embedding: A survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 1888–1903, Fourth Quarter 2013.

[2] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the internet impasse through virtualization," *Computer*, vol. 38, no. 4, pp. 34–41, April 2005.

[3] Y. Wang, Q. Hu, and X. Cao, "Connectivity as a service: Towards optical-based network virtualization," in *International Conference on Computing, Networking and Communciations'14*, pp. 264–268.

[4] N. Feamster, L. Gao, and J. Rexford, "How to lease the internet in your spare time," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 1, pp. 61–64, January 2007.

[5] Q. Hu, Y. Wang, and X. Cao, "Resolve the virtual network embedding problem: A column generation approach," in *INFOCOM, 2013 Proceedings IEEE*, pp. 410–414.

[6] L. R. Bays, R. R. Oliveira, L. S. Buriol, M. P. Barcellos, and L. P. Gaspary, "Security-aware optimal resource allocation for virtual network embedding," in *2012 Proceedings of the 8th International Conference on Network and Service Management*, pp. 378–384.

[7] C. Xing, J. Lan, and Y. Hu, "Virtual network with security guarantee embedding algorithms," *Journal of Computers*, vol. 8, no. 11, pp. 2782–2787, November 2013.

[8] S. Liu, Z. Cai, H. Xu, and M. Xu, "Security-aware virtual network embedding," in *2014 IEEE International Conference on Communications*.

[9] N. K. Chowdhury, M. R. Rahman, and R. Boutaba, "Virtual network embedding with coordinated node and link mapping," in *Proceedings of IEEE INFOCOM'09*, April 2009, pp. 783–791.

[10] J. Lischka and H. Karl, "A virtual network mapping algorithm based on subgraph isomorphism detection," in *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, 2009, pp. 81–88.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *ACM workshop on Cloud computing security'09*, pp. 85–90.

[12] Y.-A. Pignolet, S. Schmid, and G. Tredan, "Adversarial vnet embeddings: A threat for isps?" in *INFOCOM, 2013 Proceedings IEEE*, pp. 415–419.

[13] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud! Exploring information leakage in third-party compute clouds," in *Proceedings of CCS 2009*, S. Jha and A. Keromytis, Eds. ACM Press, Nov. 2009, pp. 199–212.

[14] A. Fischer and H. D. Meer, "Position paper: Secure virtual network embedding," *Praxis der Informationsverarbeitung und Kommunikation*, vol. 34, no. 4, pp. 190–193, 2011.

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

[16] M. Furdek, "Physical-layer attacks in optical wdm networks and attack-aware network planning."

[17] H. Liu, "A new form of dos attack in a cloud and its avoidance mechanism," in *2010 Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 65–76.

[18] E. L. Haletky, *VMware vSphere and Virtual Infrastructure Security: Securing the Virtual Environment*. Boston, MA: Pearson Education, Inc., 2009.

[19] R. Liu, P. Mordohai, W. H. Wang, and H. Xiong, "Integrity verification of k-means clustering outsourced to infrastructure as a service (iaas) providers," in *SIAM International Conference on Data Mining'13*, pp. 632–640.