Multilayer Network Monitoring and Data Analytics over Encrypted Telemetry Data

(*Invited Paper*)

Xiaoqin Pan[†‡], Shaofei Tang[†], and Zuqing Zhu[†]

[†]School of Information Science and Technology, University of Science and Technology of China, Hefei, China

[‡]Engineering Technology Center, Southwest University of Science and Technology, Mianyang, China

[†]Email: {zqzhu}@ieee.org

***Abstract*—Multilayer in-band network telemetry (ML-INT) and data analytics (DA) is the key techniques for monitoring and troubleshooting backbone networks, since they obtain real-time and fine-grained telemetry data about the optical and IP layers and facilitate artificial intelligence (AI) assisted network automation. Despite their success, there are still privacy and security issues to address for realizing a practical ML-INT&DA system. This is because a malicious party can obtain plaintext telemetry data illegally by tapping the data reporting channels between the control and data planes, derive sensitive information about the network, and launch various attacks accordingly. In this paper, we propose to realize multilayer network monitoring and data analytics over encrypted telemetry data and demonstrate a privacy-preserving ML-INT&DA system to address the aforementioned issues. More specifically, we first utilize the vector homomorphic encryption (VHE) to encrypt ML-INT data, *i.e.*, the threats from data tapping can removed, and then architect a deep learning (DL) model for anomaly detection, which can directly operate on the encrypted data. We implement and experimentally demonstrate the feasibility of the proposed system in a real IP over elastic optical network (IP-over-EON) testbed, and the results confirm the effectiveness of our proposal.**

***Index Terms*—In-band network telemetry (INT), Deep learning (DL), Vector homomorphic encryption (VHE).**

I. Introduction

Nowadays, the infrastructure of multilayer backbone networks (namely, IP-over-Optical) is experiencing dramatic changes, which are driven by the raising of emerging network services (*e.g.*, Big Data and cloud computing) [1, 2], and the fast deployment of virtualization technologies, such as network function virtualization (NFV) [3–5] and virtual network embedding (VNE) [6–8]. These changes have made the network control and management (NC&M) in backbone networks increasingly complicated [9, 10], and thus detecting and locating network exceptions accurately and timely has become more and more challenging [11, 12]. The difficulties motivated people to consider the artificial intelligence (AI) assisted network automation [10, 13], which can make intelligent and timely decisions to satisfy the quality-of-service (QoS) of various network services and to detect and resolve network exceptions to maintain the QoS levels. However, the AI-assisted network automation can never be realized without an agile and powerful network monitoring and troubleshooting scheme that can promote real-time and fine-grained NC&M.

The new challenges on network monitoring can be addressed by leveraging the in-band network telemetry (INT) [14]. Specifically, INT relies on programmable data plane (PDP) [15–17] to realize customized packet processing pipelines for capturing ephemeral changes in networks quickly, and provides network operators the flexibility to design their own network monitoring schemes. The research and development on INT techniques have gained intensive attentions in recent years. To reduce the overheads on bandwidth and packet processing, Tang *et al.* [18] developed a selective INT scheme (Sel-INT) to realize selective insertion of telemetry data in packets. A programmable INT event pre-filtering mechanism has been proposed in [19] to improve the accuracy and efficiency of network monitoring. The authors of [20, 21] have expanded INT to handle the multilayer INT (ML-INT) in backbone networks, and the obtained ML-INT techniques can visualize both the IP and optical layers in real-time.

The advances on INT have boosted the research and development on AI-assisted network automation. Following the idea of knowledge-defined networking (KDN) [22–24], the authors of [13] proposed an architecture for self-driving network with the help of AI and INT. Meanwhile, several ML-INT and data analytics (DA) schemes have been designed in [10, 20, 21] to achieve real-time and fine-grained NC&M. Specifically, ML-INT allows the network operator to collect the statistics of each traffic flow in real-time, while the DA analyzes the statistics to realize end-to-end flow monitoring. Although the integration of ML-INT with DA has been proven to be effective in backbone network monitoring, the important issues about privacy and security should also be addressed [25, 26].

There are two reasons for realizing a privacy-preserving ML-INT&DA system. Firstly, it is known that in a software-defined networking (SDN) environment, the control channels between the control and data planes for reporting/collecting ML-INT data are vulnerable to various attack scenarios [26]. Therefore, if a malicious party eavesdrops these channels, it can analyze the stolen ML-INT data to derive sensitive information about the configuration and operation of the backbone network, and cause serious security breaches [27]. Secondly, the training/testing data sets for the deep learning (DL) models in DA should be privacy-preserving. Hence, when the necessary labor/hardware/software resources to design and train the DL models are not available, the operators can outsource the training/verification process of the DL models to a third party by leveraging “machine-learning-as-a-service (MLaaS)” [28].

In this invited paper, we discuss our research progress on

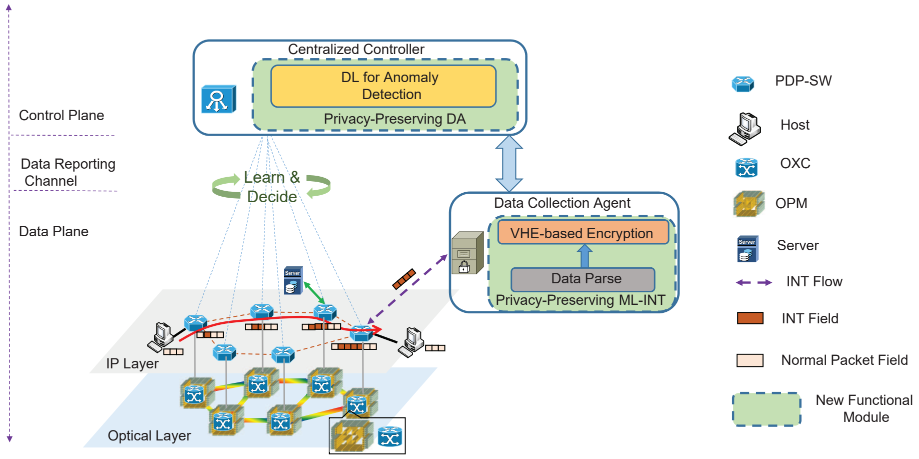


Fig. 1. Privacy-preserving ML-INT&DA system, PDP-SW: PDP switch, OXC: optical cross-connect, OPM: optical performance monitor (adapted from [26]).

the privacy-preserving ML-INT&DA system that can realize multilayer network monitoring over encrypted ML-INT data in IP-over-Optical networks. We first leverage the vector homomorphic encryption (VHE) scheme [29, 30] to encrypt the plaintext ML-INT data in the data plane. Then, we architect a DL model in the control plane to directly analyze the ciphertext ML-INT data for anomaly detection. The privacy-preserving ML-INT&DA system is implemented in an IP over elastic optical network (IP-over-EON) testbed, for experimental demonstrations. Experimental results confirm that the VHE-based encryption hides sensitive information about the data plane well, and our DL-based DA can find the root-causes of exceptions accurately by classifying encrypted ML-INT data.

The rest of the paper is organized as follows. Section II elaborates on the architecture and operation principle of our ML-INT&DA system. We describe the implementation details in Section III. The experimental demonstrations are discussed in Section IV. Finally, Section V summarizes the paper.

II. System Design and Operation Principle

Fig. 1 shows the overall architecture of our privacy-preserving ML-INT&DA system, which is based on SDN. The data plane is an IP-over-Optical network. Here, optical cross-connects (OXCs) and fiber links build the optical layer, and the OXCs support bandwidth-variable optical switching to facilitate flexible-grid spectrum allocation [31–34]. The IP layer consists of PDP switches, application servers, client hosts, and data collection agents.

The operation principle of a generic ML-INT&DA system is as follows [10, 20]. The optical performance monitor (OPM) attaches to each OXC collects status data about the active lightpaths passing through it, which includes the power-level, spectral shape, optical-signal-to-noise ratio (OSNR), dispersion parameters, *etc.*, and sends the collected data to the PDP switch that is locally connected to the OXC. Then, the PDP switch encodes the optical telemetry data together with that about the IP layer as INT fields, and inserts them into the headers of related packets. Before such a packet reaching its destination host, the egress PDP switch pops out all the INT fields from its header, and forwards them to a data collection agent. After being parsed and aggregated, the data collection agent reports the received ML-INT data to the centralized SDN controller through control channels. Finally, the DA in the controller utilizes a DL model to analyze the received ML-INT data, and provides suggestions to the SDN controller on how to implement network adjustments to address the dynamic environment in the data plane.

Note that, the ML-INT&DA system developed in [10, 20] was not a privacy-preserving one, because plaintext ML-INT data gets reported from the data plane to the control plane. Therefore, our latest studies in [25, 26] designed and implemented a few new functional modules (*i.e.*, the VHE-based encryption and DL model for anomaly detection in Fig. 1) to avoid sending plaintext ML-INT data in the control channels. The privacy-preserving ML-INT&DA system works as follows. After receiving, parsing and aggregating ML-INT data from packets, each data collection agent organizes a set of multi-dimensional ML-INT data with its time-stamp as a plaintext vector ($\mathbf{x}$). Here, the multi-dimensional ML-INT data includes the telemetry data that records the status of each electrical/optical network element (NE) on a flow's routing path. For instance, the packet forwarding latency and input/output bandwidth of the PDP switches in the IP layer, and the power-level, OSNR, dispersion parameters, and bit-error-rate (BER) of the related lightpaths in the optical layer.

Then, the VHE-based encryption module in the the data collection agent transforms the plaintext vector $\mathbf{x}$ into a ciphertext vector $\mathbf{c}'$. For privacy-preserving, VHE-based encryption will map each unique plaintext vector $\mathbf{x}$ to dispersive ciphertext vectors in different rounds. However, the correlations buried in the ML-INT data will be kept through the VHE-based encryption, such that the DL model can directly analyze and classify the ciphertext vectors for anomaly detection [26]. According to the suggestions from the DL-based DA, the SDN controller makes suitable NC&M decisions to handle network changes and exceptions [35–39].

III. System Implementation

In this section, we present the implementation details of our privacy-preserving ML-INT&DA system, and elaborate on the

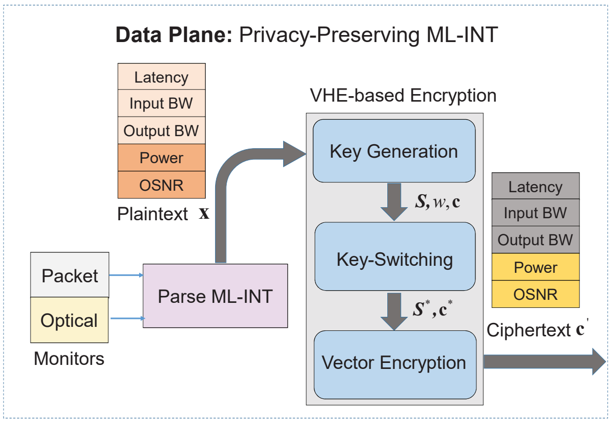


Fig. 2. Privacy-preserving ML-INT in data plane (adapted from [26]).

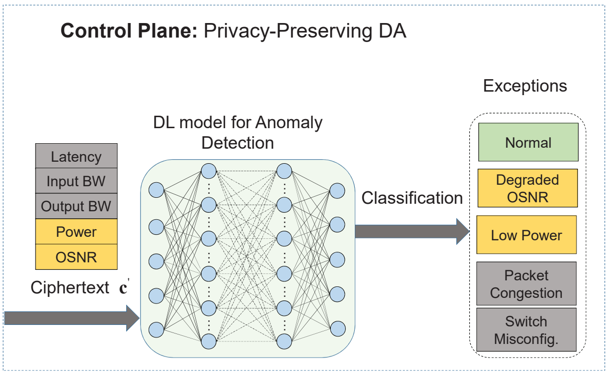


Fig. 3. Privacy-preserving DA in control plane (adapted from [26]).

VHE-based encryption and DL model for anomaly detection.

A. VHE-based Encryption

Fig. 2 explains the operation of the VHE-based encryption in the data collection agent, which includes three phases, *i.e.*, the key generation, key-switching, and vector encryption [29, 30]. We denote the plaintext vector as $\mathbf{x}$, the private key as $\mathbf{S}$, predefined weight as w, random noise as $\mathbf{e}$, and the ciphertext vector as $\mathbf{c}$. These are the parameters and variables considered in the VHE-based encryption, and they satisfy $\mathbf{S}\cdot\mathbf{c} = w\cdot\mathbf{x}+\mathbf{e}$. The key generation first uses an identity matrix $\mathbf{I}$ as the initial private key $\mathbf{S}$ and sets the initial noise vector as $\mathbf{e} = \mathbf{0}$. Hence, this leads to the initial ciphertext vector as $\mathbf{c} = w \cdot \mathbf{x}$.

Next, the key-switching changes the private key $\mathbf{S}$ to a new one $\mathbf{S}^*$ in the binary-related form, and transforms the ciphertext vector $\mathbf{c}$ into a new ciphertext $\mathbf{c}^*$ in the bipolar representation accordingly. Then, we have $\mathbf{S}\cdot\mathbf{c} = \mathbf{S}^*\cdot\mathbf{c}^*$, where both $\mathbf{S}^*$ and $\mathbf{c}^*$ are the intermediate parameter for improving the strength of the encryption. Finally, the vector encryption generates three random integer matrices, *i.e.*, $\mathbf{T}$, $\mathbf{E}$ and $\mathbf{A}$, to construct an integer matrix $\mathbf{M} = \begin{bmatrix} \mathbf{S}^* + \mathbf{E} - \mathbf{T}\cdot\mathbf{A} \\ \mathbf{A} \end{bmatrix}$, and set the final private key as $\mathbf{S}' = [\mathbf{I}, \mathbf{T}]$. Hence, the final ciphertext vector can be obtained as $\mathbf{c}' = \mathbf{M}\cdot\mathbf{c}^*$, and it will be easy to verify that we have $\mathbf{S}^*\cdot\mathbf{c}^* = \mathbf{S}'\cdot\mathbf{c}'$. Therefore, the final private key $\mathbf{S}'$ and ciphertext vector $\mathbf{c}'$ are obtained, and based on the hardness assumption of the extended learning with error (LWE) problem [40], the strength of the VHE-based encryption is guaranteed by the "public key" (*i.e.*, the integer matrix $\mathbf{M}$). To this end, we can see that it is difficult for a malicious party to illegally decrypt ciphertext ML-INT vectors with reasonable computational complexity.

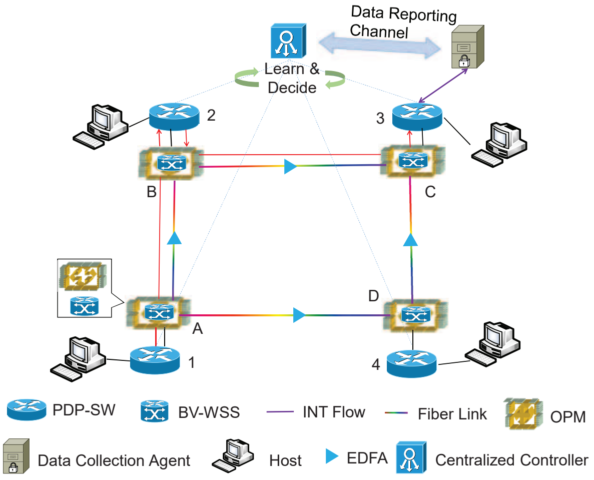


Fig. 4. Experimental setup.

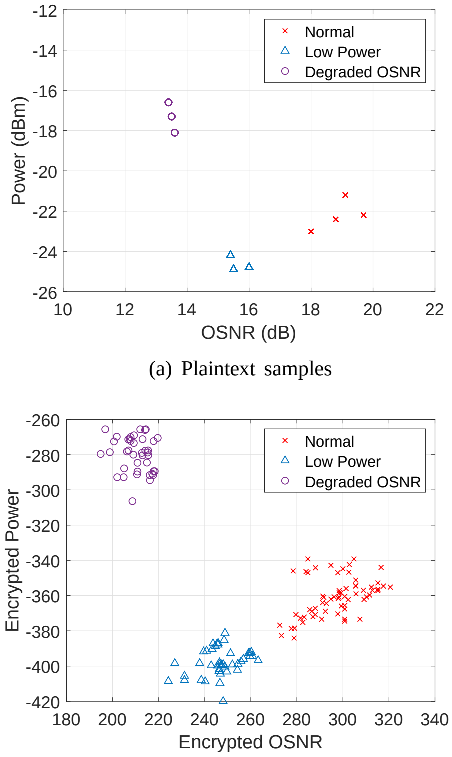
B. DL model for Anomaly Detection

Fig. 3 describes the operation of the privacy-preserving DA in the controller. The DL model for the DA is architected based on a deep neural network (DNN) to realize the anomaly detection based on classification. There are 7 layers in the DNN, where the number of neurons in the input layer is equal to the dimension of a ciphertext vector $\mathbf{c}'$, the number of neurons in the output layer is just the number of exception types plus one (*i.e.*, the normal case), and the hidden layers in between of them has 256, 128, 64, 32, and 16 neurons, respectively. The loss of the DL model is designed based on the categorical cross-entropy function, and we apply supervised learning to train the DL model until its loss is less than a preset threshold.

IV. Experimental Demonstrations

We build a real IP-over-EON testbed as shown in Fig. 4. The data plane consists of erbium-doped fiber amplifiers (EDFAs), fiber links, and four nodes, each of which includes a client host, a P4-based PDP switch [16], and an optical switch based on bandwidth-variable wavelength-selective switches (BV-WSS'). We use a commercial traffic generator/analyzer to emulate each host, which can send/receive data at 10 Gbps. The PDP switches are 3.2-Tbps Barefoot switches equipped with 10 GbE optical ports. The homemade data collection agents run on Linux servers to complete the privacy-preserving ML-INT, and together with the hosts, they build the IP layer. Each BV-WSS operates within $[1528.43, 1566.88]$ nm and provides a spectrum allocation granularity of 12.5 GHz. Hence, the BV-WSS', EDFAs, and fiber links construct an EON, which is the optical layer.

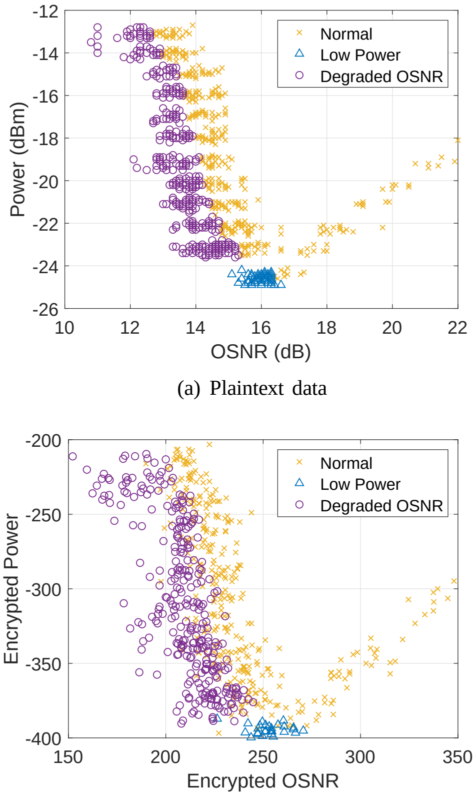
On each BV-WSS, we place OPMs to gather the input power-level and OSNR of its optical ports in realtime. Each



(a) Plaintext samples

(b) Ciphertext samples

Fig. 5. Results for applying VHE-based encryption to ML-INT samples.



(a) Plaintext data

(b) Ciphertext data

Fig. 6. Applying VHE-based encryption to a large set of ML-INT data.

PDP switch collects the packet forwarding latency and input/output bandwidth regarding each pair of its switch ports. Each data collection agent organizes the ML-INT data about data plane elements as vectors, encrypts them, and sends the results to the control plane. The centralized controller is developed based on the ONOS platform to monitor and manage both the IP and optical layers, and the DL model in privacy-preserving DA classifies the received ciphertext ML-INT vectors for anomaly detection.

With the IP-over-EON testbed, we demonstrate anomaly detection in the multilayer IP-over-EON to verify the effectiveness of our privacy-preserving ML-INT&DA system. As hard failure detection has already been studies intensively long time ago [41, 42], we focus on detecting soft failures, which only induce minor performance degradations and thus are more difficult to be detected and located. We setup a 10 Gbps packet flow from the host connecting to *PDP Switch 1* to the one on *PDP Switch 3*, as indicated by the red solid line in Fig. 4. Then, we apply various settings in the IP-over-EON to emulate different exceptions in both layers, such as different EDFA settings and noise insertions for lightpaths, various bandwidth usages and flow-table configurations in the PDP switches. The system collects a set of ML-INT data that includes $18,000$ samples, and applies VHE-based encryption to convert these plaintext samples into ciphertext vectors. Meanwhile, we label each encrypted vector to indicate the root-cause of its exception, and more specifically, we consider exception labels as “Low Power”, “Switch Misconfiguration”, “Degraded OSNR”, and “Packet Congestion”, and if there is no exception, we label the corresponding vectors as “Normal”. The encrypted vectors are partitioned into training and testing sets, which consists of 90% and 10% of them, respectively.

Fig. 5(a) plots the correlation between the plaintext power-level and OSNR of a lightpath, and after applying the VHE-based encryption to each plaintext sample in Fig. 5(a) for multiple times, we obtain the ciphertext samples in Fig. 5(b). We observe that a plaintext sample is mapped to a cluster of ciphertext ones in different encryption rounds. Hence, our scheme prevents the ciphertext ML-INT data from being decrypted illegally by a malicious party. Hence, the VHE-based encryption is capable of hiding the sensitive information about the backbone network well. In the meantime, by comparing the plaintext and ciphertext samples for a large set of ML-INT data (*i.e.*, in Figs. 6(a) and 6(b), respectively), we can see clearly that the original inner correlations between the power-level and OSNR get kept through the VHE-based encryption.

Finally, we conduct an experiment to compare the privacy-preserving ML-INT&DA with a benchmark, whose DL model operates on plaintext ML-INT samples. Specifically, we use the plaintext ML-INT data to train a DL model whose structure is the same as the one in Fig. 2. It takes 14.95 seconds to accomplish the training, while the training of the DL model in the privacy-preserving ML-INT&DA uses 14.91 seconds. This suggests that the training time of the two is almost identical. For the anomaly detection, the classification accuracy of the privacy-preserving DA is also very similar to that of the benchmark (*i.e.*, 97.91% and 98.83%, respectively).

V. Conclusion

In this paper, we discussed a privacy-preserving ML-INT&DA system with enhanced security for realizing AI-assisted network automation. The system first leveraged VHE-based encryption to encrypt plaintext ML-INT data but kept the inner correlations of them. Then, it utilized a DL model that can directly operate on the ciphertext ML-INT data for anomaly detection. We implemented the system in a real IP-over-EON testbed for experimental demonstrations, and the experimental results confirmed that sensitive information regarding the data plane can be hidden well, while the DL-based DA can find the root-causes of exceptions accurately.

Acknowledgments

This work was supported in part by the NSFC projects 61871357, 61771445 and 61701472, Zhejiang Lab Research Fund 2019LE0AB01, CAS Key Project (QYZDY-SSW-JSC003), SPR Program of CAS (XDC02070300), and Fundamental Funds for Central Universities (WK3500000006).

References

[1] P. Lu *et al.*, “Highly-efficient data migration and backup for Big Data applications in elastic optical inter-datacenter networks,” *IEEE Netw.*, vol. 29, pp. 36–42, Sept./Oct. 2015.

[2] J. Yao, P. Lu, L. Gong, and Z. Zhu, “On fast and coordinated data backup in geo-distributed optical inter-datacenter networks,” *J. Lightw. Technol.*, vol. 33, pp. 3005–3015, Jul. 2015.

[3] M. Zeng, W. Fang, and Z. Zhu, “Orchestrating tree-type VNF forwarding graphs in inter-DC elastic optical networks,” *J. Lightw. Technol.*, vol. 34, pp. 3330–3341, Jul. 2016.

[4] W. Fang *et al.*, “Joint spectrum and IT resource allocation for efficient vNF service chaining in inter-datacenter elastic optical networks,” *IEEE Commun. Lett.*, vol. 20, pp. 1539–1542, Aug. 2016.

[5] J. Liu *et al.*, “On dynamic service function chain deployment and readjustment,” *IEEE Trans. Netw. Serv. Manag.*, vol. 14, pp. 543–553, Sept. 2017.

[6] L. Gong and Z. Zhu, “Virtual optical network embedding (VONE) over elastic optical networks,” *J. Lightw. Technol.*, vol. 32, pp. 450–460, Feb. 2014.

[7] L. Gong, Y. Wen, Z. Zhu, and T. Lee, “Toward profit-seeking virtual network embedding algorithm via global resource capacity,” in *Proc. of INFOCOM 2014*, pp. 1–9, Apr. 2014.

[8] L. Gong, H. Jiang, Y. Wang, and Z. Zhu, “Novel location-constrained virtual network embedding (LC-VNE) algorithms towards integrated node and link mapping,” *IEEE/ACM Trans. Netw.*, vol. 24, pp. 3648–3661, Dec. 2016.

[9] R. Govindan *et al.*, “Evolve or die: High-availability design principles drawn from Google’s network infrastructure,” in *Proc. of ACM SIGCOMM 2016*, pp. 58–72, Aug. 2016.

[10] S. Tang, J. Kong, B. Niu, and Z. Zhu, “Programmable multilayer INT: An enabler for AI-assisted network automation,” *IEEE Commun. Mag.*, vol. 58, pp. 26–32, Jan. 2020.

[11] J. Yin *et al.*, “Experimental demonstration of building and operating QoS-aware survivable vSD-EONs with transparent resiliency,” *Opt. Express*, vol. 25, pp. 15 468–15 480, 2017.

[12] Z. Zhu *et al.*, “Build to tenants’ requirements: On-demand application-driven vSD-EON slicing,” *J. Opt. Commun. Netw.*, vol. 10, pp. A206–A215, Feb. 2018.

[13] J. Hyun, V. Nguyen, and J. Hong, “Towards knowledge-defined networking using in-band network telemetry,” in *Proc. of NOMS 2018*, pp. 1–7, Apr. 2018.

[14] C. Kim *et al.*, “In-band network telemetry (INT),” *Tech. Spec.*, Jun. 2016. [Online]. Available: https://p4.org/assets/INT-current-spec.pdf

[15] S. Li *et al.*, “Protocol oblivious forwarding (POF): Software-defined networking with enhanced programmability,” *IEEE Netw.*, vol. 31, pp. 12–20, Mar./Apr. 2017.

[16] P. Bosshart *et al.*, “P4: Programming protocol-independent packet processors,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, pp. 87–95, Jul. 2014.

[17] S. Li *et al.*, “Improving SDN scalability with protocol-oblivious source routing: A system-level study,” *IEEE Trans. Netw. Serv. Manag.*, vol. 15, pp. 275–288, Mar. 2018.

[18] S. Tang *et al.*, “Sel-INT: A runtime-programmable selective in-band network telemetry system,” *IEEE Trans. Netw. Serv. Manag.*, vol. 17, pp. 708–721, Jun. 2020.

[19] J. Vestin *et al.*, “Programmable event detection for in-band network telemetry,” *arXiv preprint arXiv:1909.12101*, 2019. [Online]. Available: https://arxiv.org/abs/1909.12101

[20] B. Niu *et al.*, “Visualize your IP-over-optical network in realtime: A P4-based flexible multilayer in-band network telemetry (ML-INT) system,” *IEEE Access*, vol. 7, pp. 82 413–82 423, 2019.

[21] M. Anand, R. Subrahmaniam, and R. Valiveti, “POINT: An intent-driven framework for integrated packet-optical in-band network telemetry,” in *Proc. of ICC 2018*, pp. 1–6, Jun. 2018.

[22] A. Mestres *et al.*, “Knowledge-defined networking,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, pp. 2–10, Jul. 2017.

[23] H. Fang *et al.*, “Predictive analytics based knowledge-defined orchestration in a hybrid optical/electrical datacenter network testbed,” *J. Lightw. Technol.*, vol. 37, pp. 4921–4934, Oct. 2019.

[24] Q. Li *et al.*, “Scalable knowledge-defined orchestration for hybrid optical/electrical datacenter networks,” *J. Opt. Commun. Netw.*, vol. 12, pp. A113–A122, Feb. 2020.

[25] X. Pan, S. Tang, , and Z. Zhu, “Privacy-preserving multilayer in-band network telemetry and data analytics,” in *Proc. of ICCC 2020*, pp. 1–6, Aug. 2020.

[26] X. Pan *et al.*, “Privacy-preserving multilayer in-band network telemetry and data analytics: For safety, please do not report plaintext data,” *J. Lightw. Technol., in Press*, 2020.

[27] J. Guo and Z. Zhu, “When deep learning meets inter-datacenter optical network management: Advantages and vulnerabilities,” *J. Lightw. Technol.*, vol. 36, pp. 4761–4773, Oct. 2018.

[28] M. Ribeiro, K. Grolinger, and M. Capretz, “MLaaS: Machine learning as a service,” in *Proc. of ICMLA 2015*, pp. 896–902, Dec. 2015.

[29] H. Zhou and G. Wornell, “Efficient homomorphic encryption on integer vectors and its applications,” in *Proc. of ITA 2014*, pp. 1–9, Feb. 2014.

[30] A. Yu, W. Lai, and J. Payor. (2015, May) Efficient integer vector homomorphic encryption. [Online]. Available: https://pdfs.semanticscholar.org/602e/5995b9366c156fe4d57fc451090181256779.pdf

[31] Z. Zhu, W. Lu, L. Zhang, and N. Ansari, “Dynamic service provisioning in elastic optical networks with hybrid single-/multi-path routing,” *J. Lightw. Technol.*, vol. 31, pp. 15–22, Jan. 2013.

[32] L. Gong *et al.*, “Efficient resource allocation for all-optical multicasting over spectrum-sliced elastic optical networks,” *J. Opt. Commun. Netw.*, vol. 5, pp. 836–847, Aug. 2013.

[33] Y. Yin *et al.*, “Spectral and spatial 2D fragmentation-aware routing and spectrum assignment algorithms in elastic optical networks,” *J. Opt. Commun. Netw.*, vol. 5, pp. A100–A106, Oct. 2013.

[34] L. Zhang and Z. Zhu, “Spectrum-efficient anycast in elastic optical inter-datacenter networks,” *Opt. Switch. Netw.*, vol. 14, pp. 250–259, Aug. 2014.

[35] X. Chen, F. Ji, and Z. Zhu, “Service availability oriented p-cycle protection design in elastic optical networks,” *J. Opt. Commun. Netw.*, vol. 6, pp. 901–910, Oct. 2014.

[36] C. Chen *et al.*, “Demonstrations of efficient online spectrum defragmentation in software-defined elastic optical networks,” *J. Lightw. Technol.*, vol. 32, pp. 4701–4711, Dec. 2014.

[37] B. Kong *et al.*, “Demonstration of application-driven network slicing and orchestration in optical/packet domains: On-demand vDC expansion for Hadoop MapReduce optimization,” *Opt. Express*, vol. 26, pp. 14 066–14 085, 2018.

[38] S. Liu *et al.*, “DL-assisted cross-layer orchestration in software-defined IP-over-EONs: From algorithm design to system prototype,” *J. Lightw. Technol.*, vol. 37, pp. 4426–4438, Sept. 2019.

[39] W. Lu *et al.*, “AI-assisted knowledge-defined network orchestration for energy-efficient data center networks,” *IEEE Commun. Mag.*, vol. 58, pp. 86–92, Jan. 2020.

[40] Z. Brakerski, C. Gentry, and S. Halevi, “Packed ciphertexts in LWE-based homomorphic encryption,” in *Proc. of PKC 2013*, pp. 1–13, Feb. 2013.

[41] D. Kilper *et al.*, “Optical performance monitoring,” *J. Lightw. Technol.*, vol. 22, pp. 294–304, Jan. 2004.

[42] Z. Zhu *et al.*, “Jitter and amplitude noise accumulations in cascaded all-optical regenerators,” *J. Lightw. Technol.*, vol. 26, pp. 1640–1652, Jun. 2008.