Privacy-Preserving Multilayer In-Band Network Telemetry and Data Analytics

(*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*—As a new paradigm for the monitoring and troubleshooting of backbone networks, the multilayer in-band network telemetry (ML-INT) with deep learning (DL) based data analytics (DA) has recently been proven to be effective on real-time visualization and fine-grained monitoring. However, the existing studies on ML-INT&DA systems have overlooked the privacy and security issues, *i.e.*, a malicious party can apply tapping in the data reporting channels between the data and control planes to illegally obtain plaintext ML-INT data in them. In this paper, we discuss a privacy-preserving DL-based ML-INT&DA system for realizing AI-assisted network automation in backbone networks in the form of IP-over-Optical. We first show a lightweight encryption scheme based on integer vector homomorphic encryption (IVHE), which is used to encrypt plaintext ML-INT data. Then, we architect a DL model for anomaly detection, which can directly analyze the ciphertext ML-INT data. Finally, we present the implementation and experimental demonstrations of the proposed system. The privacy-preserving DL-based ML-INT&DA system is realized in a real IP over elastic optical network (IP-over-EON) testbed, and the experimental results verify the feasibility and effectiveness of our proposal.**

***Index Terms*—In-band network telemetry (INT), Deep learning (DL), Integer vector homomorphic encryption (IVHE), Privacy-preserving network monitoring, Soft failures.**

I. Introduction

RECENTLY, the Internet infrastructure has been undergoing dramatic changes to adapt to ever-growing and fast-evolving network services [1, 2]. These developments have complicated the monitoring and managing of multilayer backbone networks (*i.e.*, IP-over-Optical) [3, 4]. Moreover, to improve cost-effectiveness, virtualization technologies (*e.g.*, network slicing [5–7] and network function virtualization (NFV) [8–10]) have become more and more popular in backbone networks. However, as they loose or even completely break the tie between network services and physical network elements, they make the detecting and locating of network exceptions increasingly difficult [11, 12]. Hence, people were seeking for new and more powerful network monitoring and troubleshooting techniques to address the challenges. Among recent proposals, the in-band network telemetry (INT) [13] has been considered as a promising one because it realizes real-time visualization and fine-grained monitoring, which are the weakness of traditional techniques (*e.g.*, SNMP [14]).

Specifically, INT leverages the advances on programmable data plane (PDP) [15–17] to enable a network operator to program packet processing pipelines in switches, such that ephemeral changes cross its network can be captured quickly, and the scheme of telemetry data collection can be customized flexibly for various end-to-end monitoring scenarios. Hence, INT has been treated as a key enabling technique for the network control and management (NC&M) in future Internet, and thus it has gained significant attentions from both the academia and industry recently. For instance, Barefoot Deep Insight [18] used INT to fully enable per-packet visibility into packet networks, Netcope [19] achieved INT-based linerate monitoring with 100Gbps-capable hardware, Sel-INT [20] was proposed to realize selective insertion of INT header fields for reducing the overheads on bandwidth and packet processing, and a programmable INT event pre-filtering mechanism was designed in [21] to make INT-based monitoring more precise and efficient. Furthermore, to tackle the monitoring and troubleshooting of backbone networks, researchers have expanded the applications of INT to address multilayer network architectures, *i.e.*, accomplishing multilayer telemetry (ML-INT) to observe IP and optical layers simultaneously [22, 23].

The implementation of INT will greatly enrich the telemetry data collected for network operators to make NC&M decisions, which provides opportunities for data analytics (DA) and promotes the idea of knowledge-defined networking (KDN) [24–27]. More specifically, one can integrate INT with deep learning (DL) based DA schemes to realize artificial intelligence (AI) assisted network automation [4, 28]. For example, in [4], the authors showed the big picture of realizing AI-assisted network automation by combining ML-INT with DA. Here, ML-INT provides the network operator a complete and realtime view about the electrical/optical network elements (NEs) on each traffic flow's routing path through an IP-over-Optical network, while the DL-based DA conducts comprehensive analysis on the statistics of both layers for accurate and timely monitoring and troubleshooting. Note that, even though the combination of INT/ML-INT and DL-based DA has shown a few desired advantages, none of the existing proposals on it has considered the important issues about privacy and security.

The necessity of realizing a privacy-preserving DL-based ML-INT&DA system is two-fold. Firstly, in ML-INT, the data plane aggregates and transmits plaintext telemetry data to the control plane for getting analyzed. However, the telemetry data is so rich that it can be analyzed to infer sensitive information about the configuration and operation of the back-

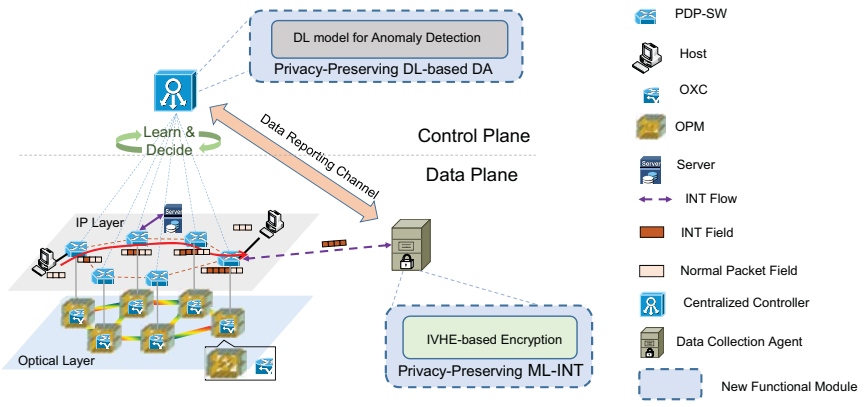


Fig. 1. Architecture of privacy-preserving DL-based ML-INT&DA system, PDP-SW: PDP switch, OXC: optical cross-connect, OPM: optical performance monitor.

bone network. Therefore, if a malicious party eavesdrops the data reporting channels, the security breach could be serious [29]. Secondly, the privacy-preserving scheme can ensure the security of both the training/testing data sets for the DL-based DA. Hence, if the operator does not have the necessary labor/hardware/software resources to design and train the DL model for DA, it can outsource the training/verification process of the DL model to a third party, by leveraging the well-known "machine-learning-as-a-service (MLaaS)" scenario [30].

In this paper, we discuss a privacy-preserving DL-based ML-INT&DA system for realizing AI-assisted network automation in backbone networks in the form of IP-over-Optical. We first show a lightweight encryption scheme based on integer vector homomorphic encryption (IVHE) [31, 32], which is used to encrypt plaintext ML-INT data. Then, we architect a DL model for anomaly detection, which can directly analyze the ciphertext ML-INT data. Finally, we present the implementation and experimental demonstrations of the proposed system. The privacy-preserving ML-INT&DA system is realized in a real IP over elastic optical network (IP-over-EON) testbed, and the experimental results verify the feasibility and effectiveness of our proposal. Specifically, the IVHE-based encryption not only hides sensitive information regarding the data plane well, but also keeps the relation buried in ML-INT data, such that the DL-based DA can classify ciphertext data to detect the root-causes of exceptions accurately.

The rest of the paper is organized as follows. We describe the architecture and operation principle of our proposed system in Section II. Then, Section III introduces the implementation details. Next, the experimental demonstrations are discussed in Section IV. Finally, Section V summarizes the paper.

II. System Design

This section describes the overall design of our privacy-preserving ML-INT&DA system, including its architecture and operation principle. Fig. 1 shows the overall architecture, and it can be seen that our design involves both the data and control planes. The data plane is a multilayer network taking the form of IP-over-Optical. Here, the optical layer is built with optical cross-connects (OXCs) and fiber links, and since we would like to facilitate flexible-grid spectrum allocation [33–36] in the optical layer, the OXCs all support bandwidth-variable optical switching. The IP layer consists of PDP switches, application servers, client hosts, and data collection agents.

The DL-based ML-INT&DA system works as follows [4, 22]. The optical performance monitor (OPM) on each OXC collects telemetry data regarding active lightpaths (*e.g.*, power levels, optical-signal-to-noise ratios (OSNRs), and central wavelengths), and sends the data to the local PDP switch that attaches to the OXC. Then, the PDP switch encodes the received telemetry data together with that about the IP layer as INT fields, and inserts them in the corresponding packets that are transmitting over the lightpaths. When a packet is about to exit the network, the egress PDP switch pops all the INT fields in it and mirrors them to a data collection agent, where all the telemetry data will be parsed, aggregated and processed to obtain the ML-INT data for end-to-end monitoring. Based on the software-defined networking (SDN) architecture, the data collection agent forwards the ML-INT data to the SDN controller through a data reporting channel. Finally, the DL-based DA analyzes the multi-dimensional ML-INT data to detect anomalies, and implements network adjustments for AI-assisted network automation. As we also want to address the privacy and security issues, we make sure that the ML-INT&DA system is a privacy-preserving one, by designing and implementing the IVHE-based encryption module and DL model for anomaly detection in Fig. 1.

The IVHE-based encryption module and DL model for anomaly detection work as follows. According to the time-stamp, the data collection agent organizes each set of received ML-INT data as a plaintext vector ($\mathbf{x}$). Specifically, a plaintext vector contains a set of ML-INT data that tells the status of both layers, such as the packet forwarding latency and port bandwidth usage of PDP switches in the IP layer, and the power level, OSNR, and central wavelength of lightpaths in the optical layer. For privacy-preserving, the IVHE-based encryption module converts $\mathbf{x}$ into a ciphertext vector $\mathbf{c}'$. Note that, each unique plaintext vector will be mapped to diverse ciphertext vectors in different rounds of encryption, to prevent unlawful decryption. In the meantime, the IVHE-based encryption is capable of preserving the inner correlations buried in the ML-INT data, such that the DL model in the

controller can operate on the ciphertext vectors directly for anomaly detection. Based on the classification results from the DL model, the centralized controller makes proper NC&M decisions to deal with the detected exceptions [37–41].

III. Implementations of System

This section presents the implementation details of our proposed privacy-preserving DL-based ML-INT&DA system, and elaborates on the two key functional modules (*i.e.*, the IVHE-based encryption and the DL model for anomaly detection).

A. IVHE-based Encryption

As explained in Fig. 2, the IVHE-based encryption includes three phases, *i.e.*, key generation, key-switching, and vector encryption [31, 32]. The key generation provides the initially private key $\mathbf{S}$, biased weight w, and random noise $\mathbf{e}$, which satisfy $\mathbf{S}\cdot\mathbf{c} = w\cdot\mathbf{x}+\mathbf{e}$. Next, in the key-switching, we get the intermediate parameter $\mathbf{S}^*$ and $\mathbf{c}^*$, where $\mathbf{S}^*$ is a new private key in a binary-related form, and $\mathbf{c}^*$ is a new ciphertext in the bipolar representation, such that $\mathbf{S}\cdot\mathbf{c} = \mathbf{S}^*\cdot\mathbf{c}^*$. Lastly, the vector encryption obtains the final private key $\mathbf{S}'$ and ciphertext $\mathbf{c}'$ according to $\mathbf{S}^*\cdot\mathbf{c}^* = \mathbf{S}'\cdot\mathbf{c}'$. The hardness assumption of the extended learning with error (LWE) problem [42] guarantees the strength of the IVHE-based encryption.

The procedure of the IVHE-based encryption used in our system is illustrated in *Algorithm* 1. *Line* 1 is for the initialization, n' denotes the predefined length of the final ciphertext vector. *Lines* 2-3 realize the key generation, set the initial private key $\mathbf{S}$ as an identity matrix $\mathbf{I}$, calculate the initial ciphertext vector $\mathbf{c}$ as $w\cdot\mathbf{x}$, and select the initial noise vector as $\mathbf{e} = \mathbf{0}$. The key-switching is achieved with *Lines* 4-5, and the vector encryption is accomplished by *Lines* 6-9, where we get the final pair of private key and ciphertext by constructing a "public key" (*i.e.*, the integer matrix $\mathbf{M}$).

Algorithm 1: IVHE-based Encryption

Input: plaintext vector $\mathbf{x}$, weight w.
Output: private key $\mathbf{S}'$, ciphertext vector $\mathbf{c}'$.
1 set the column of $\mathbf{x}$ as m, and $n' = m+1$;
2 obtain initial private key $\mathbf{S}$ as an identity matrix;
3 get initial ciphertext vector $\mathbf{c} = w\cdot\mathbf{x}$;
4 convert $\mathbf{c}$ into intermediate parameter $\mathbf{c}^*$;
5 transform $\mathbf{S}$ into intermediate parameter $\mathbf{S}^*$;
6 generate three random integer matrixs $\mathbf{T}$, $\mathbf{E}$ and $\mathbf{A}$;
7 construct an integer matrix, $\mathbf{M} = \begin{bmatrix} \mathbf{S}^* + \mathbf{E} - \mathbf{T}\cdot\mathbf{A} \\ \mathbf{A} \end{bmatrix}$;
8 get the final private key $\mathbf{S}' = [\mathbf{I}, \mathbf{T}]$;
9 calculate the final ciphertext vector $\mathbf{c}' = \mathbf{M}\cdot\mathbf{c}^*$;
10 **return**($\mathbf{c}'$, $\mathbf{S}'$);

B. DL model for Anomaly Detection

Fig. 2 also describes the operation of the privacy-preserving DL-based DA in the controller. We design the DL model for anomaly detection with a deep neural network (DNN). The DNN consists of seven layers, where the number of neurons in the input layer equals the dimension of a ciphertext ML-INT vector, there are five hidden layers with 256, 128, 64, 32, and 16 neurons, respectively, and the output layer has neurons matching to the number of exceptions plus one (*i.e.*, for the normal case). Only the output layer utilizes softmax as its activation function, while the remaining layers all use relu-based activation functions. We design the loss function to describe the DNN's accuracy by using the categorical cross-entropy function. As the DL model essentially needs to solve a classification problem, the DNN is trained in the off-line manner until the loss function reaches a preset threshold.

IV. Experimental Demonstrations

In this section, we implement the privacy-preserving DL-based ML-INT&DA system in a real network testbed, experimentally demonstrate its effectiveness, and evaluate its performance. As the techniques for hard failure detection have been mature [43, 44], our demonstrations focus on detecting soft failures, which only cause minor service degradations and thus can be more difficult to detect and locate.

A. Testbed Setup

1) Data Plane: We build a small-scale but real IP-over-EON testbed as the data plane, the EON consists of disaggregated optical line system (OLS) and bandwidth-variable wavelength-selective switches (BV-WSS'), both of which are commercial products. The disaggregated OLS utilizes bandwidth-variable transponders (BV-T) that support the PM-QPSK/16-QAM modulation formats to achieve the line-rates within $\{100, 200, 400\}$ Gbps. The OLS should also include fiber links with in-line erbium-doped fiber amplifiers (EDFAs), but due to the limited budget, we do not have enough fiber links. Hence, we take advantage of an amplified spontaneous emission (ASE) noise generator, power attenuators, and dispersion compensation modules to simulate the effects of fiber transmissions. The BV-WSS' operate within $[1528.43, 1566.88]$ nm, and enable a spectrum allocation granularity of 12.5 GHz. We implement our ML-INT scheme in the EON to collect the telemetry data regarding the power levels, OSNRs and central wavelengths of lightpaths in it.

The IP layer is built with PDP switches, data collection agents, and client hosts. The PDP switches are 3.2-Tbps Barefoot switches equipped with 10/40 GbE optical ports, which can be programmed with the P4 language [15] to realize the ML-INT operations. We emulate each host with a commercial traffic generator/analyzer. The data collection agents are in charge of collecting and encrypting ML-INT data, and they are homemade and running on Linux servers.

2) Control Plane: The control plane of our testbed is developed based on the open network operating system (ONOS) platform [45]. The controller is responsible for monitoring and managing the data plane, and also runs on a Linux server. It receives ciphertext ML-INT data from the data collection agents through TCP connection, and processes the data with a homemade DL model for anomaly detection.

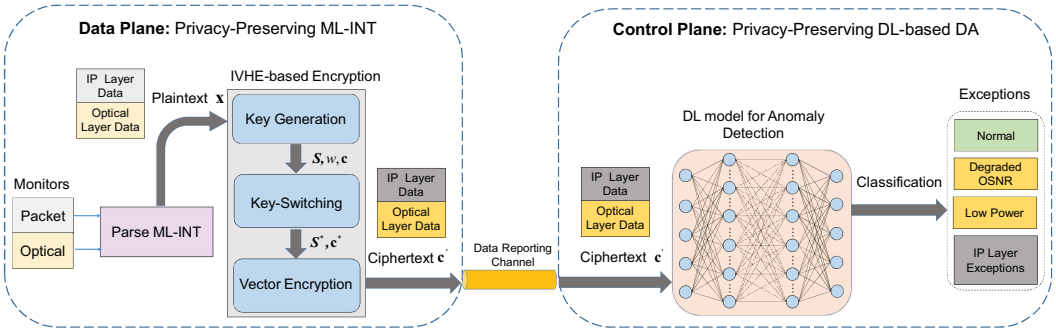


Fig. 2. Operation of privacy-preserving functional modules in DL-based ML-INT&DA system.

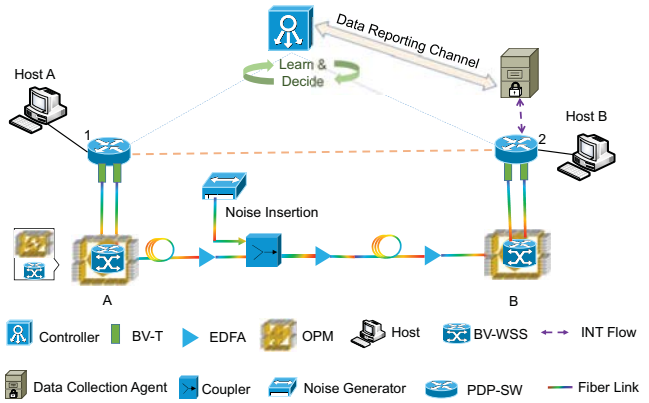
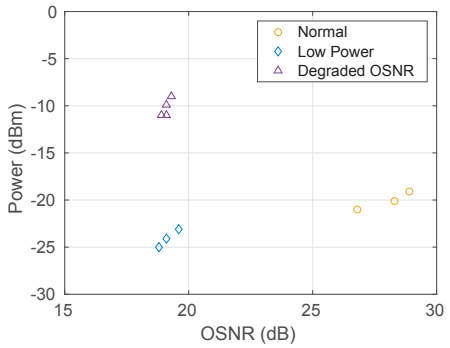
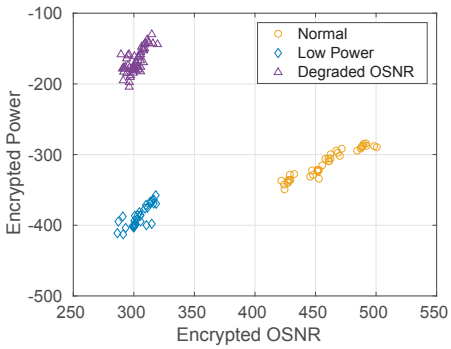


Fig. 3. Experimental setup.



(a) Plaintext samples



(b) Ciphertext samples

Fig. 4. Results for applying IVHE-based encryption to ML-INT data.

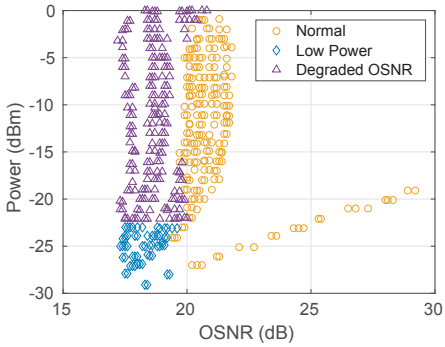
B. Experimental Scenario

To verify the performance of our proposal, we first consider a scenario of optical layer anomaly detection in the testbed. As indicated in Fig. 3, we have a 100 Gbps lightpath (*i.e. Node A* $\rightarrow$ *Node B*), whose central wavelength and bandwidth are 1550.39 nm and 50 GHz, respectively. The ASE noise generator is placed in the fiber link to insert noise and cause quality-of-transmission (QoT) degradation.

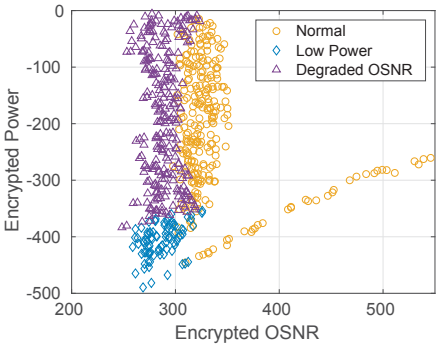
To emulate exceptions in the optical layer, we apply different configurations to the OLS system, such that the receiver experiences various combinations of power level and OSNR. Then, we utilize the privacy-preserving DL-based ML-INT&DA system to collect the power-level, OSNR and bit-error-rate before forward error correction (BERbFEC) of the lightpath. Next, the data collection agent organizes the received power-level and OSNR as plaintext ML-INT vectors, and tags them based on their corresponding BERbFECs. Specifically, if the ML-INT vector corresponds to a BERbFEC that is lower than the preset threshold, we tag it as "Normal". Otherwise, we tag it as "Low Power" or "Degraded OSNR" in accordance with the actual reason that leads to the high BER value. Then, the data collection agent performs encryption and reports ciphertext vectors to the centralized controller. We collect $\sim 31,000$ ML-INT data samples in this scenario.

C. Feature Validation

Taking the correlation between the OSNR and power level of a lightpath as an example, we verify the privacy-preserving feature of our proposal. Fig. 4(a) plots the combinations of OSNR and power level of a lightpath, and the telemetry data is in plaintext. Then, after applying the IVHE-based encryption to each data sample in Fig. 4(a) for multiple times, we obtain the ciphertext samples are shown in Fig. 4(b). It can be seen that the IVHE-based encryption encrypts a plaintext sample to different values in different encryption rounds, and thus it would be difficult for a malicious party to decrypt the ciphertext samples illegally. Therefore, the sensitive information regarding the data plane gets protected well. Meantime, the ciphertext data in Fig. 4(b) also indicates that the original correlations of the power-level and OSNR are kept through the encryption. This can be further justified, if we compare the plaintext and ciphertext data in Figs. 5(a) and 5(b), respectively, when much more samples are considered.



(a) Plaintext data



(b) Ciphertext data

Fig. 5. Applying IVHE-based encryption to a larger set of ML-INT data.

To verify the performance of our privacy-preserving DL-based DA, we conduct an experiment to compare it with a DL model that directly operates on plaintext data. Specifically, the data is divided into training and testing sets, which include 90% and 10% samples, respectively. Then, we use the plaintext data to train a DL model whose structure is similar to that of the one in Fig. 2, and consider it as the benchmark. The training time is almost identical for the two DL models, *i.e.*, the ones operate on plaintext and ciphertext data sets take 44.33 and 45.30 seconds to accomplish their training, respectively. After being trained, the DL models perform well in the controller for anomaly detection. Here, the one on ciphertext data achieves a classification accuracy of 99.48%, which is very similar to that of the benchmark (99.31%). These results confirm the feasibility of our proposal.

D. Stress Tests

Next, we conduct two stress tests to evaluate the computing overheads of the privacy-preserving scheme. In the first test, we let the data collection agent encrypt a burst of tremendous ML-INT data vectors that flood in within a second. The processing time in Fig. 6 suggests that the data collection agent completes the whole data encryption within 2.1 seconds, when it burstily receives 10^4 ML-INT vectors in a second. The results confirm that our IVHE-based encryption algorithm is lightweight in terms of computing load.

In the second test, we flood a large amount of ML-INT data to the controller within a second, and measure the total processing time on it, which includes both the time used to receive the data though TCP connections and that for anomaly detection in the DL model. Fig. 6 indicates that the total processing time on ciphertext is similar as that on plaintext. Hence, the results further confirm that our privacy-preserving scheme will not cause significant computing overheads to slow down the processing in the control plane.

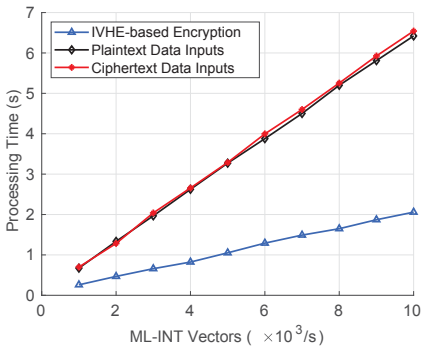


Fig. 6. Results of stress tests in data collection agent and controller.

V. Conclusion

In this paper, we proposed a privacy-preserving DL-based ML-INT&DA system for realizing AI-assisted network automation in IP-over-Optical networks with enhanced security. We first presented a lightweight IVHE-based encryption scheme, which can be used to encrypt plaintext ML-INT data but maintain the inner correlations of ML-INT data. Then, we architected a DL model for anomaly detection, which can directly analyze the ciphertext ML-INT data. Finally, we showed the implementation and experimental demonstrations of the proposed system. The privacy-preserving DL-based ML-INT&DA system was realized in a real IP-over-EON testbed, and the experimental results verified the feasibility and effectiveness of our proposal. Specifically, the IVHE-based encryption not only hid sensitive information regarding the data plane well, but also kept the inner correlations of the ML-INT data, such that the DL-based DA can classify ciphertext data to detect 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] "Cisco global cloud index: Forecast and methodology, 2016-2021." [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

[2] 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.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

[14] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "A simple network management protocol (SNMP)," *RFC 1098*, May 1990. [Online]. Available: https://tools.ietf.org/html/rfc1157

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

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

[17] ——, "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] "Barefoot Deep Insight." [Online]. Available: https://www.barefootnetworks.com/products/brief-deep-insight/

[19] "100g in-band network telemetry with Netcope P4." [Online]. Available: https://www.netcope.com/Netcope/media/content/100G-In-band-Network-Telemetry-With-Netcope-P4.pdf

[20] S. Tang *et al.*, "Sel-INT: A runtime-programmable selective in-band network telemetry system," *IEEE Trans. Netw. Serv. Manag., in Press*, 2019.

[21] 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

[22] 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.

[23] 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.

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

[25] N. Xue *et al.*, "Demonstration of OpenFlow-controlled network orchestration for adaptive SVC video manycast," *IEEE Trans. Multimedia*, vol. 17, pp. 1617–1629, Sept. 2015.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

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

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

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

[33] 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.

[34] 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.

[35] 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.

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

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

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

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

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

[45] Open network operating system (ONOS). [Online]. Available: https://onosproject.org/.