Secure Multi-Party Computation and Statistics Sharing for ML Model Training in Multi-domain Multi-vendor Networks

Pooyan Safari*, Behnam Shariati*, Geronimo Bergk, and Johannes Karl Fischer

Fraunhofer Institute for Telecommunications Heinrich Hertz Institute, Einsteinufer 37, 10587 Berlin, Germany, (email address of the corresponding author: pooyan.safari@hhi.fraunhofer.de)

Abstract: *We propose a secure aggregation algorithm that allows proprietary-owned domains, hosting statistically different datasets, train and operate ML models in a Horizontally Federated Learning fashion. The obtained results show a compelling test accuracy of 98.60% for a QoT estimation use-case in multi-domain multi-vendor networks.*

Introduction

Machine Learning (ML) is expected to play a significant role in the transformation towards zero-touch autonomous networking [1-2]. On the one hand, the success of ML-based solutions relies heavily on the quality of the data and its inclusive distribution, defined as its comprehensiveness to include a wide range of data instances to sufficiently model the real world. On the other hand, considering the published works, one can observe that a large number of them rely solely on synthetic data for their investigation [3-5], a small number of them rely on experimental data collected in the lab or field-trials [6-9], while a negligible number of them really use real field-collected data [10][11], and yet of very limited amount.

It is agreed that the regulatory issues imposed by telecom operators and the reluctance of vendors to share their business-critical data, are among the top showstoppers to create datasets for different networking use cases that are inclusive enough to drive the developments of reliable ML models. One solution to improve the accuracy of ML models for different networks with limited data availability is Transfer Learning (TL) [12]. However, TL does not secure the ML model from attacks that, for instance, aim at gaining access to the actual information [13]. A more promising solution is Federated Learning (FL) that enables training on sensitive data of multiple data holders without sharing the data itself [14]. We recently proposed a Distributed Learning Framework (DLFi), based on a flavour of FL called Horizontal FL (HFL), that allows data owners hosting various data instances, each with the same feature set (see Fig 1a), to collaboratively train a ML model [15][16]. However, the presented Federated Averaging (FedAvg) algorithm is yet prone to attacks [14].

Key Contributions

In this work, we present an advanced ML model development approach for DLFi based on Secure Multi-Party Computation (SMPC). Our proposal allows multiple parties (e.g. an operator, a system vendor, or a software provider) to cooperatively develop and own a ML model with a privacy-protection level far beyond what can be achieved with FedAvg. Moreover, we propose a novel data processing solution, hereafter refered to as Secure Statistics Sharing (SSS), for DLFi that offers globally optimum data scaling to improve the accuracy of the ML models when different parties host statistically different datasets. We validate our proposals in the development of a multi-domain QoT classifier.

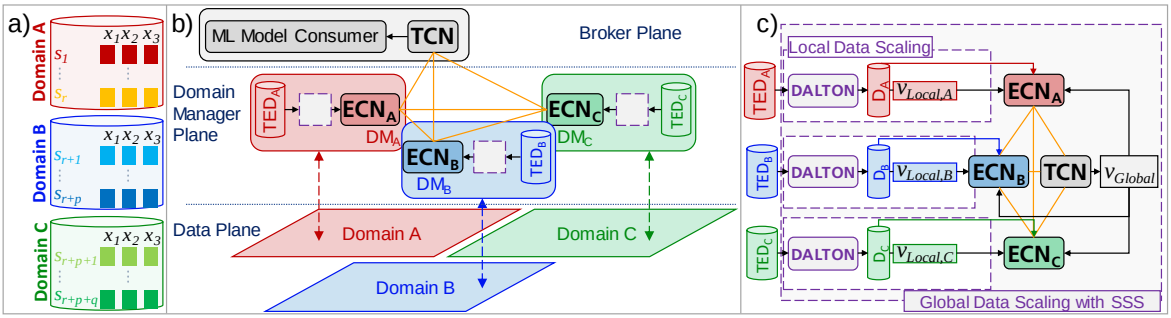

Fig 1. a) Domain datasets hosting data instances with the same feature-set, b) multi-domain multi-vendor network, and c) the data processing pipeline. Our Data Analytics Toolkit for Optical Networks (DALTON) transforms the Traffic Engineering Database (TED) of each domain to use-case specific datasets. The local pipeline provides a locally scaled dataset of each domain to the corresponding Edge Contribute Node (ECN) of DLFi. The global pipeline provides a globally scaled dataset of each domain to the corresponding ECN based on the Secure Statistics Sharing (SSS) algorithm presented in Algorithm 2.

978-1-6654-3868-1/21/$31.00 ©2021 IEEE

* These authors have equally contributed to this work.

Secure Aggregation and Statistics Sharing

DLFi exploits data of multiple owners distributed over a set of distributed nodes to train a global ML model. It comprises two components, 1) Edge Contributor Node (ECN) and 2) Training Coordinator Node (TCN). In our scenario, each ECN is considered as a Virtualized Network Function (VNF) with access to the data of a single domain. DLFi runs multiple rounds to train a model. Each round comprises an eligibility check of the ECNs, communicating the config files, and the return of the local models to the TCN that aggregates the local models [14-15].

It is recommended to use Secure Aggregation to avoid information leakage from the model parameters. Secure Aggregation is referred to the problem of computing a multiparty sum where no party reveals its update in a clear way, not even to the aggregator [17]. To achieve this level of privacy, we can take advantage of the SMPC protocol [18-19]. SMPC executes secure calculations to publish the result only to a single instance while guaranteeing that the values of the calculation are not known to anyone but the contributor itself. The curator only receives the resulting combination of all local models but not the values of a single local model. Therefore, they cannot spy on a single model. In this work we employed the SPDZ protocol [20-21], which is a secret-sharing-based SMPC method. It takes advantage of the additive secret sharing algorithm. It is the process of randomly splitting up a parameter into multiple shares and send them to each corresponding party, in a way that the summation of all these shares equals to the original value. The original value can be reconstructed only when all these shares are combined together. Therefore, each individual share is of no value by its own. Our proposed solution is presented in Algorithm 1.

Another important challenge for FL algorithms is the variations in the distributions of the training data on each ECN. This sometimes makes data scaling methods less effective as a pre-processing stage. One solution is to directly send the data statistics to the TCN to compute the global statistics and further use these statistics

Algorithm 1: FL with Secure Aggregation using SMPC for a list of ECNs $\chi = \{1, \dots, M\}$. mod is the modulo operator, and rand.range means random numbers in a specific range. l is the loss for the training and $\mathcal{L}$ is the average loss over a minibatch. y_n is the ground-truth label used for the training. The model is updated with learning rate η.

send config and initial model θ_g^0 to all ECNs
for each **round** r in R:
  on each ECN m **in parallel do**:
    for each **epoch** in E:
      for each minibatch b in $\mathcal{B}$:
        compute the model output $\hat{y}_n$
        loss $\mathcal{L}(\theta_m^r) = \frac{1}{|b|}\sum_{n=1}^{|b|} l\,(\theta_m^r; \hat{y}_n, y_n)$
        gradient of loss $g_m = \nabla_{\theta_m}\mathcal{L}(\theta_m^r)$
        update model params $\theta_m^r \leftarrow \theta_m^r - \eta g_m$
    to secret-share θ_m^r among all ECNs **do**:
      encode θ_m^rvalues to fixed precision
      consider Q as a very large prime number
      for j in $\{1, \cdots, M-1\}$ **do**:
        from rand.range$(0, Q)$ create $\theta_m^{r,j}$
      $\theta_m^{r,M} = mod(\theta_m^r - \sum_{j=1}^{M-1}\theta_m^{r,j}, Q)$
    for j in χ **do**:
      send the shares $\theta_m^{r,j}$ to ECN j
  when each ECN j receives all shares **do**:
    $\theta_j^{r,T} = \sum_{m=1}^{M}\theta_m^{r,j}$
    send $\theta_j^{r,T}$ to the TCN
  when TCN receives all collective shares **do**:
    decode all $\theta_m^{r,T}$to float precision
    $\theta_g^r = \frac{1}{M}\sum_{m=1}^{M}\theta_m^{r,T}$
    send θ_g^r to each ECN for validation
  on all ECNs **in parallel do**:
    validate global model θ_g^r on ECN's data
    compute validation metric (e.g., accuracy)
    secret-share validation metric among ECNs
  when TCN receives validation metric **do**:
      decide (continue or terminate) training
      if continue:
        send θ_g^r to all ECNs
      else:
        return θ_g^r as the trained model

Algorithm 2: Secure Statistics Sharing (SSS) algorithm to compute the global statistics given the local ones for a list of ECNs $\chi = \{1, \dots, M\}$. mod is the modulo operator, and rand.range means random numbers in a specific range.

on each of the ECNs m in parallel **do**:
  compute # training samples (N_m)
  $\Sigma_m = \mu_m \times N_m$
  $\xi_m = \sigma_m^2 \times (N_m - 1) + \Sigma_m^2/N_m$
  to secret-share$\{N_m, \Sigma_m, \xi_m\}$ among ECNs **do**:
    encode $\{\Sigma_m, \xi_m\}$ values to fixed precision
    consider Q as a very large prime number
    for j in $\{1, \cdots, M-1\}$ **do**:
      from rand.range$(0, Q)$ create $\{N_m^j, \Sigma_m^j, \xi_m^j\}$
    $N_m^M = mod(N_m - \sum_{j=1}^{M-1} N_m^j, Q)$
    $\Sigma_m^M = mod(\Sigma_m - \sum_{j=1}^{M-1} \Sigma_m^j, Q)$
    $\xi_m^M = mod(\xi_m - \sum_{j=1}^{M-1} \xi_m^j, Q)$
  for k in χ **do**:
    send the shares $\{N_m^k, \Sigma_m^k, \xi_m^k\}$ to ECN k
when each ECN m receives all shares **do**:
  $N_m^T = \sum_{i=1}^{M} N_i^m$
  $\Sigma_m^T = \sum_{i=1}^{M} \Sigma_i^m$
  $\xi_m^T = \sum_{i=1}^{M} \xi_i^m$
  send $\{N_m^T, \Sigma_m^T, \xi_m^T\}$ to the TCN
when TCN receives all collective shares **do**:
  $N = \sum_{i=1}^{M} N_i^T$ (global number of samples)
  $\Sigma = \sum_{i=1}^{M} \Sigma_i^T$
  $\xi = \sum_{i=1}^{M} \xi_i^T$
  decode $\{\Sigma_m, \xi_m\}$ to float precision
  $\mu = \Sigma/N$ (global mean)
  $\sigma^2 = (\xi - \Sigma^2/N)/(N-1)$ (global variance)
  send global statistics $\{N, \mu, \sigma^2\}$ to all ECNs

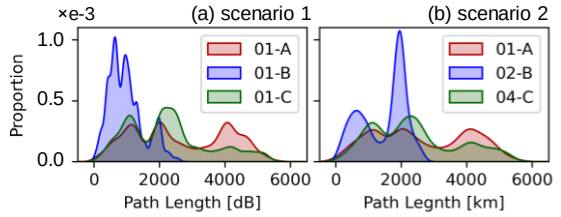

Fig 2. Domain-wise path length distribution.

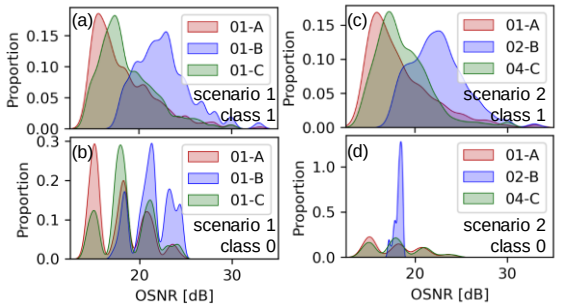

Fig 3. Domain-wise and class-wise OSNR distribution.

for data pre-processing purposes. However, communicating data statistics may compromise the privacy of the data owners. In order to circumvent this problem, we present an algorithm based on SPDZ for sharing the statistics of the data such as mean and variance without compromising their privacy. This process is explained in Algorithm 2.

Problem Formulation

We consider a ML-based QoT estimation use case in a multi-domain network similar to the one conceptionally illustrated in Fig 1b to demonstrate the performance of the proposed SMPC and SSS algorithms. We aim to use the domain-specific data of each Domain Manager (DM) to collaboratively train a ML model while keeping the data on the corresponding DMs. We further define two scenarios in which DMs operate over 1) topologically different domains with statistically similar traffic patterns, and 2) topologically different domains with statistically different traffic patterns.

We use the publicly available QoT estimation datasets 01, 02, and 04 [22][23]. For obtaining domain-specific datasets from the dataset, we define three domains A, B, and C within the topology of CORONET CONUS (depicted in Fig.2b of [15]). As presented in Table 1, we build scenario 1 based on dataset 01, which offers similar traffic patterns across domains .We build scenario 2 by forming the dataset of each domain using the datasets 01, 02, and 04, which offer different traffic patterns, for domain A, B, and C, respectively. We process the obtained datasets to be class-balanced (check Table 1). The statistical distribution of domain B is significantly different than the ones of A and C. To reveal the statistical differences of different domains in both scenarios, we visualize the domain-wise

Table 1. The number of training samples used for each scenario and domain is provided in square brackets.

	Domain A	Domain B	Domain C
Scenario 1	01-A [29581]	01-B [30869]	01-C [21908]
Scenario 2	01-A [3987]	02-B [3653]	04-C [4321]

Table 2. The identified options for each scenario based on FedAvg and SMPC algorithms as well as the proposed data scaling solutions. CL is reported as baseline.

	Options	Training	Validation	Test
Scenario 1	FedAvg – Local	91.46 %	90.78 %	91.11 %
	SMPC – Local	91.55 %	91.67 %	91.32 %
	SMPC – Global	98.01 %	97.99 %	**97.91 %**
	CL	98.37 %	98.40 %	98.16 %
Scenario 2	FedAvg – Local	86.82 %	87.39 %	87.26 %
	SMPC – Local	86.79 %	87.34 %	87.03 %
	SMPC – Global	98.71 %	98.36 %	**98.60 %**
	CL	98.87 %	98.57 %	98.60 %

distribution of path length, as a very informative feature in the dataset, and the domain-wise class-wise distribution of Optical Signal to Noise Ratio (OSNR), respectively, in Fig 2 and Fig 3. The variation of the statistical distribution of the domains is more significant for class 0 samples.

Results and Concluding Remarks

We split the domain-wise datasets in train, validation, and test sets, with 70%, 20%, and 10% share, respectively. We define three scenarios for our evalution: 1) FedAvg and 2) SMPC with local data scaling, as well as 3) SMPC with global data scaling using SSS. We consider Centralized Learning (CL) as the baseline, which is the case where we combine the data of the three domains and perform the training in a centralzied way. In all the scenarios, we consider a feed-forward neural network with an input dimension of 16 and a single hidden layer of size 256. We use tanh as the activation function for the hidden layer and a binary cross-entropy for the loss function. We report the results in terms of accuracy in Table 2.

Our SMPC algorithm shows competetive performance compared to the FedAvg when they use only local data scaling. However, both suffer ~7% and ~11% inaccuracy compared to CL, in scenario 1 and scenario 2, respectively. With the incorporation of our proposed SSS algorithm that allows global data scaling in a secure way, the accuracy of our SMPC algorithm gets very close to the CL baseline, with less than 0.5% performance degradation for both scenarios. The results showcase that our secure aggregation and SSS algorithms enable collaborative ML model training over *statistically different datasets* owned by multiple parties without revealing any raw data or statistics of their datasets.

The reported achievements pave the way for the realization of shared governance and ownership of ML models in multi-party telecom ecosystems.

Acknowledgement: This work received funding from BMBF in AI-NET PROTECT (KIS8CEL010).

References

[1] TM Forum Introductory Guide, “Autonomous networks technical architecture,” Version 1.0.0, Nov 2020.

[2] ETSI White Paper No. 40, “Autonomous networks, supporting tomorrow’s ICT business,” Oct 2020, ISBN No. 979-10-92620-37-6.

[3] F. N. Khan, Q. Fan, C. Lu, A. P. T. Lau, “An optical communications’ perspective on machine learning and its applications,” JLT, vol. 37, no. 2, pp. 493-516, Feb 2019.

[4] F. Musumeci, C. Rottondi, A. Nag, I. Macaluso, D. Zibar, M. Ruffini, M. Tornatore, “An overview on application of machine learning techniques in optical networks,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1383-1408, Nov 2018.

[5] L. Velasco, B. Shariati, F. Boitier, P. Layec, and M. Ruiz, “Learning life cycle to speed up autonomic optical transmission and networking adoption,” JOCN, vol. 11, pp. 226-237, May 2019.

[6] J. Yu, W. Mo, Y.-K. Huang, E. Ip, D. C. Kilper, “Model transfer of QoT prediction in optical networks based on artificial neural networks,” JOCN, vol. 11, no. 10, pp. C48-C57, Oct 2019.

[7] Z. Gao, S. Yan, J. Zhang, M. Mascarenhas, R. Nejabati, Y. Ji, D. Simeonidou, “ANN-based multi-channel QoT-prediction over a 563.4-km field-trial testbed,” JLT, vol. 38, no. 9, pp. 2646-2655, Feb 2020.

[8] K. Christodoulopoulos, C. Delezoide, N. Sambo, A. Kretsis, I. Sartzetakis, A. Sgambelluri, N. Argyris, G. Kanakis, P. Giardina, G. Bernini, D. Roccato, A. Percelsi, R. Morro, H. Avramopoulos, P. Castoldi, P. Layec, and S. Bigo, “Toward efficient, reliable, and autonomous optical networks: the ORCHESTRA solution,” JLT, vol. 11, no. 9, pp. C10-C24, Aug 2019.

[9] B. Shariati, J. J. Pedreno-Manresa, A. Dochhan, A. S. Muqaddas, R. Casellas, O. González de Dios, L. L. Canto, B. Lent, J. E. López de Vergara, S. López-Buedo, F. J. Moreno, P. Pavón, L. Velasco, S. Patri, A. Giorgetti, F. Cugini, A. Sgambelluri, R. Nejabati, D. Simeonidou, R,-P, Braun, A. Autenrieth, J.-P. Elbers, J. K. Fischer, R. Freund, “A latency-aware real-time video surveillance demo: network slicing for improving public safety,” in Proc. OFC, 2021.

[10] K. Kaeval, T. Fehenberger, J. Zou, S. L. Jansen, K. Grobe, H. Griesser, J.-P Elbers, M. Tikas, G. Jervan, “ QoT assessment of the optical spectrum as as service in disaggregated network scenarios,” JOCN, vol. 13, no. 10, pp. E1-E12, Oct 2021.

[11] C. Delezoide, P. Ramantanis, P. Layec, “Leveraging field data for the joint optimization of capacity and availability in low-margin optical networks,” JLT, vol. 38, no. 24, pp.6709-6718, Dec 2020.

[12] C. Y. Liu, X. Chen, R. Proietti, S. J. B. Yoo, “Performance studies of evolutionary transfer learning for end-to-end QoT estimation in multi-domain optical networks,” JOCN, vol. 13, no. 4, pp. B1-B11, Jan 2021.

[13] X. Liu, L. Xie, Y. Wang, J. Zou, J. Xiong, Z. Ying, A. V. Vasilakos,“ Privacy and security issues in deep learning: a survey,” IEEE Acces, vol. 9, pp. 4566-4593, Dec 2020.

[14] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. Arcaset, “Communication-efficient learning of deep networks from decentralized data,” in Proc. of the 20th International Conference on Artificial Intelligence and Statistics, 2017.

[15] P. Safari, B. Shariati, and J. K. Fischer, “Privacy-preserving distributed learning framework for 6G telecom ecosystems,” arXiv preprint arXiv:2008.07225, 2020.

[16] B. Shariati, P. Safari, A. Mitrovska, N. Hashemi, J. K. Ficher, and R. Freund, “Demonstration of federated learning over edge-computing enabled metro optical networks,” in Proc. ECOC, Brussels, Belgium, Dec 2020.

[17] K. Bonawitz, et al., “Practical secure aggregation for privacy-preserving machine learning,” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

[18] M. Keller, P. Valerio, and R. Dragos. “Overdrive: Making SPDZ great again,” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2018.

[19] C. Zhao, et al. "Secure multi-party computation: theory, practice and applications." Information Sciences 476 (2019): 357-372.

[20] I. Damgård, et al. "Practical covertly secure MPC for dishonest majority–or: breaking the SPDZ limits." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2013.

[21] I. Damgård, et al. "Multiparty computation from somewhat homomorphic encryption." Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2012.

[22] G. Bergk, B. Shariati, P. Safari, and J. K. Fischer, “QoT Dataset Collection, ” [online – accessed May 2021] https://www.hhi.fraunhofer.de/networkdata

[23] P. Safari, B. Shariati, G. Bergk, and J. K. Fischer, ”Deep convolutional neural network for network-wide QoT estimation,” in Proc. OFC, 2021.