NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium | 978-1-6654-7716-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/NOMS56928.2023.10154226

SFL-LEO: Secure Federated Learning Computation Based on LEO Satellites for 6G Non-Terrestrial Networks

†Sheikh Salman Hassan, †Umer Majeed, ‡Zhu Han, and †Choong Seon Hong
†Department of Computer Science and Engineering, Kyung Hee University, Yongin, 17104, Republic of Korea
‡Department of Electrical and Computer Engineering, University of Houston, Houston, TX, 77004-4005, USA
Email: {salman0335, umermajeed, cshong}@khu.ac.kr, zhan2@uh.edu

***Abstract*—We propose using federated learning (FL) in low Earth orbit (LEO) satellite networks for the Internet of Remote Things (IoRTs) to enable adaptive learning in massively networked devices while reducing costly traffic in satellite communication (SatCom). In this resource-constrained space setting, FL techniques in LEO satellite-based learning can improve system energy efficiency and save time. However, FL raises security and risk concerns, as local model updates can be used to infer device information by a hostile federated aggregator server in space. To address this, we propose using homomorphic-based encryption and decryption security techniques for federated aggregators and IoRTs. We evaluate the secure learning performance of our proposed framework using simulations on advanced datasets and aggregation approach. The results show that compared to the benchmark scheme, the proposed secured computing networks improve communication overhead and latency performance.**

***Index Terms*—6G, federated learning, security, and privacy.**

I. Introduction & Background

6G networking is around the corner [1]. Through the connected Internet of Remote Things (IoRTs), e.g., mobile sensors, wearable technology, smartphones, connected cars, and unmanned aerial vehicles (UAVs), an unexpected amount of data is produced, along with new smart applications i.e., augmented/virtual reality (AR/VR) and digital twin (DT). It is impractical to gather and transmit entire data to a single server due to communication resource limits or delays. Meanwhile, data protection (e.g., the GDPR in Europe [2] to protect personal data, i.e., healthcare or monetary archives), data analysis, and inference close to the source have become increasingly important in avoiding delay, communication overhead, and privacy breaches. Thus decentralized machine learning (DML) leveraging intelligence edge computing, where data is kept distributedly (locally) is one alternative to data analysis, especially for large-scale ML models. So federated learning (FL) expands the computation of AI applications onto a large number of end devices without infringing on privacy [3]. The key advantages of FL are communication efficiency and data privacy, as model parameters rather than raw data are transmitted. However, existing FL protocols have limitations that adversaries might use to undermine the trained model [4]–[7].

The global number of active Internet of Things (IoTs) is expected to nearly triple from 8.74 billion in 2020 to more than 25.4 billion in 2030 [8]. Despite the widespread deployment of mobile networks, many devices in distant places (i.e., deserts and oceans) still lack connectivity services. Due to harsh topography, communication distance, and economic and engineering problems, terrestrial networks (TNs) only cover around 20% of the worldwide land area and less than 6% of the earth's surface [1]. There is an agreement in academia and industry that satellite communication (SatCom) networks are a feasible supplementary alternative to TNs for achieving global coverage [9]–[11] and seamless connection to serve different computation jobs, i.e., edge-AI [12] [13]. Existing literature mentioned in [3], [14]–[20] discussed only satellite role in communication, terrestrial-based FL, and security for ground network devices. However, none of the previous studies jointly investigated LEO satellite[1]-based communication, FL computation, and security. Thus, we propose a secure FL computation on LEO networks. In particular, we studied FL in the context of LEO and space security challenges. To the best of our knowledge, the proposed contributions are novel in the given network environment, which are given as follows:

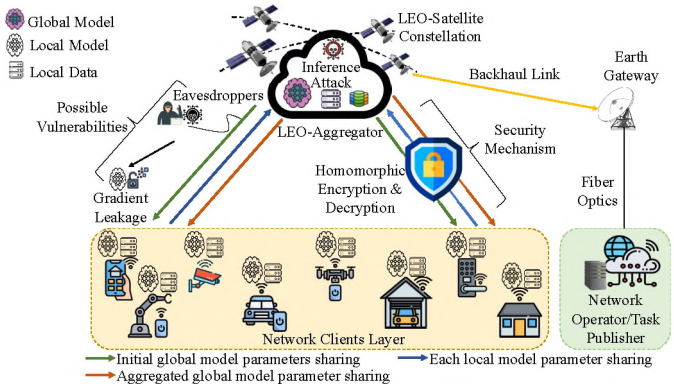


Fig. 1: Secure FL-based LEO satellite 6G network.

- We present a novel security-enabled LEO network to perform FL for IoRTs, which employs homomorphic encryption (HE) at the IoRT and FL-aggregation at the LEO aggregator to perform the secure FL task.
- During FL, our proposed HE-based SFL-LEO protocol ensures the anonymity of IoRTs' local gradients. Even if the LEO server colludes with numerous IoRTs, we assert that attackers will not obtain any meaningful knowledge about IoRTs' local gradients.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A4A1018607), Institute of Information & communications Technology Planning & Evaluation (IITP) Grant funded by MSIT (Artificial Intelligence Innovation Hub) under Grant 2021-0-02068, IITP grant funded by MSIT (No.2019-0-01287, Evolvable Deep Learning Model Generation Platform for Edge Computing), and IITP grant funded by MSIT (No. RS-2022-00155911, Artificial Intelligence Convergence Innovation Human Resources Development (Kyung Hee University). Dr. CS Hong is the corresponding author.

[1]Hereafter the LEO satellite is considered an LEO unless otherwise stated.

II. System Model Overview

A. LEO Satellite-based Communication Channel & Link

As illustrated in Fig. 1, the system model composes a set $\mathcal{S}$ of S LEO that will support a set $\mathcal{U}$ of U IoRTs. We consider Ka-band (mm-Wave) for SFL-LEO communication with the time division multiple access (TDMA) schemes to avoid interference in the network [21]. The IoRTs need to deliver their data, i.e., model hyperparameters, to an LEO in the time horizon T. The composite channel captures small and large-scale fading between LEO s and IoRT u is $g_{s,u} = \beta_{s,u}(\xi_{s,u})^{-1/2},\ \forall s \in \mathcal{S},\ \forall u \in \mathcal{U}$, where $\beta_{s,u}$ is the Rician fading channel coefficient and $\xi_{s,u}$ is large-scale fading for pathloss. Here, $d_{s,u} = \sqrt{(x_s - x_u)^2 + (y_s - y_u)^2 + (z_s - z_u)^2}$ is the distance between LEO s and IoRT u. Thus, large-scale path loss on the mmWave links is $\xi_{s,u}(\mathrm{dB}) = \omega_{s,u} + \zeta_{s,u} 10\log_{10}\left(\frac{d_{s,u}}{d_0}\right) + \psi_{s,u}, \forall s \in \mathcal{S},\ \forall u \in \mathcal{U}$, where $\zeta_{s,u}$ is path loss exponent, $\omega_{s,u}$ is path loss at reference distance d_0, and $\psi_{s,u}$ is a zero-mean Gaussian random variable with standard deviation $\delta_{s,u}$ [21]. The small-scale fading coefficient is $\beta_{s,u} = \sqrt{\frac{K_{s,u}}{1+K_{s,u}}} + \sqrt{\frac{1}{1+K_{s,u}}}\Xi_{s,u},\ \forall s \in \mathcal{S},\ \forall u \in \mathcal{U}$, where $K_{s,u}$ is the Rician factor and $\Xi_{s,u} \sim \mathcal{N}(0,1)$. Let's simplify the channel gain:

$$g_{s,u}(n) = \left(\frac{d_0}{d_{s,u}(n)}\right)^{\frac{\zeta_{s,u}}{2}} 10^{-\frac{\omega_{s,u}+\psi_{s,u}}{20}} \left(\sqrt{\frac{K_{s,u}}{1+K_{s,u}}} + \sqrt{\frac{1}{1+K_{s,u}}}\Xi_{s,u}\right),\ \forall s \in \mathcal{S}, u \in \mathcal{U}, \tag{1}$$

Thus, the signal-to-noise ratio (SNR) between this link is $\gamma_{s,u} = \frac{p_{s,u} g_{s,u}}{\sigma^2},\ \forall s \in \mathcal{S}, u \in \mathcal{U}$, where $p_{s,u}$ is the transmit power between LEO s and IoRT u. The achievable data rate between satellite s and IoRT u is $r_{s,u} = B_{s,u}\log_2(1+\gamma_{s,u}),\ \forall s \in \mathcal{S},\ \forall u \in \mathcal{U}$, where $B_{s,u}$ is the bandwidth allocated to the link between LEO s and IoRT u.

B. Transmission Latency, Propagation, & Computation Delay

The end-to-end transmission delay of a wireless communication system is made up of two parts: propagation delay and transmission delay. Thus the end-to-end latency of the computational data offloading time of IoRT u is $t_{s,u} = \frac{D^{\text{local}}_{s,u}}{r_{s,u}} + \frac{d_{s,u}}{c},\ \forall s \in \mathcal{S},\ \forall u \in \mathcal{U}$, where $D^{\text{local}}_{s,u}$ is data size that IoRT u uploads to the LEO s, and c is the speed of light. The computation time required for learning in each IoRT u is proportional to its data size $\mathrm{S}(\mathcal{D}_u)$ in bits and the CPU frequency f_u as $t_u^{\text{training}} = \frac{c_u S(\mathcal{D}_u)}{f_u}$, where c_u is the number of CPU cycles required to process one data sample. Similarly, the computation delay at the LEO s is $t_s^{\text{aggregation}} = \frac{c_s S(\mathcal{D}_s)}{f_s}$, where $S(D_s)$ is the computational data size, c_s denotes the number of CPU cycles required to process one bit of data, and f_s CPU frequency of the LEO s.

C. Federated Learning Model Computation

Each IoRT u inside the LEO s coverage region contains their local dataset $\mathcal{D}_u^{\text{local}}$, which is used to train a local FL model by stochastic gradient descent (SGD) [3], where $m_u = |D_u|$ is the D_u data samples, and $m = \sum_{u\in\mathcal{U}} D_u$ is overall samples of all the datasets D_u. The training process is managed by the network operator (NO) on LEO s referred to as the LEO-aggregator. Each local data set $\mathcal{D}_u^{\text{local}}$ of IoRT is unknown to the LEO-aggregator and is not shared with it. For compact Euclidean feature space X and label space $Y = [C]$, the DNN contains C classes, where $[C] = 1, 2, ..., C$. The collaborative objective of FL is to figure out which DNN model parameters minimize a global loss function is $\min_w f(\boldsymbol{w}) = \sum_{u\in\mathcal{U}} \frac{m_u}{m} F_u(\boldsymbol{w})$, where F_u is the local loss function as $F_u(\boldsymbol{w}) = \frac{1}{m_u}\sum_{\boldsymbol{v}\in\mathcal{D}_u} f_v(\boldsymbol{w})$, where $f_v(\boldsymbol{w})$ is the multi-class cross-entropy loss on a data sample $\{\boldsymbol{x}, y\}$ for one-hot-encoded labels at IoRT u that is dependent on the specific learning situation as: $f_v(\boldsymbol{w}) = -\sum_{r=1}^{C} \mathbb{1}_{y=r} \log p_r(\boldsymbol{x}, \boldsymbol{w})$, where $\boldsymbol{w}$ is the DNN weight matrix and $p_r(\boldsymbol{x}, \boldsymbol{w})$ is the probability value of $x \in X$ in class r. We utilize the federated averaging (FedAvg) algorithm by i) sending the global parameters $\boldsymbol{w}$ from the LEO aggregator to the IoRTs, ii) utilizing SGD, training the local model at the IoRTs, iii) transmitting the acquired local parameters to the LEO aggregator, and iv) aggregating the parameters via the LEO-aggregator. This method is repeated for multiple global epochs until convergence occurs. The local training stages for each IoRT u are regarded as the ML phase. Every IoRT u minimizes its loss function with i local SGD iterations and updates the local copy of the global model parameters as: $\boldsymbol{w}_u^{n,i} = \boldsymbol{w}_u^{n,i-1} - \eta\nabla F_u(\boldsymbol{w}_u^{n,i-1})$, where η is the learning rate, n is the global epochs, $i \geq 1$ local iterations in epoch n, and $\boldsymbol{w}_u^{n,0} = \boldsymbol{w}^n$ is configured by the obtained global model parameters $\boldsymbol{w}^n$. The LEO aggregates the local updates $(w_u^{n,i})_{u\in\mathcal{U}}$ from every IoRT device u into a new version of the global model parameters as $\boldsymbol{w}^{n+1} = \sum_{u=1}^{U} \frac{m_u}{m} \boldsymbol{w}_u^{n,i}$, and progresses to the next epoch until the global convergence condition is reached.

D. Security Issues in FL Model Communication

The protection of transmitted data from passive attacks, i.e., eavesdropping (data confidentiality [22]), which could listen to the transmission or use data sniffing techniques to acquire the IoRT's private data if sent without encryption or insufficient encryption [23]. When an attacker alters data sent from the IoRT to the LEO, the data's integrity is jeopardized. Man-in-the-middle attacks can alter data without the recipient LEO being aware of it. Similarly, several threats remain in allowing security and privacy-preserving FL [24]. 1) Inference attacks in FL aren't a complete data privacy solution on their own. An attacker might execute inference attacks using the device's model updates from local learning $w_u^{n,i}$. The aggregation server may also infer device information during the model updates from local learning results. 2) Aggregation attacks are malicious adversaries that may attack the aggregation server and generate the aggregated global model incorrectly. Thus, the global model is erroneous. This will increase the time it takes for the FL global model to converge.

III. Proposed SFL-LEO Framework

In the proposed framework as shown in Fig. 2, the NO acts as the FL-task publisher (FL-TP). The steps as per the sequence diagram are as follows:

- Step 1: The FL-TP/NO will devise the model architecture for the FL-task.
- Step 2: The FL-TP/NO will also devise the aggregation scheme for the FL-task.

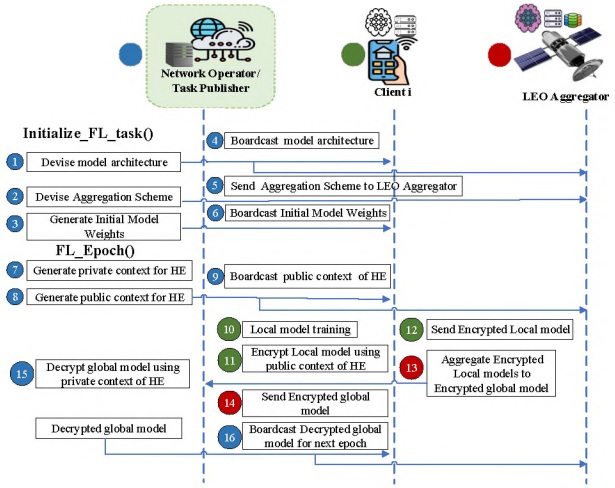


Fig. 2: Sequence of interactions in SFL-LEO framework.

- Step 3: Similarly, the FL-TP/NO will also generate the initial model weights $\boldsymbol{w}_u^{n,i}$ for the FL task as per the FL model architecture.
- Step 4: The FL-TP/NO will broadcast the generated model architecture to the IoRTs as well as the LEO aggregator.
- Step 5: The FL-TP/NO will send the aggregation scheme for the FL task to the LEO aggregator.
- Step 6: The FL-TP/NO will broadcast the initial model weights for the FL-task to the IoRTs.

Step 1 - Step 6 is utilized to initialize the FL task. Afterward, steps 7 - Step 16 are performed for each global epoch n.

- Step 7: The FL-TP/NO will generate the HE private context valid only in the ongoing global epoch n.
- Step 8: The FL-TP/NO will also generate the associated public context for the HE valid only in the ongoing global epoch n.
- Step 9: Similarly, the FL-TP/NO will broadcast the public context for the HE valid only in the ongoing global epoch n to the IoRTs as well as the LEO aggregator.
- Step 10: The IoRTs will perform the local model training on the local datasets.
- Step 11: The IoRTs will encrypt their local model $\hat{\boldsymbol{w}}_u^{n,i}$ using the public context for the HE valid only in the ongoing global epoch n.
- Step 12: The IoRTs will send their encrypted local model for the current global epoch to the LEO aggregator.
- Step 13: The LEO aggregator will aggregate the encrypted local models using the public context for the HE valid only in the ongoing global epoch n to the encrypted global model for the current global epoch n.
- Step 14: The LEO aggregator will send the encrypted global model in the ongoing global epoch n to the FL-TP/NO.
- Step 15: The FL-TP/NO decrypts the encrypted global model for the current global epoch using the HE private context valid only in the ongoing global epoch n.
- Step 16: If the required level of accuracy is not achieved and several global epochs are not reached, the FL-TP/NO broadcasts the decrypted global model in the ongoing global epoch to the IoRTs for local training in the succeeding global epoch $n+1$.

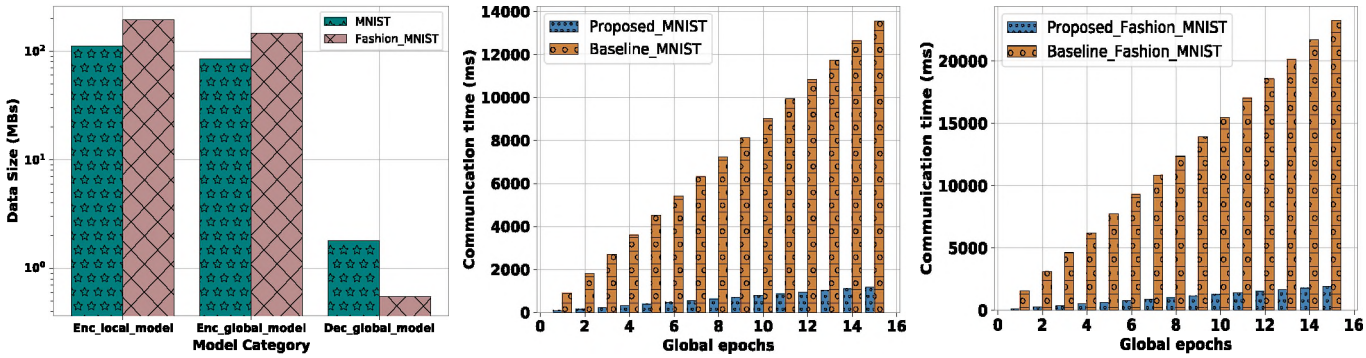
The following steps comprise the proposed SFL-LEO framework. First, we deployed the network architecture, which included LEO and IoRTs, following the system architecture. Second, the NO created IoRTs' local models and aggregation techniques and sent them to the IoRTs and LEOs. Following that, NO generates public and private HE contexts in each global iteration. The NO then provides the LEO and IoRTs with the public HE context. Then, in parallel, each IoRT u does local training and encrypts their local models before sending them to the LEO s for aggregation. Thus, following aggregation, the LEO sends encrypted data to the NO for decryption. Finally, NO transmits the decrypted local model to the IoRTs for the next global epoch.

IV. System Evaluation & Discussion

We consider a 2000 km x 2000 km area, where the LEO satellite is deployed at a height of 560 km in orbit. We consider IoRTs $U = 100$ that are dispersed independently and identically distributed (IID) over under-served locations and are equipped with computing and memory to train a model of interest. Moreover, we assume that LEO satellites and ground-based cloud centers are resource-enriched; therefore, we neglect their computation time. It is worth noting that we evaluate IID data settings for IoRTs and disregard Non-IID settings since they only affect the accuracy of the FL global model and have no bearing on network security or latency. The FL-model is trained on the well-known MNIST and fashion-MNIST datasets [25]. The training data is partitioned in an IID manner into N blocks. Because of low response time caused by opportunistic offline or delayed or expensive connections, only 10% of IoRTs are randomly selected to participate in the learning process in each learning cycle.

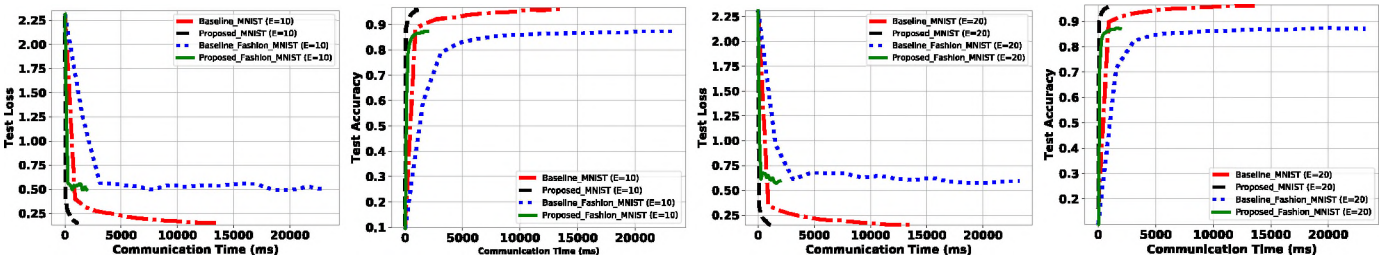
We used two neural networks to assess the SFL-LEO framework: a dense neural network (DNN) for MNIST and a convolution neural network (CNN) for Fashion-MNIST. FedAvg was simulated on our model using PyTorch [26]. The OpenMined TenSEAL is utilized for Single-Key (SK) HE deployment [27]. The amount of storage needed for FL aggregation is determined by the model design. Python's pickle library is utilized to store model state_dicts. We present in Fig. 3a both model sizes for state_dicts, i.e., DNN (MNIST categorization) and CNN (Fashion-MNIST categorization) concerning their category, e.g., an encrypted local model, an aggregated encrypted global model, and an aggregated decrypted global model. To accomplish encryption using TenSEAL, the simple unencrypted state_dicts is changed from tensors to the list by utilizing the tolist() method. Thus, the model size is greatly expanded for each local and global model to protect the FL method's input privacy via HE.

Our SFL-LEO findings were compared to those of a ground cloud server (NO), with the LEO functioning as a network relay. Additionally, because FL's method is iterative, the overall communication overhead rises. Furthermore, all HE-encrypted



(a) Model sizes of datasets in each category (b) Convergence for MNIST dataset. (c) Convergence for Fashion-MNIST dataset.

Fig. 3: Illustration of proposed model sizes and scheme convergence time comparison with baseline



(a) Loss vs comm. time. (b) Accuracy vs comm. time. (c) Loss vs comm. time. (d) Accuracy vs. comm. time.

Fig. 4: SFL-LEO performance in LEO satellite-based communication systems as measured by the MNIST & Fashion-MNIST dataset with fixed local epochs $E = 10$ & $E = 20$.

local models are sent to the NO via LEO, where the NO performs the aggregate, which is insecure and may indicate a vulnerability.

Fig. 3b and Fig. 3c compare the model convergence time with global epochs for the proposed and baseline algorithms for both datasets when local epochs are fixed, i.e., $E = 10$ and $E = 20$. Our technique outperforms the baseline in terms of communication time, which is a particularly critical metric for IoRTs. Furthermore, our approach yields a 167.713% for MNIST and a 169.527% for Fashion-MNIST improvement in communication time over the baseline. This difference demonstrates that the proposed scheme may be used for future time-sensitive and secure SFL-LEO.

As shown in Fig. 4, we examine the learning performance of the proposed SFL-LEO framework in terms of latency and the number of local epochs. Each epoch is defined as the number of training cycles per communication round that each IoRT runs over its local dataset, represented by E, while communication time is defined as the sum of transmission time for uploading and downloading model parameters and propagation time.

In particular, in Fig. 4a we show the test loss when $E = 10$ compared with the baseline for communication time. It can be observed that the proposed scheme performs better, i.e., it achieves fast convergence within less time than the baseline. In Fig. 4b we show the test accuracy when $E = 10$ compared with the baseline for communication time. Similarly, proposed schemes achieve fast results for both datasets, i.e., MNIST and Fashion-MNIST in terms of accuracy compared with a baseline, which achieves similar results but at a slower rate. The proposed approach produces results that perform aggregation at LEO (more privacy from NO inference attacks), only the HE-encrypted global model is transferred to NO, and the baseline suffers from extra communication costs, i.e., inter-satellite link (ISL) latency and communication time between NO and LEOs in each communication round.

Fig. 4 demonstrates how the local number of training epochs affects the performance of both schemes. In particular, we evaluate the test loss for $E = 20$ relative to the baseline for communication time in Fig. 4a. It can be shown that our approach outperforms the baseline for both datasets, achieving quick convergence in less time. We illustrate the test accuracy for $E = 20$ relative to the baseline for communication time in Fig. 4d. Similarly, our techniques offer quick accuracy outcomes as compared to baseline, which obtains comparable results but at a slower rate.

V. Conclusion

We studied the security-aware LEO-based FL for the IoRTs. FL over wireless networks has the potential to significantly improve learning performance on future 6G networks, which will be required to fulfill more stringent data security, privacy, and communication overhead standards. Initially, the suggested designs considered FL and LEO system integration. The performance evaluation shows that the proposed FL integration inside the LEO constellation has realistic accuracy on the MNIST and Fashion-MNIST datasets. SFL-LEO systems provide significantly reduced communication overheads with privacy than the traditional approach. The suggested technique has minimal transmission costs, leakage of information, and delay.

REFERENCES

[1] L. Zhang, Y. Liang, and D. Niyato, "6G visions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence," *China Communications*, vol. 16, no. 8, pp. 1–14, Aug. 2019.

[2] I. G. P. Team, "EU general data protection regulation (GDPR) - An implementation and compliance guide," 2020, IT Governance Ltd.

[3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proc. of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, ser. Machine Learning Research, A. Singh and J. Zhu, Eds., vol. 54. Florida, USA: PMLR, Apr. 2017, pp. 1273–1282. [Online]. Available: http://proceedings.mlr.press/v54/mcmahan17a.html

[4] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63 229–63 249, Apr. 2021.

[5] L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. H. Nguyen, and C. S. Hong, "Federated learning for edge networks: Resource optimization and incentive mechanism," *IEEE Communications Magazine*, vol. 58, no. 10, pp. 88–93, Nov. 2020.

[6] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys Tutorials*, vol. 23, no. 3, pp. 1759–1799, June. 2021.

[7] D. Ye, R. Yu, M. Pan, and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23 920–23 935, Jan. 2020.

[8] "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030," https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, 2021, [Online].

[9] S. S. Hassan, D. H. Kim, Y. K. Tun, N. H. Tran, W. Saad, and C. S. Hong, "Seamless and energy efficient maritime coverage in coordinated 6G space-air-sea non-terrestrial networks," *IEEE Internet of Things Journal*, pp. 1–1, Nov. 2022.

[10] S. S. Hassan, Y. M. Park, Y. K. Tun, W. Saad, Z. Han, and C. S. Hong, "Satellite-based ITS data offloading & computation in 6G networks: A cooperative multi-agent proximal policy optimization DRL with attention approach," Dec. 2022. [Online]. Available: https://arxiv.org/abs/2212.05757

[11] S. S. Hassan, Y. K. Tun, W. Saad, Z. Han, and C. S. Hong, "Blue data computation maximization in 6G space-air-sea non-terrestrial networks," in *the proc. of IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, Dec. 2021, pp. 1–6.

[12] B. Mao, F. Tang, Y. Kawamoto, and N. Kato, "AI models for green communications towards 6G," *IEEE Communications Surveys Tutorials*, pp. 1–1, Nov. 2021.

[13] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite communications in the new space era: A survey and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, Oct. 2021.

[14] "Why in the next decade companies will launch thousands more satellites than in all of history," https://www.cnbc.com/2019/12/14/spacex/oneweb/and/amazon/to/launch/thousands/more/satellites/in/2020s.html/, 2019, [Online].

[15] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14 399–14 417, Mar. 2021.

[16] I. F. Akyildiz and A. Kak, "The Internet of Space Things/Cubesats," *IEEE Network*, vol. 33, no. 5, pp. 212–218, Aug. 2019.

[17] B. Denby and B. Lucia, "Orbital edge computing: Nanosatellite constellations as a new class of computer system," in *Proc. of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, Lausanne, Switzerland, Mar. 2020, pp. 939–954.

[18] G. Giuffrida, L. Diana, F. de Gioia, G. Benelli, G. Meoni, M. Donati, and L. Fanucci, "Cloudscout: A deep neural network for on-board cloud detection on hyperspectral images," *Remote Sensing*, vol. 12, no. 14, p. 2205, July. 2020.

[19] G. Furano, G. Meoni, A. Dunne, D. Moloney, V. Ferlet-Cavrois, A. Tavoularis, J. Byrne, L. Buckley, M. Psarakis, K.-O. Voss, and L. Fanucci, "Towards the use of artificial intelligence on the edge in space systems: Challenges and opportunities," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 12, pp. 44–56, Dec. 2020.

[20] U. S. Agency, "Take-off for UK-built supercomputer nanosatellites," https://www.gov.uk/government/news/takeoff-for-uk-built-supercomputer-nanosatellites/, 2019, [Online].

[21] Y. Hu, M. Chen, and W. Saad, "Joint access and backhaul resource management in satellite-drone networks: A competitive market approach," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3908–3923, Mar. 2020.

[22] N. Sklavos, "Book review: Stallings, w. cryptography and network security: Principles and practice," *Information Security Journal: A Global Perspective*, vol. 23, no. 1-2, pp. 49–50, Apr. 2014. [Online]. Available: https://doi.org/10.1080/19393555.2014.900834

[23] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, June. 2017.

[24] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Generation Computer Systems*, vol. 115, pp. 619–640, Feb. 2021.

[25] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, Oct. 2016.

[26] A. Paszke, S. Gross, F. Massa, A. Lerer, J. Bradbury, G. Chanan, T. Killeen, Z. Lin, N. Gimelshein, L. Antiga, A. Desmaison, A. Kopf, E. Yang, Z. DeVito, M. Raison, A. Tejani, S. Chilamkurthy, B. Steiner, L. Fang, J. Bai, and S. Chintala, "Pytorch: An imperative style, high-performance deep learning library," in *Proc. of the Advances in Neural Information Processing Systems*, vol. 32. Vancouver, Canada: Curran Associates, Inc., Dec. 2019. [Online]. Available: https://proceedings.neurips.cc/paper/2019/file/bdbca288fee7f92f2bfa9f7012727740-Paper.pdf

[27] A. Benaissa, B. Retiat, B. Cebere, and A. E. Belfedhal, "TenSEAL: A Library for Encrypted Tensor Operations Using Homomorphic Encryption," *arXiv preprint arXiv:2104.03152*, Apr. 2021.