Financiado por la Unión Europea NextGenerationEU

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Plan de Recuperación, Transformación y Resiliencia

E3. Initial report on ML-based analytics and privacy aspects

Project: MAP-6G

PROGRAMA DE UNIVERSALIZACIÓN DE INFRAESTRUCTURAS DIGITALES PARA LA COHESIÓN

UNICO I+D 5G 2021

Fecha: 30/06/2023

Versión: 1.0

Deliverable information

Description: Initial specification of ML-based analytics for movement prediction and network decision making with specific focus on native privacy-preserving machine learning algorithms.

Due date: 30/06/2023

Responsible: IMDEA Networks

Partners involved: IMDEA Networks + Telefónica

Work Package 3 (WP3): Machine Learning-based Movement and Network Analytics

Activity 6: ML-based analytics for movements of people

This activity is planned as Subcontracted. The company will take care of the work on joint optimization of RIS, mobile network and communication link configuration to improve network performance and coverage. At the date of production of this deliverable, the tender procedure is finished, and the work has been assigned to Pi Lighting. We are preparing the last administrative procedures in order to sign the contract as soon as possible and start the work.

Activity 7: ML-based analytics for network control (Telefónica)

Description: Initial report on the State of Art on design data-driven decisions, real-time and automated network optimization with Machine Learning for the effective operation of 6G networks

In the scope of this task, we will be investigating how Machine Learning (ML) can be leveraged to control various aspects of the network. The current 5G networks face several challenges such as management and orchestration of Ultra-Dense Small Cells deployment as well as multiple-input multiple-output (MIMO) processing, interference issues, control and data plane separation, latency reduction and intelligent authentication, among others. These challenges are going to be significantly aggravated in the near future, with mobile data traffic experiencing a 50% to 100% growth every year.

The upcoming 6G technology, while currently in the conceptual phase, aims to achieve significant advancements in various areas. These include a minimum latency improvement of 10 times (reduced to 1ms), increased device density to 10 devices per square meter, user experience data rates of at least 100 Gb/s, enhanced capacity of 150 Tpb/s per square kilometer, a substantial 30-fold increase in location accuracy (down to 1 cm), and a remarkable 300-fold boost in energy efficiency. These goals are part of the 6G European vision outlined in 2021.

ML has emerged as one of the most promising techniques to address challenges for network orchestration and management tasks, having the potential to automatically learn and dynamically adapt to system dynamics and predict future scenarios. ML algorithms for wireless networks are expected to enable ubiquitous connectivity across the 6G communication platforms, application-based traffic steering across the access networks, high automation levels on the network edge, and dynamic network slicing.

ML-based analytics network decision making allows integration within the wireless technology to provide more efficient approaches to optimize network performance, resulting in a reduction of capital expenditures (CapEx), operational expenditures (OpEx), energy consumption, and increased Quality of Experience (QoE).

Currently, wireless systems orchestration is mainly based on simple network analytics and inaccurate/suboptimal mathematical models. Instead, ML can provide model-agnostic solutions that automatically and dynamically adapt to optimize key metrics (Ali et al., 2020). Other uses include optimizing or improving specific tasks, such as replacing brute force methods or heuristics. To manage and maintain large-scale telecommunication networks, mobile network operators rely on a complex system of solutions that can gradually embrace algorithms driven by Artificial Intelligence (AI) for scheduling and orchestration purposes, which require the computational power of fog and cloud environments to efficiently deal with the large amounts of multi-dimensional data, e.g., originating from the highly dynamic traffic patterns of mobile end users. For instance, the performance of a cellular network is dynamic; it changes over time, it is prone to hardware and software failures, and it is affected by regular (e.g., holiday events, seasonal changes) and irregular events (e.g., traffic, weather conditions, flash crowds).

There have been many applications of ML and deep learning on 5G/6G wireless networks (Mao et al., 2018; Zhao et al., 2020; Patil et al., 2022). With regards to network management, AI techniques have involved the design and resource allocation in wireless communications (HO et al., 2019). Specifically, ML algorithms applied to networks can be classified into three main classes, namely supervised learning, unsupervised learning, and reinforcement learning (RL), see (Syed et al., 2019) for a review. Supervised learning has applications in both the physical and network layers and can be deployed for caching, traffic classification, and delay mitigation, and some other applications related to these layers (Piran et al., 2019). Unsupervised learning has been applied to problems such as routing, coding and modulation, channel modeling, traffic optimization, parameter prediction in the network layer, and anomaly detection for both enhanced security and predictive maintenance.

Deep RL applications include network availability optimization, scheduling, transmission optimization, on-demand beamforming, traffic prediction, packet scheduling, and multi-objective routing (Piran et al., 2019; Shafin et al., 2019). To manage the ever-increasing connectivity density, a correct handling of the allocated spectrum is necessary, accounting for scarcity and underutilization. This requires dynamic techniques, such as symbiotic radio, cognitive radio and blockchain technology (Hong et al., 2014; Hewa et al., 2020).

Federated learning-based analytics

In recent years, networks have been increasingly becoming decentralized, making (privacy preserving) Federated Learning (FL) arise as another promising direction, by facilitating mobile devices to collaboratively learn a shared ML model without data exchange among them (Marmol et al., 2021). With regards to FL, it can enable the 6G shift from a centralized cloud-based system to a decentralized system spread across the cloud-edge continuum (Letaief et. al., 2019; Shafin et al., 2019; Tariq et al., 2020). Also, FL can allow the deployment of generalized models across many devices (Cousik et al., 2019) by distributing the training tasks to multiple decentralized edge nodes.
However, FL requires the coordination of a central server that orchestrates the training, the client's selection, the updates collection, and weights aggregation. This server constitutes a centralized authority that (1) users are forced to blindly trust to protect them from various information leakage attacks (Hitaj et al., 2017; Melis

et al., 2018), where malicious participating clients can de-anonymize sensitive training data through observation and isolation of a victim's model updates, while at the same time (2) such centralized service is a single point of failure, which can become a bottleneck hindering the overall system scalability and performance (Lian et al., 2017). To address these emerging issues, existing approaches either use (1) differential privacy (Bellet et al., 2018), thus decreasing the utility of the shared gradients, or (2) specialized hardware (e.g., Trusted Execution Environments (Mo et al., 2021)).

Reinforcement learning for network performance optimization

RL has attracted much interest among the networking community. RL algorithms are generally relevant for multi-objective high dimensional combinatorial optimization problems. These include mobile handover in cellular networks, MIMO processing, VNF-FG placement, coding scheme selection, modulation, beam forming, and power control, among others. As such, it has been broadly explored for a plethora of classical network-related problems (Luong et al., 2019; Tanveer et al., 2022). Among these problems, mobility management is a pivotal aspect in cellular networks. Next, we describe some of the most relevant works in this area.

Sana et al. (Sana et al., 2020, Sana et al., 2020b) propose a multi-agent reinforcement learning (MARL) framework respectively applied to user association, and handover optimization in cellular networks. In these works, agents are deployed on User Equipment (UE), and their objective is to optimize the global network sum-rate (i.e., the total data rate exchanged between UEs and base stations). Other works consider the case of multi-objective optimization. For example, in Li et al. (2017) the authors propose ORLA, an online RL algorithm applied to user association in vehicular networks. Agents are deployed in cells, and they seek to maximize the users' service rate while minimizing the variance across users. Agents collect historical information of user associations in their own cells, but they do not exchange state information between them. Similarly, in Dinh et al. (2021) the authors follow a similar approach for handover optimization in dense mmWave networks. They propose to distribute agents on UEs, and agents seek to jointly optimize cell-user associations and the beamforming configuration in MIMO antennas. Also, Ding et al. (2020) propose a multi-agent DQN-based framework for user association and power control in heterogeneous networks. Agents are deployed on UEs and they aim to optimize energy efficiency on UEs (i.e., ratio between throughput and power consumption). Likewise, Guo et al. (2020) uses a multi-agent Proximal Policy Optimization (PPO) algorithm to maximize the overall throughput while reducing the handover frequency between cells. Agents are deployed on UEs, and they jointly optimize handovers and power allocation. Lastly, Shao et al. (2021) propose a novel method based on RL and Graph Attention Networks. In contrast to the previous works, here the authors propose a multi-agent system where agents are deployed in base stations and exchange information between them. Particularly, this system is applied to distributed slicing resource management in dense cellular networks.

Work Package 4 (WP4): Machine Learning-based Privacy Preserving Analytics

Activity 8: Native privacy-preserving machine learning algorithms for localization (IMDEA)

Description: To initiate the development of privacy-preserving machine learning algorithms for localization, we have started to deploy a 5G test bed using OpenAirInterface open-source software. In this task, this test bed allows us to perform localization of User Equipment (UE) using conventional methods such as the Closed-Form and NNLS/Brute-Force algorithms.

Having accomplished this initial phase, our subsequent focus is to apply machine learning techniques that prioritize privacy in order to determine the user's position. By incorporating privacy-preserving machine learning algorithms into the localization process, we aim to enhance the security and confidentiality of user data while still achieving accurate localization results.

From Experiments to Insights: A Journey in 5G New Radio Localization

In this work, we present an efficient methodology for deploying an experimental setup with three gNBs. Our objective is to assess and validate algorithms and research findings by utilizing over-the-air measurements of 5G localization signals. We take into consideration standardized localization procedures and real-world operating conditions. To begin with, we perform a comprehensive analysis of the existing landscape of open-source platforms and associated hardware for 5G localization. This analysis sheds light on the key technical components involved. Subsequently, we showcase the effectiveness of a testbed focused on positioning reference signals (PRS) for 5G localization. This testbed utilizes an open-source platform based on PRS technology. *This study has been accepted for presentation at the 21st Mediterranean Communication and Computer Networking Conference (MedHoc Net 2023).*

When examining the open-source platforms, our focus is on describing the primary open-source software (SW) platforms and tools that are available for implementing a 5G Standalone (SA) mobile network infrastructure. This includes both the Next Generation Radio Access Network (NG-RAN) and the 5G Core Network (5GCN). We aim to provide an overview of the main open-source solutions that can be utilized to develop and deploy a 5G SA network, encompassing both the radio access and core network components.

Primary open-source software (SW) platforms

i. OpenAirInterface: The OpenAirInterface (OAI) offers 5G Core, gNB, and UE implementations that are compliant with NR Release 15/16. The source code of OAI is developed in C programming language, prioritizing real-time performance requirements. It is important to note that the distribution of the OAI source code is governed by the OAI Public License, which outlines the terms and conditions for its usage and distribution.

ii. srsRAN: The srsRAN platform is considered to be the most similar to OAI in terms of functionality. Like OAI, srsRAN provides software implementations of the gNB and UE, supporting features up to NR Release 15. However, unlike OAI, srsRAN does not include its own implementation of the 5G Core Network (5GCN). Instead, it relies on Open5GS, which is an open-source implementation of the 5G Core conforming to 3GPP Release 16. Open5GS is written in the C programming language. In terms of programming languages, srsRAN is written in both C and C++. It is important to note that the distribution of srsRAN is subject to the GNU AGPLv3 license, which specifies the terms and conditions for its usage and distribution.

iii. Aether: Aether is a project endorsed by the Open Networking Foundation (ONF) with a focus on implementing private cellular networks. Unlike OAI and srsRAN, Aether goes beyond providing implementations of just the Radio Access Network (RAN) and 5G Core Network (5GCN). While it includes these components, Aether aims to provide a comprehensive solution for private cellular networks, encompassing additional functionalities and features. Aether's RAN is based on OAI.

Among the options of OAI, srsRAN, and Aether, it is worth noting that OAI is considered the most advanced platform. It is directly implemented in our experimental setup, indicating its suitability for our specific needs and requirements. The decision to utilize OAI highlights its level of development and readiness for practical implementation in our experimental environment.

Experimental setup

To conduct 5G PRS (Positioning Reference Signal) Time of Arrival (TOA) measurements, the DL-TDOA technique is employed. This technique utilizes the PRS signal transmitted by a group of neighboring gNBs (base stations) and received by the UE (user equipment). By measuring the relative timing difference (RSTD) or Time Difference of Arrival (TDOA) between each pair of gNBs, the UE's position can be estimated. The estimation of the UE's position is achieved through multilateration or trilateration calculations, which are based on the principles of hyperbolic geometry. These calculations utilize the measured timing differences between the PRS signals received from different gNBs to determine the position of the UE in the 5G network.

So outdoor measurements were conducted together with our partners at the University of Rome, Tor Vergata. These measurements are carried out under optimal conditions, ensuring clear visibility of GPS satellites for accurate synchronization. The experimental testbed area, depicted in Figure 1, encompasses an area of nearly 60 square meters. It is important to note that all tests are conducted in an environment where there are no humans in close proximity to minimize any potential interference. We use 13 different selected UE locations to test our experimental positioning system as shown in Figure 1 (right).

In the experimental localization testbed, the 5G NR (New Radio), Time Division Duplex (TDD) channel was set up using the N78 frequency band, which operates at 3500 MHz. The channel configuration included an instantaneous bandwidth of 80 MHz, which corresponds to 217 Resource Blocks (RBs). Additionally, a subcarrier spacing of 30 kHz was utilized in the testbed to facilitate the transmission and reception of signals for localization purposes. We use Software Defined Radios (SDRs) comprises four USRP X310 devices, three as gNBs and one as a UE.

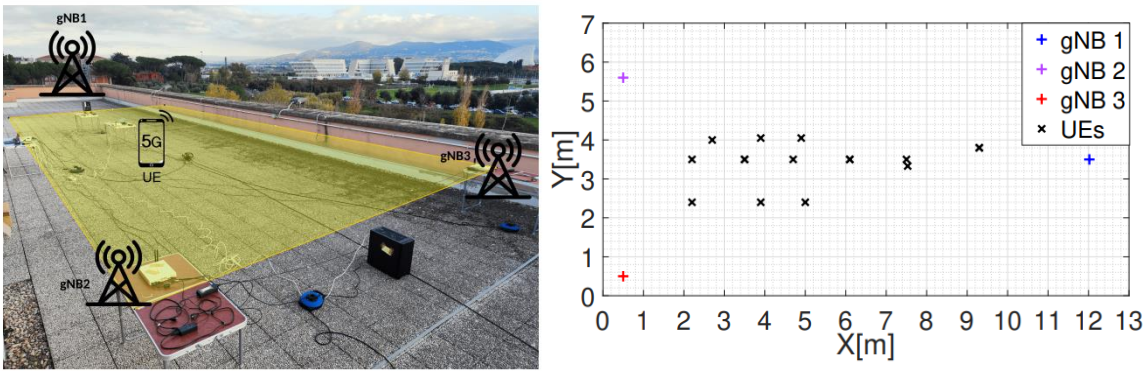

Figure 1: Outdoor scenario and floor map representation where measurements are performed.

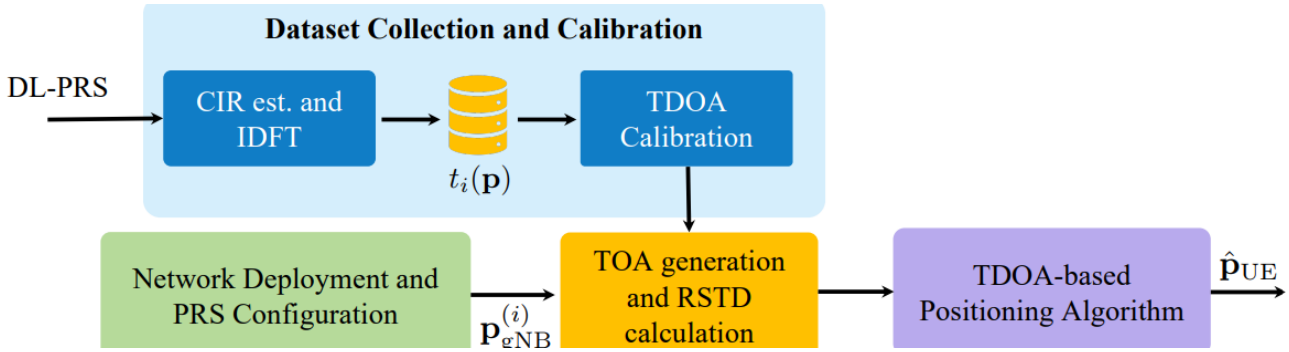

Figure 2: Illustration of the main step for dataset collection, calibration, and TDOA-based positioning, CIR is the Channel Impulse Response estimation and IDFT is the Inverse Discrete Fourier Transform, RSTD is the Reference Signal Timing Difference

The data was then collected and calibrated according to Figure 2, and then the UE measured the reference signal timing difference (RSTD) or TDOA of the PRS positioning signal from two base stations to estimate it's position, i.e., time difference of arrival from gNB 1-2, gNB 1-3, and gNB 2-3.

Evaluation and Results

In our evaluation of localization accuracy, we assessed the performance of several algorithms: the Closed-Form Solution, Brute-Force, and Non-Linear Least Squares (NLLS). The Closed-Form Solution involves algebraically solving Time Difference of Arrival (TDOA) equations. For a 2D scenario, this method requires three receivers to accurately determine the position.

On the other hand, both the Brute-Force and NLLS algorithms aim to minimize the 2-norm discrepancy between the predicted and estimated TDOA values. They iteratively search for the optimal solution by adjusting the position estimates.

These algorithms were utilized to gauge the accuracy of localization in our experimental setup, allowing us to compare their performance and determine the most effective approach.

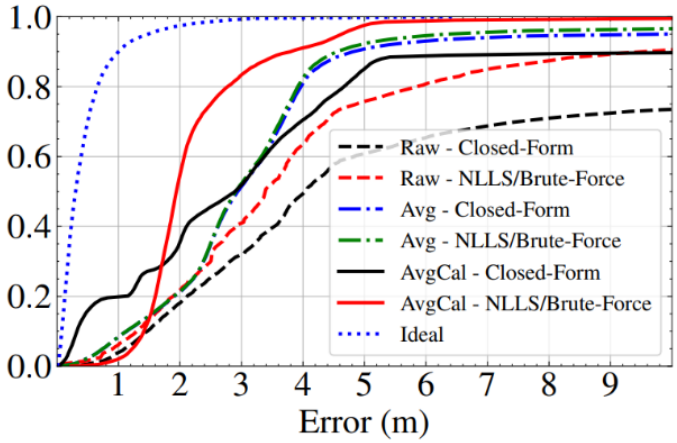

Figure 3: CDF of the positioning error varying the localization algorithm

In Figure 3, it is shows that Closed-Form algorithm deteriorates while the NNLS/Brute-Force algorithms exhibit significant improvement, achieving a positioning error of approximately 3m in 90% of cases.

Activity 9: Scalable and distributed privacy-preserving algorithms (Telefónica)

Description: In the scope of this task, we will be investigating the so-called Privacy-Preserving Machine Learning (PPML) algorithms and various adversarial attacks that can be mounted on the data, models, systems, and networks building and using them. The reason is because recent academic and industrial studies have demonstrated that adversaries can execute various types of attacks to retrieve sensitive information from the parameters of the ML model built, and the data used. Prominent examples of such attacks are various types of inference attacks, as well as data reconstruction and poison attacks. Motivated by these attacks, researchers have recently introduced several countermeasures to prevent them. Existing solutions can be grouped into three main categories depending on whether they rely on: (i) homomorphic encryption, (ii) multi-party computation (MPC) or (iii) differential privacy (DP). However, these solutions suffer from important privacy or performance limitations, or negatively affect the utility or fairness of the model.

Federated Learning (FL)

In this task, we focus on studying a PPML method called Federated Learning (FL) in McMahan et al. (2016) which has several benefits and allows us to get closer to the design of an ideal PPML algorithm that trains an ML model useful for central or distributed parties, without exposing data or model to unauthorized parties. In FL, the data required for training ML models are not explicitly exchanged between parties (clients and server). Instead, the model training is distributed among devices (clients) that have access to their local data shards for training local models. The global server receives these local models and performs aggregation and create a global FL model.

Compared to centralized approaches, FL has a larger attack surface due to:

i. Data distribution: Training data is distributed across multiple devices, increasing the risk of data breaches or attacks on individual devices with varying security levels.

ii. Communication channels: Communication between the central server and participating devices occurs over potentially insecure networks, making it susceptible to interception, eavesdropping, or man-in-the-middle attacks.

iii. Client-side vulnerabilities: Vulnerabilities in client or edge devices can be exploited, compromising the integrity of the training process.

iv. Aggregation and model updates: The central server aggregates model updates, making the aggregation process a potential vulnerability. Malicious clients could manipulate or poison updates, leading to compromised or biased global models.

v. Privacy concerns: While FL aims to improve data privacy by avoiding the need to share raw data for training models, attacks aiming to compromise training data privacy can still be successful.

To mitigate these risks and reduce the attack surface, robust privacy and security measures should be implemented. These include secure communication protocols, encryption, device authentication, access controls, privacy-preserving and fairness guaranteeing machine learning methods, and regular security audits.

Differential Privacy

Differential Privacy (DP) was proposed by Dwork et al. (2014) to define DP, we let ε be a positive real number, and A be a randomized algorithm that takes a dataset as input. The algorithm A is said to provide ε-DP if, for all datasets D1 and D2 that differ on a single element, and all subsets O of the outcomes of running A:

$$\Pr[\mathcal{A}(D_1) \in \mathbf{O}] \leq e^{\varepsilon} \cdot \Pr[\mathcal{A}(D_2) \in \mathbf{O}]$$

where the probability is over the randomness of the algorithm A. ε is also known as the privacy budget. DP is achieved by adding noise chosen from a specific distribution to provide the indistinguishability guarantee mentioned earlier in Balle et al. (2018) and Geng et al. (2015). The traditional model of DP defined earlier, also known as the central DP (CDP) model, implicitly assumes the existence of a trusted entity that does not deviate from protocol specification and adds the calibrated noise to provide the DP guarantee. Thus, the outcomes are DP by post-processing. However, such assumptions may not always hold in all settings. To alleviate these strong trust assumptions, local DP (LDP)5 assumes that each data contributor adds the noise locally, i.e., in-situ. This ensures that the inputs themselves are DP, and any function calculated atop of it is DP by post-processing. Naturally, such a mechanism has limited knowledge of the overall function being computed on all the data and overestimates the amount of noise required to provide privacy. The relationship between LDP and CDP is dependent on the mechanism used to achieve DP. For example, the Laplacian mechanism2 ensures that ε-LDP also provides ε-CDP. In this task, we plan to make use of DP and its different variants to design effective and efficient, privacy-preserving ML algorithms.

Federated Learning with Differential Privacy

McMahan et al. (2017) propose the first approach where DP can be combined with FL to provide formal privacy guarantees. Similar ideas are proposed in the work of Geyer et al. (2017). Bonawitz et al. (2016, 2017) propose the notion of secure aggregation, a variant of MPC which provides the central aggregator an

aggregated view of all gradients (noisy/non-noisy) from the clients. Truex et al. (2018) combine advances from LDP and MPC (through thresholding cryptography schemes) to provide a hybrid scheme to provide better privacy. Truex et al. (2020) also propose an approach using LDP. However, they formulate this based on an alternative DP definition. In this task, we plan to make use of the technologies of FL with DP and the different variants that can be produced, to design effective and efficient, privacy-preserving ML algorithms that are executed in a decentralized/federated fashion.

Hierarchical Federated Learning (HFL)

Abad et al. (2019) propose a mechanism to ensure communication-efficient and coordinated learning in the context of HFL. Here, the notion of hierarchies stems from the presence of clients communicating with small base stations (or cellular towers) which act as intermediaries, who further communicate with macro base stations (or the central aggregator). Similarly, Yuan et al. (2020) also propose a new protocol to optimize for communication efficiency in the LAN-WAN setting. This form of HFL is significantly different from that proposed by Briggs et al. (2020) which aims to segregate clusters of similar clients which can be independently trained on heterogeneous models. Across these prior works, the actors are consistent: there are the federated clients as in the status quo.

In this task, we plan to make use of the implicit and explicit hierarchies that exist in nowadays networks, as well as the aforementioned technologies of FL with DP and their different variants, to design scalable, hierarchical-based, privacy-preserving ML algorithms that are executed in a decentralized/federated fashion.

Adversarial Attacks

It is important within this project and task to define what are the possible attacks we anticipate in FL systems and models. Next, we list such attacks that we must consider, as identified in literature:

i. Targeted attacks (backdoor attacks) such as Input-instance and pattern key strategies
ii. Untargeted attacks such as Byzantine attacks
iii. Data-poisoning attacks (DPA)
iv. Model-poisoning attacks (MPA)
v. Distribution inference attacks (DIA)
vi. Property and Attribute inference attacks (PIA & AIA)
vii. Membership inference attacks (MIA)
viii. Reconstruction attacks (RA)

The PPML methods we design within this project and task will have to take such attacks into account, and offer solutions to the attacks that are relevant for the considered experimental and operational settings and threat models.

Performance Metrics

To assess the performance of the PPML methods we design within this project and task, we plan to take into account the following metrics, grouped in the type of dimension they focus on. The following is not an exhaustive list, and we will adapt it depending on design of the PPML methods, use cases and data

considered, etc.:

i. ML model performance such as Test Accuracy, Test Area Under Curve, F1 Score, Precision, Recall

ii. Privacy performance such as Epsilon and Clipping used in DP for defining privacy guarantees.

iii. Fairness performance such as Disparate Impact, Equality of Opportunity, Equalized odds, etc

iv. System performance such as Communication cost, Computational cost, Scalability, Asynchronicity

Experimental Models

In order to assess the performance of the PPML methods we design within this project and task, using the metrics proposed above, we plan to execute various types of experiments, using existing, state of art models. Some examples can be found next from open-source repositories such as:

i. TensorFlow Repository (https://github.com/tensorflow/models/tree/master/official)

ii. Kaggle Repository (https://www.kaggle.com/models)

Experimental Datasets

In order to assess the performance of the PPML methods we design within this project and task, using the metrics proposed above, we plan to execute various types of experiments, using existing, state of art benchmark datasets. Some examples can be found next from open-source repositories (TensorFlow (https://research.google/resources/datasets/), Kaggle (https://www.kaggle.com/datasets), etc.)

References

Abad, M.S., Ozfatura, E., Gündüz, D., & Erçetin, Ö. (2019). Hierarchical Federated Learning ACROSS Heterogeneous Cellular Networks. ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 8866-8870.

Arapakis, I., Papadopoulos, P., Katevas, K., & Perino, D. (2023). P4L: Privacy Preserving Peer-to-Peer Learning for Infrastructureless Setups. ArXiv, abs/2302.13438.

Ali, S., Saad, W., & Rajatheya, "6G White Paper on Machine Learning in Wireless Communication Networks", arXiv:2004.13875v1, 2020.

Balle, B., & Wang, Y. (2018). Improving the Gaussian Mechanism for Differential Privacy: Analytical Calibration and Optimal Denoising. International Conference on Machine Learning.

Bellet A., Guerraoui R., Taziki M., and Tommasi M. Personalized and private peer-to-peer machine learning. In AISTATS'18.

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical Secure Aggregation for Privacy-Preserving Machine Learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2016). Practical Secure Aggregation for Federated Learning on User-Held Data. ArXiv, abs/1611.04482.

Briggs, C., Fan, Z., & András, P. (2020). Federated learning with hierarchical clustering of local updates to improve training on non-IID data. 2020 International Joint Conference on Neural Networks (IJCNN), 1-9.

Cheng H.-P., Yu P., Hu H., Zawad S., Yan F., Li S., Li H., and Chen Y.. Towards decentralized deep learning with differential privacy. In CLOUD'19.

Cousik T., Shafin R., Zhou Z., Kleine K., Reed J., and Liu L., "CogRF: A new frontier for machine learning and artificial intelligence for 6G RF systems," arXiv:1909.06862, 2019.

Ding, Hui, et al. "A deep reinforcement learning for user association and power control in heterogeneous networks." Ad Hoc Networks 102 (2020): 102069.

Dinh, Thi Ha Ly, et al. "Deep reinforcement learning-based user association in sub6ghz/mmwave integrated networks." 2021 IEEE CCNC.

Dwork, Cynthia and Aaron Roth. "The Algorithmic Foundations of Differential Privacy." Found. Trends Theor. Comput. Sci. 9 (2014): 211-407.

Geng, Quan et al. "The Staircase Mechanism in Differential Privacy." IEEE Journal of Selected Topics in Signal Processing 9 (2015): 1176-1184.

Geyer, R.C., Klein, T., & Nabi, M. (2017). Differentially Private Federated Learning: A Client Level Perspective. ArXiv, abs/1712.07557.

Guo, Delin, et al. "Joint optimization of handover control and power allocation based on multi-agent deep reinforcement learning." IEEE Transactions on Vehicular Technology 69.11 (2020): 13124-13138.

Hewa, T., Gurkan, G., Kalla, A., & Ylianttila, "The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions", 2nd 6G wireless Summit (6G SUMMIT), DOI: 10.1109/6GSUMMIT49458.2020.9083784, 2020

Hitaj B., Ateniese G., and Perez-Cruz F. Deep models under the gan: Information leakage from collaborative deep learning. In CCS '17.

Ho T., Tran T., Nguyen T., Kazmi S., Le L., Hong C., and Hanzo L., "Next-generation wireless solutions for the smart factory, smart vehicles, the smart grid and smart cities," arXiv preprint arXiv:1907.10102, 2019.

Hong, X., Jing, W., & Jianghong, S. (2014). Cognitive radio in 5G: a perspective on energy-spectral efficiency trade–off. IEEE communications Magazine. DOI: 10.1109/MCOM.2014.6852082.

Letaief K., Chen W., Shi Y., Zhang J., and Zhang Y., "The roadmap to 6G: AI empowered wireless networks," IEEE Communications Magazine, vol. 57, no. 8, pp. 84–90, 2019.

Li, L. et al., "A Measurement Study on TCP Behaviors in HSPA+ Networks on High- speed Rails", INFOCOM, 2015

Li, Zhong, Cheng Wang, and Chang-Jun Jiang. "User association for load balancing in vehicular networks: An online reinforcement learning approach." IEEE Transactions on Intelligent Transportation Systems 18.8 (2017): 2217-2228.

Lian X., Zhang C., Zhang H., Hsieh C.-J., Zhang W., and Liu J.. Can decentralized algorithms outperform centralized algorithms? a case study for decentralized parallel stochastic gradient descent. In NIPS'17

Luong, Nguyen Cong, et al. "Applications of deep reinforcement learning in communications and networking: A survey." IEEE Communications Surveys & Tutorials 21.4 (2019): 3133-3174.

Mao Q., Hu F., and Hao Q., "Deep learning for intelligent wireless networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2595–2621, 2018.

Marmol Campos, Enrique & Saura, Pablo & González Vidal, Aurora & Hernández-Ramos, José & Bernal Bernabe, Jorge & Baldini, Gianmarco & Skarmeta, Antonio. (2021). "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges". Computer Networks. 203. 108661. 10.1016/j.comnet.2021.108661, arXiv:2108.00974v1.

McMahan, H.B., Ramage, D., Talwar, K., & Zhang, L. (2017). Learning Differentially Private Language Models Without Losing Accuracy. ArXiv, abs/1710.06963.

McMahan, H. B., Eider Moore, Daniel Ramage, Seth Hampson and Blaise Agüera y Arcas. "Communication-Efficient Learning of Deep Networks from Decentralized Data." International Conference on Artificial Intelligence and Statistics (2016).

Melis L., Song C., Cristofaro E. De, and Shmatikov V.. Inference attacks against collaborative learning. arXiv preprint arXiv:1805.04049, 2018.

Mo F., Haddadi H., Katevas K., Marin E., Perino D., and Kourtellis N.. Ppfl: Privacy-preserving federated learning with trusted execution environments. In MobiSys'21.

Pappas C., Chatzopoulos D., Lalis S. and Vavalis M., "IPLS: A Framework for Decentralized Federated Learning," 2021 IFIP Networking Conference (IFIP Networking), Espoo and Helsinki, Finland, 2021, pp. 1-6, doi: 10.23919/IFIPNetworking52078.2021.9472790.

Patil A., Iyer S. and Pandya R., "Machine Learning Algorithms for 6G Wireless Networks: A Survey", 10.4018/978-1-6684-3921-0.ch003, 2022

Piran M. and Suh D., "Learning-Driven wireless communications, towards 6G," in 2019 International Conference on Computing, Electronics and Communications Engineering (ICCECE). IEEE, 2019, pp. 219 224.

Sana, Mohamed, et al. "Multi-agent reinforcement learning for adaptive user association in dynamic mmWave networks." IEEE Transactions on Wireless Communications 19.10 (2020): 6520-6534.

Sana, Mohamed, et al. "Multi-agent deep reinforcement learning for distributed handover management in dense mmWave networks." ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2020.

Shafin R., Liu L., Chandrasekhar V., Chen H., Reed J., and Zhang J., "Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G," arXiv:1907.07862, 2019.

Shao, Yan, et al. "Graph attention network-based multi-agent reinforcement learning for slicing resource management in dense cellular network." IEEE Transactions on Vehicular Technology 70.10 (2021): 10792-10803.

Shayan M., Fung C., Yoon C. J. M., and Beschastnikh I.. Biscotti: A ledger for private and secure peer-to-peer machine learning, 2019.

6G European vision, 2021. https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf

Soualah O., et al. “A monitoring aware strategy for 5g core slice embedding,” in Proc. of AINA 2021.

Syed, J.N., Shree, K.S., Shurjeel, W., Mohammad, N., & Md. Asaduzz, A. (2019). Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future. IEEE Access, 7: 46317-46350.

Tanveer, Jawad, et al. "An overview of reinforcement learning algorithms for handover management in 5G ultra-dense small cell networks." Applied Sciences 12.1 (2022): 426.

Tariq F., Khandaker M., Wong K., Imran M., Bennis M., and Debbah M., “A speculative study on 6G,” IEEE Wireless Communications, vol. 27, no. 4, pp. 118–125, 2020.

Truex, S., Liu, L., Chow, K., Gursoy, M.E., & Wei, W. (2020). LDP-Fed: federated learning with local differential privacy. Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking.

Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., & Zhang, R. (2018). A Hybrid Approach to Privacy-Preserving Federated Learning. Informatik Spektrum, 42, 356 - 357.

Yuan, J., Xu, M., Ma, X., Zhou, A., Liu, X., & Wang, S. (2020). Hierarchical Federated Learning through LAN-WAN Orchestration. ArXiv, abs/2010.11612.

Zhao, Y., Zhai, W., Zhao, J., Zhang, T., Sun, S., Niyato, D., & Yan Lam, K. (2020). “A Survey of 6G Wireless Communications: Emerging Technologies”. arXiv:2004.08549v3.