

A Collaborative Learning Framework via Federated Meta-Learning

Sen Lin, Guang Yang and Junshan Zhang

School of EECE, Arizona State University, Tempe, AZ 85287

Abstract—Many IoT applications at the network edge demand intelligent decisions in a real-time manner. The edge device alone, however, often cannot achieve real-time edge intelligence due to its constrained computing resources and limited local data. To tackle these challenges, we propose a platform-aided collaborative learning framework where a model is first trained across a set of source edge nodes by a federated meta-learning approach, and then it is rapidly adapted to learn a new task at the target edge node, using a few samples only. Further, we investigate the convergence of the proposed federated meta-learning algorithm under mild conditions on node similarity and the adaptation performance at the target edge. To combat against the vulnerability of meta-learning algorithms to possible adversarial attacks, we further propose a robust version of the federated meta-learning algorithm based on distributionally robust optimization, and establish its convergence under mild conditions. Experiments on different datasets demonstrate the effectiveness of the proposed Federated Meta-Learning based framework.

I. INTRODUCTION

Since most of IoT devices reside at the network edge, pushing the AI frontier to achieve real-time edge intelligence is highly nontrivial, due to the requirements in performance, cost and privacy. Clearly, the conventional wisdom of transporting the data bulks from the IoT devices to the cloud datacenters for analytics would not work well, simply because the requirements in terms of high bandwidth and low latency would be extremely demanding and stringent. As a result, it is anticipated that a high percentage of IoT data will be stored and processed locally. However, running AI applications directly on edge devices to process the IoT data locally, if not designed intelligently, would suffer from poor performance and energy inefficiency, simply because many AI applications typically require high computational power that greatly outweighs the capacity of resource- and energy-constrained IoT devices. To address the above challenges, edge computing has recently emerged, and the marriage of edge computing and AI has given rise to a new research area, namely edge intelligence or edge AI [1] [2].

It is highly challenging for a single edge node alone to achieve real-time edge intelligence. A key observation is that learning tasks across edge nodes often share some similarity, which can be leveraged to tackle these challenges. With this insight, we propose a platform-aided collaborative learning framework where the model knowledge is learnt collaboratively by a federation of edge nodes, in a distributed manner, and then is transferred via the platform to the target edge node for fine-tuning with its local dataset. Then, the next key

question to ask is “What knowledge should the federation of edge nodes learn and be transferred to the target edge node for achieving real-time edge intelligence?”

Federated learning has recently been developed for model training across multiple edge nodes, where a single global model is trained across all edge nodes in a distributed manner. It has been shown that limited performance is achieved when fine-tuning the global model for adaptation to a new (target) edge node with a small dataset [3]. Along a different line, federated multi-task learning [4] has been proposed to train different but related models for different nodes, aiming to deal with the model heterogeneity among edge nodes. In particular, every source edge node, which is also a target edge node, is able to learn a unique model through capitalizing the computational resource and data belonging to other nodes. This, however, inevitably requires intensive computation and communications and is time-consuming, and hence could not meet the latency requirement for real-time edge intelligence.

Building on the recent exciting advances in meta-learning [5] [6], in this paper we propose a federated meta-learning approach to address the questions mentioned above. The underlying rationale behind meta-learning is to train the model’s initial parameters over many tasks, such that the pre-trained model can achieve maximal performance on a new task after quick adaptation using only a small amount of data corresponding to that new task. Thus inspired, we advocate a federated meta-learning approach where all source edge nodes collaboratively learn a global model initialization such that maximal performance can be obtained with the model parameters updated with only a few data samples at the target edge node, thereby achieving real-time edge intelligence.

Different from meta-learning which requires the knowledge of the task distribution [6], the federated meta-learning proposed in this work removes this assumption, by making use of the fact that different edge nodes often have distinct local models while sharing some similarity, and it can automate the process of task construction because each edge node is continuously making intelligent decisions. Further, the federated meta-learning eliminates the need of centralized computation and thus offers the flexibility to strike a good balance between the communication cost and local computation cost (e.g., via controlling the number of local update steps).

The main contributions in this paper can be summarized as follows.

- We propose a platform-aided collaborative learning framework where a model is first trained by a federated

meta-learning approach across multiple edge nodes, and then is transferred via the platform to the target edge node such that rapid adaptation can be achieved with the model updated (e.g., through one gradient step) with small local datasets, in order to achieve real-time edge intelligence. To the best of our knowledge, this is the first work to apply meta-learning to obtain real-time edge intelligence in a distributed manner.

- We study the convergence behavior of the federated meta-learning algorithm and examine the adaptation performance of the fine-tuned model at the target edge node. In particular, we are the first to investigate the impact of the node similarity and the number of local update steps on the convergence subject to communication and computation cost constraints. To establish the convergence, we impose bounds on the variations of the gradients and Hessians of local loss functions (with respect to the hyper-parameter) across edge nodes, thereby removing the assumption in meta-learning that requires all tasks follow a (known) distribution.
- To combat against the possible vulnerability of meta-learning algorithms, we propose a robust version of federated meta-learning, building on recent advances in distributionally robust optimization (DRO). We further show that the proposed algorithm still converges under mild technical conditions. To the best of our knowledge, this is the first work to exploit DRO for improving the robustness of meta-learning algorithms.
- We evaluate the performance of the proposed collaborative learning framework using different datasets, which corroborates the effectiveness of federated meta-learning and showcases the robustness of the DRO-based robust federated meta-learning.

II. RELATED WORK

The concept of meta-learning is not new, but the recent advances through gradient-based optimization bring it into the light again as a promising solution for fast learning. In particular, Finn et al. [6] propose one gradient-based algorithm called MAML, which directly optimizes the learning performance with respect to an initialization of the model such that even one-step gradient decent from that initialization can still produce good results on a new task. To circumvent the need of the second derivatives in MAML, Nichol et al. [7] propose a first-order method named Reptile, which is similar to joint training but surprisingly works well as a meta-learning algorithm. A similar meta-learning framework is studied by Chen et al. [8] for recommendation systems through assigning one task to every user, which nevertheless does not consider any system modeling in federated learning.

To the best of our knowledge, we are among the first to establish the convergence of (federated) meta-learning. During the preparation of this work, the preprint of one concurrent work [9] about convergence analysis of meta-learning algorithms became available online. It is worth noting that [9] studies the convergence of centralized MAML algorithms for

non-convex functions, whereas this paper focuses on the convergence and adaptation performance of the federated meta-learning algorithm with node similarity to achieve real-time edge intelligence in a federated setting, where multiple local update steps are allowed to balance the trade-off between the communication cost and local computation cost.

The susceptibility of meta-learning algorithms such as MAML to adversarial attacks is first investigated in [10]. And recently [11] also demonstrates the significant performance degradation of MAML with adversarial samples. To make meta-learning more robust, [11] proposes a meta-learning algorithm called ADML which exploits both clean and adversarial samples to push the inner gradient update to arm-wrestle with the meta-update. Unfortunately, this type of approaches are generally intractable. The DRO-based robust federated meta-learning algorithm proposed in this work is not only computationally tractable, but also resistant to more general perturbations, e.g., out-of-distribution samples. In addition, the trade-off between robustness and accuracy can be fine-tuned by the size of the distributional uncertainty set.

Federated learning is first proposed by McMahan et al. [12] which performs a variable number of local updates on a subset of devices to enable flexible and efficient communication patterns but without any theoretical convergence guarantee. Based on this, Wang et al. [13] analyze the convergence with fixed number of local updates for non-independent and identically distributed (i.i.d) data distributions across devices, and introduce a control algorithm to dynamically adapt the frequency of global aggregation to minimize the loss under fixed resource constraints. Departing from the need of manually tuning the number of local updates, Sahu et al. [14] propose a more generalized algorithm, so called FedProx, to tackle the statistical heterogeneity inherent in federated learning and characterize the convergence behaviour for non-convex loss functions. Notwithstanding, federated learning is not designed for fast learning with small datasets. In particular, federated learning intends to find a global model that fits the data as accurately as possible for all participating nodes, whereas federated meta-learning learns a model initialization, from which fast adaptation from even small datasets can still reach good performance, and also keeps the node heterogeneity in the sense that different models would be learnt for different nodes after quick adaptation from the global model initialization.

Both meta-learning and multi-task learning [15] [16] [4] aim to improve the learning performance by leveraging other related tasks. However, meta-learning focuses on the fast learning ability with small sample size and the performance improvement at the target (learning at the source is irrelevant), whereas multi-task learning tries to learn both the source and target tasks simultaneously and accurately. Besides, the model initialization learned by meta-learning can be fine-tuned with good performance on various target tasks using minimal data points, while multi-task learning may favor tasks with significantly larger amount of samples than others.

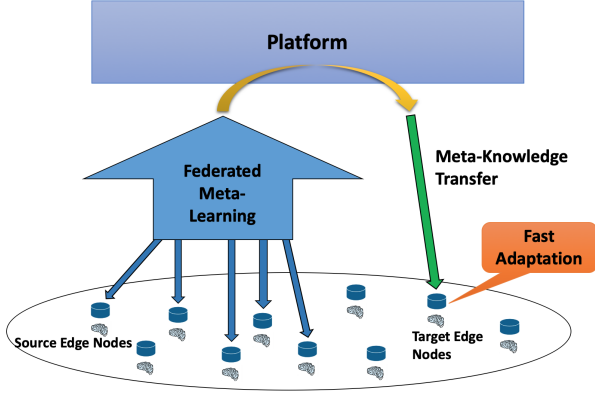


Fig. 1: A Platform-Aided Collaborative Learning Framework with Federated Meta-Learning for Real-Time Edge Intelligence.

III. FEDERATED META-LEARNING FOR ACHIEVING REAL-TIME EDGE INTELLIGENCE

As illustrated in Figure 1, we consider a platform-aided architecture where a set \mathcal{S} of source edge nodes (each with a task) join force for federated meta-learning, and the learned model would be transferred from the platform to a target edge node t (not in \mathcal{S}), for rapid adaptation based on its local data. The primary objective of the proposed federated meta-learning is to train a meta-model that can quickly adapt to the task at the target edge node to achieve real-time edge intelligence, using only a few local data points. To accomplish this, the meta-model is trained during a meta-learning phase across the source edge nodes in a distributed manner.

A. Problem Formulation

Specifically, we assume that the tasks across edge nodes follow a meta-model, represented by a parametrized function f_{θ} with parameters $\theta \in \mathbb{R}^d$. For source edge node $i \in \mathcal{S}$, let D_i denote its local dataset $\{(\mathbf{x}_i^1, \mathbf{y}_i^1), \dots, (\mathbf{x}_i^j, \mathbf{y}_i^j), \dots, (\mathbf{x}_i^{|D_i|}, \mathbf{y}_i^{|D_i|})\}$, where $|D_i|$ is the dataset size and $(\mathbf{x}^j, \mathbf{y}^j) \in \mathcal{X} \times \mathcal{Y}$ is a sample point with \mathbf{x}^j being the input and \mathbf{y}^j the output. We further assume that $(\mathbf{x}_i^j, \mathbf{y}_i^j)$ follows an unknown distribution P_i . Denote the loss function by $l(\theta, (\mathbf{x}^j, \mathbf{y}^j)) : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$. The empirical loss function for node i is then defined as

$$L(\theta, D_i) \triangleq \frac{1}{|D_i|} \sum_{(\mathbf{x}_i^j, \mathbf{y}_i^j) \in D_i} l(\theta, (\mathbf{x}_i^j, \mathbf{y}_i^j)), \quad (1)$$

which we write as $L_i(\theta)$ for brevity. Moreover, we use $L_w(\theta)$ to denote the overall loss function across all edge nodes in \mathcal{S} :

$$L_w(\theta) \triangleq \sum_{i \in \mathcal{S}} \omega_i L_i(\theta), \quad (2)$$

where $\omega_i = \frac{|D_i|}{\sum_{i \in \mathcal{S}} |D_i|}$ and the weight ω_i of each edge node depends on its own local data size.

In the same spirit as MAML, we consider that the target edge node t has K data samples, i.e., $|D_t| = K$. For each source edge node $i \in \mathcal{S}$, D_i is divided into two disjoint sets, the training set D_i^{train} and the testing set D_i^{test} , where $|D_i^{train}| = K$ (assuming $|D_i| > K$ for all $i \in \mathcal{S}$). Given the

model parameter θ , the edge node i first updates θ using one step gradient descent based on D_i^{train} :

$$\phi_i(\theta) = \theta - \alpha \nabla_{\theta} L(\theta, D_i^{train}), \quad (3)$$

with α being the learning rate, and then evaluates the loss $L(\phi_i, D_i^{test})$ for the updated model parameter ϕ_i based on D_i^{test} . It follows that the overall objective of the federated meta-learning is given by

$$\min_{\theta} \sum_{i \in \mathcal{S}} \omega_i L(\phi_i(\theta), D_i^{test}). \quad (4)$$

Intuitively, by considering how the test error on local testing datasets changes with respect to the updated model parameters, we aim to obtain a model initialization such that small changes in the model parameters, i.e., altering in the direction of the loss gradient, would lead to substantial performance improvements for any task across the edge nodes.

Departing from MAML which assumes that a distribution over tasks is given, we do not require such an assumption here. Instead, we will quantify the node similarity in terms of the variations of the gradients and Hessians of local loss functions with respect to the hyper-parameter. Worth noting is that without knowing the data, the platform cannot directly solve the problem (4).

B. Federated Meta-Learning (FedML)

Motivated by federated learning, we propose to solve the meta-learning objective (4) in a distributed manner, in the sense that each node locally updates the model parameter θ based on its own dataset and transmits the updated value to the platform for a global aggregation. To better utilize the local computing resource of edge nodes and reduce the communication cost between the platform and edge nodes which is often a significant bottleneck in wireless networks, each edge node is allowed to locally update θ for T_0 steps before uploading the results to the platform.

Federated Meta-Training across Source Nodes: More specifically, the platform transfers an initialized θ^0 to all nodes in \mathcal{S} at time $t = 0$. As outlined in Algorithm 1, there are two major steps:

- **Local Update:** For $t \neq nT_0$ where $n \in \mathbb{N}^+$, each node $i \in \mathcal{S}$ first updates θ_i^t using the training dataset D_i^{train} based on (3) and then locally updates θ_i^t again through evaluating ϕ_i^t on the testing dataset D_i^{test} :

$$\theta_i^{t+1} = \theta_i^t - \beta \nabla_{\theta} L(\phi_i^t, D_i^{test}), \quad (5)$$

where β is the meta learning rate and θ_i^{t+1} will be used as the starting point for the next iteration at node i .

- **Global Aggregation:** For $t = nT_0$, each node also needs to transmit the updated θ_i^{t+1} to the platform. The platform then performs a global aggregation to achieve θ^{t+1} :

$$\theta^{t+1} = \sum_{i \in \mathcal{S}} \omega_i \theta_i^{t+1}, \quad (6)$$

and sends θ^{t+1} back to all edge nodes for the next iteration.

The details are summarized in Algorithm 1.

Algorithm 1 Federated meta-learning (FedML)

Inputs: $M, K, T, T_0, \alpha, \beta, \omega_i$ for $i \in \mathcal{S}$

Outputs: Final model parameter θ

- 1: Platform randomly initializes θ^0 and sends it to all edge nodes in \mathcal{S} ;
 - 2: **for** $t = 1, 2, \dots, T$ **do**
 - 3: **for** each node $i \in \mathcal{S}$ **do**
 - 4: Compute the updated parameter with one-step gradient descent using D_i^{train} : $\phi_i^t = \theta_i^t - \alpha \nabla_{\theta} L(\theta_i^t, D_i^{train})$;
 - 5: Obtain θ_i^{t+1} based on (5) using D_i^{test} ; **//local update**
 - 6: **if** t is a multiple of T_0 **then**
 - 7: Send θ_i^{t+1} to the platform;
 - 8: Receive θ^{t+1} from the platform where θ^{t+1} is obtained based on (6);
 - 9: Set $\theta_i^t \leftarrow \theta^{t+1}$; **//global aggregation**
 - 10: **else**
 - 11: Set $\theta_i^t \leftarrow \theta_i^{t+1}$;
 - 12: **return** θ .
-

Fast Adaptation towards Real-time Edge Intelligence at

Target Node: Given the model parameter θ from the platform, the target edge node t can quickly adapt the model based on its local dataset D_t and obtain a new model parameter ϕ_t through one step gradient descent:

$$\phi_t = \theta - \alpha \nabla_{\theta} L(\theta, D_t). \quad (7)$$

In a nutshell, instead of training each source edge node to learn a global model as in federated learning, the source nodes join force to learn how to learn quickly with only a few data samples in a distributed manner, i.e., learn θ such that just one step gradient descent from θ can bring up a new model suitable for a specific target node. This greatly improves the fast learning capability at the edge with the collaboration among edge nodes.

IV. PERFORMANCE ANALYSIS

In this section, we seek to answer the following two key questions : (1) What is the convergence performance of the proposed federated meta-learning algorithm? (2) Can the fast adaptation at the target node achieve good performance?

A. Convergence Analysis

For ease of exposition, we define function $G_i(\theta) \triangleq L_i(\phi_i(\theta))$ and $G(\theta) \triangleq \sum_{i \in \mathcal{S}} \omega_i G_i(\theta)$ such that problem (4) can be written as:

$$\min_{\theta} G(\theta). \quad (8)$$

For convenience, we assume $T = NT_0$ and make the following assumptions to the loss function for all $i \in \mathcal{S}$:

Assumption 1. Each $L_i(\theta)$ is μ -strongly convex, i.e., for all $\theta, \theta' \in \mathbb{R}^d$,

$$\langle \nabla L_i(\theta) - \nabla L_i(\theta'), \theta - \theta' \rangle \geq \mu \|\theta - \theta'\|^2.$$

Assumption 2. Each $L_i(\theta)$ is H -smooth, i.e., for all $\theta, \theta' \in \mathbb{R}^d$,

$$\|\nabla L_i(\theta) - \nabla L_i(\theta')\| \leq H \|\theta - \theta'\|,$$

and there exist constant B such that for all $\theta \in \mathbb{R}^d$

$$\|\nabla L_i(\theta)\| \leq B.$$

Assumption 3. The Hessian of each $L_i(\theta)$ is ρ -Lipschitz, i.e., for all $\theta, \theta' \in \mathbb{R}^d$,

$$\|\nabla^2 L_i(\theta) - \nabla^2 L_i(\theta')\| \leq \rho \|\theta - \theta'\|.$$

Assumption 4. There exists constants δ_i and σ_i such that for all $\theta \in \mathbb{R}^d$

$$\|\nabla L_i(\theta) - \nabla L_w(\theta)\| \leq \delta_i \text{ and } \delta = \sum_{i \in \mathcal{S}} \omega_i \delta_i,$$

$$\|\nabla^2 L_i(\theta) - \nabla^2 L_w(\theta)\| \leq \sigma_i \text{ and } \sigma = \sum_{i \in \mathcal{S}} \omega_i \sigma_i.$$

Assumptions 1-2 are standard and hold in many machine learning applications, e.g., in logistic regression over a bounded domain and squared-SVM. Assumption 3 is concerned with the high-order smoothness of the local loss function at each edge node, which makes it possible to characterize the landscape of the local meta-learning objective function. Assumption 4 is imposed to capture the node similarity. Specifically, we impose the condition that the variations of the gradients and Hessians of local loss functions (with respect to the hyper-parameter) across edge nodes are upper bounded by some constant. Intuitively, a small (large) constant indicates that the tasks are more (less) similar, and this constant can be tuned over a wide range to obtain a general understanding. Further, for a task distribution with task gradients uniformly bounded above (as is standard), Assumption 4 follows directly because $\|\nabla L_i(\theta) - \nabla L_w(\theta)\|$ (also Hessian) can be viewed as the distance between a typical realization and the sample average. In a nutshell, the task similarity assumption here is more general and realistic than the assumption in meta-learning that all tasks follow a (known) distribution. It is worth noting that these assumptions do not trivialize the meta-learning setting.

To characterize the convergence behavior of the federated meta-learning algorithm, we first examine the structural properties of the global meta-learning objective $G(\theta)$. Next, we study the impact of the task similarity across different edge nodes on the convergence performance of the federated meta-learning, which is further complicated by multiple local updates at each node to reduce the communication overhead.

Convexity and Smoothness of the Federated Meta-Learning Objective Function: Based on Theorem 1 in [17], we first have the following result about the structural properties of function $G(\theta)$.

Lemma 1. Suppose Assumptions 1-3 hold. When $\alpha \leq \min\{\frac{\mu}{2\mu H + \rho B}, \frac{1}{\mu}\}$, $G(\theta)$ is μ' -strongly convex and H' -smooth, where $\mu' = \mu(1 - \alpha H)^2 - \alpha \rho B$ and $H' = H(1 - \alpha \mu)^2 + \alpha \rho B$.

Lemma 1 indicates that when the learning rate α is relatively small, the meta-learning objective function $G(\theta)$ formed by the one-step gradient descent on local datasets is as well-behaved as the local loss function.

Bounded Dissimilarity across Local Learning tasks: Next, we characterize the impact of the similarity across local learning tasks.

Theorem 1. *Suppose Assumptions 2 and 4 hold. Then there exists a constant C such that*

$$\|\nabla G_i(\theta) - \nabla G(\theta)\| \leq \delta_i + \alpha C(H\delta_i + B\sigma_i + \tau),$$

where $\tau = \sum_{i \in \mathcal{S}} \omega_i \delta_i \sigma_i$.

Given the bounded variance of gradients and Hessians of local loss functions, we can find upper bounds on the gradient variance of the local meta-learning objective functions, while still preserving the node heterogeneity. As a sanity check, if all the edge nodes have same data points, it follows that $\delta_i = \sigma_i = 0$ for all $i \in \mathcal{S}$. Consequently, all edge nodes have the same local learning objective.

Based on Lemma 1 and Theorem 1, we can have the following result about the convergence performance of the federated meta-learning algorithm.

Theorem 2. *Suppose that Assumptions 1-4 hold, and the learning rates α and β are chosen to satisfy that $\alpha \leq \min\{\frac{\mu}{2\mu H + \rho B}, \frac{1}{\mu}\}$ and $\beta < \min\{\frac{1}{2\mu'}, \frac{2}{H'}\}$. Then*

$$G(\theta^T) - G(\theta^*) \leq \xi^T [G(\theta^0) - G(\theta^*)] + \frac{B(1 - \alpha\mu)}{1 - \xi T_0} h(T_0),$$

where $\xi = 1 - 2\beta\mu' \left(1 - \frac{H'\beta}{2}\right)$, $h(x) \triangleq \frac{\alpha'}{\beta H'} [(1 + \beta H')^x - 1] - \alpha' x$, $\alpha' = \beta[\delta + \alpha C(H\delta + B\sigma + \tau)]$.

Intuitively, the term $\frac{B(1 - \alpha\mu)}{1 - \xi T_0} h(T_0)$ captures the error introduced by both task dissimilarity and multiple local updates through the function $h(T_0)$. Specifically, observe that $h(T_0)$ increases with δ and σ , which clearly indicates how the task similarity and the number of local update steps T_0 impact the convergence performance, i.e., given a fixed duration T the convergence error decreases with the task similarity while increasing with the number of local update steps when T_0 is large. Correspondingly, the platform is able to balance between the platform-edge communication cost and the local computation cost via controlling the number of local update steps T_0 per communication round, depending on the task similarity across the edge nodes.

Different from MAML, multiple local updates are allowed in Algorithm 1 to reduce the communication cost, which has nontrivial impact on the convergence behavior. As shown in Theorem 2, the convergence gap for federated meta-learning would be large if the number of local update steps T_0 is large even if the tasks are very similar. When $T_0 = 1$, i.e., each edge node only updates the model locally for one iteration, the term $\frac{B(1 - \alpha\mu)}{1 - \xi T_0} h(T_0)$ disappears because $h(1) = 0$. We have the following result for this case.

Corollary 1. *Suppose that Assumptions 1-4 hold, and the learning rates α and β are chosen to satisfy that $\alpha \leq \min\{\frac{\mu}{2\mu H + \rho B}, \frac{1}{\mu}\}$ and $\beta < \min\{\frac{1}{2\mu'}, \frac{2}{H'}\}$. When $T_0 = 1$, $G(\theta^T) - G(\theta^*) \leq \xi^T [G(\theta^0) - G(\theta^*)]$.*

B. Performance Evaluation of Fast Adaptation

The fast learning performance at the target edge node t depends on not only its local sample size D_t but also the similarity with the source edge nodes in the federated meta-learning. Denote θ_c as the output of the federated meta-learning at the platform and θ_c^* as the optimal meta-learning model. We assume that the convergence error $\|\theta_c - \theta_c^*\|$ of the federated meta-learning algorithm is upper bounded by ϵ_c . For convenience, we further define $L_t^*(\theta)$ as the local average loss over the underlying data distribution P_t :

$$L_t^*(\theta) \triangleq \mathbb{E}_{(\mathbf{x}_t^j, \mathbf{y}_t^j) \sim P_t} l(\theta, (\mathbf{x}_t^j, \mathbf{y}_t^j)). \quad (9)$$

Then, the empirical loss $L_t(\theta)$ is the sample average approximation of $L_t^*(\theta)$. Let $\phi_t = \theta_c - \alpha \nabla L_t(\theta_c)$ and $\phi_t^* = \arg \min L_t^*(\phi) = \theta_t^* - \alpha \nabla L_t^*(\theta_t^*)$. The following result characterizes the trade-off between the target-source similarity and local sample size.

Theorem 3. *Suppose $l(\theta, (\mathbf{x}_t^j, \mathbf{y}_t^j))$ is H -smooth with respect to θ for all $\theta \in \mathbb{R}^d$ and $(\mathbf{x}_t^j, \mathbf{y}_t^j) \sim P_t$. For any $\epsilon > 0$, there exist positive constants C_t and $\eta = \eta(\epsilon)$ such that with probability at least $1 - C_t e^{-K\eta}$ we can have*

$$\|L_t^*(\phi_t) - L_t^*(\phi_t^*)\| \leq \alpha H \epsilon + H(1 + \alpha H) \epsilon_c + H(1 + \alpha H) \|\theta_t^* - \theta_c^*\|.$$

Theorem 3 sheds light on how the task similarity and local sample size impact the learning performance at the target edge node t . In particular, the performance gap between the optimal model and the model after fast adaptation is upper bounded by the surrogate difference, denoted by $\|\theta_t^* - \theta_c^*\|$, which serves as a guidance for the platform to determine how similar the source edge nodes in the federated meta-learning should be with the target node in order to achieve given learning performance via fast adaptation and hence edge intelligence at the target edge node.

V. ROBUST FEDERATED META-LEARNING (FEDML)

It has been shown in [11] and [10] that meta-learning algorithms (e.g., MAML) are vulnerable to adversarial attacks, leading to possible significant performance degradation of the locally fast adapted model at the target when facing perturbed data inputs. Thus motivated, we next devise a robust federated meta-learning algorithm and study the trade-off between robustness and accuracy therein (cf. [18]).

A. Robust Federated Meta-Learning

To combat against the possible vulnerability of meta-learning algorithms, we propose to obtain a model initialization from which the model updated with local training data at the target not only is robust against data distributions that are distance π away from the target data distribution

P_t , but also guarantees good performance when fed with the clean target data. Based on recent advances in distributionally robust optimization (DRO), this can be achieved by solving the following problem:

$$\min_{\theta} \left\{ L_t(\phi_t) + \max_{P: D(P, P_t) \leq \pi} \mathbb{E}_P[l(\phi_t, (\mathbf{x}, \mathbf{y}))] \right\}, \quad (10)$$

where $D(P, P_t)$ is a distance metric on the space of probability distributions.

To solve (10) with federated meta-learning, based on the general machine learning principle that train and test conditions must match, we can reformulate the federated meta-learning objective (4) as:

$$\begin{aligned} \min_{\theta} \quad & \sum_{i \in \mathcal{S}} \omega_i F_i(\phi_i), \\ \text{s.t.} \quad & F_i(\phi_i) = L(\phi_i, D_i^{test}) + \max_P \mathbb{E}_P[l(\phi_i, (\mathbf{x}_i, \mathbf{y}_i))], \\ & \phi_i = \theta - \alpha \nabla_{\theta} L(\theta, D_i^{train}), \\ & D(P, P_i) \leq \pi, \end{aligned} \quad (11)$$

where a distributionally robust objective function similar with the target node is set for every source edge node $i \in \mathcal{S}$.

B. Wasserstein Distance based Robust Federated Meta-Learning

The choice of the distributional distance metric clearly affects both the richness of the uncertainty set and the tractability of problem (11). To enable distance measure between distributions with different support, we use Wasserstein distance as the distance metric on the space of probability distributions. More specifically, let the transportation cost $c : (\mathcal{X} \times \mathcal{Y}) \times (\mathcal{X} \times \mathcal{Y}) \rightarrow \mathbb{R}_+$ be lower-semicontinuous and satisfy $c((\mathbf{x}, \mathbf{y}), (\mathbf{x}, \mathbf{y})) = 0$, which quantifies the cost of transporting unit mass from (\mathbf{x}, \mathbf{y}) to $(\mathbf{x}', \mathbf{y}')$. For any two probability measure P and Q supported on $\mathcal{X} \times \mathcal{Y}$, let $\Pi(P, Q)$ denote the set of all couplings (transport plans) between P and Q , meaning measures W with $W(A, \mathcal{X} \times \mathcal{Y}) = P(A)$ and $W(\mathcal{X} \times \mathcal{Y}, A) = Q(A)$. The Wasserstein distance is then defined as

$$D_w(P, Q) \triangleq \inf_{W \in \Pi(P, Q)} \mathbb{E}_W[c((\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}'))], \quad (12)$$

which represents the optimal transport cost, i.e., the lowest expected transport cost, that is achievable among all couplings between P and Q .

Since the Wasserstein distance based optimization problem is computationally demanding for complex models, based on [19], we consider the following Lagrangian relaxation of the inner maximization problem of (11) with penalty parameter $\lambda \geq 0$:

$$\max_P \{ \mathbb{E}_P[l(\phi_i, (\mathbf{x}_i, \mathbf{y}_i))] - \lambda D_w(P, P_i) \}, \quad (13)$$

where λ is inversely proportional to π . The duality result below in [20] based on Kantorovich's duality, a widely used approach to solve the Wasserstein distance based DRO problem in

optimal transport, provides us an efficient way to solve (13) through a robust surrogate loss:

Lemma 2. *Let $l : \mathbb{R}^d \times (\mathcal{X} \times \mathcal{Y}) \rightarrow \mathbb{R}$ and $c : (\mathcal{X} \times \mathcal{Y}) \times (\mathcal{X} \times \mathcal{Y}) \rightarrow \mathbb{R}_+$ be continuous. Define the robust surrogate loss as $l_{\lambda}(\theta, (\mathbf{x}_0, \mathbf{y}_0)) \triangleq \sup_{\mathbf{x} \in \mathcal{X}} \{ l(\theta, (\mathbf{x}, \mathbf{y}_0)) - \lambda c((\mathbf{x}, \mathbf{y}_0), (\mathbf{x}_0, \mathbf{y}_0)) \}$. For any distribution Q and $\lambda \geq 0$, we have*

$$\max_P \{ \mathbb{E}_P[l(\theta, (\mathbf{x}, \mathbf{y}))] - \lambda D_w(P, Q) \} = \mathbb{E}_Q[l_{\lambda}(\theta, (\mathbf{x}, \mathbf{y}))].$$

Lemma 2 divulges a worst-case joint probability measure W^* corresponding to a transport plan that transports mass from \mathbf{x} to the optimizer of the local optimization problem $\sup_{\mathbf{x} \in \mathcal{X}} \{ l(\theta, (\mathbf{x}, \mathbf{y}_0)) - \lambda c((\mathbf{x}, \mathbf{y}_0), (\mathbf{x}_0, \mathbf{y}_0)) \}$. Hence, we can replace (13) with the expected robust surrogate loss $\mathbb{E}_{P_i}[l_{\lambda}(\phi_i, (\mathbf{x}_i, \mathbf{y}_i))]$. Moreover, we typically replace P_i by the empirical distribution \hat{P}_i because P_i is unknown.

In what follows, we focus on the following relaxed robust problem:

$$\begin{aligned} \min_{\theta} \quad & \sum_{i \in \mathcal{S}} \omega_i \{ L(\phi_i, D_i^{test}) + \mathbb{E}_{\hat{P}_i}[l_{\lambda}(\phi_i, (\mathbf{x}_i, \mathbf{y}_i))] \}, \\ \text{s.t.} \quad & \phi_i = \theta - \alpha \nabla_{\theta} L(\theta, D_i^{train}). \end{aligned} \quad (14)$$

Under suitable conditions, the robust surrogate loss $l_{\lambda}(\theta, (\mathbf{x}_0, \mathbf{y}_0))$ is strongly-concave for $\lambda \geq H_{\mathbf{x}}$ [19], which indicates the computational benefits of relaxing the strict robustness requirements of (13). Therefore,

$$\nabla_{\phi_i} l_{\lambda}(\phi_i, (\mathbf{x}_i, \mathbf{y}_i)) = \nabla_{\phi_i} l(\phi_i, (\mathbf{x}^*, \mathbf{y}_i)), \quad (15)$$

where

$$\mathbf{x}^* = \arg \max_{\mathbf{x} \in \mathcal{X}} \{ l(\phi_i, (\mathbf{x}, \mathbf{y}_i)) - \lambda c((\mathbf{x}, \mathbf{y}_i), (\mathbf{x}_i, \mathbf{y}_i)) \}. \quad (16)$$

Here \mathbf{x}^* can be regarded as an adversarial perturbation of \mathbf{x}_i under current model ϕ_i and efficiently approximated by gradient-ascent methods, revealing that problem (14) can be efficiently solved by gradient-based methods.

C. Robust Meta-Training across Edge Nodes

To solve problem (14), similar to [21], we use an adversarial data generation process, i.e., approximately solving (16) with gradient ascent, to the federated meta-learning algorithm. More specifically, for every $N_0 T_0$ iterations, each edge node i constructs adversarial data samples using T_a steps gradient ascent and adds them to its own adversarial dataset D_i^{adv} . Note that this sample construction procedure can only be repeated up to R times considering the local computational resources constraints. For $t \neq nT_0$ (no global aggregation), each node i first updates θ_i^t using the training dataset:

$$\phi_i^t = \theta_i^t - \alpha \nabla_{\theta} L(\theta_i^t, D_i^{train}), \quad (17)$$

then locally updates θ_i^t again using both the testing dataset and the constructed adversarial dataset:

$$\theta_i^{t+1} = \theta_i^t - \beta \nabla_{\theta} \{ L(\phi_i^t, D_i^{test}) + L(\phi_i^t, D_i^{adv}) \}. \quad (18)$$

When $t = nT_0$, each node transmits the updated θ_i^{t+1} for the global aggregation (6). The details are summarized in Algorithm 2.

Algorithm 2 Robust FedML

Inputs: $K, T, T_0, T_a, N_0, R, \alpha, \beta, \nu, \omega_i$ for $i \in \mathcal{S}$
Outputs: Final model parameter θ

- 1: Platform randomly initializes θ^0 and sends it to all nodes in \mathcal{S} ; For each node i , $D_i^{adv} \leftarrow \emptyset$ and $r \leftarrow 0$;
- 2: **for** $t = 1, 2, \dots, T$ **do**
- 3: **for** each node $i \in \mathcal{S}$ **do**
- 4: $D_i^{comb} \leftarrow D_i^{test} \cup D_i^{adv}$;
- 5: Compute the updated parameter with one-step gradient descent using D_i^{train} : $\phi_i^t = \theta_i^t - \alpha \nabla_{\theta} L(\theta_i^t, D_i^{train})$;
- 6: Obtain θ_i^{t+1} based on (18); **//local update**
- 7: **if** $t \bmod T_0 = 0$ **then**
- 8: Send θ_i^{t+1} to the platform;
- 9: Receive θ^{t+1} from the platform where θ^{t+1} is obtained based on (6);
- 10: Set $\theta_i^t \leftarrow \theta^{t+1}$; **//global aggregation**
- 11: **else**
- 12: Set $\theta_i^t \leftarrow \theta_i^{t+1}$;
- 13: **if** $t \bmod N_0 T_0 = 0$ and $r < R$ **then** **//adversarial data generation**
- 14: Uniformly sample $(\mathbf{x}_i^j, \mathbf{y}_i^j)_{j=1, \dots, |D_i^{test}|}$ from D_i^{comb}
- 15: **for** $j = 1, \dots, |D_i^{test}|$ **do**
- 16: $\mathbf{x}_i^{jr} \leftarrow \mathbf{x}_i^j$;
- 17: **for** $t = 1, \dots, T_a$ **do**
- 18: $\mathbf{x}_i^{jr} \leftarrow \mathbf{x}_i^{jr} + \nu \nabla_{\mathbf{x}} \{l(\phi_i^t, (\mathbf{x}_i^{jr}, \mathbf{y}_i^j)) - \lambda c((\mathbf{x}_i^{jr}, \mathbf{y}_i^j), (\mathbf{x}_i^j, \mathbf{y}_i^j))\}$;
- 19: Append $(\mathbf{x}_i^{jr}, \mathbf{y}_i^j)$ to D_i^{adv} ;
- 20: $r \leftarrow r + 1$;
- 21: **return** θ .

D. Convergence Analysis

Similar with Section 4.1, for clarity we rewrite problem (14) as the following:

$$\min_{\theta} \tilde{G}(\theta), \quad (19)$$

where $\tilde{G}(\theta) = \sum_{i \in \mathcal{S}} \omega_i \tilde{G}_i(\theta)$ and $\tilde{G}_i(\theta) = L(\phi_i(\theta), D_i^{test}) + \mathbb{E}_{P_i} [l_{\lambda}(\phi_i(\theta), (\mathbf{x}_i, \mathbf{y}_i))]$.

Assumption 5. The function c is continuous. And for every $(\mathbf{x}_0, \mathbf{y}_0) \in \mathcal{X} \times \mathcal{Y}$, $c((\mathbf{x}, \mathbf{y}_0), (\mathbf{x}_0, \mathbf{y}_0))$ is 1-strongly convex with respect to \mathbf{x} .

Assumption 6. The loss function $l : \mathbb{R}^d \times (\mathcal{X} \times \mathcal{Y}) \rightarrow \mathbb{R}$ is μ -strongly convex with respect to θ .

Assumption 7. The loss function $l : \mathbb{R}^d \times (\mathcal{X} \times \mathcal{Y}) \rightarrow \mathbb{R}$ is smooth with respect to both θ and \mathbf{x} , i.e.,

$$\begin{aligned} \|\nabla_{\theta} l(\theta, (\mathbf{x}, \mathbf{y})) - \nabla_{\theta} l(\theta', (\mathbf{x}, \mathbf{y}))\| &\leq H \|\theta - \theta'\|, \\ \|\nabla_{\theta} l(\theta, (\mathbf{x}, \mathbf{y})) - \nabla_{\theta} l(\theta, (\mathbf{x}', \mathbf{y}))\| &\leq H_{\theta \mathbf{x}} \|\mathbf{x} - \mathbf{x}'\|, \\ \|\nabla_{\mathbf{x}} l(\theta, (\mathbf{x}, \mathbf{y})) - \nabla_{\mathbf{x}} l(\theta, (\mathbf{x}', \mathbf{y}))\| &\leq H_{\mathbf{x} \mathbf{x}} \|\mathbf{x} - \mathbf{x}'\|, \\ \|\nabla_{\mathbf{x}} l(\theta, (\mathbf{x}, \mathbf{y})) - \nabla_{\mathbf{x}} l(\theta', (\mathbf{x}, \mathbf{y}))\| &\leq H_{\mathbf{x} \theta} \|\theta - \theta'\|, \end{aligned}$$

and there exists a constant B such that $\|\nabla_{\theta} l(\theta, (\mathbf{x}, \mathbf{y}))\| \leq B$ for all $\theta \in \mathbb{R}^d$ and $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{Y}$.

Note that Assumptions 6-7 can be stronger replacements of Assumptions 1-2, respectively. We characterize the robust federated meta-learning objective $\tilde{G}(\theta)$ below:

Theorem 4. Suppose Assumptions 3 and 5-7 hold. When $\alpha \leq \min\{\frac{\mu}{2\mu H + \rho B}, \frac{1}{\mu}\}$ and $\lambda \geq H_{\mathbf{x} \mathbf{x}} + \frac{H_{\theta \mathbf{x}} H_{\mathbf{x} \theta}}{\mu}$, problem (19) has a unique minimizer.

Theorem 4 implies that when the learning rate α is sufficiently small and the Lagrangian penalty parameter λ is large enough, the relaxed robust meta-learning objective function $\tilde{G}(\theta)$ is strongly convex and hence has a unique solution. Further, as outlined in Algorithm 2, through pre-training each edge node to learn to protect against adversarial perturbations on the testing dataset while securing the model accuracy on clean data with Algorithm 2, the learned model via meta-training automatically gains the ability to prevent future adversarial attacks without significantly sacrificing the learning accuracy with quick adaptation at the target edge node.

VI. EXPERIMENTS

In this section, we first introduce the experimental setup, and then evaluate the performance of FedML and Robust FedML. In particular, we investigate the impact of node similarity and number of local update step T_0 on the convergence of federated meta-learning, and compare the fast adaptation performance of federated meta-learning (FedML) with the model learnt from federated learning (Fedavg) [12].

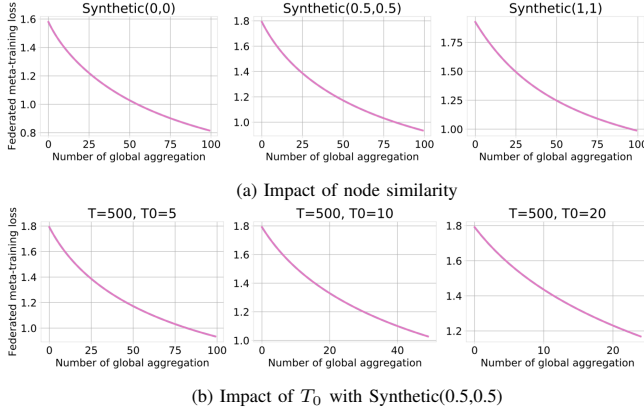
A. Experimental Setting

Synthetic data. To evaluate the impact of node similarity on the performance of convergence and fast adaptation, we follow a similar setup in [14] to generate synthetic data. Specifically, the synthetic sample $(\mathbf{x}_i^j, \mathbf{y}_i^j)$ for each node i is generated from the model $\mathbf{y} = \arg\max(\text{softmax}(\mathbf{W}\mathbf{x} + \mathbf{b}))$ where $\mathbf{x} \in \mathbb{R}^{60}$, $\mathbf{W} \in \mathbb{R}^{10 \times 60}$ and $\mathbf{b} \in \mathbb{R}^{10}$. Moreover, $\mathbf{W}_i \sim \mathcal{N}(\mathbf{u}_i, \mathbf{I})$, $\mathbf{b}_i \sim \mathcal{N}(\mathbf{u}_i, \mathbf{I})$, $\mathbf{u}_i \sim \mathcal{N}(0, \tilde{\alpha})$; $\mathbf{x}_i^j \sim \mathcal{N}(\mathbf{v}_i, \Sigma)$ where the covariance matrix Σ is diagonal with $\Sigma_{k,k} = k^{-1.2}$ and $\mathbf{v}_i \sim \mathcal{N}(B_i, \mathbf{I})$, $B_i \sim \mathcal{N}(0, \tilde{\beta})$. Intuitively, $\tilde{\alpha}$ and $\tilde{\beta}$ control the local model similarity across all nodes, which can be changed to generate heterogeneous local datasets named Synthetic($\tilde{\alpha}, \tilde{\beta}$). For all synthetic datasets, we consider 50 nodes in total and the number of samples on each node follows a power law. The objective is to learn the model parameters \mathbf{W} and \mathbf{b} with the cross-entropy loss function.

Real data. We also explore two real datasets, MNIST [22], and Sentiment140 (Sent140) [23] used for text sentiment analysis on tweets. For MNIST, we sample part of data and distribute the data among 100 nodes such that every node has samples of only two digits and the number of samples per device follows a power law. We study a convex classification problem with MNIST using multinomial logistic regression. Next, we consider a more complicated classification problem on Sent140 by taking each twitter account as a node, where the model takes a sequence of 25 characters as input, embeds each of the character into a 300 dimensional space by looking up the pretrained 300D GloVe embedding [24], and outputs

TABLE I: Statistics of Datasets

Dataset	Nodes	Sample per Node	
		mean	stdev
Synthetic	50	17	5
MNIST	100	34	5
Sent140	706	42	35

Fig. 2: Impact of Node Similarity and T_0 on the Convergence of FedML

one character per training sample through a network with 3 hidden layers with sizes 256, 128, 64, each including batch normalization and ReLU nonlinearities, followed by a linear layer and softmax. The loss function is the cross-entropy error between the predicted and true class for all models.

Implementation. For each node, we divide the local dataset as a training set and a testing set. We select 80% nodes as the source nodes and evaluate the fast adaptation performance on the rest. When training with FedML, we vary the size of the training set, i.e., K , for the one-step gradient update, whereas the entire dataset is used for training in Fedavg. During testing, the trained model is first updated with the training set of testing nodes, and then evaluated on their testing sets. For FedML, we set both the learning rate α and meta learning rate β as 0.01 for synthetic data and MNIST, while $\alpha = 0.01$ and $\beta = 0.3$ for Sent140. Fedavg has the same learning rate with β .

B. Evaluation of Federated Meta-Learning

Convergence behaviour. We evaluate the convergence error for (a) three different synthetic datasets with $T_0 = 10$ (b) the same dataset but different T_0 with $T = 500$. As illustrated in Figure 2, the experimental results corroborate Theorem 2 that the convergence error of FedML decreases with the node similarity but increases with T_0 given a fixed algorithm duration T . Moreover, the result in Sent140 (Figure 3(a)) shows that FedML also achieves good convergence performance in practical non-convex settings.

Fast adaptation performance. As shown in Figure 3(b), FedML achieves the best adaptation performance on Synthetic(0,0) where the nodes are the most similar. We also compare the fast adaptation performance between FedML and Fedavg on three different datasets, Synthetic(0.5,0.5), MNIST and Sent140. As shown in Figure 3(c)-3(e), the model learnt from FedML can achieve significantly better adaptation performance at the target nodes compared with that in Fedavg,

and this performance gap increases when the target node has small local datasets. It can be seen that the model learnt in Fedavg turns to have overfitting issues when fine-tuned with a few data samples, whereas the meta-model in FedML improves with additional gradient steps without overfitting.

C. Evaluation of Robust Federated Meta-Learning

We compare the adaptation performance of FedML and Robust FedML on MNIST with $T_0 = 5$ during training. For adversarial perturbations only to feature vectors in supervised learning, we consider the transportation cost function as: $c((\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}')) = \|\mathbf{x} - \mathbf{x}'\|_2^2 + \infty \cdot \mathbf{1}(\mathbf{y} - \mathbf{y}')$. The learning rate $\nu = 1$, $R = 2$, $N_0 = 7$ and $T_a = 10$ for adversarial data generation. For testing at the target, we first update the meta-model with clean training data, and then evaluate the adaptation performance on clean test data and adversarial data, where the adversarial data is generated by using the Fast Gradient Sign Method [25] with parameter ξ , respectively. Since the size of distributional uncertainty set controls the trade-off between robustness and accuracy, we compare the performance of Robust FedML with $\lambda = 0.1, 1, 10$, where the smaller λ is, the more robustness Robust FedML provides.

Robustness-Accuracy tradeoff. As shown in Figure 4(a)-4(d), when λ decreases, Robust FedML has slightly worse performance on clean data and the performance on adversarial data is much better. Compared with the case where $\lambda = 10$, Robust FedML with $\lambda = 0.1$ significantly improves the robustness against adversarial data without sacrificing too much on the accuracy with clean data. Moreover, Robust FedML with smaller λ is more robust than FedML. Note that the uncertainty set is too small to positively affect the robustness when $\lambda = 10$.

Impact of ξ . Clearly, both FedML and Robust FedML achieve better performance when facing smaller perturbation (smaller ξ) of testing data. Figure 4(e) further indicates that the improvement of Robust FedML over FedML is higher with more perturbed data.

VII. CONCLUSION

In this paper, we propose a platform-aided collaborative learning framework, where a model is first trained across a set of source edge nodes by a federated meta-learning approach, and then it is rapidly adapted to achieve real-time edge intelligence at the target edge node, using a few samples only. We investigate the convergence of FedML under mild conditions on node similarity, and study the adaptation performance to achieve edge intelligence at the target node. To combat against the vulnerability of meta-learning algorithms, we further propose a robust FedML algorithm based on DRO with convergence guarantee. Experimental results on various datasets corroborate the effectiveness of the proposed collaborative learning framework.

REFERENCES

- [1] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Network*, 2019.

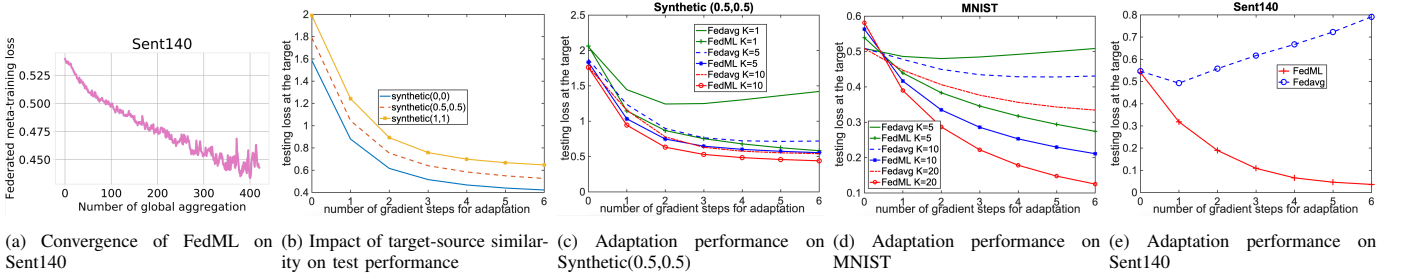


Fig. 3: Convergence and Fast Adaptation Performance of FedML on Different Datasets with $T_0 = 5$

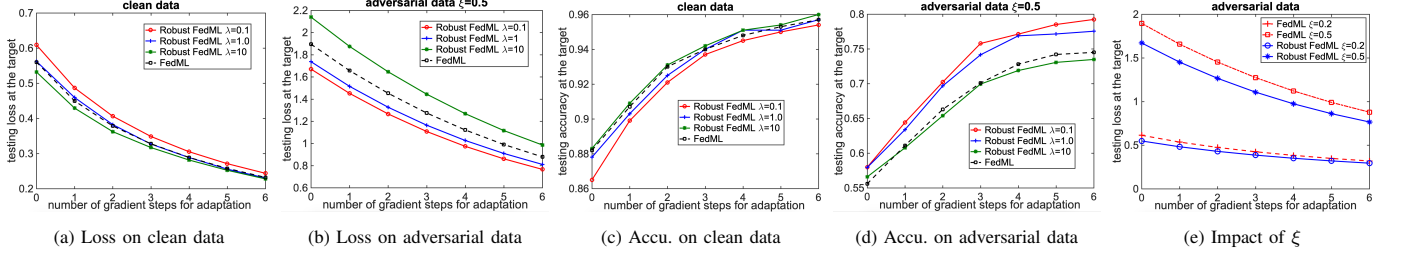


Fig. 4: Adaptation Performance of Robust FedML on MNIST with $T_0 = 5$

- [2] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, “Edge intelligence: Paving the last mile of artificial intelligence with edge computing,” *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.
- [3] S. Ravi and H. Larochelle, “Optimization as a model for few-shot learning,” in *International conference on learning representations*, 2017.
- [4] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar, “Federated multi-task learning,” in *Advances in Neural Information Processing Systems*, 2017, pp. 4424–4434.
- [5] J. Schmidhuber, “Evolutionary principles in self-referential learning,” Ph.D. dissertation, Technische Universität München, 1987.
- [6] C. Finn, P. Abbeel, and S. Levine, “Model-agnostic meta-learning for fast adaptation of deep networks,” in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*. JMLR. org, 2017, pp. 1126–1135.
- [7] A. Nichol, J. Achiam, and J. Schulman, “On first-order meta-learning algorithms,” *arXiv preprint arXiv:1803.02999*, 2018.
- [8] F. Chen, Z. Dong, Z. Li, and X. He, “Federated meta-learning for recommendation,” *arXiv preprint arXiv:1802.07876*, 2018.
- [9] A. Fallah, A. Mokhtari, and A. Ozdaglar, “On the convergence theory of gradient-based model-agnostic meta-learning algorithms,” *arXiv preprint arXiv:1908.10400*, 2019.
- [10] R. Edmunds, N. Golmant, V. Ramasesh, P. Kuznetsov, P. Patil, and R. Puri, “Transferability of adversarial attacks in model-agnostic meta-learning,”
- [11] C. Yin, J. Tang, Z. Xu, and Y. Wang, “Adversarial meta-learning,” *arXiv preprint arXiv:1806.03316*, 2018.
- [12] H. B. McMahan, E. Moore, D. Ramage, S. Hampson *et al.*, “Communication-efficient learning of deep networks from decentralized data,” *arXiv preprint arXiv:1602.05629*, 2016.
- [13] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, “Adaptive federated learning in resource constrained edge computing systems,” *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.
- [14] A. K. Sahu, T. Li, M. Sanjabi, M. Zaheer, A. Talwalkar, and V. Smith, “On the convergence of federated optimization in heterogeneous networks,” *arXiv preprint arXiv:1812.06127*, 2018.
- [15] T. Evgeniou and M. Pontil, “Regularized multi-task learning,” in *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2004, pp. 109–117.
- [16] S. Ruder, “An overview of multi-task learning in deep neural networks,” *arXiv preprint arXiv:1706.05098*, 2017.
- [17] C. Finn, A. Rajeswaran, S. Kakade, and S. Levine, “Online meta-learning,” *arXiv preprint arXiv:1902.08438*, 2019.
- [18] D. Tsipras, S. Santurkar, L. Engstrom, A. Turner, and A. Madry, “Robustness may be at odds with accuracy,” *arXiv preprint arXiv:1805.12152*, 2018.
- [19] A. Sinha, H. Namkoong, and J. Duchi, “Certifying some distributional robustness with principled adversarial training,” *arXiv preprint arXiv:1710.10571*, 2017.
- [20] J. Blanchet and K. Murthy, “Quantifying distributional model risk via optimal transport,” *Mathematics of Operations Research*, vol. 44, no. 2, pp. 565–600, 2019.
- [21] R. Volpi, H. Namkoong, O. Sener, J. C. Duchi, V. Murino, and S. Savarese, “Generalizing to unseen domains via adversarial data augmentation,” in *Advances in Neural Information Processing Systems*, 2018, pp. 5334–5344.
- [22] Y. LeCun, L. Bottou, Y. Bengio, P. Haffner *et al.*, “Gradient-based learning applied to document recognition,” *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.
- [23] A. Go, R. Bhayani, and L. Huang, “Twitter sentiment classification using distant supervision,” *CS224N Project Report, Stanford*, vol. 1, no. 12, p. 2009, 2009.
- [24] J. Pennington, R. Socher, and C. Manning, “Glove: Global vectors for word representation,” in *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, 2014, pp. 1532–1543.
- [25] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” *arXiv preprint arXiv:1412.6572*, 2014.
- [26] A. Shapiro, D. Dentcheva, and A. Ruszczyński, *Lectures on stochastic programming: modeling and theory*. SIAM, 2009.

APPENDIX A PROOF OF LEMMA 1

We first show that $G_i(\theta)$ is μ' -strongly convex and L' -smooth. Specifically, observe that

$$\begin{aligned}
 & \|\nabla G_i(\theta) - \nabla G_i(\theta')\| \\
 &= \|\nabla L_i(\phi_i) - \alpha \nabla^2 L_i(\theta) \nabla L_i(\phi_i) - \nabla L_i(\phi'_i) \\
 & \quad + \alpha \nabla^2 L_i(\theta') \nabla L_i(\phi'_i)\| \\
 &= \|\nabla L_i(\phi_i) - \alpha \nabla^2 L_i(\theta) \nabla L_i(\phi_i) + \alpha \nabla^2 L_i(\theta') \nabla L_i(\phi'_i) \\
 & \quad - \nabla L_i(\phi'_i) + \alpha \nabla^2 L_i(\theta) \nabla L_i(\phi'_i) - \alpha \nabla^2 L_i(\theta') \nabla L_i(\phi'_i)\| \\
 &= \|[I - \alpha \nabla^2 L_i(\theta)][\nabla L_i(\phi_i) - \nabla L_i(\phi'_i)] \\
 & \quad - \alpha \nabla L_i(\phi'_i)[\nabla^2 L_i(\theta) - \nabla^2 L_i(\theta')]\|, \tag{20}
 \end{aligned}$$

where $\phi_i = \theta - \alpha \nabla L_i(\theta)$ and $\phi'_i = \theta' - \alpha \nabla L_i(\theta')$.

To establish the convexity, it suffices to show $\|\nabla G_i(\theta) - \nabla G_i(\theta')\| \geq \mu' \|\theta - \theta'\|$. It can be seen from (20) that

$$\begin{aligned} & \|\nabla G_i(\theta) - \nabla G_i(\theta')\| \\ & \geq (1 - \alpha H) \|\nabla L_i(\phi_i) - \nabla L_i(\phi'_i)\| \\ & \quad - \alpha \|\nabla L_i(\phi'_i)\| \|\nabla^2 L_i(\theta) - \nabla^2 L_i(\theta')\| \\ & \geq \mu(1 - \alpha H) \|\phi_i - \phi'_i\| - \alpha \rho B \|\theta - \theta'\|. \end{aligned} \quad (21)$$

Since $\nabla \phi_i = I - \alpha \nabla^2 L_i(\theta)$, it follows from Assumption 1 and 2 that $1 - \alpha H \leq \nabla \phi_i \leq 1 - \alpha \mu$, which indicates

$$(1 - \alpha H) \|\theta - \theta'\| \leq \|\phi_i - \phi'_i\| \leq (1 - \alpha \mu) \|\theta - \theta'\|. \quad (22)$$

Combining (21) and (22), we have

$$\|\nabla G_i(\theta) - \nabla G_i(\theta')\| \geq \mu' \|\theta - \theta'\|,$$

where $\mu' = \mu(1 - \alpha H)^2 - \alpha \rho B > 0$.

To establish the smoothness, it suffices to show $\|\nabla G_i(\theta) - \nabla G_i(\theta')\| \leq H' \|\theta - \theta'\|$. From (20) and (22), we have

$$\begin{aligned} & \|\nabla G_i(\theta) - \nabla G_i(\theta')\| \\ & \leq (1 - \alpha \mu) \|\nabla L_i(\phi_i) - \nabla L_i(\phi'_i)\| \\ & \quad + \alpha \|\nabla L_i(\phi'_i)\| \|\nabla^2 L_i(\theta) - \nabla^2 L_i(\theta')\| \\ & \leq H(1 - \alpha \mu) \|\phi_i - \phi'_i\| + \alpha \rho B \|\theta - \theta'\| \\ & \leq H' \|\theta - \theta'\|, \end{aligned}$$

where $H' = H(1 - \alpha \mu)^2 + \alpha \rho B$, thereby completing the proof of Lemma 1.

APPENDIX B PROOF OF THEOREM 1

Observe that $\nabla G_i(\theta) = \nabla L_i(\phi_i) - \alpha \nabla^2 L_i(\theta) \nabla L_i(\phi_i)$ involves the product between Hessian matrix and gradient, which admits an upper bound outlined as follows:

$$\begin{aligned} & \|\nabla^2 L_i(\theta) \nabla L_i(\theta) - \sum_{i \in \mathcal{S}} \omega_i \nabla^2 L_i(\theta) \nabla L_i(\theta)\| \\ & = \|\nabla^2 L_i(\theta) \nabla L_i(\theta) - \nabla^2 L_w(\theta) \nabla L_w(\theta) \\ & \quad + \nabla^2 L_w(\theta) \nabla L_w(\theta) - \sum_{i \in \mathcal{S}} \omega_i \nabla^2 L_i(\theta) \nabla L_i(\theta)\| \\ & \leq \|\nabla^2 L_i(\theta) \nabla L_i(\theta) - \nabla^2 L_i(\theta) \nabla L_w(\theta)\| \\ & \quad + \|\nabla^2 L_i(\theta) \nabla L_w(\theta) - \nabla^2 L_w(\theta) \nabla L_w(\theta)\| \\ & \quad + \|\sum_{i \in \mathcal{S}} \omega_i [(\nabla L_i(\theta) - \nabla L_w(\theta))(\nabla^2 L_i(\theta) - \nabla^2 L_w(\theta))]\| \\ & \leq \|\nabla^2 L_i(\theta)\| \|\nabla L_i(\theta) - \nabla L_w(\theta)\| \\ & \quad + \|\nabla L_w(\theta)\| \|\nabla^2 L_i(\theta) - \nabla^2 L_w(\theta)\| \\ & \quad + \sum_{i \in \mathcal{S}} \omega_i \|\nabla L_i(\theta) - \nabla L_w(\theta)\| \|\nabla^2 L_i(\theta) - \nabla^2 L_w(\theta)\| \\ & \leq H \delta_i + B \sigma_i + \tau. \end{aligned} \quad (23)$$

Next, it follows from Taylor's Theorem that

$$\nabla L_i(\phi_i) = \nabla L_i(\theta) + \nabla^2 L_i(\theta)(\phi_i - \theta) + O(\|\phi_i - \theta\|^2).$$

That is to say,

$$\nabla L_i(\phi_i) = \nabla L_i(\theta) - \alpha \nabla^2 L_i(\theta) \nabla L_i(\theta) + O(\alpha^2 B^2).$$

Therefore, we have

$$\begin{aligned} & \|\nabla G_i(\theta) - \nabla G(\theta)\| \\ & = \|[I - \alpha \nabla^2 L_i(\theta)] \nabla L_i(\phi_i) - \sum_{i \in \mathcal{S}} \omega_i [I - \alpha \nabla^2 L_i(\theta)] \nabla L_i(\phi_i)\| \\ & = \|[I - \alpha \nabla^2 L_i(\theta)] [\nabla L_i(\phi_i) - \nabla L_i(\theta) + \nabla L_i(\theta)] \\ & \quad - \sum_{i \in \mathcal{S}} \omega_i [I - \alpha \nabla^2 L_i(\theta)] [\nabla L_i(\phi_i) \nabla - L_i(\theta) + \nabla L_i(\theta)]\| \\ & = \|\nabla L_i(\theta) - \nabla L_w(\theta) - 2\alpha \nabla^2 L_i(\theta) \nabla L_i(\theta) \\ & \quad + 2\alpha \sum_{i \in \mathcal{S}} \omega_i \nabla^2 L_i(\theta) \nabla L_i(\theta) + O(\alpha^2 B^2) \\ & \quad + \alpha^2 [\nabla^2 L_i(\theta)]^2 \nabla L_i(\theta) - \alpha^2 \sum_{i \in \mathcal{S}} \omega_i [\nabla^2 L_i(\theta)]^2 \nabla L_i(\theta)\| \\ & \leq \|\nabla L_i(\theta) - \nabla L_w(\theta)\| + O(\alpha^2 B^2) \\ & \quad + 2\alpha \|\nabla^2 L_i(\theta) \nabla L_i(\theta) - \sum_{i \in \mathcal{S}} \omega_i \nabla^2 L_i(\theta) \nabla L_i(\theta)\| \\ & \quad + \alpha^2 \|[\nabla^2 L_i(\theta)]^2 \nabla L_i(\theta) - \sum_{i \in \mathcal{S}} \omega_i [\nabla^2 L_i(\theta)]^2 \nabla L_i(\theta)\| \\ & \leq \delta_i + 2\alpha(H\delta_i + B\sigma_i + \tau) + O(\alpha^2 B^2) \\ & \quad + \alpha^2 \|[\nabla^2 L_i(\theta)]^2 \nabla L_i(\theta) - \alpha^2 \sum_{i \in \mathcal{S}} \omega_i [\nabla^2 L_i(\theta)]^2 \nabla L_i(\theta)\|. \end{aligned}$$

Along the same line as in finding an upper bound for $\|\nabla^2 L_i(\theta) \nabla L_i(\theta) - \sum_{i \in \mathcal{S}} \omega_i \nabla^2 L_i(\theta) \nabla L_i(\theta)\|$, we can find an upper bound on the last term of the above inequality with $\alpha^2(H\delta'_i + B\sigma_i + \tau')$ where $\delta'_i = H\delta_i + B\sigma_i + \tau$ and $\tau' = \sum_{i \in \mathcal{S}} \omega_i \delta'_i \sigma_i$. We conclude that when α is suitably small, there exists a constant C such that the right hand side of the above inequality is upper bounded by $\delta_i + \alpha C(H\delta_i + B\sigma_i + \tau)$.

APPENDIX C PROOF OF THEOREM 2

Following the same method as in [13], we first define a virtual sequence for global aggregation at each iteration as $\mathbf{v}_{[n]}^t$ for $t \in [(n-1)T_0, nT_0]$, where the interval $[(n-1)T_0, nT_0]$ is denoted as $[n]$. More specifically,

$$\mathbf{v}_{[n]}^{t+1} = \mathbf{v}_{[n]}^t - \beta \nabla G(\mathbf{v}_{[n]}^t), \quad (24)$$

and $\mathbf{v}_{[n]}^t$ is assumed to be “synchronized” with θ^t at the beginning of interval $[n]$, i.e., $\mathbf{v}_{[n]}^{(n-1)T_0} = \theta^{(n-1)T_0}$, where $\theta^{(n-1)T_0}$ is the weighted average of local parameters $\theta_i^{(n-1)T_0}$ as shown in (6). To show the convergence, we first analyze the gap between the virtual global parameter $\mathbf{v}_{[n]}^t$ and the local weighted average θ^t during each interval, and then evaluate the convergence performance of θ^t through evaluating the convergence performance of virtual sequence $\mathbf{v}_{[n]}^t$ by taking the gap into consideration.

To analyze the gap between $\mathbf{v}_{[n]}^t$ and θ^t during interval $[n]$, we first look into the gap between $\mathbf{v}_{[n]}^t$ and the local update

θ_i^t . Specifically,

$$\begin{aligned}
& \|\theta_i^{t+1} - v_{[n]}^{t+1}\| \\
&= \|\theta_i^t - \beta \nabla G_i(\theta_i^t) - v_{[n]}^t + \beta \nabla G(v_{[n]}^t)\| \\
&\leq \|\theta_i^t - v_{[n]}^t\| + \beta \|\nabla G_i(\theta_i^t) - \nabla G(v_{[n]}^t)\| \\
&\leq \|\theta_i^t - v_{[n]}^t\| + \beta \|\nabla G_i(\theta_i^t) - \nabla G_i(v_{[n]}^t)\| \\
&\quad + \beta \|\nabla G_i(v_{[n]}^t) - \nabla G(v_{[n]}^t)\| \\
&\leq (1 + \beta H') \|\theta_i^t - v_{[n]}^t\| + \beta [\delta_i + \alpha C(H\delta_i + B\sigma_i + \tau)]. \quad (25)
\end{aligned}$$

By induction, we can show that $\|\theta_i^t - v_{[n]}^t\| \leq g(t - (n-1)T_0)$ where $g(x) \triangleq \frac{\delta_i + \alpha C(H\delta_i + B\sigma_i + \tau)}{H'} [(1 + \beta H')^x - 1]$. Therefore, for $t \in [(n-1)T_0, nT_0]$ we can get

$$\begin{aligned}
& \|\theta^t - v_{[n]}^{t+1}\| \\
&= \left\| \sum_{i \in \mathcal{S}} \omega_i \theta_i^{t+1} - v_{[n]}^{t+1} \right\| \\
&= \|\theta^t - \beta \sum_{i \in \mathcal{S}} \omega_i \nabla G_i(\theta_i^t) - v_{[n]}^t + \beta \nabla G(v_{[n]}^t)\| \\
&\leq \|\theta^t - v_{[n]}^t\| + \beta \left\| \sum_{i \in \mathcal{S}} \omega_i (\nabla G_i(\theta_i^t) - \nabla G_i(v_{[n]}^t)) \right\| \\
&\leq \|\theta^t - v_{[n]}^t\| + \beta \sum_{i \in \mathcal{S}} \omega_i \|\nabla G_i(\theta_i^t) - \nabla G_i(v_{[n]}^t)\| \\
&\leq \|\theta^t - v_{[n]}^t\| + \beta H' \sum_{i \in \mathcal{S}} \omega_i \|\theta_i^t - v_{[n]}^t\| \\
&\leq \|\theta^t - v_{[n]}^t\| + \beta H' \sum_{i \in \mathcal{S}} \omega_i g(t - (n-1)T_0) \\
&= \|\theta^t - v_{[n]}^t\| + \alpha' [(1 + \beta H')^{t - (n-1)T_0} - 1], \quad (26)
\end{aligned}$$

where $\alpha' = \beta[\delta + \alpha C(H\delta + B\sigma + \tau)]$. Since $\theta^{(n-1)T_0} = v_{[n]}^{(n-1)T_0}$, we have

$$\begin{aligned}
& \|\theta^t - v_{[n]}^t\| \\
&\leq \sum_{j=1}^{t - (n-1)T_0} \{\alpha' [(1 + \beta H')^j - 1]\} \\
&= \frac{\alpha'}{\beta H'} [(1 + \beta H')^{t - (n-1)T_0} - 1] - \alpha' [t - (n-1)T_0] \\
&\triangleq h(t - (n-1)T_0). \quad (27)
\end{aligned}$$

Next, we evaluate the convergence performance of virtual sequence $v_{[n]}^t$ during the interval $[n]$ for $t \in [(n-1)T_0, nT_0]$. Since $G(\cdot)$ is H' -smooth, we can have

$$\begin{aligned}
G(v_{[n]}^{t+1}) - G(v_{[n]}^t) &\leq \langle \nabla G(v_{[n]}^t), v_{[n]}^{t+1} - v_{[n]}^t \rangle \\
&\quad + \frac{H'}{2} \|v_{[n]}^{t+1} - v_{[n]}^t\|^2 \\
&\leq -\beta \left(1 - \frac{H'\beta}{2}\right) \|\nabla G(v_{[n]}^t)\|^2. \quad (28)
\end{aligned}$$

Moreover, since $G(\cdot)$ is μ' -strongly convex, it follows that

$$G(v_{[n]}^t) \leq G(\theta^*) + \frac{1}{2\mu'} \|\nabla G(v_{[n]}^t)\|^2. \quad (29)$$

Combining (28) and (29) gives us

$$G(v_{[n]}^{t+1}) - G(v_{[n]}^t) \leq -2\beta\mu' \left(1 - \frac{H'\beta}{2}\right) [G(v_{[n]}^t) - G(\theta^*)]$$

which is equivalent with

$$\begin{aligned}
G(v_{[n]}^{t+1}) - G(\theta^*) &\leq \left[1 - 2\beta\mu' \left(1 - \frac{H'\beta}{2}\right)\right] [G(v_{[n]}^t) - G(\theta^*)] \\
&= \xi [G(v_{[n]}^t) - G(\theta^*)],
\end{aligned}$$

where $\xi = 1 - 2\beta\mu' \left(1 - \frac{H'\beta}{2}\right) \in (0, 1)$ given $\beta < \min\{\frac{1}{2\mu'}, \frac{2}{H'}\}$. Iteratively, we can obtain

$$\begin{aligned}
G(v_{[n]}^{nT_0}) - G(\theta^*) &\leq \xi [G(v_{[n]}^{nT_0-1}) - G(\theta^*)] \\
&\leq \xi^2 [G(v_{[n]}^{nT_0-2}) - G(\theta^*)] \\
&\dots \\
&\leq \xi^{T_0} [G(v_{[n]}^{(n-1)T_0}) - G(\theta^*)] \\
&= \xi^{T_0} [G(v_{[n-1]}^{(n-1)T_0}) - G(\theta^*)] \\
&\quad + \xi^{T_0} [G(v_{[n]}^{(n-1)T_0}) - G(v_{[n-1]}^{(n-1)T_0})]. \quad (30)
\end{aligned}$$

Note that

$$\begin{aligned}
\|\nabla G(\theta)\| &= \left\| \sum_{i \in \mathcal{S}} \omega_i [(I - \alpha \nabla^2 L_i(\theta)) \nabla L_i(\phi_i)] \right\| \\
&\leq \sum_{i \in \mathcal{S}} \omega_i \|I - \alpha \nabla^2 L_i(\theta)\| \|\nabla L_i(\phi_i)\| \\
&\leq (1 - \alpha\mu)B. \quad (31)
\end{aligned}$$

From the Mean Value Theorem, we conclude that $\|G(\theta) - G(\theta')\| \leq (1 - \alpha\mu)B\|\theta - \theta'\|$. Hence, we can upper bound $G(v_{[n]}^{(n-1)T_0}) - G(v_{[n-1]}^{(n-1)T_0})$ as follows.

$$\begin{aligned}
& G(v_{[n]}^{(n-1)T_0}) - G(v_{[n-1]}^{(n-1)T_0}) \\
&= G(\theta^{(n-1)T_0}) - G(v_{[n-1]}^{(n-1)T_0}) \\
&\leq B(1 - \alpha\mu) \|\theta^{(n-1)T_0} - v_{[n-1]}^{(n-1)T_0}\| \\
&\stackrel{(a)}{\leq} B(1 - \alpha\mu)h(T_0), \quad (32)
\end{aligned}$$

where (a) is from (27). Substitute (32) in (30), we have

$$\begin{aligned}
& G(v_{[n]}^{nT_0}) - G(\theta^*) \\
&\leq \xi^{T_0} [G(v_{[n-1]}^{(n-1)T_0}) - G(\theta^*)] + \xi^{T_0} B(1 - \alpha\mu)h(T_0).
\end{aligned}$$

Iteratively, it follows that

$$\begin{aligned}
& G(v_{[N]}^{NT_0}) - G(\theta^*) \\
&\leq \xi^{T_0} [G(v_{[N-1]}^{(N-1)T_0}) - G(\theta^*)] + \xi^{T_0} B(1 - \alpha\mu)h(T_0) \\
&\leq \xi^{2T_0} [G(v_{[N-2]}^{(N-2)T_0}) - G(\theta^*)] + (\xi^{T_0} + \xi^{2T_0}) B(1 - \alpha\mu)h(T_0) \\
&\dots \\
&\leq \xi^{(N-1)T_0} [G(v_{[1]}^{T_0}) - G(\theta^*)] + \sum_{j=1}^{N-1} \xi^{jT_0} B(1 - \alpha\mu)h(T_0) \\
&\leq \xi^{NT_0} [G(v_{[1]}^0) - G(\theta^*)] + \sum_{j=1}^{N-1} \xi^{jT_0} B(1 - \alpha\mu)h(T_0) \\
&= \xi^{NT_0} [G(\theta^0) - G(\theta^*)] + \sum_{j=1}^{N-1} \xi^{jT_0} B(1 - \alpha\mu)h(T_0).
\end{aligned}$$

Therefore, we can conclude that

$$\begin{aligned}
& G(\boldsymbol{\theta}^T) - G(\boldsymbol{\theta}^*) \\
&= G(\mathbf{v}_{[N+1]}^{NT_0}) - G(\boldsymbol{\theta}^*) \\
&= G(\mathbf{v}_{[N]}^{NT_0}) - G(\boldsymbol{\theta}^*) + G(\mathbf{v}_{[N+1]}^{NT_0}) - G(\mathbf{v}_{[N]}^{NT_0}) \\
&\leq \xi^{NT_0} [G(\boldsymbol{\theta}^0) - G(\boldsymbol{\theta}^*)] + \sum_{j=1}^{N-1} \xi^{jT_0} B(1 - \alpha\mu)h(T_0) \\
&\quad + B(1 - \alpha\mu)h(T_0) \\
&= \xi^T [G(\boldsymbol{\theta}^0) - G(\boldsymbol{\theta}^*)] + \frac{1 - \xi^T}{1 - \xi^{T_0}} B(1 - \alpha\mu)h(T_0) \\
&\leq \xi^T [G(\boldsymbol{\theta}^0) - G(\boldsymbol{\theta}^*)] + \frac{B(1 - \alpha\mu)}{1 - \xi^{T_0}} h(T_0),
\end{aligned}$$

thereby completing the proof of Theorem 2.

APPENDIX D PROOF OF THEOREM 3

Recall that the optimal model parameter is denoted as $\phi_t^* = \boldsymbol{\theta}_t^* - \alpha \nabla L_t^*(\boldsymbol{\theta}_t^*)$, i.e., ϕ_t^* can be obtained through one-step gradient update from parameter $\boldsymbol{\theta}_t^*$. However, through the fast adaptation from the meta-learned model $\boldsymbol{\theta}_c$, we have $\phi_t = \boldsymbol{\theta}_c - \alpha \nabla L_t(\boldsymbol{\theta}_c)$, where $\boldsymbol{\theta}_c$ can be regarded as an estimation of $\boldsymbol{\theta}_t^*$ and $L_t(\cdot)$ is the sample average approximation of $L_t^*(\cdot)$. To evaluate the learning performance at the target, we next evaluate the gap between $L_t^*(\phi_t^*)$ and $L_t^*(\phi_t)$, i.e., the gap between the optimal loss and the actual loss based on learned parameter ϕ_t .

For convenience, denote $\tilde{\phi}_t = \boldsymbol{\theta}_t^* - \alpha \nabla L_t(\boldsymbol{\theta}_t^*)$. Note that

$$\begin{aligned}
\|\phi_t - \phi_t^*\| &= \|\phi_t - \tilde{\phi}_t + \tilde{\phi}_t - \phi_t^*\| \\
&\leq \underbrace{\|\phi_t - \tilde{\phi}_t\|}_{(a)} + \underbrace{\|\tilde{\phi}_t - \phi_t^*\|}_{(b)},
\end{aligned} \tag{33}$$

where (a) represents the error introduced by the gap between meta-learned model $\boldsymbol{\theta}_c$ and the target optimal $\boldsymbol{\theta}_t^*$, and (b) captures the error from the sample average approximation of the loss function.

We have the following bound on the term in (a):

$$\begin{aligned}
\|\phi_t - \tilde{\phi}_t\| &= \|\boldsymbol{\theta}_c - \boldsymbol{\theta}_t^* - \alpha(\nabla L_t(\boldsymbol{\theta}_c) - \nabla L_t(\boldsymbol{\theta}_t^*))\| \\
&\leq \|\boldsymbol{\theta}_c - \boldsymbol{\theta}_t^*\| + \alpha \|\nabla L_t(\boldsymbol{\theta}_c) - \nabla L_t(\boldsymbol{\theta}_t^*)\| \\
&\leq (1 + \alpha H) \|\boldsymbol{\theta}_c - \boldsymbol{\theta}_t^*\| \\
&= (1 + \alpha H) \|\boldsymbol{\theta}_c - \boldsymbol{\theta}_c^* + \boldsymbol{\theta}_c^* - \boldsymbol{\theta}_t^*\| \\
&\leq (1 + \alpha H) [\|\boldsymbol{\theta}_c - \boldsymbol{\theta}_c^*\| + \|\boldsymbol{\theta}_c^* - \boldsymbol{\theta}_t^*\|] \\
&\leq (1 + \alpha H) [\epsilon_c + \|\boldsymbol{\theta}_c^* - \boldsymbol{\theta}_t^*\|].
\end{aligned} \tag{34}$$

To evaluate the term in (b), we first note that $\|\tilde{\phi}_t - \phi_t^*\| = \alpha \|\nabla L_t(\boldsymbol{\theta}_t^*) - \nabla L_t^*(\boldsymbol{\theta}_t^*)\|$. Here, $\nabla L_t(\cdot) = \frac{1}{K} \sum_{(\mathbf{x}_t^j, \mathbf{y}_t^j) \in D_t} \nabla l(\cdot, (\mathbf{x}_t^j, \mathbf{y}_t^j))$, and $\nabla L_t^*(\cdot) = \mathbb{E}_{(\mathbf{x}_t, \mathbf{y}_t) \sim P_t} \nabla l(\cdot, (\mathbf{x}_t, \mathbf{y}_t))$. Define $q_t(\cdot) \triangleq \nabla l_t(\cdot)$. Then

$$Q_t(\boldsymbol{\theta}_t^*) \triangleq \frac{1}{K} \sum_{(\mathbf{x}_t^j, \mathbf{y}_t^j) \in D_t} q_t(\boldsymbol{\theta}_t^*, (\mathbf{x}_t^j, \mathbf{y}_t^j)) = \nabla L_t(\boldsymbol{\theta}_t^*),$$

and

$$Q_t^*(\boldsymbol{\theta}_t^*) \triangleq \mathbb{E}_{(\mathbf{x}_t, \mathbf{y}_t) \sim P_t} q_t(\boldsymbol{\theta}_t^*, (\mathbf{x}_t, \mathbf{y}_t)) = \nabla L_t^*(\boldsymbol{\theta}_t^*).$$

Clearly $Q_t(\cdot)$ is the sample average approximation of $Q_t^*(\cdot)$. Since $l(\boldsymbol{\theta}, (\mathbf{x}_t^j, \mathbf{y}_t^j))$ is H -smooth for all $\boldsymbol{\theta} \in \mathbb{R}^d$ and $(\mathbf{x}_t^j, \mathbf{y}_t^j) \sim P_t$, from Theorem 7.73 in [26] about uniform law of large number, we can know that for any $\epsilon > 0$ there exist positive constants C_t and $\eta = \eta(\epsilon)$ such that

$$\Pr \left\{ \sup_{\boldsymbol{\theta} \in \Theta} \|Q_t(\boldsymbol{\theta}) - Q_t^*(\boldsymbol{\theta})\| \geq \epsilon \right\} \leq C_t e^{-K\eta},$$

where $\Theta = \{\boldsymbol{\theta} \mid \|\boldsymbol{\theta} - \boldsymbol{\theta}_c\| \leq D\}$ and D is some constant. Hence, we have

$$\Pr \left\{ \|\tilde{\phi}_t - \phi_t^*\| \leq \alpha\epsilon \right\} \geq 1 - C_t e^{-K\eta}. \tag{35}$$

Since $L_t^*(\cdot)$ is also H -smooth, combining (34) and (35) proves Theorem 3.

APPENDIX E PROOF OF THEOREM 4

Let $\tilde{l}(\boldsymbol{\theta}, \mathbf{x}) \triangleq l(\boldsymbol{\theta}, (\mathbf{x}, \mathbf{y}_0)) - \lambda c((\mathbf{x}, \mathbf{y}_0), (\mathbf{x}_0, \mathbf{y}_0))$, then the robust surrogate loss $l_\lambda(\boldsymbol{\theta}, (\mathbf{x}_0, \mathbf{y}_0)) = \sup_{\mathbf{x} \in \mathcal{X}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x})$. Based on Assumption 5 and 7, it can be easily shown that $\tilde{l}(\boldsymbol{\theta}, \mathbf{x})$ is $(\lambda - H_{\mathbf{xx}})$ -strongly concave with respect to \mathbf{x} . Let $\mathbf{x}^*(\boldsymbol{\theta}) = \arg\max_{\mathbf{x} \in \mathcal{X}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x})$. From Lemma 1 in [19], we conclude that l_λ is differentiable and $\nabla_{\boldsymbol{\theta}} l_\lambda(\boldsymbol{\theta}, (\mathbf{x}_0, \mathbf{y}_0)) = \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta}))$. Moreover,

$$\|\mathbf{x}^*(\boldsymbol{\theta}) - \mathbf{x}^*(\boldsymbol{\theta}')\| \leq \frac{H_{\mathbf{x}\boldsymbol{\theta}}}{\lambda - H_{\mathbf{xx}}} \|\boldsymbol{\theta} - \boldsymbol{\theta}'\|, \tag{36}$$

and

$$\begin{aligned}
\|\nabla_{\boldsymbol{\theta}} l_\lambda(\boldsymbol{\theta}) - \nabla_{\boldsymbol{\theta}} l_\lambda(\boldsymbol{\theta}')\| &\leq \left(H + \frac{H_{\boldsymbol{\theta}\mathbf{x}} H_{\mathbf{x}\boldsymbol{\theta}}}{\lambda - H_{\mathbf{xx}}} \right) \|\boldsymbol{\theta} - \boldsymbol{\theta}'\| \\
&\triangleq H_\lambda \|\boldsymbol{\theta} - \boldsymbol{\theta}'\|.
\end{aligned}$$

Besides,

$$\begin{aligned}
& \|\nabla_{\boldsymbol{\theta}} l_\lambda(\boldsymbol{\theta}) - \nabla_{\boldsymbol{\theta}} l_\lambda(\boldsymbol{\theta}')\| \\
&= \|\nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta})) - \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}', \mathbf{x}^*(\boldsymbol{\theta}'))\| \\
&= \|\nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta})) - \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta}')) + \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta}')) \\
&\quad - \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}', \mathbf{x}^*(\boldsymbol{\theta}'))\| \\
&\geq \|\nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta}')) - \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}', \mathbf{x}^*(\boldsymbol{\theta}'))\| \\
&\quad - \|\nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta})) - \nabla_{\boldsymbol{\theta}} \tilde{l}(\boldsymbol{\theta}, \mathbf{x}^*(\boldsymbol{\theta}'))\| \\
&\geq \mu \|\boldsymbol{\theta} - \boldsymbol{\theta}'\| - H_{\boldsymbol{\theta}\mathbf{x}} \|\mathbf{x}^*(\boldsymbol{\theta}) - \mathbf{x}^*(\boldsymbol{\theta}')\| \\
&\geq \left(\mu - \frac{H_{\boldsymbol{\theta}\mathbf{x}} H_{\mathbf{x}\boldsymbol{\theta}}}{\lambda - H_{\mathbf{xx}}} \right) \|\boldsymbol{\theta} - \boldsymbol{\theta}'\| \triangleq \mu_\lambda \|\boldsymbol{\theta} - \boldsymbol{\theta}'\|.
\end{aligned}$$

So the strongly convexity and smoothness of the robust surrogate loss l_λ still hold if λ is large enough. Based on the triangle inequality, $\mathbb{E}_{P_i} [l_\lambda(\boldsymbol{\theta}, (\mathbf{x}_i, \mathbf{y}_i))]$ is μ_λ -strongly convex and H_λ -smooth both with respect to $\boldsymbol{\theta}$ for all $i \in \mathcal{S}$.

Denote $\tilde{H}_i(\boldsymbol{\theta}) = \mathbb{E}_{P_i} [l_\lambda(\boldsymbol{\theta}, (\mathbf{x}_i, \mathbf{y}_i))]$. Then we have

$$\begin{aligned}
& \|\nabla_{\boldsymbol{\theta}} \mathbb{E}_{P_i} [l_\lambda(\phi_i(\boldsymbol{\theta}), (\mathbf{x}_i, \mathbf{y}_i))] - \nabla_{\boldsymbol{\theta}} \mathbb{E}_{P_i} [l_\lambda(\phi_i'(\boldsymbol{\theta}'), (\mathbf{x}_i, \mathbf{y}_i))]\| \\
&= \|\nabla \tilde{H}_i(\phi_i) [I - \alpha \nabla^2 L_i(\boldsymbol{\theta})] - \nabla \tilde{H}_i(\phi_i') [I - \alpha \nabla^2 L_i(\boldsymbol{\theta}')] \| \\
&= \|\nabla \tilde{H}_i(\phi_i) [I - \alpha \nabla^2 L_i(\boldsymbol{\theta})] - \nabla \tilde{H}_i(\phi_i') [I - \alpha \nabla^2 L_i(\boldsymbol{\theta}')] \| \\
&\quad + \alpha \nabla \tilde{H}_i(\phi_i') \nabla^2 L_i(\boldsymbol{\theta}) - \alpha \nabla \tilde{H}_i(\phi_i') \nabla^2 L_i(\boldsymbol{\theta}) \| \\
&= \|\nabla \tilde{H}_i(\phi_i) - \nabla \tilde{H}_i(\phi_i')\| [I - \alpha \nabla^2 L_i(\boldsymbol{\theta})] \\
&\quad - \alpha \nabla \tilde{H}_i(\phi_i') [\nabla^2 L_i(\boldsymbol{\theta}) - \nabla^2 L_i(\boldsymbol{\theta}')] \|.
\end{aligned} \tag{37}$$

Since $\nabla\phi_i = I - \alpha\nabla^2 L_i(\boldsymbol{\theta})$, it follows from Assumption 6 and 7 that $1 - \alpha H \leq \nabla\phi_i \leq 1 - \alpha\mu$, which indicates

$$(1 - \alpha H)\|\boldsymbol{\theta} - \boldsymbol{\theta}'\| \leq \|\phi_i - \phi_i'\| \leq (1 - \alpha\mu)\|\boldsymbol{\theta} - \boldsymbol{\theta}'\|.$$

Continuing with (37), it is clear that

$$\begin{aligned} & \|\nabla_{\boldsymbol{\theta}} \mathbb{E}_{P_i}[l_{\lambda}(\phi_i(\boldsymbol{\theta}), (\mathbf{x}_i, \mathbf{y}_i))] - \nabla_{\boldsymbol{\theta}} \mathbb{E}_{P_i}[l_{\lambda}(\phi_i'(\boldsymbol{\theta}'), (\mathbf{x}_i, \mathbf{y}_i))]\| \\ & \geq (1 - \alpha H)\|\nabla\tilde{H}_i(\phi_i) - \nabla\tilde{H}_i(\phi_i')\| \\ & \quad - \alpha B\|\nabla^2 L_i(\boldsymbol{\theta}) - \nabla^2 L_i(\boldsymbol{\theta}')\| \\ & \geq \mu_{\lambda}(1 - \alpha H)\|\phi_i - \phi_i'\| - \alpha B\rho\|\boldsymbol{\theta} - \boldsymbol{\theta}'\| \\ & \geq [\mu_{\lambda}(1 - \alpha H)^2 - \alpha B\rho]\|\boldsymbol{\theta} - \boldsymbol{\theta}'\|, \end{aligned}$$

and

$$\begin{aligned} & \|\nabla_{\boldsymbol{\theta}} \mathbb{E}_{P_i}[l_{\lambda}(\phi_i(\boldsymbol{\theta}), (\mathbf{x}_i, \mathbf{y}_i))] - \nabla_{\boldsymbol{\theta}} \mathbb{E}_{P_i}[l_{\lambda}(\phi_i'(\boldsymbol{\theta}'), (\mathbf{x}_i, \mathbf{y}_i))]\| \\ & \leq (1 - \alpha\mu)\|\nabla\tilde{H}_i(\phi_i) - \nabla\tilde{H}_i(\phi_i')\| \\ & \quad + \alpha B\|\nabla^2 L_i(\boldsymbol{\theta}) - \nabla^2 L_i(\boldsymbol{\theta}')\| \\ & \leq H_{\lambda}(1 - \alpha\mu)\|\phi_i - \phi_i'\| + \alpha B\rho\|\boldsymbol{\theta} - \boldsymbol{\theta}'\| \\ & \leq [H_{\lambda}(1 - \alpha\mu)^2 + \alpha B\rho]\|\boldsymbol{\theta} - \boldsymbol{\theta}'\|. \end{aligned}$$

From the definition of $\tilde{G}_i(\boldsymbol{\theta})$, we can have that $\tilde{G}_i(\boldsymbol{\theta})$ is μ_R -strongly convex and H_R -smooth, where $\mu_R = \mu + \mu_{\lambda}(1 - \alpha H)^2 - \alpha B\rho$ and $H_R = H + H_{\lambda}(1 - \alpha\mu)^2 + \alpha B\rho$. Based on the triangle inequality, Theorem 4 can be proved.