Technical Report:
Mitigating Distributed DoS Attacks on Bandwidth Allocation for Federated Learning in Mobile Edge Networks

Yang Xu, Shanshan Zhang, Chen Lyu, Jia Liu, Yulong Shen and Shiratori Norio

May, 2023

In this technical report, we provide the detailed proofs for Theorem 3, Theorem 4 and Theorem 5 in the manuscript: *Mitigating Distributed DoS Attacks on Bandwidth Allocation for Federated Learning in Mobile Edge Networks.*

1 Appendix A
Proof of Theorem 3

Proof. The statement in [1] suggests that if $\frac{\mathrm{d}\dot{\eta}_k}{\mathrm{d}\eta_k} < 0$ holds for any η_k, then the evolutionary equilibrium $\boldsymbol{\eta}^e$ is asymptotically stable.

Therefore, we first change the replicator dynamics of Equation (15) to the following form:

$$\dot{\eta}_k = \alpha\eta_k \sum_{j\in\mathcal{K}\setminus\{k\}} \eta_j(c_k(\eta_k) - c_j(\eta_j)). \tag{35}$$

For $\dot{\eta}_k$, we computer the derivative with respect to b_k

$$\begin{aligned}\frac{\mathrm{d}\dot{\eta}_k}{\mathrm{d}\eta_k} = \alpha\eta_k \sum_{j\in\mathcal{K}\setminus\{k\}} \eta_j(\frac{\mathrm{d}c_k(\eta_k)}{\mathrm{d}\eta_k} - \frac{\mathrm{d}c_j(\eta_j)}{\mathrm{d}\eta_k}) \\ + \alpha \sum_{j\in\mathcal{K}\setminus\{k\}} \eta_j(c_k(\eta_k) - c_j(\eta_j)).\end{aligned} \tag{36}$$

According to Theorem 1, we have

$$c_j(\eta_j) = c_k(\eta_k), \forall j \in \mathcal{K}\setminus\{k\}. \tag{37}$$

Hence, we can obtain

$$\sum_{j\in\mathcal{K}\setminus\{k\}} \eta_j(c_k(\eta_k) - c_j(\eta_j)) = 0. \tag{38}$$

Since $\eta_j = 1-\eta_k-\sum_{l\in\mathcal{K}\setminus\{k,j\}}\eta_l$, the cost function $c_j(\eta_j)$ can be rewritten as the function of η_k:

$$c_j(\eta_k) = l_j^L + \frac{\psi_k}{B_j(1-\eta_k-\sum_{l\in\mathcal{K}\setminus\{k,j\}}\eta_{n,l})}. \tag{39}$$

By taking the derivative of c_j to η_k, we have

$$\frac{\mathrm{d}c_j}{\mathrm{d}\eta_k} = \frac{\psi_k}{B_j(1-\eta_k-\sum_{l\in\mathcal{K}\setminus\{k,j\}}\eta_{n,l})^2} > 0. \tag{40}$$

Based on Equation (17) and (40), it is found that $\frac{\mathrm{d}c_k}{\mathrm{d}\eta_k} < 0$ and $\frac{\mathrm{d}c_j}{\mathrm{d}\eta_k} > 0$. Hence, we have $\frac{\mathrm{d}c_k}{\mathrm{d}\eta_k} - \frac{\mathrm{d}c_j}{\mathrm{d}\eta_k} < 0$, and obtain $\frac{\mathrm{d}\dot{\eta}_k}{\mathrm{d}\eta_k} < 0$ for any η_k in Equation (36). □

2 Appendix B
Proof of Theorem 4

Proof. According to the update rule for Lagrange multipliers in (34), the dynamics of the variables are defined as $\hat{\lambda}_i(t) = \lambda_i^{(t+1)} - \lambda_i^{(t)}$ and $\hat{\mu}_{ji}(t) = \mu_i^{(t+1)} - \mu_i^{(t)}$, which can be also expressed as:

$$\hat{\lambda}_i(t) = \begin{cases} \sum_{j=1}^{N} y_{i,j} - B_i & \lambda_i > 0, \\ 0 & \lambda_i = 0, \end{cases} \forall i \in \mathcal{M}, \tag{41}$$

$$\hat{\mu}_{ji}(t) = \begin{cases} x_{j,i} - y_{i,j} & \mu_{ji} > 0, \\ 0 & \mu_{ji} = 0, \end{cases} \forall i \in \mathcal{M}, \forall j \in \mathcal{N}. \tag{42}$$

Then, the Lyapunov function is defined as:

$$Z(\boldsymbol{\lambda}, \boldsymbol{\mu}) = \frac{1}{2}\sum_{i=1}^{M}(\lambda_i - \lambda_i^{\dagger})^2 + \frac{1}{2}\sum_{j=1}^{N}\sum_{i=1}^{M}(\mu_{j,i} - \mu_{j,i}^{\dagger})^2. \tag{43}$$

Taking the first derivative of the Lyapunov function $Z(\boldsymbol{\lambda},\boldsymbol{\mu})$ with respect to t, we can obtain:

$$\frac{dZ(\boldsymbol{\lambda}, \boldsymbol{\mu})}{dt} = \sum_{i=1}^{M}(\lambda_i - \lambda_i^{\dagger})\hat{\lambda}_i(t) + \sum_{j=1}^{N}\sum_{i=1}^{M}(\mu_{j,i} - \mu_{j,i}^{\dagger})\hat{\mu}_{ji}(t). \tag{44}$$

We can also write the following inequalities for $\hat{\lambda}_i(t)$ and $\hat{\mu}_{ji}(t)$:

$$\hat{\lambda}_i(t) \leqslant \left(\sum_{j=1}^{N} y_{i,j} - B_i\right), \tag{45}$$

$$\hat{\mu}_{ji}(t) \leqslant (x_{j,i} - y_{i,j}). \tag{46}$$

Based on Equations (44)-(46), we can derive the upper bound of the Lyapunov function as follows:

$$\begin{aligned} \frac{dZ(\boldsymbol{\lambda}, \boldsymbol{\mu})}{dt} \leqslant & \sum_{i=1}^{M}(\lambda_i - \lambda_i^{\dagger})\left(\sum_{j=1}^{N} y_{i,j} - B_i\right) \\ & + \sum_{j=1}^{N}\sum_{i=1}^{M}(\mu_{j,i} - \mu_{j,i}^{\dagger})(x_{j,i} - y_{i,j}). \end{aligned} \tag{47}$$

The inequality (47) can be equivalently transformed into:

$$\begin{aligned}\frac{dZ(\boldsymbol{\lambda},\boldsymbol{\mu})}{dt} \leqslant & \sum_{i=1}^{M}(\lambda_i-\lambda_i^{\dagger})\left(\sum_{j=1}^{N}y_{i,j}-\sum_{j=1}^{N}y_{i,j}^{\dagger}\right)\\ &+\sum_{i=1}^{M}(\lambda_i-\lambda_i^{\dagger})(\sum_{j=1}^{N}y_{i,j}^{\dagger}-B_i)\\ &+\sum_{j=1}^{N}\sum_{i=1}^{M}(\mu_{j,i}-\mu_{j,i}^{\dagger})(x_{j,i}^{\dagger}-y_{i,j}^{\dagger})\\ &+\sum_{j=1}^{N}\sum_{i=1}^{M}(\mu_{j,i}-\mu_{j,i}^{\dagger})[(x_{j,i}-x_{j,i}^{\dagger})-(y_{i,j}-y_{i,j}^{\dagger})].\end{aligned} \tag{48}$$

After using KKT conditions and the complementary relaxation conditions that are satisfied at the equilibrium, (48) can be transformed as:

$$\begin{aligned}\frac{dZ(\boldsymbol{\lambda},\boldsymbol{\mu})}{dt} \leqslant & \sum_{j=1}^{N}\sum_{i=1}^{M}(\frac{\partial U_{SP_j}(\mathbf{x}_j)}{\partial \mathbf{x}_j}-\frac{\partial U_{SP_j}(\mathbf{x}_j^{\dagger})}{\partial \mathbf{x}_j^{\dagger}})(x_{j,i}-x_{j,i}^{\dagger})\\ &+\sum_{j=1}^{N}\sum_{i=1}^{M}(\frac{\partial U_{NO}(\mathbf{y}_i^{\dagger})}{\mathbf{y}_i^{\dagger}}-\frac{\partial U_{NO}(\mathbf{y}_i)}{y_{i,j}})(y_{i,j}-y_{i,j}^{\dagger}).\end{aligned} \tag{49}$$

Due to the strictly concave property of SP's utility function and the strictly convex property of NO's cost function, we have

$$\begin{aligned}&\sum_{j=1}^{N}\sum_{i=1}^{M}(\frac{\partial U_{SP_j}(\mathbf{x}_j)}{\partial \mathbf{x}_j}-\frac{\partial U_{SP_j}(\mathbf{x}_j^{\dagger})}{\partial \mathbf{x}_j^{\dagger}})(x_{j,i}^{\dagger}-x_{j,i})\leqslant 0,\\ &\sum_{j=1}^{N}\sum_{i=1}^{M}(\frac{\partial U_{NO}(\mathbf{y}_i)}{\mathbf{y}_i}-\frac{\partial U_{NO}(\mathbf{y}_i^{\dagger})}{\mathbf{y}_i^{\dagger}})(y_{i,j}^{\dagger}-y_{i,j})\leqslant 0.\end{aligned} \tag{50}$$

Therefore,we can get $\frac{dZ(\lambda,\mu)}{dt}\leqslant 0$. Drawing upon the theoretical framework of Lyapunov stability theory [2, 3], we can infer that the Lagrange multipliers $\lambda_i^{(t)}$ and $\mu_{j,i}^{(t)}$ converge, confirming the stability of the DA-based allocation mechanism. □

3 Appendix C Proof of Theorem 5

Proof. The four economic properties are proven separately in what follows.

3.1 Individual Rationality

The individual rationality means that each participant in the market obtains a non-negative utility. Therefore, for each SP j, it should satisfies the following equation:

$$U_{SP_j}(\mathbf{x}_j^\dagger) - M_{SP_j}(\mathbf{p}_j^\dagger) \geqslant 0, \forall j \in \mathcal{N}. \tag{51}$$

We now prove that Equation (51) holds in the DA-based allocation mechanism. $U_{SP_j}(\mathbf{x}_j)$ is a strictly concave function of $\mathbf{x}_j$, and we have $U_{SP_j}(\mathbf{0}) = 0$. Based on Lagrange's Mean Value Theorem, we can deduce the following:

$$\begin{aligned} U_{SP_j}(\mathbf{x}_j^\dagger) &\geqslant U_{SP_j}(\mathbf{0}) + x_{j,i}^\dagger \frac{\partial U_{SP_j}(\mathbf{x}_j)}{\partial x_{j,i}^\dagger} \\ &= x_{j,i}^\dagger \frac{\partial U_{SP_j}(\mathbf{x}_j)}{\partial x_{j,i}^\dagger}. \end{aligned} \tag{52}$$

Based on the optimal bidding and payment rule of SP in the DA-based allocation mechanism, we obtain:

$$x_{j,i}^\dagger \frac{\partial U_{SP_j}(x_{j,i})}{\partial x_{j,i}^\dagger} = x_{j,i}^\dagger \frac{u_{j,i}}{x_{j,i}^\dagger} = M_{SP_j}(\mathbf{p}_j^\dagger), \tag{53}$$

which can be deduced that Equation (51) is always satisfied.

Additionally, due to the convex nature of the cost function for NOs and the optimal reward rule, we deduce that the constraint inequality for the NOs is always satisfied:

$$Q_{NO_j}(\mathbf{o}_i^\dagger) - U_{SP_j}(\mathbf{y}_j^\dagger) \geqslant 0, \forall i \in \mathcal{M}. \tag{54}$$

Hence, it can be concluded that the proposed DA-based allocation mechanism ensures individual rationality as the participants, both SPs and NOs, can always expect to receive non-negative utility from participating in the market.

3.2 Economic Efficiency and Incentive Compatibility

According to Theorem 4, our DA-based allocation mechanism converges to a point that satisfies all constraints of (22a)-(22e). Based on the pricing rules defined in (29) and (33) by the broker, the resulting optimal bids generated by the DA-based allocation mechanism lead to an optimal data allocation $\boldsymbol{X}^\dagger$ and $\boldsymbol{Y}^\dagger$. They are identical to the best solution of SWM, ensuring the overall operational efficiency of the market. Hence, the DA-based allocation mechanism not only achieves social welfare maximization but also satisfies the property of economic efficiency.

Our algorithm does not require SPs and NOs to reveal their private information to the market. They only need to determine their optimal bid by solving their own utility maximization problem in each iteration. This protects the privacy of their information and ensures that the participants have the autonomy to make decisions based on their own self-interest. Since the DA-based allocation algorithm only requires the participants to submit their optimal bids, it enables the broker to maximize the social welfare of the market through the submitted information. This design feature makes the DA-based allocation algorithm incentive-compatible, meaning that the participants have incentives to truthfully report their information and act in their self-interest.

3.3 Budget Balance

According to the local payoff maximization problem of SPs and NOs, the broker's budget $c(\mathbf{P},\ \mathbf{O})$ is defined as:

$$\begin{aligned} c(\mathbf{P},\ \mathbf{O}) &= \sum_{j=1}^{N} M_{SP_j}(\mathbf{p}_j) - \sum_{i=1}^{M} Q_{NO_i}(\mathbf{o}_i) \\ &= \sum_{j=1}^{N}\sum_{i=1}^{M}\left[p_{j,i} - \frac{(\mu_{j,i}^{\dagger} - \lambda_i^{\dagger})^2}{o_{i,j}}\right] \\ &= \sum_{j=1}^{N}\sum_{i=1}^{M}\left[\mu_{j,i}x_{j,i} - y_{i,j}(\mu_{j,i} - \lambda_i)\right]. \end{aligned} \tag{55}$$

By utilizing the optimal bids submitted by all participants, Equation (55) can be transformed into:

$$\begin{aligned} c(\mathbf{P},\ \mathbf{O}) = &\sum_{j=1}^{N}\sum_{i=1}^{M}\mu_{j,i}^{\dagger}(x_{j,i}^{\dagger} - y_{i,j}^{\dagger}) \\ &+ \sum_{i=1}^{M}\lambda_i^{\dagger}\sum_{j=1}^{N}\sum_{i=1}^{M}(y_{i,j}^{\dagger} - B_i) \\ &+ B_i\sum_{i=1}^{M}\lambda_i^{\dagger}. \end{aligned} \tag{56}$$

According to (22c)-(22e), we can conclude that when all the participants submit their optimal bids to the broker, Equation (56) is always non-negative, which proves the property of budget balance. □

References

[1] P. Semasinghe, E. Hossain, and K. Zhu, "An evolutionary game for distributed resource allocation in self-organizing small cells," *IEEE Trans. Mobile Comput.*, vol. 14, no. 2, pp. 274–287, 2014.

[2] H. H. E. Leipholz, "On conservative elastic systems of the first and second kind," *Ingenieur-Archiv*, vol. 43, no. 5, pp. 255–271, 1974.

[3] H. Leipholz, *Stability theory: an introduction to the stability of dynamic systems and rigid bodies.* Springer-Verlag, 2013.