BYZANTINE-RESILIENT DECENTRALIZED RESOURCE ALLOCATION

Runhua Wang[1] *Yaohua Liu*[2] *Qing Ling*[1]

[1]Sun Yat-Sen University [2]Nanjing University of Information Science and Technology

1. APPENDIX-NUMERICAL EXPERIMENTS

In this section, we present numerical experiments to demonstrate the resilience of BREDA to various Byzantine attacks.

1.1. Case 1: Synthetic Problem

This section presents numerical experiments to demonstrate the resilience of BREDA to various Byzantine attacks. More results on different cost functions and different fractions of Byzantine agents are left to the extended version. We consider the one-dimensional case such that $D = 1$. The upper bound of average resource is $\boldsymbol{s} = 5$. The local constraint of agent i is $\boldsymbol{\theta}_i \in \boldsymbol{C}_i = [0, 10]$. The local cost function of agent i is in the form of $f_i(\boldsymbol{\theta}_i) = -\alpha\beta_i \log(1 + \boldsymbol{\theta}_i)$ where $\alpha = 300$ is a constant and different agents i have different β_i. The variance of β_i reflects the heterogeneity of local cost functions.

We generate a connected random network consisting of $N = 100$ agents, but letting each agent have 15 neighbors. The maximum available amount of resources is 500, meaning that $\boldsymbol{s} = 5$. We randomly select $|\mathcal{B}|$ Byzantine agents, with $|\mathcal{B}| = 6$ by default. We test the performance of BREDA under two typical Byzantine attacks: max value and trimmed Gaussian attacks. With max value attacks, Byzantine agent $i \in \mathcal{B}$ sets its message as $z_i^k = 10$. For trimmed Gaussian attacks, Byzantine agent $i \in \mathcal{B}$ draws its message z_i^k from a Gaussian distribution with mean 7 and variance 9, followed by being trimmed to the range of $[0, 10]$. We set the lower and upper bounds since all the agents have the same local constraint $\boldsymbol{\theta}_i \in \boldsymbol{C}_i = [0, 10]$ such that the average demand of resource should also be within this range. We consider two baselines, Oracle and DRA. Oracle means that the Byzantine agents behave honestly, while DRA is subject to Byzantine attacks. In DRA, the weights $w_{ij} = \frac{1}{16}$ if and only if $(i, j) \in \mathcal{E}$ or $i = j$. The parameters γ and v are tuned to the best for Oracle, and then applied to DRA and BREDA. When β_i are randomly distributed within $[1, 2]$, $\gamma = 0.620$ and $v = 0.146$. The parameter of CTM is set as $b = 6$. Performance metrics include resource allocation strategy $\boldsymbol{\theta}_i^k$ for a randomly chosen honest agent i, average cost of honest agents $f(\hat{\boldsymbol{\theta}}^k)$, and constraint violation of honest agents $\frac{1}{|\mathcal{H}|}\sum_{i\in\mathcal{H}} \boldsymbol{\theta}_i^k - \boldsymbol{s}$.

Fig. 1 depicts the performance of Oracle, DRA and BREDA when β_i are randomly distributed within $[1, 2]$. Observe that the resource allocation strategy of DRA is far from its oracle value, while that of BREDA is much closer, under both Byzantine attacks. In terms of average cost and constraint violation of honest agents, the gaps between BREDA and Oracle are acceptable, while those between DRA and Oracle are significant. For the two Byzantine attacks, max value attacks are stronger than trimmed Gaussian attacks. Fig. 2 shows the performance of Oracle, DRA and BREDA when β_i follow Gaussian distribution with mean 1.5 and variance 1. Similar conclusions can be made as for Fig. 1. These two sets of numerical experiments demonstrate the vulnerability of DRA to Byzantine attacks, as well as the satisfactory Byzantine-resilience of BREDA.

In the above numerical experiments, the parameter of CTM b and the number of Byzantine agents $|\mathcal{B}|$ are both 6. In Fig. 3 we check the sensitivity of BREDA with respect to the number of Byzantine agents, by varying $|\mathcal{B}|$ as 1, 3 and 6. DRA fails in all cases, while BREDA is almost insensitive to $|\mathcal{B}|$.

1.2. Case 2: Economic Dispatch for IEEE 118-Bus Test System

Consider the power dispatch problem on the IEEE-118 bus test system with 54 generators [1]. Each generator i has a cost function of generated power $\boldsymbol{\theta}_i$, given by $f_i(\boldsymbol{\theta}_i) = \xi_i + \zeta_i\boldsymbol{\theta}_i + \eta_i\boldsymbol{\theta}_i^2$. The coefficients are in the ranges of $\xi_i \in [6.78, 74.33]$, $\zeta_i \in [8.3391, 37.6968]$, and $\eta_i \in [0.0024, 0.0697]$. Each $\boldsymbol{\theta}_i$ belongs to the set $[\boldsymbol{\theta}_i^{min}, \boldsymbol{\theta}_i^{max}]$, where $\boldsymbol{\theta}_i^{min} \in [5, 150]$ and $\boldsymbol{\theta}_i^{max} \in [30, 420]$. The total load is 6000 as in [2]. We let the physical connection between any two neighboring generators be bidirectional such that the graph is undirected. We randomly select $|\mathcal{B}| = 1$ Byzantine generator. The parameters γ and v are set as 0.5 and 0, respectively.

We test the performance of BREDA under max value and trimmed Gaussian attacks. For max value attacks, the Byzantine generator sets its message as 420. For trimmed Gaussian attacks, the Byzantine generator sets its message from a Gaussian distribution with mean 150 and variance 900, followed by being trimmed to the range of $[5, 420]$. In DRA, $\boldsymbol{W}$ is generated by the Metropolis constant weight rule [3]. Fig. 4 shows the performance of Oracle, DRA and BREDA. DRA fails under Byzantine attacks, while BREDA is close to Oracle and demonstrates to be Byzantine-resilient.

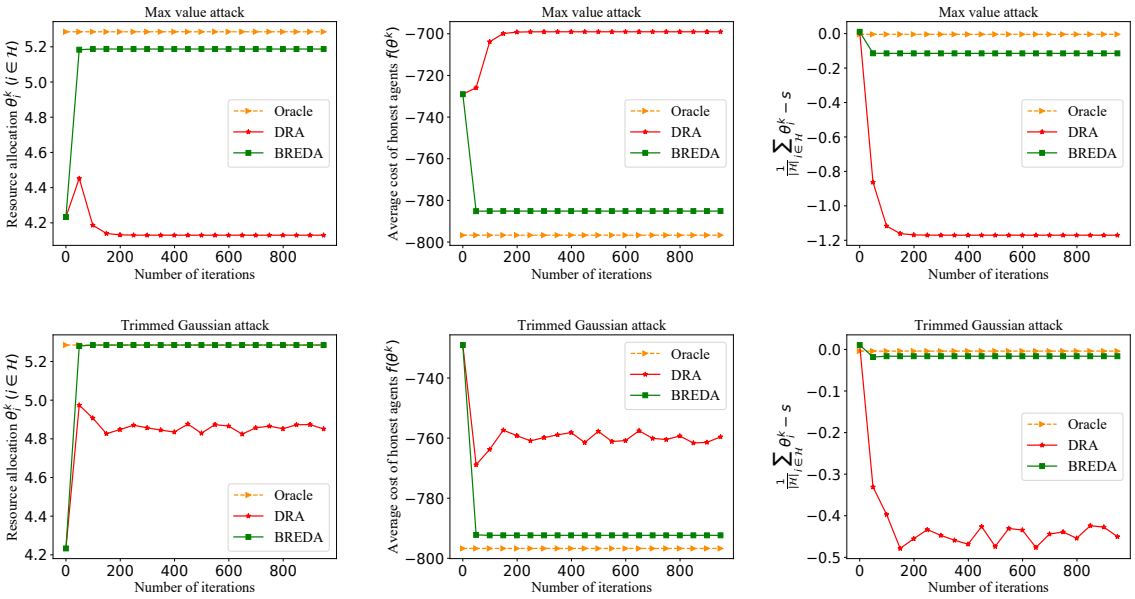

Fig. 1. Oracle without Byzantine attacks, DRA and BREDA under Byzantine attacks on synthetic problem, when β_i are randomly distributed within $[1, 2]$. From top to bottom: max value attacks and trimmed Gaussian attacks. From left to right: resource allocation of a randomly chosen honest agent i, average cost of honest agents, and constraint violation of honest agents.

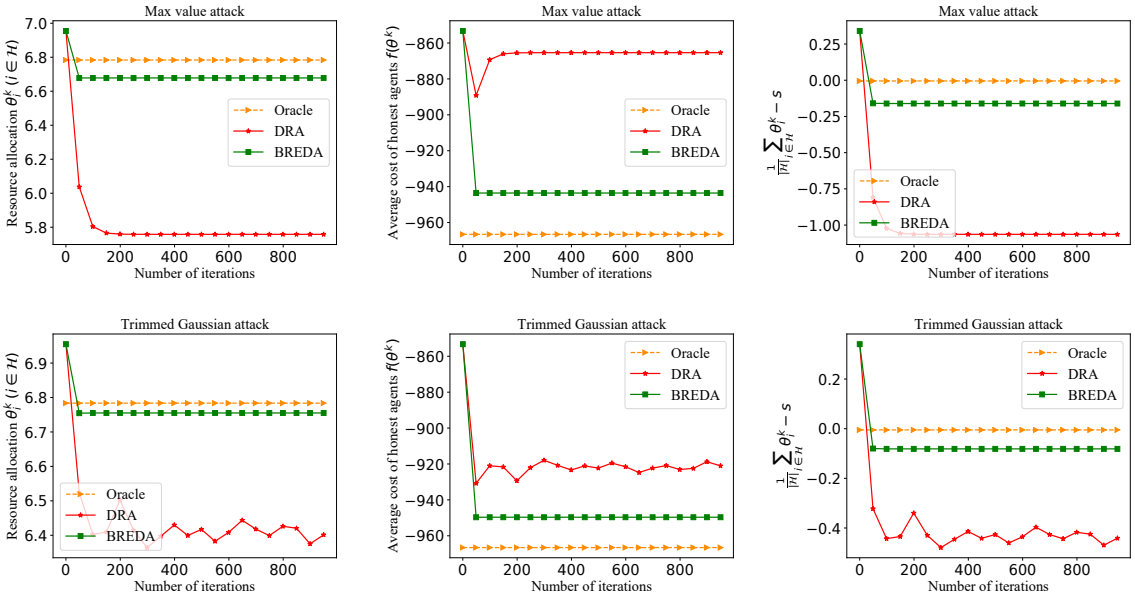

Fig. 2. Oracle without Byzantine attacks, DRA and BREDA under Byzantine attacks on synthetic problem, when β_i follow Gaussian distribution with mean 1.5 and variance 1. From top to bottom: max value attacks and trimmed Gaussian attacks. From left to right: resource allocation of a randomly chosen honest agent i, average cost of honest agents, and constraint violation of honest agents.

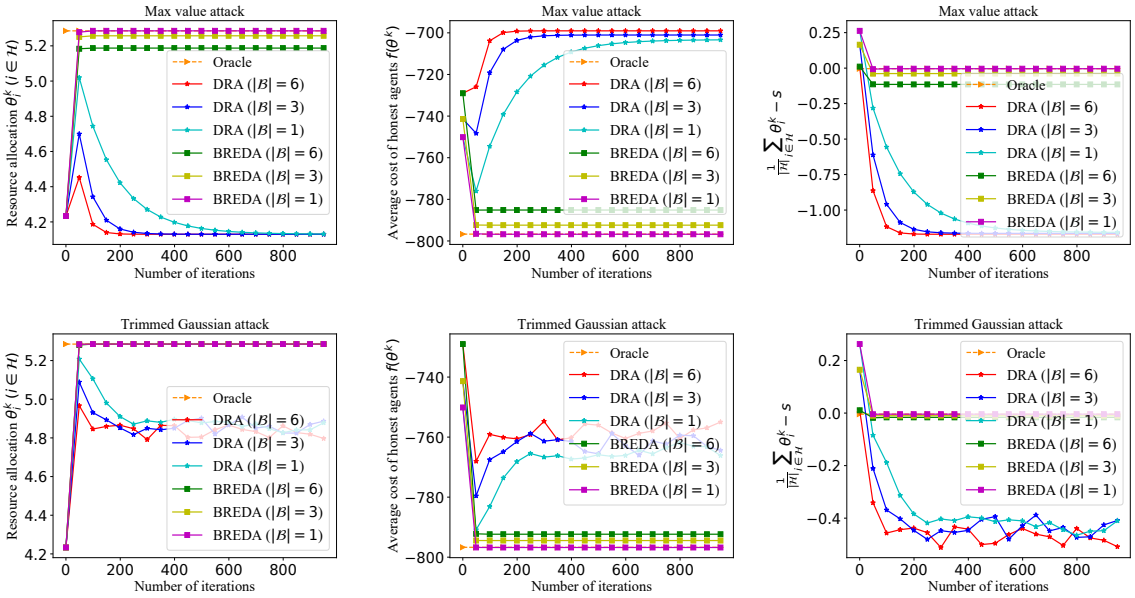

Fig. 3. Oracle without Byzantine attacks, DRA and BREDA under Byzantine attacks on synthetic problem, when β_i are randomly distributed within $[1, 2]$. The number of Byzantine agents $|\mathcal{B}|$ is set as 1, 3 and 6. From top to bottom: max value attacks and trimmed Gaussian attacks. From left to right: resource allocation of a randomly chosen honest agent i, average cost of honest agents, and constraint violation of honest agents.

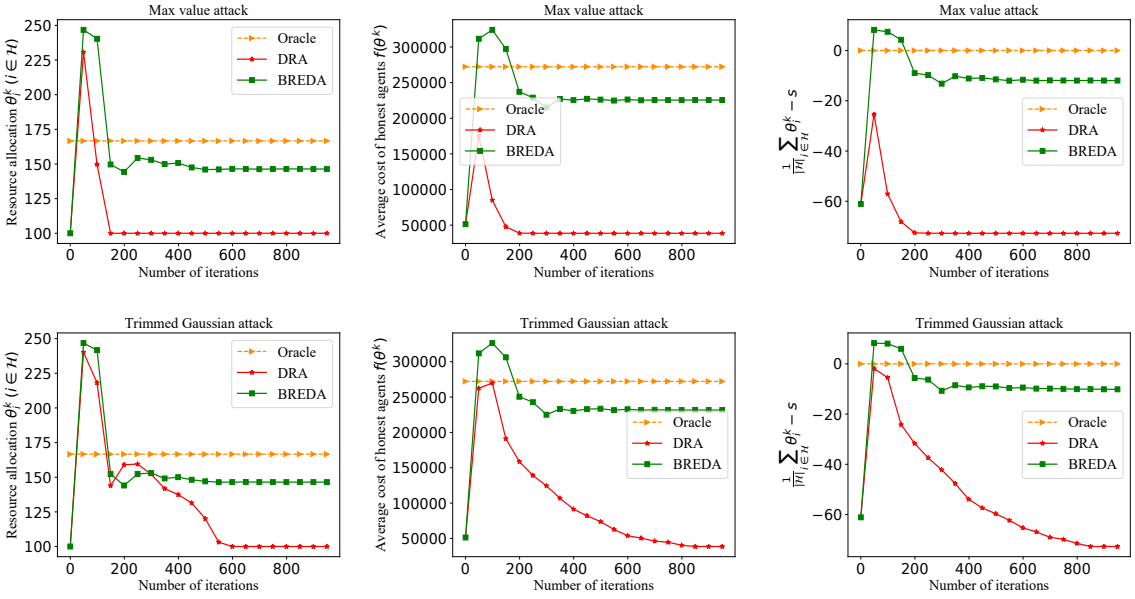

Fig. 4. Oracle without Byzantine attacks, DRA and BREDA under Byzantine attacks on economic dispatch problem. From top to bottom: max value attacks and trimmed Gaussian attacks. From left to right: resource allocation of a randomly chosen honest agent i, average cost of honest agents, and constraint violation of honest agents.

2. REFERENCES

[1] "IEEE 118 Bus System," [Online]. Available: https://www.al-roomi.org/power-flow/118-bus-system

[2] T. T. Doan, and C. L. Beck, "Distributed resource allocation over dynamic networks with uncertainty," IEEE Transactions on Automatic Control, vol. 66, no. 9, pp. 4378–4384, 2021.

[3] W. Shi, Q. Ling, G. Wu, and W. Yin, "EXTRA: An exact first-order algorithm for decentralized consensus optimization," SIAM Journal on Optimization, vol. 25, no. 2, pp. 944–966, 2015.