

Algorithm	Without Attack		ALIE	
	Total Time	Round time	Total Time	Round time
ADAM	6348.24	41.14 \pm 4.20	9321.00	62.14 \pm 4.83
FLTRUST	9418.31	62.79 \pm 14.53	12685.50	84.57 \pm 15.17
RECESS	12983.00	86.55 \pm 5.08	14782.50	98.55 \pm 3.24
ZENO	7539.43	50.26 \pm 4.35	10084.50	67.23 \pm 8.42
CC	10035.21	66.90 \pm 7.65	14208.45	94.72 \pm 6.17
CC+FBM	10826.48	68.24 \pm 9.81	13827.98	91.18 \pm 8.95
CC+BUCKETING	11217.39	71.11 \pm 8.71	14411.11	95.27 \pm 7.12
SAFEGUARD	7993.60	53.29 \pm 5.11	10684.13	71.23 \pm 4.67
VR MARINA	10018.68	67.12 \pm 18.24	13240.10	90.23 \pm 11.85
BANT	6925.92	46.17 \pm 3.17	10531.73	70.21 \pm 5.13
AUTOBANT	9307.05	62.05 \pm 7.67	12543.45	83.62 \pm 1.27
SIMBANT	8320.50	55.47 \pm 6.34	10873.37	72.49 \pm 7.65

Table 1: RESNET1D18 on ECG (AFIB).

Algorithm	Without Attack		ALIE	
	Total Time	Round time	Total Time	Round time
ADAM	3552.53	17.76 \pm 1.76	6148.72	30.74 \pm 1.87
FLTRUST	11527.65	57.64 \pm 7.55	14549.25	72.75 \pm 1.82
RECESS	13175.33	65.88 \pm 16.02	15397.44	76.99 \pm 6.27
ZENO	7626.38	38.13 \pm 2.26	10975.74	54.88 \pm 4.71
CC	4590.84	22.95 \pm 2.30	8667.56	43.34 \pm 6.28
CC+FBM	4814.73	23.44 \pm 2.81	9024.16	47.16 \pm 7.95
CC+BUCKETING	4167.23	20.18 \pm 2.12	8741.74	43.46 \pm 6.19
SAFEGUARD	8652.72	43.26 \pm 3.14	11658.47	58.29 \pm 2.31
VR MARINA	10897.72	55.84 \pm 9.14	14942.06	73.91 \pm 6.89
BANT	5861.51	29.31 \pm 2.56	11177.08	55.89 \pm 6.29
AUTOBANT	9850.26	49.25 \pm 5.77	13454.85	67.27 \pm 3.49
SIMBANT	6680.34	33.40 \pm 5.00	12022.55	60.11 \pm 8.70

Table 2: RESNET18 on CIFAR-10.

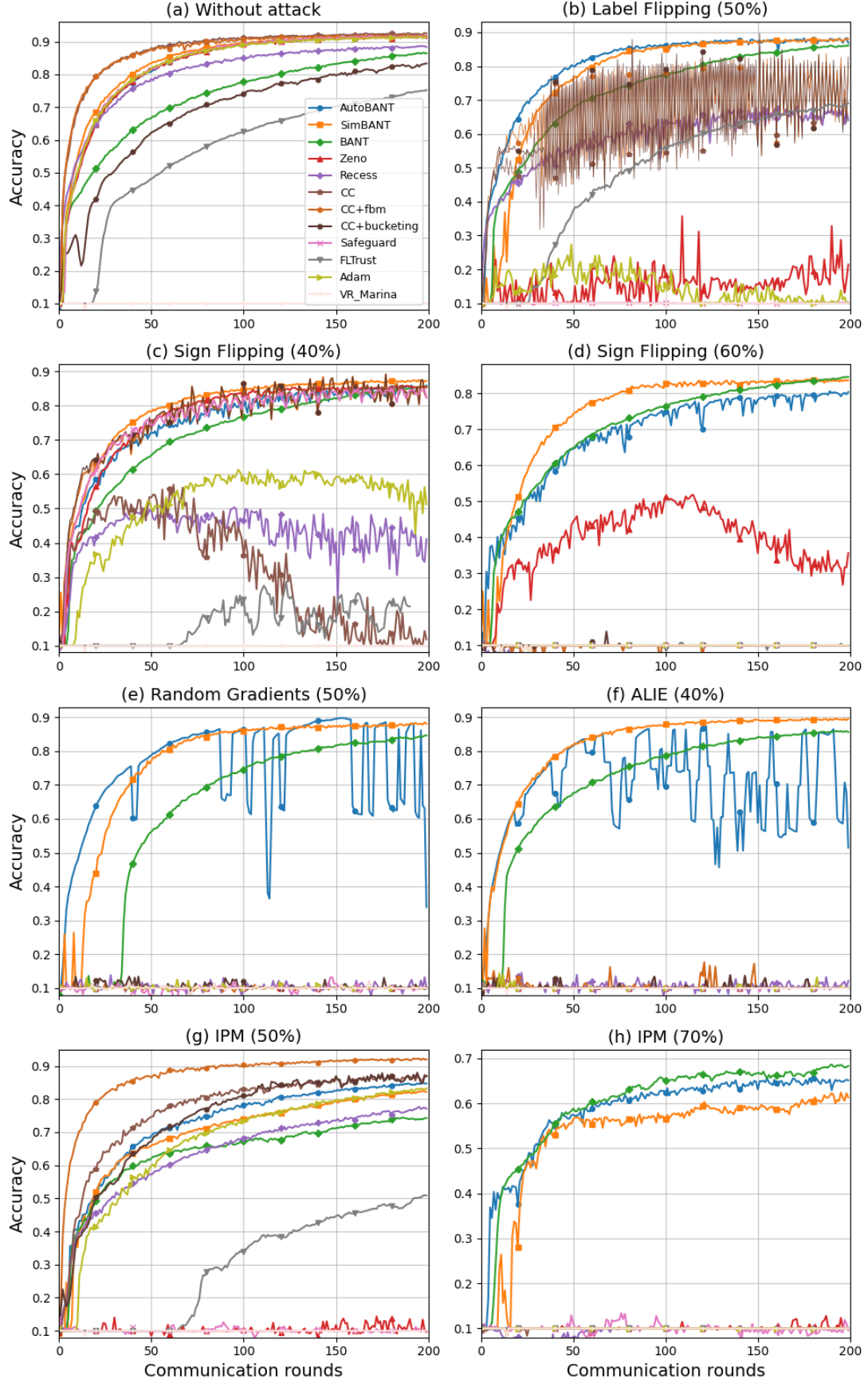


Figure 1: Test accuracy for RESNET18 on CIFAR-10. 1 additional attack scenario (Sign Flipping 60%) and 3 new techniques (CC+fbm, CC+bucketing, VR Marina) for comparison.

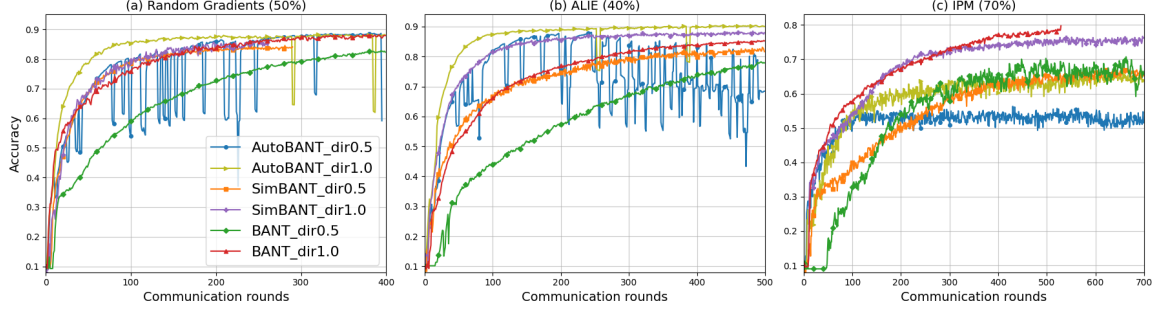


Figure 2: Test accuracy for RESNET18 on CIFAR-10 with Dirichlet heterogeneity. The suffixes DIR1.0 and DIR0.5 denote Dirichlet heterogeneity with $\alpha = 1.0$ and $\alpha = 0.5$, respectively.

Algorithm	Without Attack		Label Flipping		Sign Flipping		Random Gradients	
	G-mean	F1-score	G-mean	F1-score	G-mean	F1-score	G-mean	F1-score
ADAM	0.956±0.017	0.811±0.016	0.262±0.023	0.041±0.019	0.304±0.015	0.116±0.018	0.348±0.011	0.126±0.016
FLTRUST	0.952±0.020	0.800±0.019	0.952±0.016	0.753±0.011	0.586±0.018	0.179±0.015	0.617±0.020	0.174±0.019
RECESS	0.949±0.016	0.783±0.019	0.366±0.019	0.128±0.020	0.359±0.018	0.115±0.014	0.593±0.020	0.163±0.020
ZENO	0.953±0.018	0.806±0.017	0.950±0.020	0.753±0.019	0.949±0.016	0.745±0.018	0.954±0.020	0.770±0.017
CC	0.949±0.020	0.772±0.019	0.285±0.018	0.114±0.020	0.479±0.020	0.124±0.017	0.580±0.019	0.155±0.020
CC+FBM	0.954±0.016	0.808±0.020	0.840±0.019	0.716±0.014	0.155±0.016	0.124±0.017	0.562±0.011	0.151±0.020
CC+BUCKETING	0.947±0.013	0.790±0.018	0.829±0.011	0.708±0.020	0.137±0.017	0.119±0.010	0.570±0.012	0.164±0.018
SAFEGUARD	0.957±0.020	0.821±0.019	0.107±0.012	0.123±0.020	0.084±0.016	0.014±0.018	0.258±0.011	0.124±0.019
VR MARINA	0.010±0.014	0.120±0.010	0.027±0.018	0.123±0.020	0.096±0.017	0.078±0.019	0.176±0.012	0.103±0.013
BANT	0.953±0.017	0.830±0.020	0.956±0.016	0.777±0.020	0.943±0.019	0.792±0.019	0.948±0.018	0.809±0.020
AUTOBANT	0.953±0.019	0.781±0.020	0.790±0.020	0.276±0.020	0.737±0.020	0.243±0.019	0.946±0.019	0.748±0.018
SIMBANT	0.956±0.020	0.790±0.018	0.949±0.020	0.774±0.020	0.951±0.020	0.760±0.020	0.945±0.020	0.712±0.018

Table 3: RESNET1D18 on ECG (AFIB): G-mean and F1-score for Byzantine-tolerance techniques under 4 attacks.

Algorithm	IPM (60%)		IPM (80%)		ALIE	
	G-mean	F1-score	G-mean	F1-score	G-mean	F1-score
ADAM	0.952±0.014	0.738±0.011	0.197±0.027	0.036±0.015	0.125±0.011	0.123±0.020
FLTRUST	0.011±0.014	0.123±0.013	0.061±0.017	0.125±0.015	0.017±0.013	0.123±0.018
RECESS	0.933±0.017	0.611±0.018	0.493±0.019	0.112±0.015	0.450±0.014	0.127±0.018
ZENO	0.954±0.018	0.783±0.020	0.945±0.017	0.730±0.020	0.946±0.015	0.717±0.016
CC	0.945±0.020	0.710±0.016	0.084±0.019	0.014±0.020	0.530±0.018	0.154±0.020
CC+FBM	0.948±0.018	0.695±0.020	0.027±0.018	0.123±0.015	0.876±0.017	0.594±0.013
CC+BUCKETING	0.944±0.016	0.689±0.013	0.035±0.020	0.118±0.012	0.870±0.019	0.587±0.014
SAFEGUARD	0.109±0.010	0.123±0.016	0.951±0.018	0.082±0.020	0.010±0.009	0.123±0.012
VR MARINA	0.098±0.011	0.110±0.014	0.127±0.013	0.079±0.019	0.012±0.010	0.108±0.013
BANT	0.949±0.020	0.704±0.017	0.946±0.020	0.676±0.015	0.947±0.018	0.770±0.020
AUTOBANT	0.948±0.018	0.695±0.015	0.942±0.020	0.690±0.020	0.892±0.016	0.585±0.020
SIMBANT	0.965±0.017	0.753±0.020	0.955±0.020	0.783±0.018	0.946±0.019	0.705±0.020

Table 4: RESNET1D18 on ECG (AFIB): G-mean and F1-score for Byzantine-tolerance techniques under 3 attacks.