

Correlated Signal Attack

Model	Sample Size	F1 Score	FP	Attack	Epsilon	F1 Score (Adv)	FP (Adv)	ASR
DNN	175412	100.0%	0	FGSM	1	100.0%	0	0.0%
DNN	175412	100.0%	0	FGSM	5	100.0%	0	0.0%
DT	175412	100.0%	95	FGSM	1	100.0%	82	0.1%
DT	175412	100.0%	95	FGSM	5	99.6%	856	0.7%
RF	175412	100.0%	95	FGSM	1	100.0%	16	0.0%
RF	175412	100.0%	95	FGSM	5	100.0%	63	0.1%
ET	175412	100.0%	88	FGSM	1	100.0%	11	0.0%
ET	175412	100.0%	88	FGSM	5	100.0%	57	0.0%
XGBoost	175412	100.0%	114	FGSM	1	100.0%	47	0.0%
XGBoost	175412	100.0%	114	FGSM	5	99.9%	191	0.2%
DNN	175412	100.0%	0	BIM	1	100.0%	0	0.0%
DNN	175412	100.0%	0	BIM	5	100.0%	0	0.0%
DT	175412	100.0%	95	BIM	1	100.0%	74	0.1%
DT	175412	100.0%	95	BIM	5	100.0%	67	0.1%
RF	175412	100.0%	95	BIM	1	100.0%	16	0.0%
RF	175412	100.0%	95	BIM	5	100.0%	14	0.0%
ET	175412	100.0%	88	BIM	1	100.0%	11	0.0%
ET	175412	100.0%	88	BIM	5	100.0%	11	0.0%
XGBoost	175412	100.0%	114	BIM	1	100.0%	13	0.0%
XGBoost	175412	100.0%	114	BIM	5	100.0%	13	0.0%
DNN	175412	100.0%	0	PGD	1	100.0%	0	0.0%
DNN	175412	100.0%	0	PGD	5	100.0%	0	0.0%
DT	175412	100.0%	95	PGD	1	100.0%	82	0.1%
DT	175412	100.0%	95	PGD	5	99.8%	571	0.5%
RF	175412	100.0%	95	PGD	1	100.0%	16	0.0%
RF	175412	100.0%	95	PGD	5	100.0%	41	0.0%
ET	175412	100.0%	88	PGD	1	100.0%	11	0.0%
ET	175412	100.0%	88	PGD	5	100.0%	14	0.0%
XGBoost	175412	100.0%	114	PGD	1	100.0%	43	0.0%
XGBoost	175412	100.0%	114	PGD	5	99.9%	124	0.1%