Supplementary Materials

Leaner but Weaker? Metaheuristic Feature Selection and the Adversarial Robustness of IoT Intrusion Detection

Amnah Alshahrani *, Hana Fathi, Arar Al Tawil * and Afaf Edinat. Sensors, manuscript sensors-4697238.

All values come from the same experiments as the paper (Kaggle CPU kernels, 30 runs per method unless stated otherwise). ASR: attack success rate; RS: random search; TR: transfer PGD; IMP: importance-guided attack; RDR: post-attack detection rate; ε: L∞ budget in the scaled full feature space; L0 = 5.

Table S1. Test performance of the random-forest detector on each subset (mean ± half-width of the 95% confidence interval of the mean over 30 runs). Companion to Table 3 of the paper.

Dataset	Method	n	#Features	#Modifiable	F1	MCC	Train (s)	Infer (ms/1k)
CICIoT2023	Full set	30	39.0 ± 0.0	10.0 ± 0.0	0.9965 ± 0.0000	0.8585 ± 0.0010	23.32 ± 0.43	6.86 ± 0.18
CICIoT2023	MI top-k	30	19.0 ± 0.0	8.0 ± 0.0	0.9963 ± 0.0000	0.8524 ± 0.0012	16.81 ± 0.20	5.26 ± 0.11
CICIoT2023	NC-ALL	30	29.0 ± 0.0	0.0 ± 0.0	0.9954 ± 0.0000	0.8189 ± 0.0012	8.25 ± 0.16	6.97 ± 0.16
CICIoT2023	NC-WRAP	30	12.2 ± 0.5	0.0 ± 0.0	0.9953 ± 0.0000	0.8098 ± 0.0017	7.79 ± 0.35	5.68 ± 0.36
CICIoT2023	GA	30	16.1 ± 0.8	4.5 ± 0.4	0.9963 ± 0.0000	0.8530 ± 0.0013	17.62 ± 0.88	5.96 ± 0.31
CICIoT2023	PSO	30	17.9 ± 1.0	5.1 ± 0.5	0.9963 ± 0.0000	0.8528 ± 0.0014	18.31 ± 1.18	5.92 ± 0.20
CICIoT2023	GWO	30	20.9 ± 1.1	5.5 ± 0.5	0.9963 ± 0.0000	0.8517 ± 0.0017	18.65 ± 0.98	6.02 ± 0.19
CICIoT2023	WOA	30	20.6 ± 1.0	5.0 ± 0.4	0.9963 ± 0.0000	0.8518 ± 0.0019	16.42 ± 1.06	5.69 ± 0.30
CICIoT2023	HHO	30	19.8 ± 1.3	5.2 ± 0.5	0.9963 ± 0.0001	0.8514 ± 0.0024	15.42 ± 0.88	6.62 ± 0.29
CICIoT2023	BSA	30	18.0 ± 0.8	5.2 ± 0.6	0.9963 ± 0.0000	0.8525 ± 0.0019	15.69 ± 0.86	6.44 ± 0.22
CICIoT2023	CMO	30	19.3 ± 1.1	5.1 ± 0.5	0.9963 ± 0.0000	0.8523 ± 0.0019	15.24 ± 0.88	6.70 ± 0.31
CICIoT2023	R-GA	30	16.2 ± 1.1	5.0 ± 0.4	0.9963 ± 0.0000	0.8514 ± 0.0016	15.97 ± 0.64	6.33 ± 0.21
CICIoT2023	R-PSO	30	17.9 ± 1.0	4.8 ± 0.5	0.9963 ± 0.0001	0.8527 ± 0.0020	14.98 ± 0.81	6.53 ± 0.26
CICIoT2023	R-CMO	30	20.6 ± 0.8	5.8 ± 0.4	0.9963 ± 0.0000	0.8525 ± 0.0017	15.47 ± 1.14	6.49 ± 0.41
TON_IoT	Full set	30	33.0 ± 0.0	5.0 ± 0.0	0.9976 ± 0.0000	0.9905 ± 0.0001	8.05 ± 0.06	13.51 ± 0.15
TON_IoT	MI top-k	30	12.0 ± 0.0	4.0 ± 0.0	0.9971 ± 0.0000	0.9885 ± 0.0001	9.80 ± 0.10	12.49 ± 0.19
TON_IoT	NC-ALL	30	28.0 ± 0.0	0.0 ± 0.0	0.9825 ± 0.0000	0.9346 ± 0.0001	4.18 ± 0.03	12.06 ± 0.11
TON_IoT	NC-WRAP	30	9.0 ± 0.2	0.0 ± 0.0	0.9819 ± 0.0001	0.9324 ± 0.0004	3.18 ± 0.14	10.66 ± 0.23
TON_IoT	GA	30	10.1 ± 0.4	1.9 ± 0.3	0.9970 ± 0.0001	0.9881 ± 0.0005	5.54 ± 0.58	11.88 ± 0.40
TON_IoT	PSO	30	10.6 ± 0.6	2.3 ± 0.3	0.9971 ± 0.0001	0.9885 ± 0.0005	5.77 ± 0.59	11.68 ± 0.33
TON_IoT	GWO	30	12.7 ± 0.7	2.0 ± 0.3	0.9970 ± 0.0001	0.9879 ± 0.0005	5.23 ± 0.59	11.42 ± 0.29
TON_IoT	WOA	30	13.5 ± 0.6	2.6 ± 0.3	0.9971 ± 0.0001	0.9885 ± 0.0005	5.93 ± 0.76	11.54 ± 0.35
TON_IoT	HHO	30	13.3 ± 0.5	2.3 ± 0.3	0.9971 ± 0.0001	0.9887 ± 0.0004	5.07 ± 0.55	11.23 ± 0.38
TON_IoT	BSA	30	11.2 ± 0.6	1.9 ± 0.3	0.9971 ± 0.0001	0.9884 ± 0.0004	4.99 ± 0.53	10.46 ± 0.35
TON_IoT	CMO	30	13.5 ± 0.7	2.3 ± 0.3	0.9969 ± 0.0002	0.9878 ± 0.0006	4.80 ± 0.52	10.91 ± 0.24
TON_IoT	R-GA	30	10.7 ± 0.5	1.1 ± 0.1	0.9966 ± 0.0002	0.9864 ± 0.0009	5.25 ± 0.40	12.06 ± 0.12
TON_IoT	R-PSO	30	12.5 ± 0.7	1.4 ± 0.2	0.9967 ± 0.0002	0.9870 ± 0.0007	4.86 ± 0.35	12.10 ± 0.34
TON_IoT	R-CMO	30	15.6 ± 0.8	1.7 ± 0.3	0.9969 ± 0.0001	0.9876 ± 0.0004	4.44 ± 0.18	11.20 ± 0.40
UNSW-NB15	Full set	30	42.0 ± 0.0	5.0 ± 0.0	0.9046 ± 0.0002	0.8294 ± 0.0003	51.35 ± 0.23	25.73 ± 0.51
UNSW-NB15	MI top-k	30	19.0 ± 0.0	4.0 ± 0.0	0.8812 ± 0.0003	0.7870 ± 0.0004	56.50 ± 0.26	22.16 ± 0.51

UNSW-NB15	NC-ALL	30	34.0 ± 0.0	0.0 ± 0.0	0.8947 ± 0.0002	0.8119 ± 0.0003	33.04 ± 0.36	27.70 ± 0.56
UNSW-NB15	NC-WRAP	30	13.8 ± 0.5	0.0 ± 0.0	0.8882 ± 0.0011	0.7999 ± 0.0022	13.13 ± 1.54	22.79 ± 1.07
UNSW-NB15	GA	30	16.2 ± 0.6	1.2 ± 0.2	0.9063 ± 0.0007	0.8322 ± 0.0013	22.14 ± 1.77	24.75 ± 0.82
UNSW-NB15	PSO	30	18.5 ± 0.9	2.0 ± 0.3	0.9053 ± 0.0008	0.8305 ± 0.0015	26.46 ± 2.34	24.68 ± 0.52
UNSW-NB15	GWO	30	19.2 ± 0.8	2.0 ± 0.3	0.9043 ± 0.0008	0.8288 ± 0.0015	27.30 ± 2.03	24.13 ± 0.55
UNSW-NB15	WOA	30	20.7 ± 1.2	2.1 ± 0.4	0.9041 ± 0.0008	0.8284 ± 0.0015	29.74 ± 2.02	24.22 ± 0.90
UNSW-NB15	HHO	30	20.0 ± 0.8	2.2 ± 0.3	0.9048 ± 0.0009	0.8297 ± 0.0016	27.63 ± 1.66	24.70 ± 1.01
UNSW-NB15	BSA	30	19.3 ± 1.0	2.0 ± 0.4	0.9046 ± 0.0007	0.8294 ± 0.0013	27.69 ± 2.22	25.47 ± 1.23
UNSW-NB15	CMO	30	20.9 ± 0.9	2.1 ± 0.3	0.9033 ± 0.0010	0.8272 ± 0.0018	29.83 ± 1.43	23.89 ± 0.44
UNSW-NB15	R-GA	30	14.4 ± 0.7	0.1 ± 0.1	0.8882 ± 0.0016	0.7995 ± 0.0031	16.55 ± 2.04	23.88 ± 0.73
UNSW-NB15	R-PSO	30	17.0 ± 1.0	0.2 ± 0.2	0.8882 ± 0.0024	0.7992 ± 0.0046	23.61 ± 2.05	25.03 ± 0.45
UNSW-NB15	R-CMO	30	20.6 ± 1.2	1.0 ± 0.4	0.8905 ± 0.0017	0.8040 ± 0.0031	27.30 ± 2.21	24.02 ± 0.63

Table S2. Attack success rate (%) against the random-forest detector at $\varepsilon \in \{0.05, 0.1\}$, $L0 \leq 5$ (mean ± half-width of the 95% confidence interval over 30 runs). Companion to Table 5.

Dataset	**Method**	**RS 0.05**	**RS 0.1**	**TR 0.05**	**TR 0.1**	**IMP 0.05**	**IMP 0.1**
CICIoT2023	Full set	0.3 ± 0.0	0.5 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.3 ± 0.0	0.5 ± 0.0
CICIoT2023	MI top-k	0.3 ± 0.0	0.6 ± 0.0	0.0 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	NC-ALL	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0
CICIoT2023	NC-WRAP	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0
CICIoT2023	GA	0.3 ± 0.0	0.6 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	PSO	0.3 ± 0.0	0.6 ± 0.0	0.0 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	GWO	0.3 ± 0.0	0.6 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	WOA	0.3 ± 0.0	0.6 ± 0.0	0.0 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	HHO	0.3 ± 0.0	0.6 ± 0.0	0.0 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	BSA	0.3 ± 0.0	0.6 ± 0.0	0.0 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	CMO	0.3 ± 0.0	0.6 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	R-GA	0.3 ± 0.0	0.6 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	R-PSO	0.3 ± 0.0	0.6 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
CICIoT2023	R-CMO	0.3 ± 0.0	0.6 ± 0.0	0.1 ± 0.0	0.1 ± 0.0	0.2 ± 0.0	0.4 ± 0.0
TON_IoT	Full set	8.4 ± 0.0	23.3 ± 1.5	4.9 ± 0.6	6.1 ± 1.0	4.1 ± 0.2	4.5 ± 0.1
TON_IoT	MI top-k	19.9 ± 1.1	39.5 ± 2.0	5.9 ± 0.4	10.5 ± 1.7	10.7 ± 0.6	11.9 ± 0.8
TON_IoT	NC-ALL	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0
TON_IoT	NC-WRAP	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0
TON_IoT	GA	12.6 ± 2.5	22.9 ± 5.2	3.8 ± 1.0	6.4 ± 2.0	4.2 ± 0.5	6.2 ± 0.9
TON_IoT	PSO	15.4 ± 3.3	30.1 ± 7.0	4.2 ± 0.8	6.4 ± 2.1	5.3 ± 1.6	7.2 ± 1.9
TON_IoT	GWO	13.6 ± 3.4	27.5 ± 6.1	4.5 ± 1.0	7.9 ± 2.0	4.7 ± 2.3	6.0 ± 2.5
TON_IoT	WOA	14.4 ± 3.5	28.1 ± 5.9	5.6 ± 1.4	8.0 ± 2.0	4.4 ± 0.8	6.4 ± 1.0
TON_IoT	HHO	13.5 ± 2.4	23.6 ± 5.5	4.1 ± 0.9	6.2 ± 2.0	4.2 ± 0.3	5.3 ± 0.8
TON_IoT	BSA	13.0 ± 2.3	23.8 ± 5.7	3.7 ± 0.8	5.7 ± 1.7	4.3 ± 0.4	5.9 ± 0.9
TON_IoT	CMO	11.2 ± 2.0	24.0 ± 4.5	3.9 ± 0.9	7.8 ± 2.1	3.7 ± 0.4	5.5 ± 1.0
TON_IoT	R-GA	7.0 ± 1.1	17.4 ± 1.2	1.4 ± 0.9	4.1 ± 1.1	2.7 ± 0.3	5.8 ± 0.6
TON_IoT	R-PSO	8.3 ± 1.6	18.7 ± 2.0	1.3 ± 0.5	3.3 ± 0.7	3.0 ± 0.7	5.6 ± 1.0
TON_IoT	R-CMO	11.5 ± 2.7	21.6 ± 5.0	2.8 ± 1.5	2.9 ± 1.1	4.1 ± 0.9	6.9 ± 1.6

UNSW-NB15	Full set	18.5 ± 0.8	20.3 ± 0.8	1.6 ± 0.2	1.8 ± 0.2	2.9 ± 0.1	2.6 ± 0.1
UNSW-NB15	MI top-k	43.4 ± 0.3	42.7 ± 0.4	1.7 ± 0.4	1.1 ± 0.7	7.5 ± 0.2	5.1 ± 0.2
UNSW-NB15	NC-ALL	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0
UNSW-NB15	NC-WRAP	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0	0.0 ± 0.0
UNSW-NB15	GA	28.2 ± 1.8	29.3 ± 1.9	5.8 ± 0.8	5.6 ± 0.9	11.0 ± 1.3	13.3 ± 1.8
UNSW-NB15	PSO	28.1 ± 1.7	30.1 ± 1.9	5.0 ± 1.0	5.3 ± 1.0	7.3 ± 1.2	7.9 ± 1.8
UNSW-NB15	GWO	26.4 ± 1.5	27.7 ± 1.8	4.5 ± 1.0	4.7 ± 1.0	6.4 ± 1.1	7.3 ± 1.7
UNSW-NB15	WOA	24.9 ± 1.6	26.6 ± 1.7	4.1 ± 0.8	4.3 ± 1.0	5.5 ± 1.1	6.2 ± 1.5
UNSW-NB15	HHO	27.5 ± 2.1	29.4 ± 2.8	4.0 ± 0.8	4.8 ± 1.1	6.7 ± 1.1	7.6 ± 1.6
UNSW-NB15	BSA	27.6 ± 1.4	28.9 ± 1.6	3.5 ± 0.9	4.0 ± 1.1	5.8 ± 1.3	6.1 ± 1.7
UNSW-NB15	CMO	24.6 ± 1.8	26.1 ± 1.9	3.6 ± 0.9	3.5 ± 1.0	5.6 ± 1.1	6.3 ± 1.6
UNSW-NB15	R-GA	0.5 ± 0.6	0.6 ± 0.7	0.2 ± 0.2	0.2 ± 0.2	0.4 ± 0.5	0.5 ± 0.6
UNSW-NB15	R-PSO	1.9 ± 1.8	1.9 ± 1.8	0.3 ± 0.3	0.3 ± 0.3	0.3 ± 0.3	0.3 ± 0.3
UNSW-NB15	R-CMO	8.5 ± 2.6	9.1 ± 2.7	1.2 ± 0.6	1.1 ± 0.5	2.3 ± 1.0	2.2 ± 1.0

Table S3. Spearman correlations between subset size and ASR and between the number of attacker-controllable features kept and ASR, ε = 0.1, pooled over the ten methods of the main comparison (300 runs per dataset).

Model	Dataset	Attack	eps	n	rho(#feat, ASR)	p	rho(#modifiable, ASR)	p (mod)
lgbm	CICIoT2023	rs	0.1	300	-0.177	0.00206	0.295	1.96e-07
lgbm	CICIoT2023	tr	0.1	300	-0.14	0.0156	0.174	0.00243
lgbm	CICIoT2023	imp	0.1	300	-0.389	2.95e-12	-0.132	0.0224
lgbm	TON_IoT	rs	0.1	300	-0.195	0.000673	0.291	2.9e-07
lgbm	TON_IoT	tr	0.1	300	-0.252	1.03e-05	0.304	7.76e-08
lgbm	TON_IoT	imp	0.1	300	-0.147	0.011	-0.021	0.711
lgbm	UNSW-NB15	rs	0.1	300	-0.354	2.73e-10	0.26	5.11e-06
lgbm	UNSW-NB15	tr	0.1	300	-0.337	2.08e-09	0.123	0.0335
lgbm	UNSW-NB15	imp	0.1	300	-0.314	2.77e-08	-0.049	0.395
rf	CICIoT2023	rs	0.1	300	-0.238	3.06e-05	-0.003	0.963
rf	CICIoT2023	tr	0.1	300	-0.236	3.7e-05	-0.234	4.41e-05
rf	CICIoT2023	imp	0.1	300	0.158	0.00595	0.238	3.2e-05
rf	TON_IoT	rs	0.1	300	-0.143	0.0131	0.583	9.33e-29
rf	TON_IoT	tr	0.1	300	-0.151	0.00882	0.372	2.81e-11
rf	TON_IoT	imp	0.1	300	-0.194	0.000724	0.11	0.0561
rf	UNSW-NB15	rs	0.1	300	-0.461	3.61e-17	0.197	0.000585
rf	UNSW-NB15	tr	0.1	300	-0.187	0.00116	-0.188	0.00108
rf	UNSW-NB15	imp	0.1	300	-0.41	1.31e-13	-0.28	8.25e-07

Table S4. Most frequently selected features across all metaheuristic runs (LightGBM), with their status in the threat model (modifiable = base feature; derived = recomputed from base features).

Dataset	Feature	Selected in (%) of runs	Modifiable
CICIoT2023	flow_duration	100.0	yes
CICIoT2023	rst_count	97.1	no

CICIoT2023	syn_count	87.9	no
CICIoT2023	http	82.1	no
CICIoT2023	fin_count	80.4	no
CICIoT2023	min	67.9	yes
CICIoT2023	weight	65.8	no
CICIoT2023	rate	60.4	yes
CICIoT2023	srate	58.8	yes
CICIoT2023	variance	57.9	no
TON_IoT	proto	87.1	no
TON_IoT	src_ip_bytes	76.7	yes
TON_IoT	conn_state	73.8	no
TON_IoT	dst_bytes	73.3	no
TON_IoT	dns_rejected	71.2	no
TON_IoT	dst_pkts	60.8	no
TON_IoT	dns_ra	56.7	no
TON_IoT	dns_rcode	55.4	no
TON_IoT	src_bytes	49.6	yes
TON_IoT	src_pkts	47.9	yes
UNSW-NB15	ct_dst_src_ltm	100.0	no
UNSW-NB15	smean	87.9	derived
UNSW-NB15	ct_srv_src	75.0	no
UNSW-NB15	dmean	72.9	no
UNSW-NB15	sbytes	71.7	yes
UNSW-NB15	sttl	66.2	no
UNSW-NB15	ct_dst_ltm	65.8	no
UNSW-NB15	ct_state_ttl	65.0	no
UNSW-NB15	dbytes	62.9	no
UNSW-NB15	ct_srv_dst	58.8	no

Table S5. Friedman tests per dataset and metric (runs as blocks) with the mean rank of every method (lower rank = lower value for ASR and number of features, higher F1) and the Nemenyi critical difference (CD).

Dataset	Metric	chi2	p	CD	Full set	MI top-k	NC-ALL	NC-WRAP	GA	PSO	GWO	WOA	HHO	BSA	CMO	R-GA	R-PSO	R-CMO
CICIoT2023	asr_rs_0.1	201.63	6.31e-36	3.62	6.65	13.78	1.5	1.5	8.2	8.52	8.07	8.0	8.32	8.52	7.92	8.27	7.7	8.07
CICIoT2023	asr_tr_0.1	166.77	8.38e-29	3.62	7.8	12.6	1.8	1.8	8.62	7.43	8.32	7.72	8.82	7.82	7.83	7.95	8.25	8.25
CICIoT2023	asr_imp_0.1	211.27	6.58e-38	3.62	3.08	10.75	1.5	1.5	8.18	9.17	9.02	9.6	8.1	8.23	9.0	8.67	9.7	8.5
CICIoT2023	f1	202.79	3.65e-36	3.62	1.75	4.77	13.43	13.57	6.5	6.27	6.93	7.73	8.32	7.6	7.95	6.62	7.03	6.53
CICIoT2023	n_feat	252.87	1.6199999999999999e-46	3.62	14.0	7.38	12.98	1.38	3.97	5.88	8.97	9.02	7.73	6.13	7.82	4.45	6.05	9.23
TON_IoT	asr_rs_0.1	170.29	1.61e-29	3.62	6.17	9.5	1.5	1.5	8.9	10.3	9.12	8.87	9.0	8.63	9.07	6.97	7.17	8.32
TON_IoT	asr_tr_0.1	199.65	1.6100000000000001e-35	3.62	8.3	11.2	1.5	1.5	8.38	9.03	9.53	10.65	8.17	8.55	9.62	7.02	6.25	5.3
TON_IoT	asr_imp_0.1	174.96	1.8099999999999997e-30	3.62	6.07	9.55	1.5	1.5	7.73	9.03	7.6	9.07	7.53	8.12	7.47	10.23	9.43	10.17
TON_IoT	f1	274.8	4.43e-51	3.62	1.15	2.53	13.0	14.0	7.05	6.3	7.17	5.53	5.8	6.4	7.47	10.0	9.7	8.9
TON_IoT	n_feat	297.28	8.93e-56	3.62	14.0	6.67	13.0	1.58	3.42	4.18	7.67	8.88	8.97	5.28	8.82	4.23	7.37	10.93

UNSW-NB15	asr_rs_0.1	325.54	1.07e-61	3.62	6.67	13.9	2.5	2.5	10.63	10.47	9.57	9.67	10.13	9.97	8.7	2.72	2.98	4.6
UNSW-NB15	asr_tr_0.1	298.76	4.37e-56	3.62	6.5	12.73	2.68	2.68	11.5	10.7	9.67	9.65	10.13	9.27	8.63	2.97	3.17	4.72
UNSW-NB15	asr_imp_0.1	281.58	1.6999999999999997e-52	3.62	7.43	10.27	2.68	2.68	11.93	10.8	10.07	9.42	10.8	9.3	8.87	2.9	3.07	4.78
UNSW-NB15	f1	325.07	1.34e-61	3.62	1.67	14.0	9.6	10.77	3.07	4.37	5.43	5.17	5.73	4.97	5.9	11.0	11.73	11.6
UNSW-NB15	n_feat	277.35	1.3e-51	3.62	14.0	7.3	13.0	1.77	4.0	6.68	7.25	8.97	8.63	7.7	9.38	2.45	4.93	8.93

Table S6. Wilcoxon signed-rank tests of R-CMO against every other method (paired by run, Holm-adjusted p values); mean difference = R-CMO minus the other method.

Dataset	Metric	vs	n	mean diff (R-CMO - other)	p	p Holm
CICIoT2023	asr_rs_0.1	Full set	30	0.0003	0.0841	0.841
CICIoT2023	asr_rs_0.1	MI top-k	30	-0.0036	1.73e-06	2.25e-05
CICIoT2023	asr_rs_0.1	NC-ALL	30	0.0091	1.73e-06	2.25e-05
CICIoT2023	asr_rs_0.1	NC-WRAP	30	0.0091	1.73e-06	2.25e-05
CICIoT2023	asr_rs_0.1	GA	30	-0.0001	0.738	1.0
CICIoT2023	asr_rs_0.1	PSO	30	-0.0001	0.393	1.0
CICIoT2023	asr_rs_0.1	GWO	30	-0.0	0.957	1.0
CICIoT2023	asr_rs_0.1	WOA	30	0.0002	0.705	1.0
CICIoT2023	asr_rs_0.1	HHO	30	0.0001	0.855	1.0
CICIoT2023	asr_rs_0.1	BSA	30	-0.0002	0.452	1.0
CICIoT2023	asr_rs_0.1	CMO	30	0.0003	0.6	1.0
CICIoT2023	asr_rs_0.1	R-GA	30	-0.0002	0.797	1.0
CICIoT2023	asr_rs_0.1	R-PSO	30	0.0003	0.673	1.0
CICIoT2023	asr_tr_0.1	Full set	30	0.0004	0.299	1.0
CICIoT2023	asr_tr_0.1	MI top-k	30	-0.0017	0.000318	0.0035
CICIoT2023	asr_tr_0.1	NC-ALL	30	0.0023	3.77e-06	4.9e-05
CICIoT2023	asr_tr_0.1	NC-WRAP	30	0.0023	3.77e-06	4.9e-05
CICIoT2023	asr_tr_0.1	GA	30	0.0001	0.919	1.0
CICIoT2023	asr_tr_0.1	PSO	30	0.0004	0.565	1.0
CICIoT2023	asr_tr_0.1	GWO	30	0.0003	0.742	1.0
CICIoT2023	asr_tr_0.1	WOA	30	0.0004	0.614	1.0
CICIoT2023	asr_tr_0.1	HHO	30	-0.0	0.968	1.0
CICIoT2023	asr_tr_0.1	BSA	30	0.0004	0.428	1.0
CICIoT2023	asr_tr_0.1	CMO	30	0.0005	0.428	1.0
CICIoT2023	asr_tr_0.1	R-GA	30	0.0004	0.51	1.0
CICIoT2023	asr_tr_0.1	R-PSO	30	0.0002	0.738	1.0
CICIoT2023	asr_imp_0.1	Full set	30	0.0015	1.71e-06	2.22e-05
CICIoT2023	asr_imp_0.1	MI top-k	30	-0.0006	0.0162	0.162
CICIoT2023	asr_imp_0.1	NC-ALL	30	0.004	1.71e-06	2.22e-05
CICIoT2023	asr_imp_0.1	NC-WRAP	30	0.004	1.71e-06	2.22e-05
CICIoT2023	asr_imp_0.1	GA	30	0.0001	0.524	1.0

CICIoT2023	asr_imp_0.1	PSO	30	-0.0001	0.171	1.0
CICIoT2023	asr_imp_0.1	GWO	30	-0.0001	0.981	1.0
CICIoT2023	asr_imp_0.1	WOA	30	-0.0002	0.304	1.0
CICIoT2023	asr_imp_0.1	HHO	30	0.0001	0.484	1.0
CICIoT2023	asr_imp_0.1	BSA	30	0.0	0.838	1.0
CICIoT2023	asr_imp_0.1	CMO	30	-0.0003	0.347	1.0
CICIoT2023	asr_imp_0.1	R-GA	30	-0.0001	0.611	1.0
CICIoT2023	asr_imp_0.1	R-PSO	30	-0.0003	0.162	1.0
CICIoT2023	f1	Full set	30	-0.0002	1.49e-05	0.000164
CICIoT2023	f1	MI top-k	30	-0.0001	0.0407	0.407
CICIoT2023	f1	NC-ALL	30	0.0011	1.73e-06	2.08e-05
CICIoT2023	f1	NC-WRAP	30	0.0012	1.86e-09	2.42e-08
CICIoT2023	f1	GA	30	-0.0	0.7	1.0
CICIoT2023	f1	PSO	30	0.0	0.968	1.0
CICIoT2023	f1	GWO	30	0.0	0.839	1.0
CICIoT2023	f1	WOA	30	0.0	0.245	1.0
CICIoT2023	f1	HHO	30	0.0001	0.0523	0.47
CICIoT2023	f1	BSA	30	0.0	0.289	1.0
CICIoT2023	f1	CMO	30	0.0	0.253	1.0
CICIoT2023	f1	R-GA	30	0.0	0.952	1.0
CICIoT2023	f1	R-PSO	30	0.0	0.761	1.0
CICIoT2023	n_feat	Full set	30	-18.4	1.52e-06	1.98e-05
CICIoT2023	n_feat	MI top-k	30	1.6	0.000406	0.00285
CICIoT2023	n_feat	NC-ALL	30	-8.4	1.52e-06	1.98e-05
CICIoT2023	n_feat	NC-WRAP	30	8.4333	1.61e-06	1.98e-05
CICIoT2023	n_feat	GA	30	4.5	4e-06	4e-05
CICIoT2023	n_feat	PSO	30	2.6667	0.000188	0.00151
CICIoT2023	n_feat	GWO	30	-0.3	0.722	1.0
CICIoT2023	n_feat	WOA	30	-0.0333	0.612	1.0
CICIoT2023	n_feat	HHO	30	0.7667	0.216	0.647
CICIoT2023	n_feat	BSA	30	2.5667	0.000427	0.00285
CICIoT2023	n_feat	CMO	30	1.3	0.0675	0.27
CICIoT2023	n_feat	R-GA	30	4.3667	6.89e-06	6.2e-05
CICIoT2023	n_feat	R-PSO	30	2.6667	0.000589	0.00295
TON_IoT	asr_rs_0.1	Full set	30	0.1023	0.0405	0.445
TON_IoT	asr_rs_0.1	MI top-k	30	-0.0065	0.715	1.0
TON_IoT	asr_rs_0.1	NC-ALL	30	0.3266	1.73e-06	2.25e-05
TON_IoT	asr_rs_0.1	NC-WRAP	30	0.3266	1.73e-06	2.25e-05
TON_IoT	asr_rs_0.1	GA	30	0.0015	0.839	1.0
TON_IoT	asr_rs_0.1	PSO	30	-0.0827	0.1	1.0
TON_IoT	asr_rs_0.1	GWO	30	-0.04	0.37	1.0
TON_IoT	asr_rs_0.1	WOA	30	-0.0187	0.584	1.0
TON_IoT	asr_rs_0.1	HHO	30	-0.0263	0.503	1.0
TON_IoT	asr_rs_0.1	BSA	30	-0.0032	0.7	1.0
TON_IoT	asr_rs_0.1	CMO	30	-0.0416	0.57	1.0
TON_IoT	asr_rs_0.1	R-GA	30	0.0858	0.1	1.0

TON_IoT	asr_rs_0.1	R-PSO	30	0.059	0.253	1.0
TON_IoT	asr_tr_0.1	Full set	30	-0.0289	5.59e-05	0.000391
TON_IoT	asr_tr_0.1	MI top-k	30	-0.0616	1.86e-09	2.42e-08
TON_IoT	asr_tr_0.1	NC-ALL	30	0.0259	1.73e-06	1.91e-05
TON_IoT	asr_tr_0.1	NC-WRAP	30	0.0259	1.73e-06	1.91e-05
TON_IoT	asr_tr_0.1	GA	30	-0.0416	0.000189	0.00113
TON_IoT	asr_tr_0.1	PSO	30	-0.0517	0.000256	0.00128
TON_IoT	asr_tr_0.1	GWO	30	-0.0547	3.05e-05	0.000244
TON_IoT	asr_tr_0.1	WOA	30	-0.0659	8.01e-08	9.61e-07
TON_IoT	asr_tr_0.1	HHO	30	-0.0348	0.00237	0.0071
TON_IoT	asr_tr_0.1	BSA	30	-0.0359	0.000256	0.00128
TON_IoT	asr_tr_0.1	CMO	30	-0.0576	1.22e-05	0.00011
TON_IoT	asr_tr_0.1	R-GA	30	-0.0161	0.0175	0.0349
TON_IoT	asr_tr_0.1	R-PSO	30	-0.0066	0.237	0.237
TON_IoT	asr_imp_0.1	Full set	30	0.0459	1.6e-05	0.000176
TON_IoT	asr_imp_0.1	MI top-k	30	0.0218	0.0449	0.269
TON_IoT	asr_imp_0.1	NC-ALL	30	0.096	1.86e-09	2.42e-08
TON_IoT	asr_imp_0.1	NC-WRAP	30	0.096	1.86e-09	2.42e-08
TON_IoT	asr_imp_0.1	GA	30	0.028	0.0145	0.116
TON_IoT	asr_imp_0.1	PSO	30	-0.0032	0.626	1.0
TON_IoT	asr_imp_0.1	GWO	30	0.0166	0.171	0.853
TON_IoT	asr_imp_0.1	WOA	30	0.0117	0.393	1.0
TON_IoT	asr_imp_0.1	HHO	30	0.0312	0.00664	0.0664
TON_IoT	asr_imp_0.1	BSA	30	0.0252	0.0262	0.184
TON_IoT	asr_imp_0.1	CMO	30	0.0305	0.0113	0.102
TON_IoT	asr_imp_0.1	R-GA	30	0.0096	0.584	1.0
TON_IoT	asr_imp_0.1	R-PSO	30	0.0152	0.318	1.0
TON_IoT	f1	Full set	30	-0.0008	1.73e-06	2.08e-05
TON_IoT	f1	MI top-k	30	-0.0007	1.73e-06	2.08e-05
TON_IoT	f1	NC-ALL	30	0.0142	1.73e-06	2.08e-05
TON_IoT	f1	NC-WRAP	30	0.0151	1.86e-09	2.42e-08
TON_IoT	f1	GA	30	-0.0002	0.0345	0.138
TON_IoT	f1	PSO	30	-0.0003	0.00711	0.0372
TON_IoT	f1	GWO	30	-0.0002	0.0473	0.142
TON_IoT	f1	WOA	30	-0.0004	4.97e-05	0.000397
TON_IoT	f1	HHO	30	-0.0004	3.45e-05	0.000311
TON_IoT	f1	BSA	30	-0.0003	4.97e-05	0.000397
TON_IoT	f1	CMO	30	-0.0001	0.184	0.368
TON_IoT	f1	R-GA	30	0.0002	0.00619	0.0372
TON_IoT	f1	R-PSO	30	0.0001	0.245	0.368
TON_IoT	n_feat	Full set	30	-17.3667	1.63e-06	2.08e-05
TON_IoT	n_feat	MI top-k	30	3.6333	3.53e-06	2.65e-05
TON_IoT	n_feat	NC-ALL	30	-12.3667	1.63e-06	2.08e-05
TON_IoT	n_feat	NC-WRAP	30	6.6	1.6e-06	2.08e-05
TON_IoT	n_feat	GA	30	5.5	1.6e-06	2.08e-05
TON_IoT	n_feat	PSO	30	5.0667	3.66e-06	2.65e-05

TON_IoT	n_feat	GWO	30	2.9	2.24e-05	8.97e-05
TON_IoT	n_feat	WOA	30	2.1333	0.00121	0.0023
TON_IoT	n_feat	HHO	30	2.3	0.000245	0.000736
TON_IoT	n_feat	BSA	30	4.4	3.31e-06	2.65e-05
TON_IoT	n_feat	CMO	30	2.1	0.00115	0.0023
TON_IoT	n_feat	R-GA	30	4.9333	2.04e-06	2.08e-05
TON_IoT	n_feat	R-PSO	30	3.1667	1.67e-05	8.37e-05
UNSW-NB15	asr_rs_0.1	Full set	30	-0.135	5.75e-06	2.87e-05
UNSW-NB15	asr_rs_0.1	MI top-k	30	-0.3927	1.86e-09	2.42e-08
UNSW-NB15	asr_rs_0.1	NC-ALL	30	0.0896	4.01e-05	0.000141
UNSW-NB15	asr_rs_0.1	NC-WRAP	30	0.0896	4.01e-05	0.000141
UNSW-NB15	asr_rs_0.1	GA	30	-0.2444	1.86e-09	2.42e-08
UNSW-NB15	asr_rs_0.1	PSO	30	-0.2503	1.86e-09	2.42e-08
UNSW-NB15	asr_rs_0.1	GWO	30	-0.2174	1.3e-08	1.04e-07
UNSW-NB15	asr_rs_0.1	WOA	30	-0.2242	3.73e-09	3.73e-08
UNSW-NB15	asr_rs_0.1	HHO	30	-0.2442	3.73e-09	3.73e-08
UNSW-NB15	asr_rs_0.1	BSA	30	-0.2302	1.3e-08	1.04e-07
UNSW-NB15	asr_rs_0.1	CMO	30	-0.1962	1.3e-08	1.04e-07
UNSW-NB15	asr_rs_0.1	R-GA	30	0.0866	3.53e-05	0.000141
UNSW-NB15	asr_rs_0.1	R-PSO	30	0.0721	0.000916	0.000916
UNSW-NB15	asr_tr_0.1	Full set	30	-0.0094	0.00129	0.00303
UNSW-NB15	asr_tr_0.1	MI top-k	30	-0.1157	2.35e-06	1.88e-05
UNSW-NB15	asr_tr_0.1	NC-ALL	30	0.0077	0.000293	0.00147
UNSW-NB15	asr_tr_0.1	NC-WRAP	30	0.0077	0.000293	0.00147
UNSW-NB15	asr_tr_0.1	GA	30	-0.0731	1.86e-09	2.42e-08
UNSW-NB15	asr_tr_0.1	PSO	30	-0.0643	1.86e-09	2.42e-08
UNSW-NB15	asr_tr_0.1	GWO	30	-0.0519	1.64e-07	1.48e-06
UNSW-NB15	asr_tr_0.1	WOA	30	-0.0525	4.33e-06	3.03e-05
UNSW-NB15	asr_tr_0.1	HHO	30	-0.0588	9.31e-09	1.02e-07
UNSW-NB15	asr_tr_0.1	BSA	30	-0.0493	4.33e-06	3.03e-05
UNSW-NB15	asr_tr_0.1	CMO	30	-0.0341	8.01e-08	8.01e-07
UNSW-NB15	asr_tr_0.1	R-GA	30	0.0066	0.00101	0.00303
UNSW-NB15	asr_tr_0.1	R-PSO	30	0.0058	0.01	0.01
UNSW-NB15	asr_imp_0.1	Full set	30	-0.0277	0.000164	0.000818
UNSW-NB15	asr_imp_0.1	MI top-k	30	-0.0517	2.82e-06	2.82e-05
UNSW-NB15	asr_imp_0.1	NC-ALL	30	0.0205	0.000293	0.00117
UNSW-NB15	asr_imp_0.1	NC-WRAP	30	0.0205	0.000293	0.00117
UNSW-NB15	asr_imp_0.1	GA	30	-0.0759	2.61e-08	3.13e-07
UNSW-NB15	asr_imp_0.1	PSO	30	-0.0638	3.51e-06	3.16e-05
UNSW-NB15	asr_imp_0.1	GWO	30	-0.0547	4.71e-07	5.18e-06
UNSW-NB15	asr_imp_0.1	WOA	30	-0.0477	3.8e-05	0.000266
UNSW-NB15	asr_imp_0.1	HHO	30	-0.0595	9.31e-09	1.21e-07
UNSW-NB15	asr_imp_0.1	BSA	30	-0.0463	5.51e-05	0.000331
UNSW-NB15	asr_imp_0.1	CMO	30	-0.044	3.79e-06	3.16e-05
UNSW-NB15	asr_imp_0.1	R-GA	30	0.0185	0.000455	0.00117
UNSW-NB15	asr_imp_0.1	R-PSO	30	0.0179	0.00128	0.00128

UNSW-NB15	f1	Full set	30	-0.0159	1.86e-09	2.42e-08
UNSW-NB15	f1	MI top-k	30	0.0089	1.86e-09	2.42e-08
UNSW-NB15	f1	NC-ALL	30	-0.0021	0.00038	0.00152
UNSW-NB15	f1	NC-WRAP	30	-0.0009	0.0293	0.088
UNSW-NB15	f1	GA	30	-0.0151	1.86e-09	2.42e-08
UNSW-NB15	f1	PSO	30	-0.0144	5.59e-09	4.47e-08
UNSW-NB15	f1	GWO	30	-0.0138	1.86e-09	2.42e-08
UNSW-NB15	f1	WOA	30	-0.014	3.73e-09	3.35e-08
UNSW-NB15	f1	HHO	30	-0.0136	5.59e-09	4.47e-08
UNSW-NB15	f1	BSA	30	-0.014	5.59e-09	4.47e-08
UNSW-NB15	f1	CMO	30	-0.0134	5.59e-09	4.47e-08
UNSW-NB15	f1	R-GA	30	-0.0005	0.0606	0.121
UNSW-NB15	f1	R-PSO	30	0.0004	1.0	1.0
UNSW-NB15	n_feat	Full set	30	-21.3667	1.58e-06	2.05e-05
UNSW-NB15	n_feat	MI top-k	30	1.6333	0.0187	0.112
UNSW-NB15	n_feat	NC-ALL	30	-13.3667	1.58e-06	2.05e-05
UNSW-NB15	n_feat	NC-WRAP	30	6.8667	3.64e-06	3.64e-05
UNSW-NB15	n_feat	GA	30	4.4667	1.59e-05	0.000143
UNSW-NB15	n_feat	PSO	30	2.1667	0.00615	0.043
UNSW-NB15	n_feat	GWO	30	1.4333	0.0767	0.383
UNSW-NB15	n_feat	WOA	30	-0.0333	0.864	1.0
UNSW-NB15	n_feat	HHO	30	0.6333	0.405	1.0
UNSW-NB15	n_feat	BSA	30	1.3	0.0868	0.383
UNSW-NB15	n_feat	CMO	30	-0.3	0.587	1.0
UNSW-NB15	n_feat	R-GA	30	6.2667	3.03e-06	3.34e-05
UNSW-NB15	n_feat	R-PSO	30	3.6667	0.000178	0.00143

Table S7. Spearman correlations between subset composition and ASR for every attack and budget, for both learners (ten methods of the main comparison).

Model	Dataset	Attack	eps	n	rho(#feat, ASR)	p	rho(#modifiable, ASR)	p (mod)
lgbm	CICIoT2023	rs	0.01	300	-0.214	0.00019	-0.182	0.00158
lgbm	CICIoT2023	rs	0.05	300	-0.351	4.22e-10	0.123	0.0326
lgbm	CICIoT2023	rs	0.1	300	-0.177	0.00206	0.295	1.96e-07
lgbm	CICIoT2023	rs	0.2	300	-0.178	0.00199	0.079	0.173
lgbm	CICIoT2023	tr	0.01	300	-0.254	8.55e-06	-0.142	0.0136
lgbm	CICIoT2023	tr	0.05	300	-0.114	0.0479	0.058	0.317
lgbm	CICIoT2023	tr	0.1	300	-0.14	0.0156	0.174	0.00243
lgbm	CICIoT2023	tr	0.2	300	-0.089	0.124	0.109	0.0587
lgbm	CICIoT2023	imp	0.01	300	-0.084	0.148	-0.035	0.546
lgbm	CICIoT2023	imp	0.05	300	-0.384	5.25e-12	-0.274	1.42e-06
lgbm	CICIoT2023	imp	0.1	300	-0.389	2.95e-12	-0.132	0.0224
lgbm	CICIoT2023	imp	0.2	300	-0.29	3.26e-07	-0.224	9.2e-05
lgbm	TON_IoT	rs	0.01	300	0.046	0.43	0.452	1.6e-16

lgbm	TON_IoT	rs	0.05	300	-0.237	3.44e-05	0.349	5.05e-10
lgbm	TON_IoT	rs	0.1	300	-0.195	0.000673	0.291	2.9e-07
lgbm	TON_IoT	rs	0.2	300	-0.024	0.683	0.631	1.02e-34
lgbm	TON_IoT	tr	0.01	300	-0.096	0.0954	-0.035	0.548
lgbm	TON_IoT	tr	0.05	300	-0.039	0.5	0.524	1.37e-22
lgbm	TON_IoT	tr	0.1	300	-0.252	1.03e-05	0.304	7.76e-08
lgbm	TON_IoT	tr	0.2	300	-0.215	0.000178	0.335	2.78e-09
lgbm	TON_IoT	imp	0.01	300	-0.156	0.00681	0.09	0.121
lgbm	TON_IoT	imp	0.05	300	-0.117	0.0422	0.284	5.74e-07
lgbm	TON_IoT	imp	0.1	300	-0.147	0.011	-0.021	0.711
lgbm	TON_IoT	imp	0.2	300	-0.314	2.6e-08	0.234	4.39e-05
lgbm	UNSW-NB15	rs	0.01	300	-0.392	1.76e-12	0.173	0.00269
lgbm	UNSW-NB15	rs	0.05	300	-0.346	7.32e-10	0.23	5.73e-05
lgbm	UNSW-NB15	rs	0.1	300	-0.354	2.73e-10	0.26	5.11e-06
lgbm	UNSW-NB15	rs	0.2	300	-0.223	9.75e-05	0.357	1.96e-10
lgbm	UNSW-NB15	tr	0.01	300	-0.251	1.07e-05	0.175	0.00235
lgbm	UNSW-NB15	tr	0.05	300	-0.326	7.54e-09	0.142	0.0137
lgbm	UNSW-NB15	tr	0.1	300	-0.337	2.08e-09	0.123	0.0335
lgbm	UNSW-NB15	tr	0.2	300	-0.274	1.46e-06	0.144	0.0127
lgbm	UNSW-NB15	imp	0.01	300	-0.043	0.453	0.502	1.52e-20
lgbm	UNSW-NB15	imp	0.05	300	-0.317	1.93e-08	0.108	0.0606
lgbm	UNSW-NB15	imp	0.1	300	-0.314	2.77e-08	-0.049	0.395
lgbm	UNSW-NB15	imp	0.2	300	-0.093	0.107	0.145	0.0118
rf	CICIoT2023	rs	0.01	300	0.124	0.0324	0.24	2.59e-05
rf	CICIoT2023	rs	0.05	300	0.121	0.0357	0.194	0.000709
rf	CICIoT2023	rs	0.1	300	-0.238	3.06e-05	-0.003	0.963
rf	CICIoT2023	rs	0.2	300	-0.405	2.72e-13	-0.302	9.96e-08
rf	CICIoT2023	tr	0.01	300	0.017	0.775	0.105	0.0684
rf	CICIoT2023	tr	0.05	300	-0.066	0.253	-0.038	0.512
rf	CICIoT2023	tr	0.1	300	-0.236	3.7e-05	-0.234	4.41e-05
rf	CICIoT2023	tr	0.2	300	-0.122	0.0349	-0.052	0.369
rf	CICIoT2023	imp	0.01	300	0.075	0.195	0.15	0.00925
rf	CICIoT2023	imp	0.05	300	0.155	0.00716	0.124	0.0315
rf	CICIoT2023	imp	0.1	300	0.158	0.00595	0.238	3.2e-05
rf	CICIoT2023	imp	0.2	300	-0.284	5.65e-07	-0.32	1.5e-08
rf	TON_IoT	rs	0.01	300	-0.24	2.66e-05	0.012	0.842
rf	TON_IoT	rs	0.05	300	-0.27	2.03e-06	0.407	2.16e-13
rf	TON_IoT	rs	0.1	300	-0.143	0.0131	0.583	9.33e-29
rf	TON_IoT	rs	0.2	300	-0.296	1.69e-07	0.487	2.73e-19
rf	TON_IoT	tr	0.01	300	-0.162	0.00489	-0.287	4.34e-07
rf	TON_IoT	tr	0.05	300	-0.038	0.515	0.508	4.600000000000001e-21
rf	TON_IoT	tr	0.1	300	-0.151	0.00882	0.372	2.81e-11
rf	TON_IoT	tr	0.2	300	-0.139	0.0163	-0.234	4.1e-05
rf	TON_IoT	imp	0.01	300	-0.21	0.000243	-0.075	0.197
rf	TON_IoT	imp	0.05	300	-0.174	0.00255	0.247	1.52e-05

rf	TON_IoT	imp	0.1	300	-0.194	0.000724	0.11	0.0561
rf	TON_IoT	imp	0.2	300	-0.339	1.61e-09	0.218	0.000145
rf	UNSW-NB15	rs	0.01	300	-0.522	2.35e-22	0.129	0.0251
rf	UNSW-NB15	rs	0.05	300	-0.481	9.57e-19	0.173	0.00262
rf	UNSW-NB15	rs	0.1	300	-0.461	3.61e-17	0.197	0.000585
rf	UNSW-NB15	rs	0.2	300	-0.417	4.75e-14	0.211	0.000226
rf	UNSW-NB15	tr	0.01	300	-0.369	3.92e-11	0.025	0.662
rf	UNSW-NB15	tr	0.05	300	-0.291	2.8e-07	-0.257	6.57e-06
rf	UNSW-NB15	tr	0.1	300	-0.187	0.00116	-0.188	0.00108
rf	UNSW-NB15	tr	0.2	300	-0.134	0.0205	-0.159	0.00591
rf	UNSW-NB15	imp	0.01	300	-0.416	5.7e-14	0.121	0.0364
rf	UNSW-NB15	imp	0.05	300	-0.444	6.27e-16	-0.191	0.000897
rf	UNSW-NB15	imp	0.1	300	-0.41	1.31e-13	-0.28	8.25e-07
rf	UNSW-NB15	imp	0.2	300	-0.366	5.89e-11	-0.258	6.09e-06

Table S8. Spearman correlations pooled over the 12 methods whose ASR is not zero by construction (LightGBM, random search, ε = 0.1; 360 runs per dataset).

Dataset	Methods	Runs	rho(size, ASR)	p	rho(#controllable, ASR)	p (ctrl)
CICIoT2023	12	360	-0.138	0.0089	0.303	4.6e-09
TON_IoT	12	360	-0.101	0.057	0.408	6.9e-16
UNSW-NB15	12	360	0.079	0.14	0.555	1.9e-30

Table S9. Robust fitness across optimisers with random forests as the final learner (ε = 0.1): means over 30 runs and Holm-adjusted Wilcoxon p values (paired by run). Companion to Table 6.

Dataset	Metric	GA	R-GA	PSO	R-PSO	CMO	R-CMO	p R-GA vs GA	p R-PSO vs PSO	p R-CMO vs CMO	p R-GA vs R-CMO	p R-PSO vs R-CMO	p R-GA vs R-PSO
CICIoT2023	F1	0.9963	0.9963	0.9963	0.9963	0.9963	0.9963	0.38	1.0	1.0	1.0	1.0	1.0
CICIoT2023	ASR rs (%)	0.58	0.59	0.61	0.61	0.6	0.59	1.0	1.0	1.0	1.0	1.0	1.0
CICIoT2023	ASR tr (%)	0.12	0.1	0.1	0.11	0.08	0.1	1.0	1.0	1.0	1.0	1.0	1.0
CICIoT2023	ASR imp (%)	0.37	0.37	0.39	0.37	0.43	0.41	1.0	0.78	1.0	0.66	0.13	1.0
TON_IoT	F1	0.997	0.9966	0.9971	0.9967	0.9969	0.9969	0.0023	0.0025	0.62	0.028	0.62	0.62
TON_IoT	ASR rs (%)	22.93	17.45	30.1	18.69	24.02	21.55	0.62	0.082	1.0	1.0	1.0	1.0
TON_IoT	ASR tr (%)	6.39	4.09	6.4	3.3	7.78	2.86	0.23	0.18	0.00092	0.3	0.3	0.3
TON_IoT	ASR imp (%)	6.19	5.83	7.22	5.63	5.5	6.94	1.0	1.0	1.0	1.0	1.0	1.0
UNSW-NB15	F1	0.9063	0.8882	0.9053	0.8882	0.9033	0.8905	1.1e-08	1.1e-08	1.1e-08	0.19	0.66	0.69
UNSW-NB15	ASR rs (%)	29.34	0.59	30.05	1.93	26.09	9.14	1.1e-08	1.1e-08	2.2e-08	0.00016	0.0016	0.16
UNSW-NB15	ASR tr (%)	5.56	0.18	5.31	0.3	3.47	1.13	1.1e-08	1.9e-08	0.00014	0.0055	0.014	0.61
UNSW-NB15	ASR imp (%)	13.25	0.51	7.95	0.35	6.32	2.25	1.1e-08	1.1e-08	0.00068	0.0049	0.0022	0.5

Table S10. Control fitness on all three datasets: standard weights (0.99/0.01), robust weights without the attack term (0.79/0.01) and the robust fitness (0.79/0.01/0.20); LightGBM, ε = 0.1, mean ± half-width of the 95% confidence interval over 30 runs. Companion to Table 8.

Dataset	Optimizer	Metric	Standard (0.99/0.01)	Control (0.79/0.01, no attack)	Robust (0.79/0.01/0.20)	p control vs standard	p robust vs control
CICIoT2023	GA	F1	0.996 ± 0.000	0.996 ± 0.000	0.996 ± 0.000	1.0	1.0
CICIoT2023	GA	#controllable kept	4.500 ± 0.401	4.800 ± 0.359	5.000 ± 0.416	0.4	0.4
CICIoT2023	GA	ASR rs (%)	0.92 ± 0.07	0.94 ± 0.06	0.93 ± 0.06	1.0	1.0
CICIoT2023	GA	ASR tr (%)	0.23 ± 0.06	0.23 ± 0.06	0.20 ± 0.05	0.87	0.64
CICIoT2023	GA	ASR imp (%)	0.39 ± 0.03	0.39 ± 0.04	0.41 ± 0.03	0.89	0.85
CICIoT2023	CMO	F1	0.996 ± 0.000	0.996 ± 0.000	0.996 ± 0.000	0.9	0.9
CICIoT2023	CMO	#controllable kept	5.100 ± 0.484	5.400 ± 0.524	5.767 ± 0.401	0.54	0.54
CICIoT2023	CMO	ASR rs (%)	0.88 ± 0.07	0.92 ± 0.06	0.91 ± 0.07	0.91	0.91
CICIoT2023	CMO	ASR tr (%)	0.18 ± 0.04	0.23 ± 0.06	0.23 ± 0.07	0.37	0.84
CICIoT2023	CMO	ASR imp (%)	0.43 ± 0.05	0.42 ± 0.04	0.40 ± 0.03	0.88	0.88
TON_IoT	GA	F1	0.997 ± 0.000	0.997 ± 0.000	0.996 ± 0.000	0.38	0.021
TON_IoT	GA	#controllable kept	1.900 ± 0.300	2.200 ± 0.284	1.100 ± 0.114	0.079	2.9e-05
TON_IoT	GA	ASR rs (%)	32.52 ± 6.39	42.93 ± 5.24	24.08 ± 2.28	0.0071	7.1e-08
TON_IoT	GA	ASR tr (%)	6.75 ± 1.98	7.11 ± 1.69	4.20 ± 1.14	0.66	0.069
TON_IoT	GA	ASR imp (%)	6.80 ± 1.30	7.50 ± 1.42	8.65 ± 1.19	0.4	0.4
TON_IoT	CMO	F1	0.997 ± 0.000	0.997 ± 0.000	0.997 ± 0.000	0.7	0.7
TON_IoT	CMO	#controllable kept	2.300 ± 0.280	2.267 ± 0.366	1.667 ± 0.266	0.97	0.0082
TON_IoT	CMO	ASR rs (%)	36.83 ± 6.76	31.40 ± 6.56	32.66 ± 6.93	0.37	0.81
TON_IoT	CMO	ASR tr (%)	8.35 ± 2.02	9.02 ± 2.31	2.59 ± 0.83	0.94	1.4e-06
TON_IoT	CMO	ASR imp (%)	6.56 ± 1.35	6.45 ± 1.08	9.60 ± 1.99	0.67	0.042
UNSW-NB15	GA	F1	0.909 ± 0.000	0.909 ± 0.000	0.894 ± 0.000	0.92	3.7e-09
UNSW-NB15	GA	#controllable kept	1.233 ± 0.188	1.233 ± 0.254	0.100 ± 0.114	0.98	9.2e-06
UNSW-NB15	GA	ASR rs (%)	33.41 ± 2.94	32.42 ± 2.98	0.30 ± 0.35	0.39	3.7e-09
UNSW-NB15	GA	ASR tr (%)	8.08 ± 1.35	7.59 ± 1.64	0.11 ± 0.14	0.66	7.6e-06
UNSW-NB15	GA	ASR imp (%)	9.64 ± 1.15	8.53 ± 1.47	0.20 ± 0.23	0.46	7.6e-06
UNSW-NB15	CMO	F1	0.907 ± 0.001	0.907 ± 0.001	0.894 ± 0.002	0.63	7.5e-09
UNSW-NB15	CMO	#controllable kept	2.100 ± 0.330	1.967 ± 0.332	1.000 ± 0.404	0.8	0.0027
UNSW-NB15	CMO	ASR rs (%)	28.59 ± 2.39	31.26 ± 2.65	8.96 ± 3.14	0.24	3.7e-09
UNSW-NB15	CMO	ASR tr (%)	4.18 ± 1.03	5.04 ± 1.15	0.77 ± 0.37	0.13	6.3e-07
UNSW-NB15	CMO	ASR imp (%)	6.45 ± 1.26	7.16 ± 1.56	2.05 ± 1.00	0.42	4.7e-05

Table S11. Spearman correlations under the expanded threat model, standard wrappers (LightGBM, random search, ε = 0.1).

Dataset	rho(#ctrl expanded, ASR)	p	rho(size, ASR)	p (size)
CICIoT2023	-0.027	0.7	-0.153	0.026
TON_IoT	0.418	2.6e-10	0.064	0.35
UNSW-NB15	0.323	1.7e-06	-0.077	0.27

Table S12. Features whose selection frequency changed most when exact duplicate rows were kept (10 runs per setting). Companion to Table 14.

Dataset	Method	Feature	Freq. dedup	Freq. kept
TON_IoT	GA	missed_bytes	0.0	0.9
TON_IoT	GA	dns_ra	0.9	0.1
TON_IoT	GA	dst_pkts	0.8	0.0
TON_IoT	GA	dst_ip_bytes	0.3	1.0
TON_IoT	GA	proto	0.9	0.3
TON_IoT	R-GA	src_bytes	0.0	1.0
TON_IoT	R-GA	dns_rcode	0.2	0.8
TON_IoT	R-GA	http_resp_mime_types	0.4	0.0
TON_IoT	R-GA	ssl_version	0.2	0.6
TON_IoT	R-GA	dns_qtype	0.2	0.6
UNSW-NB15	GA	ct_srv_src	1.0	0.2
UNSW-NB15	GA	ct_srv_dst	0.4	1.0
UNSW-NB15	GA	proto	0.3	0.8
UNSW-NB15	GA	spkts	0.0	0.5
UNSW-NB15	GA	sbytes	0.9	0.5
UNSW-NB15	R-GA	ct_srv_src	1.0	0.3
UNSW-NB15	R-GA	dloss	0.8	0.4
UNSW-NB15	R-GA	dtcpb	0.2	0.6
UNSW-NB15	R-GA	ct_state_ttl	0.3	0.7
UNSW-NB15	R-GA	dbytes	0.7	0.3

Table S13. Feature lists of the original threat model (base and derived features, Table 1 of the paper) and the additional features the attacker may set under the expanded threat model (Section 6.10).

Dataset	Base (attacker sets directly)	Derived (recomputed)	Added in the expanded threat model
CICIoT2023	flow_duration, header_length, rate, srate, tot_sum, min, max, avg, std, tot_size	none	duration, fin_flag_number, syn_flag_number, rst_flag_number, psh_flag_number, ack_flag_number, ack_count, syn_count, fin_count, urg_count, rst_count, number
TON_IoT	duration, src_bytes, src_pkts, src_ip_bytes, http_request_body_len	none	missed_bytes, conn_state, dns_qclass, dns_qtype, dns_rd, http_trans_depth, http_method
UNSW-NB15	dur, spkts, sbytes, sinpkt, sjit	smean, sload, rate	sttl, swin, stcpb, trans_depth, sloss, ct_srv_src, ct_src_ltm, ct_src_dport_ltm, ct_dst_src_ltm, ct_dst_ltm, ct_dst_sport_ltm