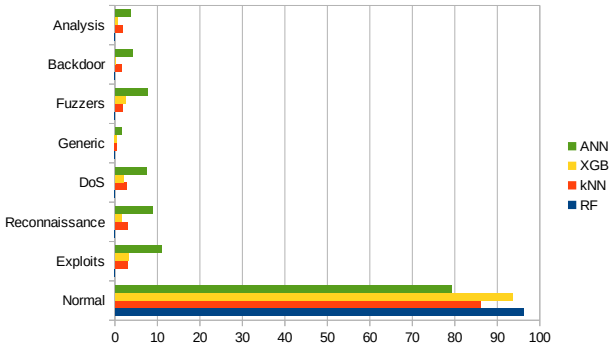
Tabela 1. Desempenho por tipo de ataque usando a Intervenção IN1 no GenIDS-CIC18 no cenário Interset.

Algoritmos	BASELINE				INTERVENÇÃO IN1				BASELINE				INTERVENÇÃO IN1			
	Fluxos	GenIDS-NB15			Fluxos	GenIDS-NB15			Fluxos	GenIDS-CIC17			Fluxos	GenIDS-CIC17		
		Acertos	Erros	SDEV*		Acertos	Erros	SDEV*		Acertos	Erros	SDEV*		Acertos	Erros	SDEV*
Random Forest	Normal	96,15	3,85	0,76	Normal	98,99	1,01	0,80	Normal	99,21	0,79	0,27	Normal	99,74	0,58	0,71
	Exploits	0,03	99,97	0,05	Exploits	1,36	98,64	1,47	Portscan	0,99	99,01	0,60	Portscan	0,27	99,73	0,32
	Reconnaissance	0,00	100,00	0,00	Reconnaissance	0,73	99,27	0,86	DDoS	0,00	100,00	0,00	DDoS	4,63	95,37	6,64
	DoS	0,03	99,97	0,06	DoS	0,17	99,83	0,19	DoS	12,21	87,79	6,60	DoS	19,09	80,91	21,79
	Generic	0,00	100,00	0,00	Generic	0,15	99,85	0,14	Bruteforce	30,45	69,55	18,48	Bruteforce	39,05	60,95	5,82
	Fuzzers	0,00	100,00	0,00	Fuzzers	0,23	99,77	0,26	Webattack	3,36	96,64	2,09	Webattack	0,06	99,94	0,14
	Backdoor	0,00	100,00	0,00	Backdoor	0,00	100,00	0,00	Botnet	0,00	100,00	0,00	Botnet	0,77	99,23	1,45
	Analysis	0,00	100,00	0,00	Analysis	0,01	99,98	0,03								
kNN	Normal	86,05	13,95	4,66	Normal	94,11	5,89	3,17	Normal	98,55	1,45	0,13	Normal	98,24	1,76	0,86
	Exploits	2,97	97,03	1,61	Exploits	5,49	94,51	4,82	Portscan	2,67	97,33	0,05	Portscan	1,69	98,31	0,16
	Reconnaissance	3,03	96,97	3,64	Reconnaissance	6,38	93,62	4,53	DDoS	0,00	100,00	0,00	DDoS	0,00	100,00	0,00
	DoS	2,65	97,35	2,39	DoS	4,10	95,90	3,74	DoS	4,79	95,21	0,28	DoS	4,44	95,56	1,75
	Generic	0,49	99,51	0,55	Generic	0,85	99,16	1,09	Bruteforce	42,69	57,31	1,12	Bruteforce	46,68	53,32	7,04
	Fuzzers	1,77	98,23	1,92	Fuzzers	3,13	96,87	2,75	Webattack	2,04	97,96	1,52	Webattack	11,38	88,62	12,93
	Backdoor	1,54	98,46	2,09	Backdoor	2,47	97,53	4,57	Botnet	0,00	100,00	0,00	Botnet	0,10	99,90	0,22
	Analysis	1,79	98,21	2,43	Analysis	2,47	97,53	4,71								
XGBoost	Normal	93,48	6,52	1,40	Normal	96,37	3,63	1,62	Normal	98,71	1,22	0,43	Normal	99,08	0,92	0,40
	Exploits	3,29	96,71	3,86	Exploits	4,69	95,31	3,03	Portscan	1,22	99,23	0,85	Portscan	0,86	99,14	0,38
	Reconnaissance	1,64	98,36	2,16	Reconnaissance	4,74	95,26	2,86	DDoS	0,00	100,00	0,00	DDoS	37,77	62,23	50,77
	DoS	2,07	97,93	2,19	DoS	1,30	98,70	1,23	DoS	12,67	87,18	9,77	DoS	53,73	46,27	28,62
	Generic	0,49	99,74	0,20	Generic	0,21	99,79	0,20	Bruteforce	76,93	19,29	31,59	Bruteforce	37,48	62,52	8,74
	Fuzzers	2,49	97,51	2,90	Fuzzers	1,61	98,39	1,55	Webattack	7,69	89,12	9,74	Webattack	0,25	99,75	0,24
	Backdoor	0,21	99,79	0,37	Backdoor	0,46	99,54	0,87	Botnet	0,00	100,00	0,00	Botnet	1,83	98,17	3,74
	Analysis	0,55	99,45	0,48	Analysis	0,71	99,29	1,25								
ANN	Normal	79,30	20,70	3,87	Normal	82,00	18,00	8,62	Normal	98,25	1,75	0,59	Normal	98,39	1,61	0,67
	Exploits	10,99	89,01	5,11	Exploits	11,70	88,30	5,68	Portscan	2,02	97,98	0,91	Portscan	2,15	97,85	0,60
	Reconnaissance	8,94	91,06	3,01	Reconnaissance	6,26	93,74	4,10	DDoS	0,00	100,00	0,00	DDoS	0,00	100,00	0,00
	DoS	7,51	92,49	4,35	DoS	5,78	94,22	3,14	DoS	34,27	65,73	28,84	DoS	18,85	81,15	15,53
	Generic	1,47	98,53	1,31	Generic	0,91	99,09	0,34	Bruteforce	41,96	58,04	0,08	Bruteforce	42,12	57,88	0,07
	Fuzzers	7,70	92,30	4,60	Fuzzers	9,18	90,82	6,10	Webattack	3,60	96,40	1,84	Webattack	2,53	97,47	2,15
	Backdoor	4,11	95,89	6,23	Backdoor	0,16	99,84	0,33	Botnet	3,42	96,58	2,03	Botnet	0,73	99,27	1,64
	Analysis	3,57	96,43	6,37	Analysis	0,44	99,56	0,31								

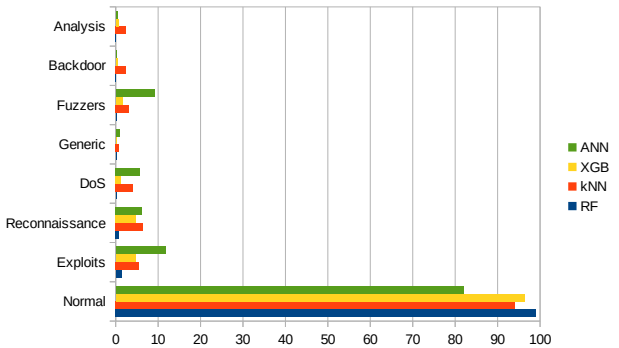
* Desvio Padrão. Fonte: Elaborado pelo autor.

A tabela apresenta o desempenho dos modelos na classificação por tipo de ataque, considerando a influência da Intervenção IN1 (Redução de Dimensão) no conjunto de dados GenIDS-CIC18, no cenário Interset. Observa-se um pequeno aumento nos percentuais de acertos e, consequentemente, uma redução nos percentuais de erros em alguns casos. O maior destaque ocorre quando os modelos são avaliados com o conjunto de dados GenIDS-CIC17, onde a identificação dos ataques DoS(S) demonstram uma maior capacidade de generalização no modelo XGBoost. É possível nota também uma melhoria na classificação dos fluxos normais.

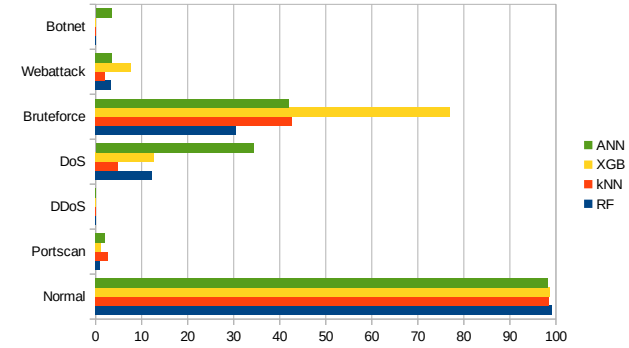
Figura 1. Desempenho do GenIDS-CIC18 por tipo de ataque no cenário Interset.



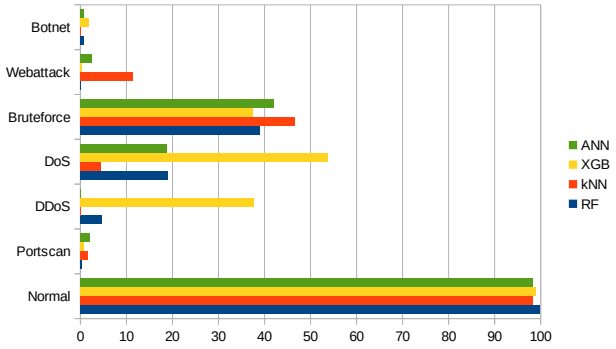
(a) Baseline no cenário Interset com teste no GenIDS-NB15



(b) Intervenção IN1 no cenário Interset com teste no GenIDS-NB15



(c) Baseline no cenário Interset com teste no GenIDS-CIC17



(d) Intervenção IN1 no cenário Interset com teste no GenIDS-CIC17

Fonte: Elaborado pelo autor.

A figura ilustra os resultados encontrados na Tabela 1, onde são apresentados os desempenhos dos modelos na classificação por tipo de ataque, considerando a influência da Intervenção IN1 (Redução de Dimensão) no conjunto de dados GenIDS-CIC18, no cenário Interset. Observa-se um pequeno aumento nos percentuais de acertos e, consequentemente, uma redução nos percentuais de erros em alguns casos. O maior destaque ocorre quando os modelos são avaliados com o conjunto de dados GenIDS-CIC17, onde a identificação dos ataques DoS(S) demonstram uma maior capacidade de generalização no modelo XGBoost. É possível nota também uma melhoria na classificação dos fluxos normais.