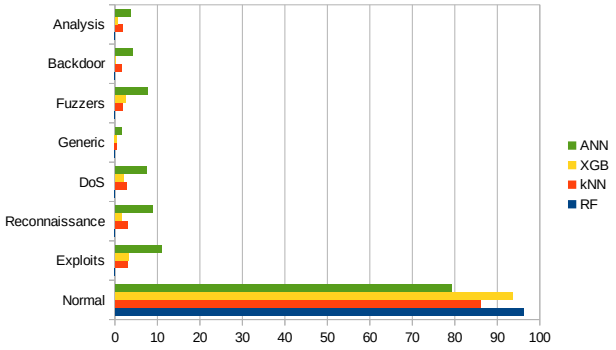
Tabela 1. Desempenho por tipo de ataque usando a Intervenção IN2 no GenIDS-CIC18 no cenário Interset.

Algoritmos	BASELINE				INTERVENÇÃO IN2				BASELINE				INTERVENÇÃO IN2			
	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	96,07	3,93	0,99	Normal	99,21	0,79	0,27	Normal	99,25	0,76	0,13
	Exploits	0,03	99,97	0,05	Exploits	0,77	99,23	1,37	Portscan	0,99	99,01	0,60	Portscan	0,40	99,60	0,22
	Reconnaissance	0,00	100,00	0,00	Reconnaissance	0,75	99,25	1,64	DDoS	0,00	100,00	0,00	DDoS	9,02	90,98	17,01
	DoS	0,03	99,97	0,06	DoS	0,36	99,64	0,53	DoS	12,21	87,79	6,60	DoS	18,86	81,14	8,09
	Generic	0,00	100,00	0,00	Generic	4,37	95,63	9,74	Bruteforce	30,45	69,55	18,48	Bruteforce	33,74	66,26	18,50
	Fuzzers	0,00	100,00	0,00	Fuzzers	0,50	99,50	0,70	Webattack	3,36	96,64	2,09	Webattack	1,92	98,08	1,37
	Backdoor	0,00	100,00	0,00	Backdoor	0,00	100,00	0,00	Botnet	0,00	100,00	0,00	Botnet	0,00	100,00	0,00
	Analysis	0,00	100,00	0,00	Analysis	0,00	100,00	0,00								
kNN	Normal	86,05	13,95	4,66	Normal	93,12	6,88	2,55	Normal	98,55	1,45	0,13	Normal	98,79	1,21	0,33
	Exploits	2,97	97,03	1,61	Exploits	5,55	94,45	6,06	Portscan	2,67	97,33	0,05	Portscan	1,66	98,34	0,30
	Reconnaissance	3,03	96,97	3,64	Reconnaissance	6,00	94,00	9,63	DDoS	0,00	100,00	0,00	DDoS	0,00	100,00	0,00
	DoS	2,65	97,35	2,39	DoS	2,42	97,58	2,14	DoS	4,79	95,21	0,28	DoS	7,62	92,38	4,84
	Generic	0,49	99,51	0,55	Generic	7,13	92,87	15,62	Bruteforce	42,69	57,31	1,12	Bruteforce	42,07	57,93	0,08
	Fuzzers	1,77	98,23	1,92	Fuzzers	1,79	98,21	2,48	Webattack	2,04	97,96	1,52	Webattack	2,79	97,21	1,48
	Backdoor	1,54	98,46	2,09	Backdoor	0,07	99,93	0,15	Botnet	0,00	100,00	0,00	Botnet	0,00	100,00	0,00
	Analysis	1,79	98,21	2,43	Analysis	0,19	99,81	0,29								
XGBoost	Normal	93,48	6,52	1,40	Normal	94,57	5,43	0,97	Normal	98,71	1,22	0,41	Normal	98,84	1,16	0,27
	Exploits	3,29	96,71	3,86	Exploits	6,88	93,12	4,04	Portscan	1,22	99,23	0,34	Portscan	0,95	99,05	0,56
	Reconnaissance	1,64	98,36	2,16	Reconnaissance	4,00	96,00	1,45	DDoS	0,00	100,00	0,00	DDoS	0,00	100,00	0,00
	DoS	2,07	97,93	2,19	DoS	2,87	97,13	2,06	DoS	12,67	87,18	9,62	DoS	11,13	88,87	6,11
	Generic	0,49	99,74	0,20	Generic	2,53	97,47	4,78	Bruteforce	76,93	19,29	27,27	Bruteforce	99,88	0,12	0,18
	Fuzzers	2,49	97,51	2,90	Fuzzers	3,16	96,84	1,84	Webattack	7,69	89,12	9,78	Webattack	1,04	98,96	1,42
	Backdoor	0,21	99,79	0,37	Backdoor	0,21	99,79	0,21	Botnet	0,00	100,00	0,00	Botnet	0,00	100,00	0,00
	Analysis	0,55	99,45	0,48	Analysis	1,23	98,77	0,77								
ANN	Normal	79,30	20,70	3,87	Normal	91,59	8,41	9,16	Normal	98,25	1,75	0,59	Normal	98,32	1,68	0,66
	Exploits	10,99	89,01	5,11	Exploits	6,09	93,91	5,85	Portscan	2,02	97,98	0,91	Portscan	4,13	95,87	0,34
	Reconnaissance	8,94	91,06	3,01	Reconnaissance	2,62	97,38	3,87	DDoS	0,00	100,00	0,00	DDoS	0,00	100,00	0,00
	DoS	7,51	92,49	4,35	DoS	3,38	96,62	3,69	DoS	34,27	65,73	28,84	DoS	4,70	95,30	1,86
	Generic	1,47	98,53	1,31	Generic	0,57	99,43	0,39	Bruteforce	41,96	58,04	0,08	Bruteforce	42,11	57,89	0,06
	Fuzzers	7,70	92,30	4,60	Fuzzers	2,78	97,22	2,84	Webattack	3,60	96,40	1,84	Webattack	2,84	97,16	1,63
	Backdoor	4,11	95,89	6,23	Backdoor	0,05	99,95	0,05	Botnet	3,42	96,58	2,03	Botnet	0,87	99,13	1,89
	Analysis	3,57	96,43	6,37	Analysis	0,09	99,91	0,14								

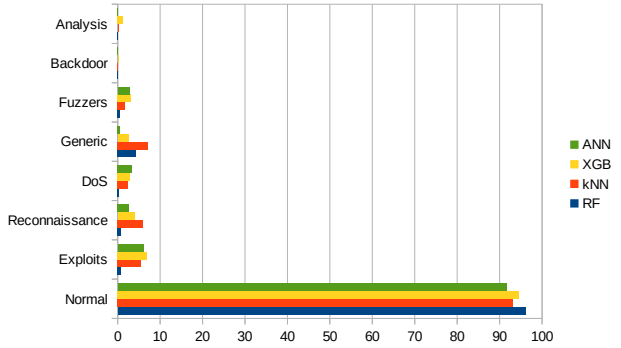
* Desvio Padrão. Fonte: Elaborado pelo autor.

A tabela apresenta o desempenho dos modelos na classificação por tipo de ataque, considerando a influência da Intervenção IN2 (Seleão de Atributos) 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. No GenIDS-NB15 é possível observar um maior equilíbrio na identificação entre os diversos tipos de ataques. Já no GenIDS-CIC17 o maior destaque na identificação dos ataques Bruteforce, onde são identificados quanse que a totalidade dos ataques no modelo XGBoost. É possível nota também uma melhoria na classificação dos fluxos normais em alguns modelos nos testes com o GenIDS-CIC17.

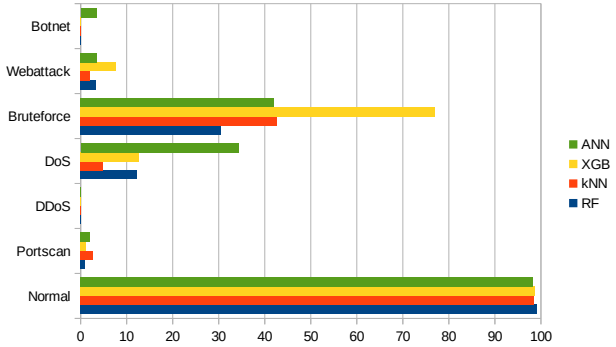
Figura 1. Desempenho por tipo de ataque usando a Intervenção IN2 no GenIDS-CIC18 no cenário Interset.



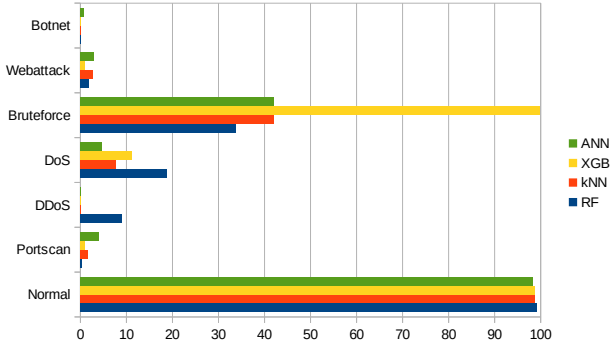
(a) Baseline no cenário Interset com teste no GenIDS-NB15



(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 IN2 (Seleção de Atributos) 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. No GenIDS-NB15 é possível observar um maior equilíbrio na identificação entre os diversos tipos de ataques. Já no GenIDS-CIC17 o maior destaque na identificação dos ataques Bruteforce, onde são identificados quanse que a totalidade dos ataques no modelo XGBoost. É possível nota também uma melhoria na classificação dos fluxos normais em alguns modelos nos testes com o GenIDS-CIC17.