UNIVERSIDADE FEDERAL DE PERNAMBUCO DEPARTAMENTO E ELETRÔNICA E SISTEMAS

DETECÇÃO DE INTRUSÃO (IF848)

A Novel Multi-Stage Approach for Hierarchical Intrusion Detection - Proposta de melhoria

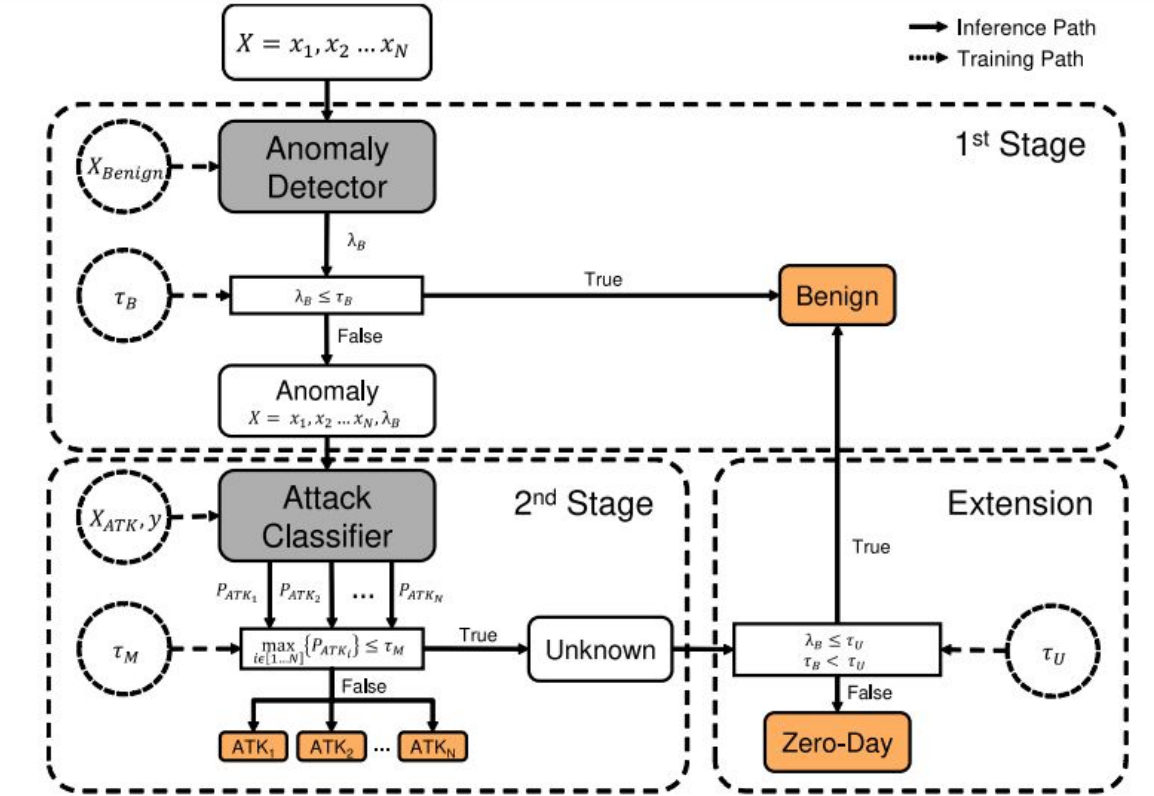
Luiz Henrique (lhbas)
Rayhene Ranúzia (rrda)
Rodrigo Abreu (raafm)

Centro de Informática UFPE

Universidade Federal de Pernambuco

FEVEREIRO, 2024

Sistema proposto pelo artigo de referência



Melhoria proposta para a solução do artigo de referência

O artigo original usava uma OCSVM lenta como detector de anomalias e uma random forest como classificador de anomalias. Como sugerido pelo próprio artigo, é conveniente que o primeiro estágio seja veloz uma vez que todos os dados passarão por eles. O segundo estágio recebe uma quantidade menor de dados e por isso pode ser mais lento e ter maior acurácia.

Seguindo esta sugestão, trocamos o primeiro modelo por uma Autoencoder mais rápido e dobramos a quantidade de árvores do classificador, no estágio de classificação mantemos uma Random Forest.

Experimentos - Hardware

Especificações da máquina usada para os experimentos no artigo:

- 4 CPUs, Intel Xeon Silver 4108 CPU @ 1.80GHz
- 16 GB RAM

Especificações da máquina usada para os experimentos pela nossa equipe:

- 8 CPUs, Intel Core i7 1.80Hz 10° geração
- 16 GB RAM

Resultados reproduzidos do artigo original

test_full_model	precision	recall	f1-score	support
(D)DOS	0.35	0.99	0.51	1076
BENIGN	1.00	0.91	0.95	100000
Botnet	0.24	1.00	0.39	1040
Brute Force	0.45	0.99	0.62	1100
Port Scan	0.95	1.00	0.97	1066
Unknown	0.00	0.00	0.00	0
Web-Attack	0.42	0.99	0.60	1038
accuracy			0.91	105320
macro avg	0.49	0.84	0.58	105320
weighted avg	0.97	0.91	0.94	105320

test_set	precision	recall	f1-score	support
(D)DOS	0.34	0.97	0.50	584
BENIGN	1.00	0.91	0.95	54387
Botnet	0.24	1.00	0.39	477
Brute Force	0.45	0.99	0.62	584
Port Scan	0.95	1.00	0.97	197
Unknown	0.06	0.89	0.11	47
Web-Attack	0.42	0.99	0.60	584
accuracy			0.92	56860
macro avg	0.51	0.96	0.60	56860
weighted avg	0.97	0.92	0.94	56860

Resultados da melhoria proposta

test_full_model	precision	recall	f1-score	support
(D)DOS	0.32	0.99	0.49	1076
BENIGN	1.00	0.88	0.94	100000
Botnet	0.24	1.00	0.39	1040
Brute Force	0.46	1.00	0.62	1100
Port Scan	0.96	1.00	0.98	1066
Unknown	0.00	0.00	0.00	0
Web-Attack	0.42	0.99	0.59	1038
accuracy			0.89	105320
macro avg	0.49	0.84	0.57	105320
weighted avg	0.97	0.89	0.92	105320

test_set	precision	recall	f1-score	support
(D)DOS	0.33	0.98	0.49	584
BENIGN	1.00	0.91	0.95	54387
Botnet	0.21	0.99	0.35	477
Brute Force	0.58	0.98	0.73	584
Port Scan	0.94	0.99	0.96	197
Unknown	0.03	0.43	0.06	47
Web-Attack	0.42	0.99	0.59	584
accuracy			0.92	56860
macro avg	0.50	0.90	0.59	56860
weighted avg	0.97	0.92	0.94	56860

Comparação do tempo de execução em segundos

	test_full_model	test_set
Stage1	9.75	5.23
Stage2	1.71	0.76
Stage3	0.00	0.00
Sistema	11.47	5.99

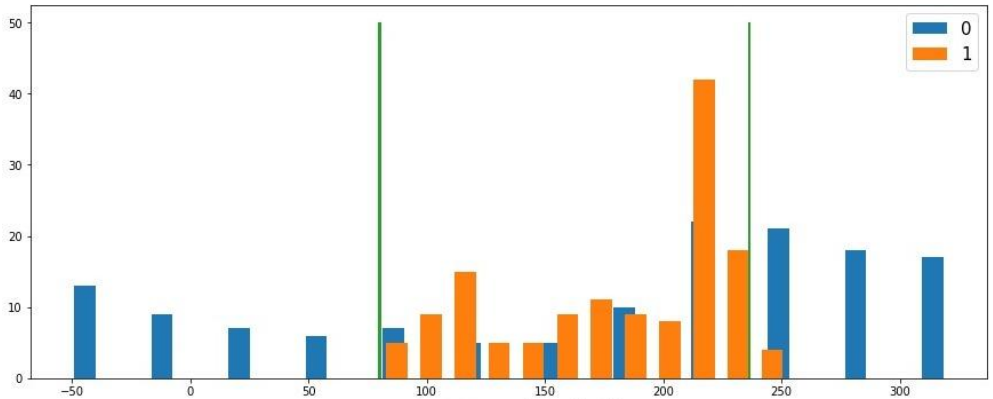
Resultado do artigo de referência

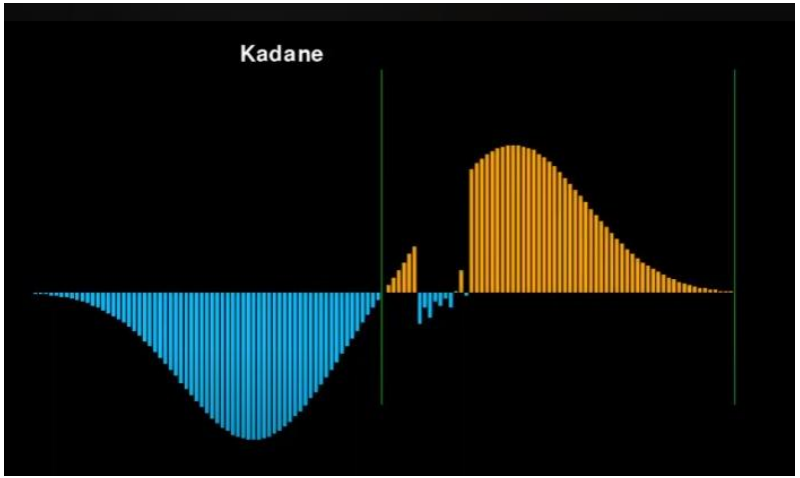
	test_full_model	test_set
Stage1	0.18	0.08
Stage2	1.96	0.78
Stage3	0.00	0.00
Sistema	2.14	0.86

Resultado da melhoria proposta

Melhoria proposta para a solução do artigo de referência

Foram testados dois algoritmos para escolha de thresholds. O primeiro busca um threshold que forneça um determinado recall em um modelo, usando um dataset de validação. É útil para controlar a quantidade de dados que passam para o próximo estágio. O segundo algoritmo busca o threshold que maximiza a acurácia para o mesmo dataset de validação.





Conclusão

A abordagem de múltiplos estágios proposta para detecção de intrusões hierárquica apresenta notáveis avanços, principalmente pela sua alta adaptabilidade, capacidade de redução de largura de banda e requisitos computacionais, bem como pela eficácia na detecção de ataques zero-day.

Os resultados experimentais indicam um desempenho superior em comparação com abordagens existentes, evidenciando a robustez do modelo. As melhorias para o sistemas propostas pelo nosso trabalho tornaram-no cerca de 7 vezes mais rápido mantendo as métricas de classificação razoavelmente próximas.