Detecção de Intrusão e Análise Cyberfísica em Redes Industriais

Wagner Carlos Mariani[1,2], Anelise Munaretto[2], Mauro Fonseca[2], Heitor Lopes[2], Tiago H. Silva[2]

1. Instituto Federal Catarinense
2. Universidade Tecnológica Federal do Paraná

Motivação

- Sistemas de controle industrial (ICSs)
  - \+ interconectados a Internet

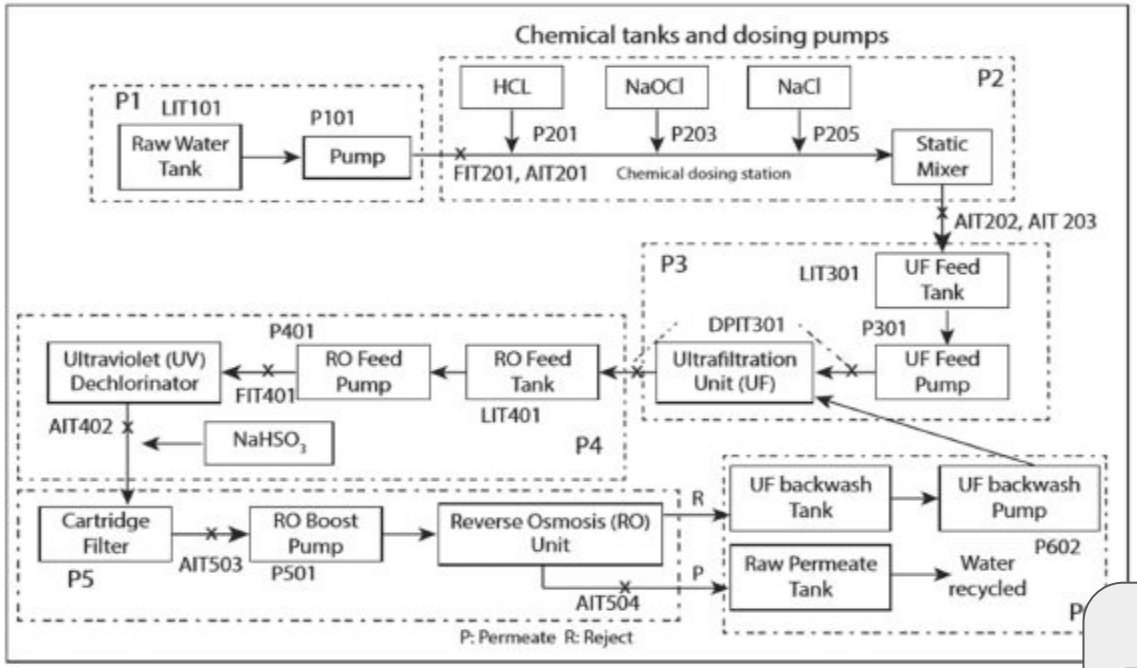
- Métodos tradicionais
  - detecção podem não ser suficientes

Objetivos

Detectar ataques com base no comportamento físico do sistema

Cenário

Dataset SWaT



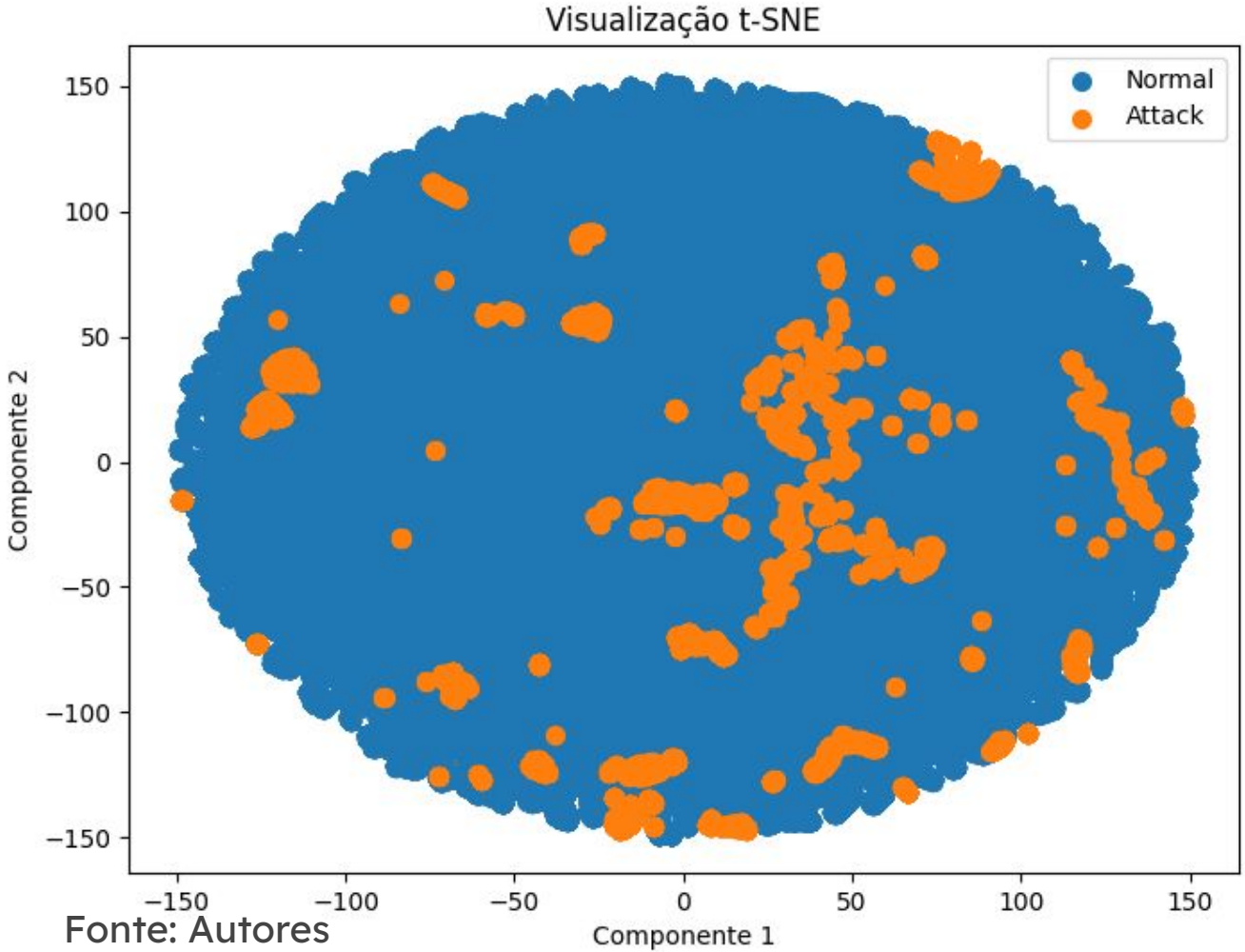
51 parâmetros. 11 dias de leituras a cada segundo

Fonte:
https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/

Classe	Seg.	%	Classe	Seg.	%	Classe	Seg.	%
Normal	615512	97.14	ATQ28	629	0.10	ATQ33	431	0.07
ATQ13	2254	0.36	ATQ25	607	0.10	ATQ07	428	0.07
ATQ26	1443	0.23	ATQ32	597	0.09	ATQ39	400	0.06
ATQ41	1202	0.19	ATQ11	561	0.09	ATQ20	392	0.06
ATQ08	970	0.15	ATQ27	534	0.08	ATQ03	384	0.06
ATQ01	935	0.15	ATQ36	516	0.08	ATQ37	374	0.06
ATQ21	702	0.11	ATQ35	481	0.08	ATQ24	320	0.05
ATQ16	690	0.11	ATQ22	466	0.07	ATQ40	296	0.05
ATQ23	684	0.11	ATQ02	445	0.07	ATQ38	280	0.04
ATQ28	629	0.10	ATQ33	431	0.07	ATQ19	258	0.04
ATQ25	607	0.10	ATQ07	428	0.07	ATQ14	233	0.04
ATQ32	597	0.09	ATQ39	400	0.06	ATQ06	199	0.03
ATQ11	561	0.09	ATQ20	392	0.06	ATQ10	161	0.03
ATQ27	534	0.08	ATQ03	384	0.06	ATQ29	143	0.02
ATQ36	516	0.08	ATQ37	374	0.06	ATQ34	99	0.02
ATQ35	481	0.08	ATQ24	320	0.05			
ATQ22	466	0.07	ATQ40	296	0.05			
ATQ02	445	0.07	ATQ38	280	0.04			

Tabela 1. Quantitativos de segundos das amostras por classes e percentuais.

Fonte: Autores



Fonte: Autores

Passos para distinguir ataques

- Preparar os dados;
- Classificação em 2 níveis;
- Classificar 1º, entre Normal e Ataque;
- Classificar, em seguida, qual o tipo de Ataque.

Normalização dos dados

Aplicação de Min-Max Scaler apenas em parâmetros que variam em escala, mantendo inalterados os dados dos atuadores que representam estados de ligado e desligado.

Extração de características de janelas temporais

.06	ATQ10	161	0.03
.06	ATQ29	143	0.02
.06	ATQ34	99	0.02
.05			
.05			
.04			

Fonte: Autores

TSFEL

https://tsfel.readthedocs.io/en/latest/

- As janelas de análise foram de 30 segundos, overlap de 6 segundos.
- Todas as caracteristicas que o TSFEL oferece foram extraidas de cada componente totalizando 2655 parâmetros no novo dataset.

Redução de Features

- FCBF (Fast Correlation Based Filter)
- ReliefF

Com a redução de Features o Dataset foi reduzido de 2655 colunas para 600, sendo (3 informativas) sendo uma média de 11,7 características para cada componente.

Balanceamento de Dados (SMOTE)

- As classes minoritárias eram de tal ordem pequenas que os classificadores acabam por ignora-las;

- A solução adotada foi balancear o dataset, criando novas amostras sintéticas
  - Essas amostras foram geradas levando em conta o tipo de ataque

- As amostras sintéticas primordialmente ajudam a diminuir o viés em favor da classe majoritária.

Divisão em treino e teste

- O dataset resultante inicialmente foi dividido em treino (70%, 3854 instancias) e teste (30%, 1652 instancias) para a 1a etapa;

- Para a 2a etapa o dataset de treino teve suas amostras do tipo Normal excluidas;

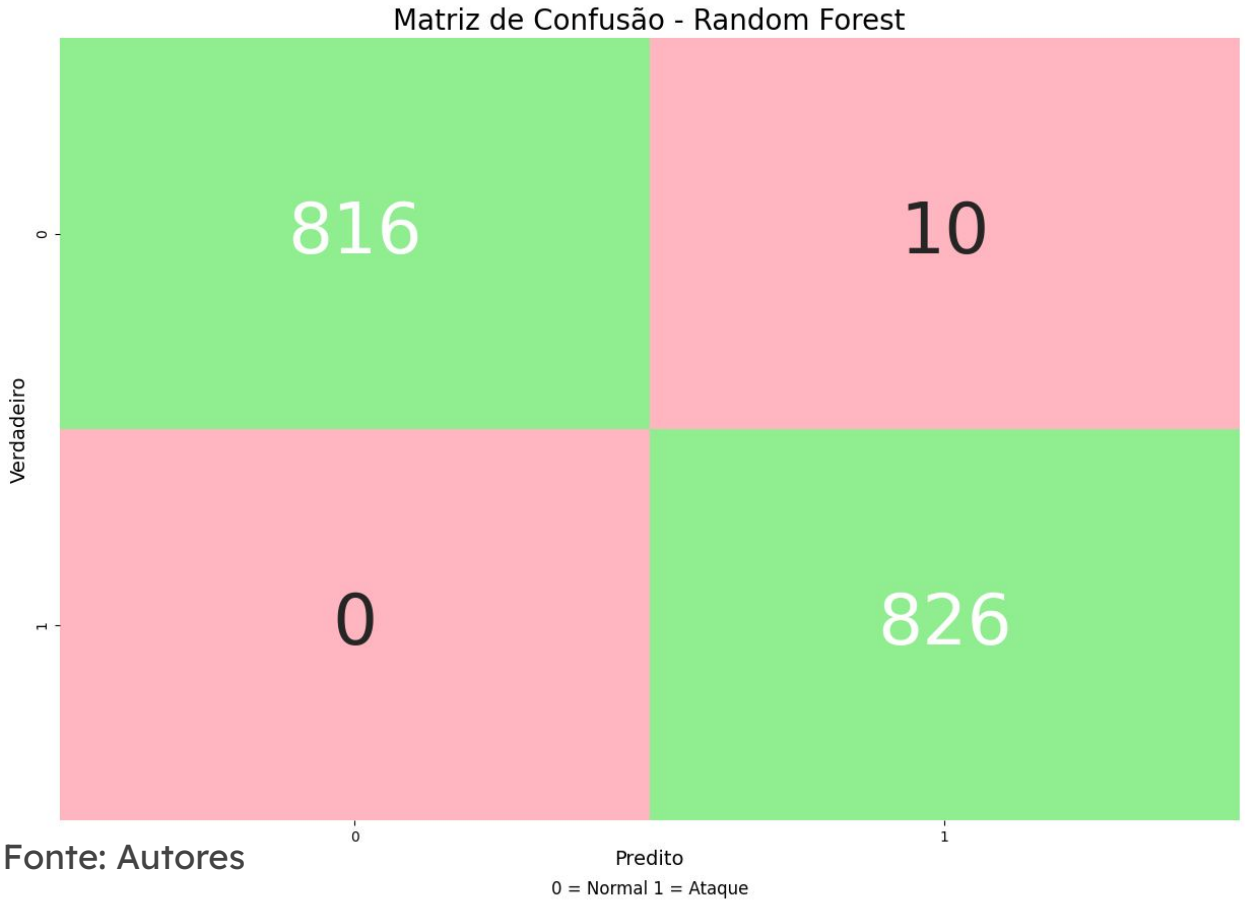
- As amostras classificadas como ataque na 1a etapa formam o dataset de teste da 2a etapa.

Resultados da 1a etapa

Classificador	F1	Precisão	Recall	ROC	Tempo (s)
Naive Bayes	0.5185	0.9455	0.3571	0.6683	0.090
SVM	0.7693	0.8561	0.6985	0.7906	4.555
KNN	0.9545	0.9319	0.9782	0.9534	0.031
Logistic Regression	0.9509	0.9515	0.9504	0.9510	67.720
Decision Tree	0.9779	0.9658	0.9903	0.9776	1.814
Random Forest	0.9940	0.9880	1.0000	0.9939	6.693

Tabela 2. Resultados dos Métodos de Classificação na Primeira Fase
Fonte: Autores

Matriz de Confusão melhor modelo 1a Etapa



Fonte: Autores

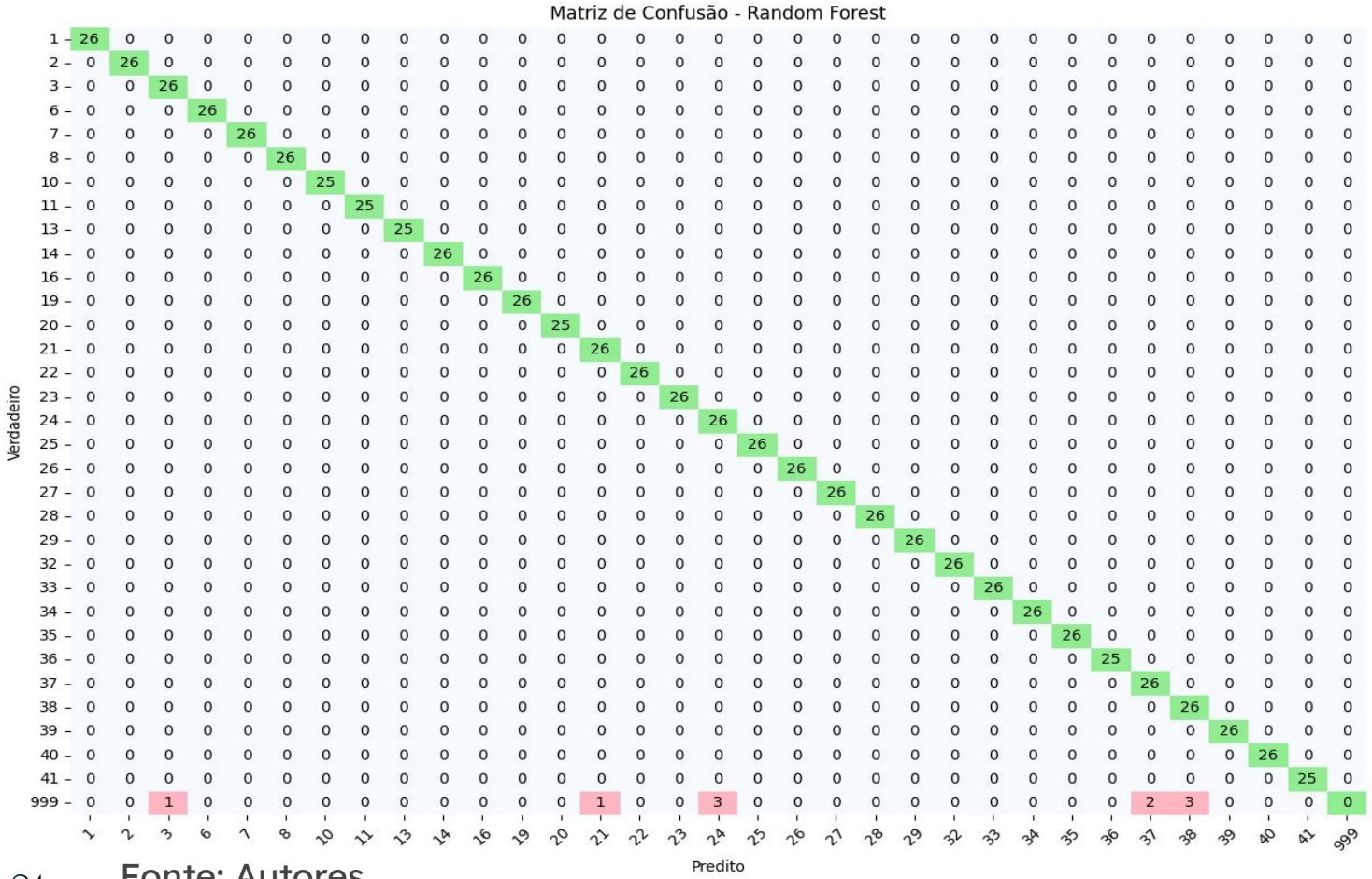
Resultados da 2a etapa

Classificador	F1	Precisão	Recall	MCC	Tempo (s)
Naive Bayes	0.9214	0.9609	0.9423	0.9398	0.05
SVM	0.6067	0.8428	0.6662	0.6682	0.33
KNN	0.8900	0.9351	0.9193	0.9193	0.02
Logistic Regression	0.9294	0.9593	0.9515	0.9513	78.82
Decision Tree	0.9497	0.9696	0.9658	0.9653	1.56
Random Forest	0.9823	0.9890	0.9880	0.9877	3.52

Tabela 3. Resultados dos Métodos de Classificação da Segunda Fase

Fonte: Autores

Matriz de Confusão melhor modelo 2a Etapa



Fonte: Autores

Conclusões.

- O método dividido em 2 etapas pode ser útil em datasets desbalanceados,
- O Randon Forest mostrou-se eficiente em cenários envolvendo Amostras Sintéticas
- As amostras Sintéticas viabilizaram o emprego de classificação no cenário proposto.

Trabalhos futuros

- Substituir a classificação por detecção de anomalias na 1a fase;
- Usar diferentes métodos em paralelo;
- Usar detectores de drift em paralelo a detecção de ataques.

Obrigado!

wagner.mariani@ifc.edu.br,

{anelise,maurofonseca,hslopes,thiagoh}
@utfpr.edu.br