Comparando Médias Móveis com Integral de Choquet para Detectar Anomalias no Tráfego de Redes

Denner Ayres, Abreu Quevedo, Graçaliz Dimuro,
Giancarlo Lucca, Bruno L. Dalmazo

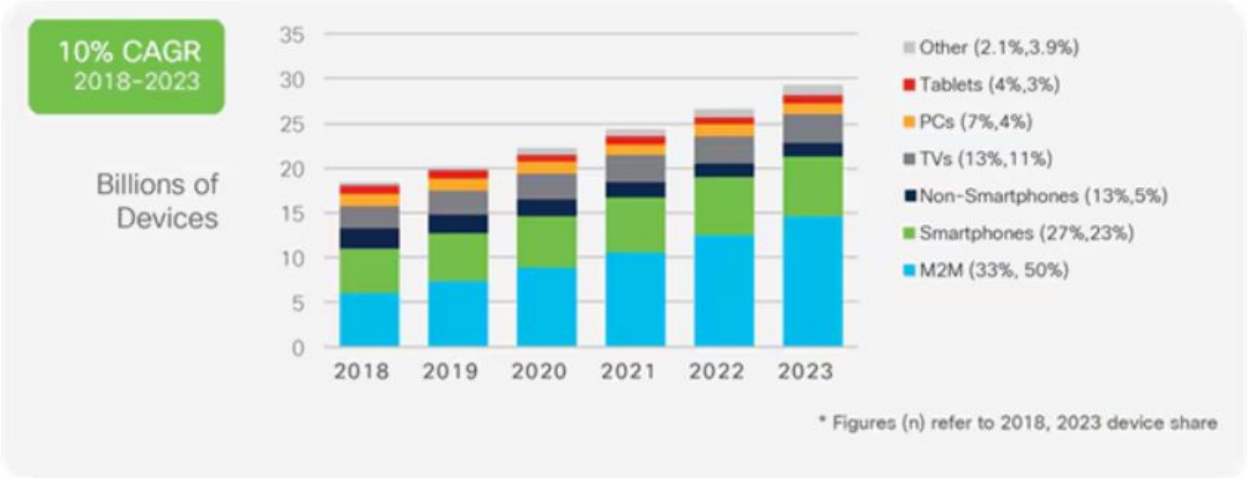
FURG

AGENDA

- Introdução
  - Contextualização
  - Motivação
  - Objetivo
- Modelo proposto
- Integrais de Choquet
- Implementação
- Resultados preliminares
- Considerações finais

INTRODUÇÃO CONTEXTUALIZAÇÃO

- A **infraestrutura de redes** é fundamental para o acesso confiável e rápido a recursos digitais.



Source: Cisco Annual Internet Report, 2018–2023

INTRODUÇÃO CONTEXTUALIZAÇÃO

- A **infraestrutura de redes** é fundamental para o acesso confiável e rápido a recursos digitais.

- Indispensável para negócios e vida cotidiana, com tantos dispositivos **interconectados**.

Apagão cibernético: como a tecnologia mundial caiu de uma só vez

Atualização de software de uma única empresa de segurança cibernética causou caos na sexta-feira (19), ressaltando a fragilidade da economia global e sua dependência de sistemas de computador

Sean Lyngaas, da CNN

20/07/2024 às 07:06

INTRODUÇÃO CONTEXTUALIZAÇÃO

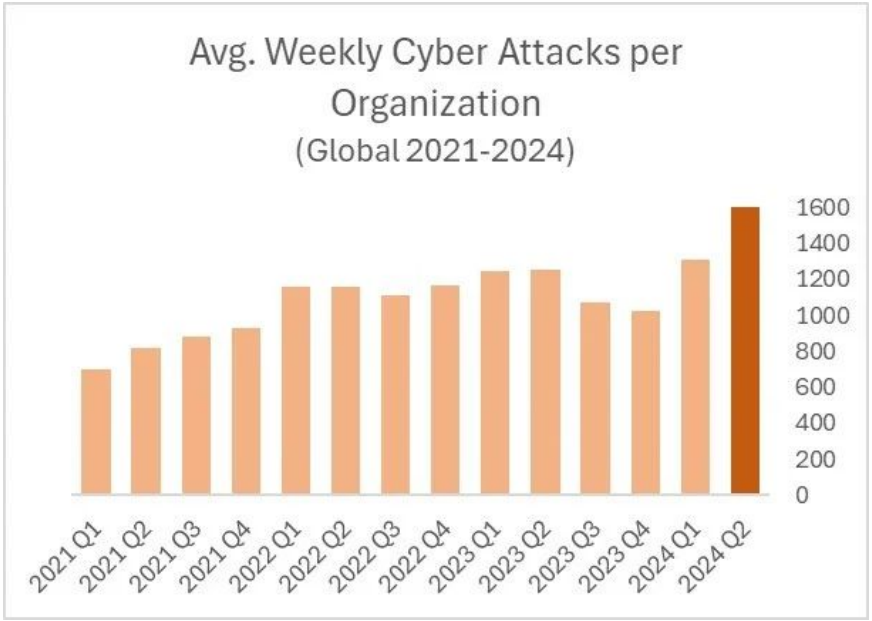
- A **infraestrutura de redes** é fundamental para o acesso confiável e rápido a recursos digitais.

- Indispensável para negócios e vida cotidiana, com tantos dispositivos **interconectados**.

- O tráfego constante de dados produzido por vários dispositivos e sensores cria dificuldades incessantes para a **gestão** e **monitoramento** da rede.

INTRODUÇÃO MOTIVAÇÃO

- Com o aumento do fluxo de dados, as redes de computadores são frequentemente **alvo de ataques**.



Disponivel em: https://pages.checkpoint.com/cyber-security-report-2023.html

INTRODUÇÃO MOTIVAÇÃO

- Com o aumento do fluxo de dados, as redes de computadores são frequentemente alvo de ataques.

- Esses ataques muitas vezes deixam rastros que podem ser detectados, motivando o desenvolvimento de **técnicas de detecção de anomalias.**


TECNOLOGIA

Empresas estão investindo em tecnologias de segurança

INTRODUÇÃO OBJETIVO

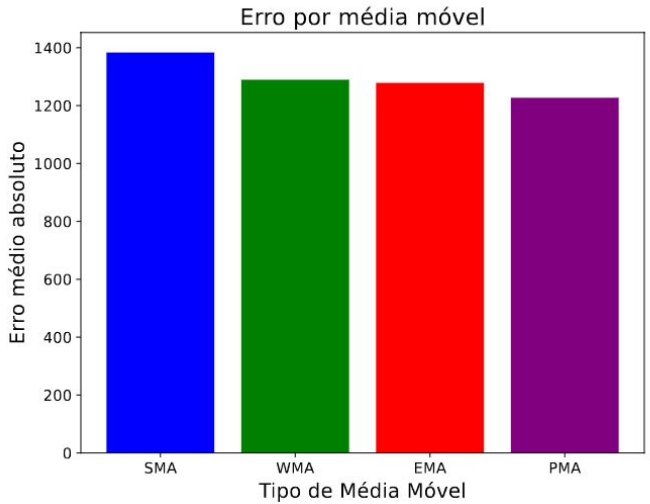
- Avaliar a eficácia da metodologia de Choquet como uma **função de agregação**

- Propor um **novo modelo** capaz de melhorar a segurança e eficácia

MODELO PROPOSTO

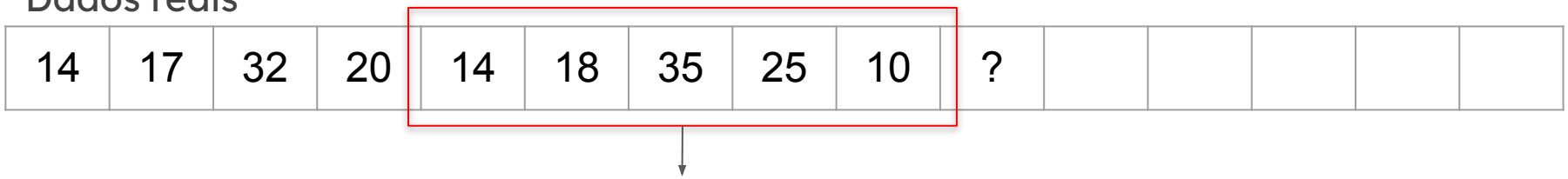
- Utiliza do produto entre os valores de entrada e os pesos

- Pesos definidos:
  - Média móvel simples (SMA)
  - Média móvel ponderada (WMA)
  - Média móvel exponencial (EMA)
  - Média móvel Poisson (PMA)



MODELO PROPOSTO

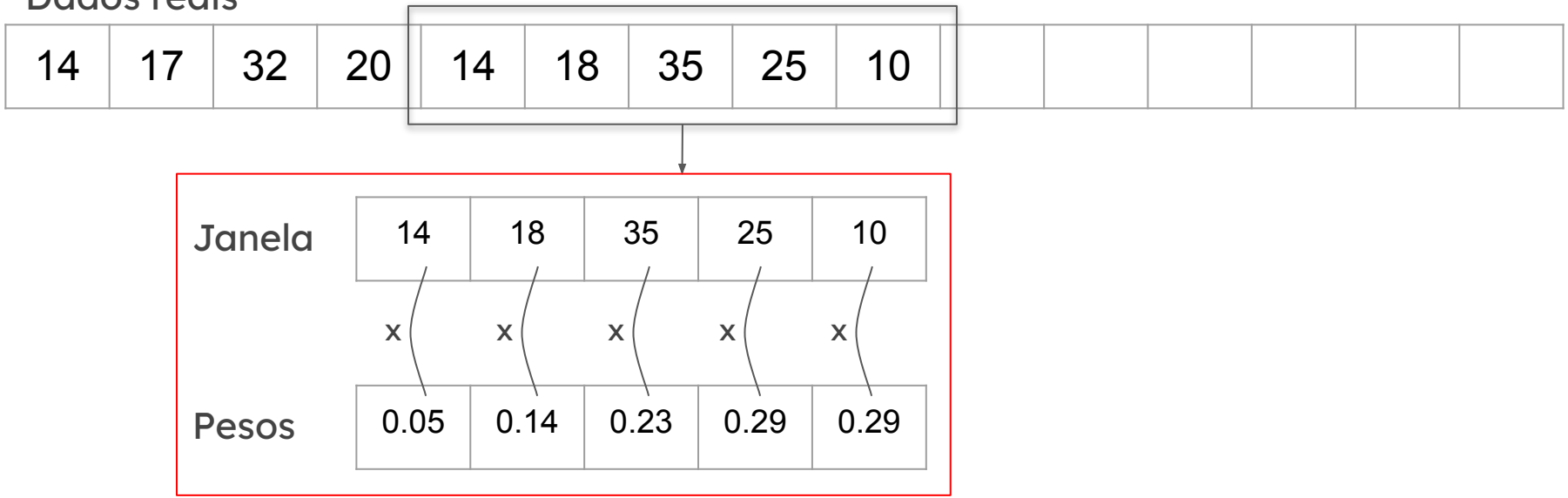
Dados reais



Janela deslizante de tamanho fixo

MODELO PROPOSTO

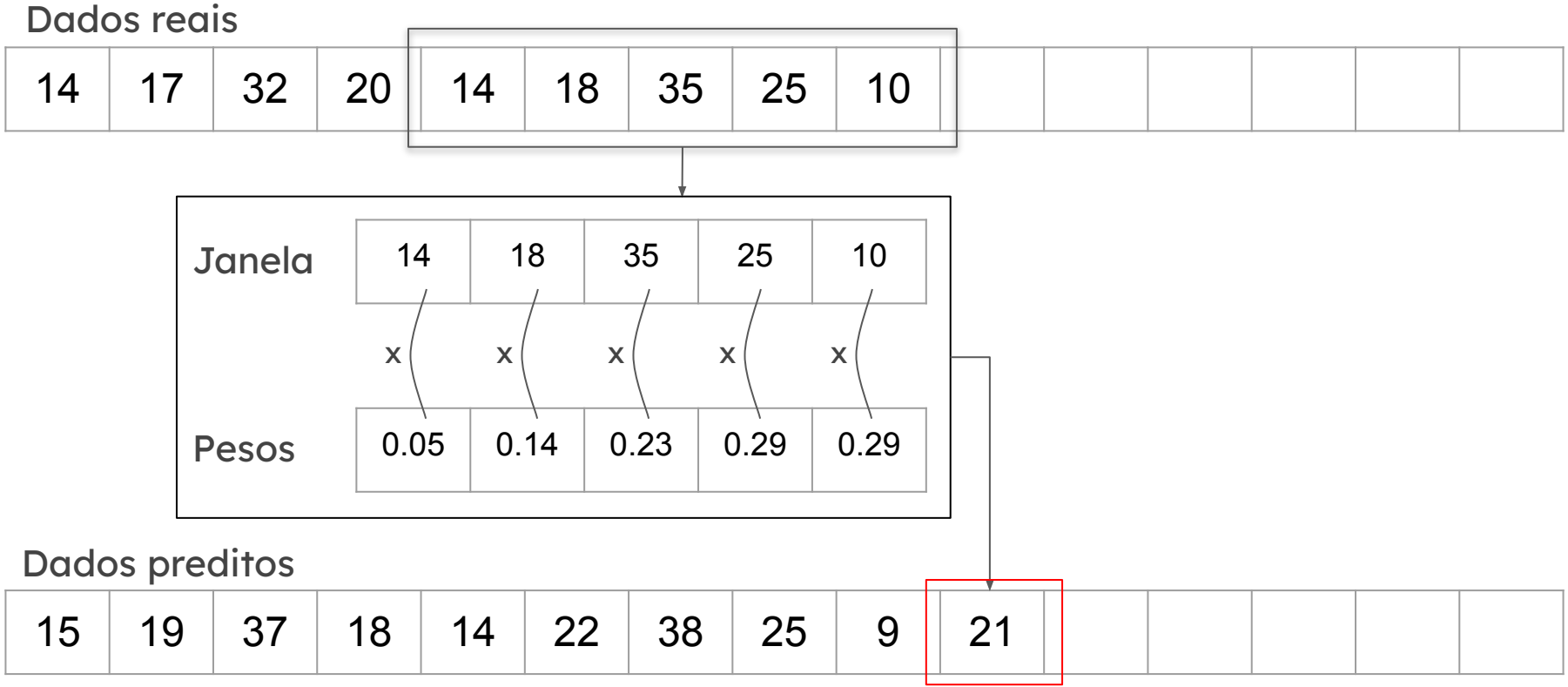
Dados reais



Dados preditos

15	19	37	18	14	22	38	25	9	t+1					

MODELO PROPOSTO

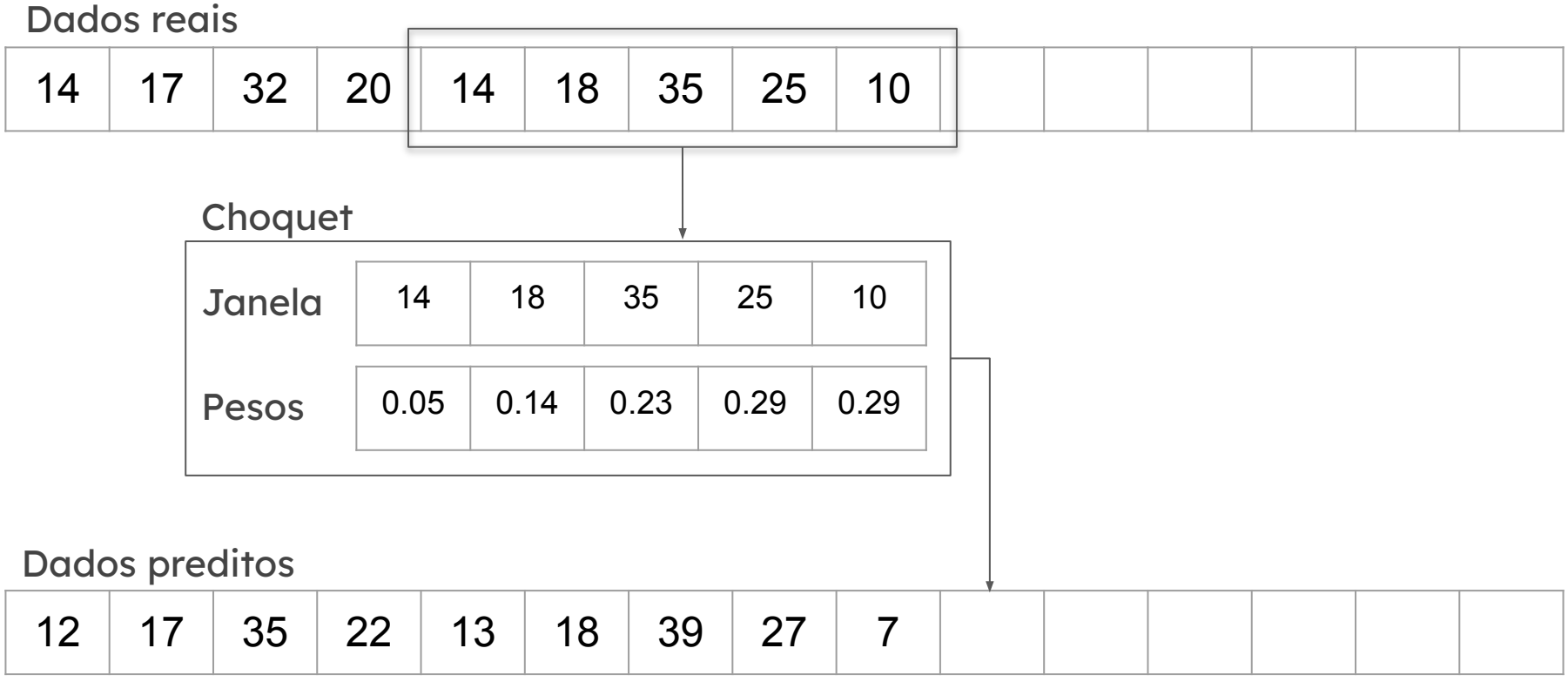


INTEGRAIS DE CHOQUET

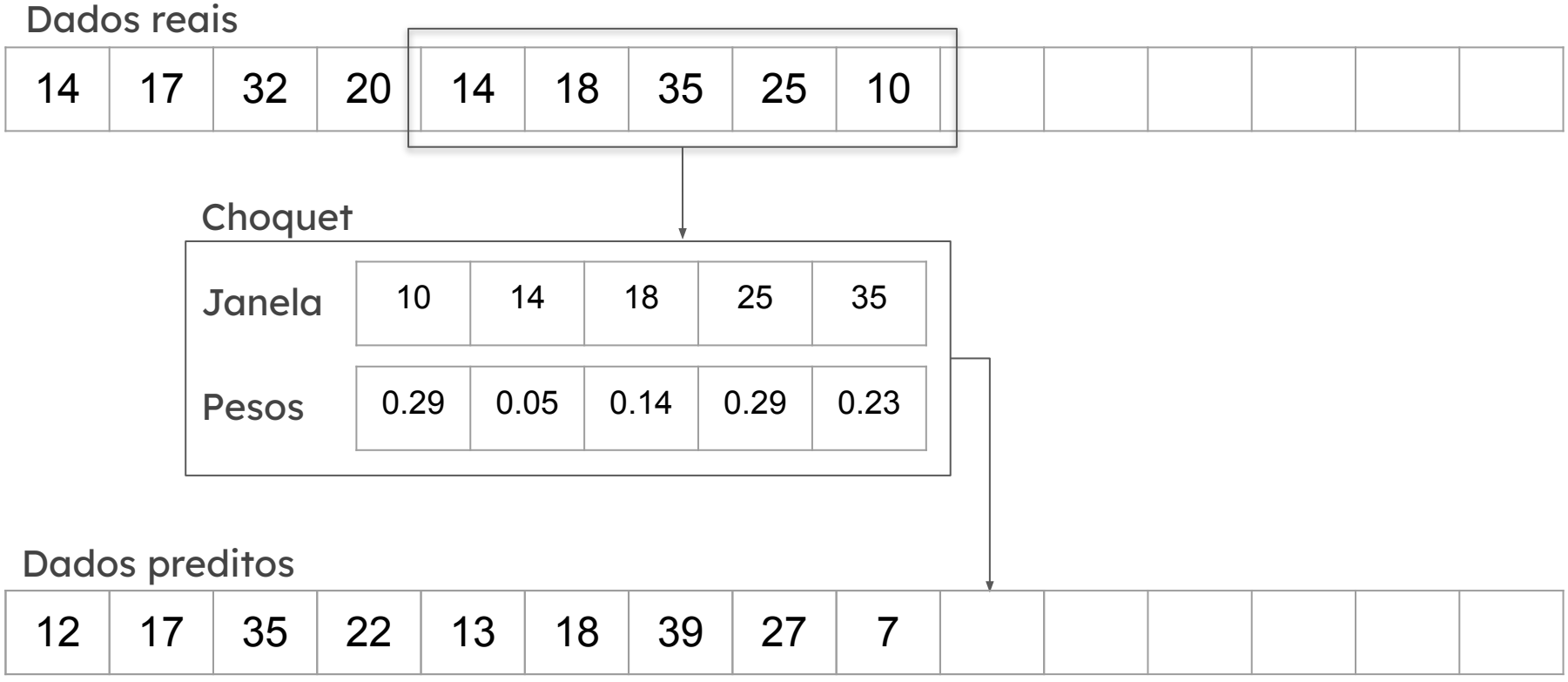
- A integral de Choquet é uma ferramenta matemática que permite o cálculo de uma **média ponderada** de valores, sendo capaz de atribuir pesos diferentes a cada valor de acordo com sua **importância relativa** e as **interações** entre eles.

$$C_m(x) = \sum_{i=1}^{n} \left(x_{(i)} - x_{(i-1)} \right) \cdot m\left(A_{(i)} \right),$$

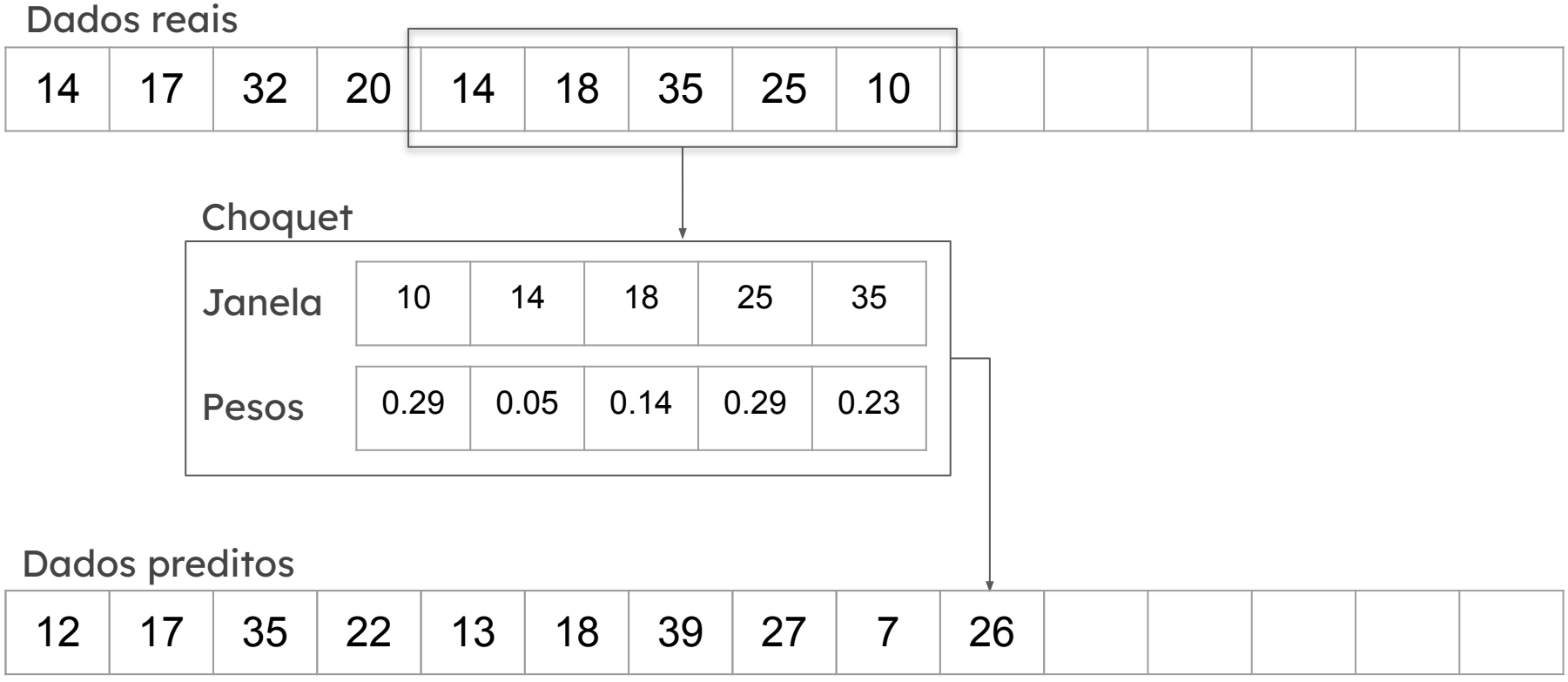
MODELO CHOQUET



MODELO CHOQUET



MODELO CHOQUET



IMPLEMENTAÇÃO

- Implementação realizada em Python
  - Pandas
  - Numpy
  - Matplotlib

- Testes conforme a base de dados: CIC-IDS2017 da University of New Brunswick (UNB)

Disponível em: https://www.unb.ca/cic/datasets/ids-2017.html

RESULTADOS

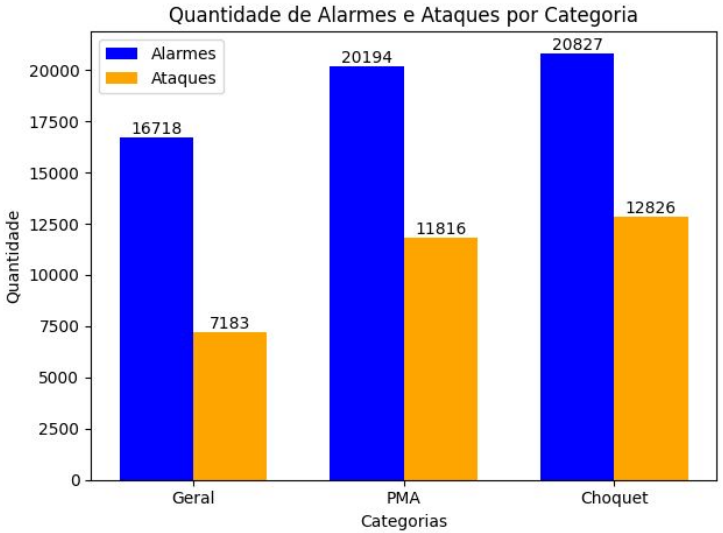
- Matriz de confusão.
  - PMA: TV P = 0.43 e TV N = 0.52
  - Choquet: TV P = 0.43 e TV N = 0.62

Tabela 2. Matriz de confusão PMA.

		Classe prevista	
		0	1
Classe esperada	0	VN: 7183	FP: 9535
	1	FN: 11816	VP: 8378

Tabela 3. Matriz de confusão Choquet.

		Classe prevista	
		0	1
Classe esperada	0	VN: 7183	FP: 9535
	1	FN: 12826	VP: 8001



CONSIDERAÇÕES FINAIS

- CONCLUSÕES:
  - PMA ainda demonstra o melhor modelo
  - Choquet tem grande potencial matemático

- TRABALHOS FUTUROS:
  - Calibração dos parâmetros do modelo
  - Novos modelos
  - Testes com novas bases de dados

Obrigado!

Denner Ayres	dennerayres@furg.br
Bruno L. Dalmazo	dalmazo@furg.br
Abreu Quevedo	abreu_rg@furg.br
Graçaliz Dimuro	graçaliz@furg.br
Giancarlo Lucca	giancarlo.lucca@ucpel.edu.br