Universidade Federal de Santa Maria – Ciência da Computação
Grupo de Microeletrônica - Gmicro

Detecção de Intrusão baseado em Séries Temporais

Bruno Dalmazo
Francisco Vogt
Tiago Perlin

Orientador:
Prof. Dr. Raul Ceretta Nunes

SBSEG'08

Sumário

- Sistemas de Detecção de Intrusão – SDI;
- Detecção de Anomalias;
- Séries Temporais:
  - Modelo ARIMA;
- Detector de Intrusões Baseado em Séries Temporais – DIBSeT;
- Trabalho em andamento.

Sistemas de Detecção de Intrusão - SDI

- Fonte de Informação
  - Host
  - Rede
- Análise
  - Assinatura (ataques conhecidos, poucos falsos positivos)
  - Anomalias (ataques desconhecidos, muitos falsos positivos)
- Resposta
  - Geração de Alertas
    - Intervenção humana
    - Intervenção automatizada

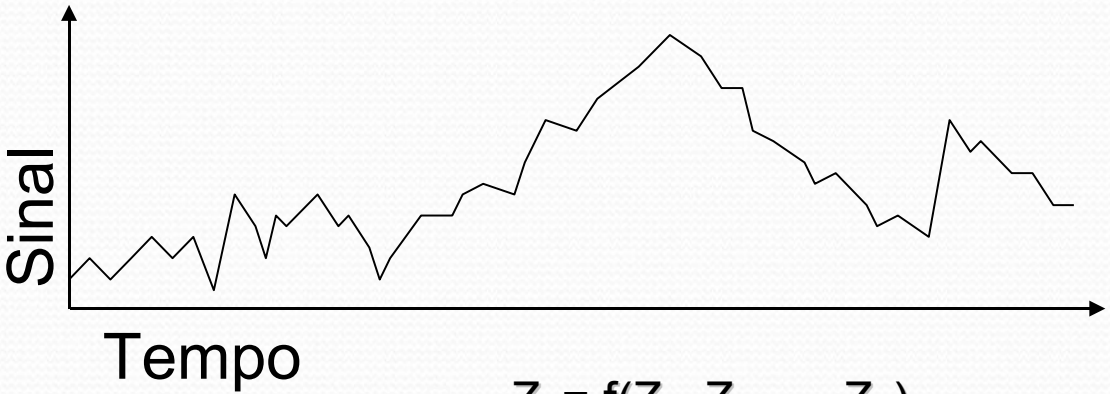
Detecção de Anomalias

Anomalia = Alteração do comportamento normal do sistema.

- Anomalias de tráfego de rede
  - Ataques/intrusão
  - Flash crowds, transferência de arquivos grandes
  - Defeito em equipamentos de rede

- Métodos
  - Métodos estatísticos, Data Mining, Markov, Redes Neurais, Wavelets, Séries Temporais, ...

Séries Temporais



$Z_t = f(Z_1, Z_2, ..., Z_N)$

- $Z_1, Z_2, ..., Z_N$ são amostras eqüidistantes no tempo.

- Usado em:
  - Bolsa de Valores
  - Previsão do Tempo
  - Predição de desempenho
  - Análise de atrasos de rede

Modelo ARIMA

- ARIMA – *Autoregressive Integrated Moving Average*
  - *S*éries estacionárias ou não
  - Previsões correlacionadas a comportamentos passados
- *Threshold adaptativo*

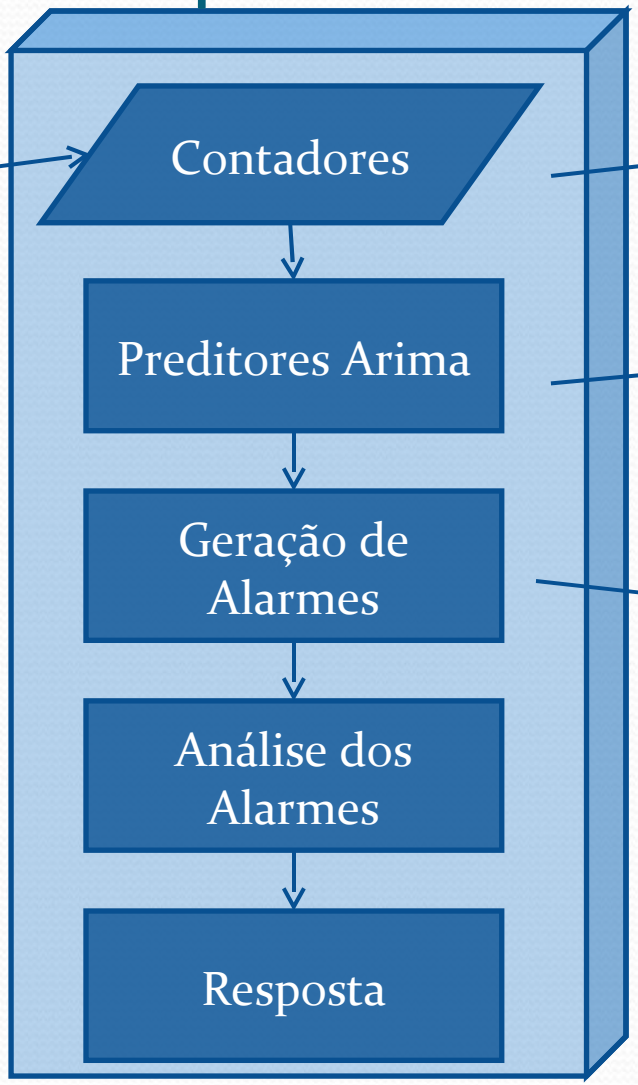
$$\hat{z}_t = \frac{\theta(B)}{\phi(B)\nabla^d} a_t$$

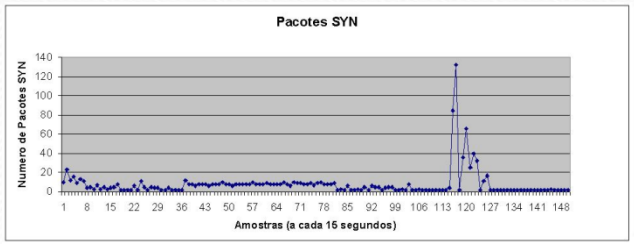
Onde:

- *B é o operador de deslocamento para trás;*
- *é o operador de diferença para trás;*
- *a_t é o ruído no instante t;*
- *d é a ordem de não estacionariedade;*
- *$\theta(B)$ e $\phi(B)$ são polinomiais de B.*

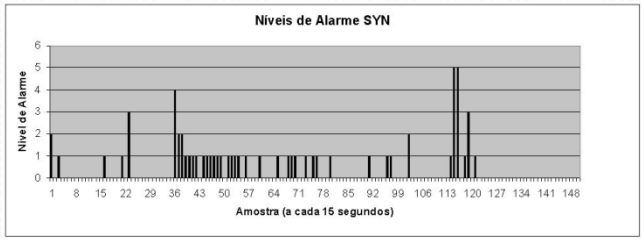
Detector de Intrusões Baseado em Séries Temporais – DIBSeT

Sistema de Análise da Internet – IAS IFIS/FHGe





$$\hat{z}_t = \frac{\theta(B)}{\phi(B)\nabla^d} a_t$$



Universidade Federal de Santa Maria 1960

GMICRO grupo de microeletrônica - universidade federal de santa maria

Detector de Intrusões Baseado em Séries Temporais – DIBSeT

- Dados coletados pelo *probe* do IAS
- Análise baseada em Séries Temporais – modelo ARIMA
- Geração de Alarmes
- Níveis de Alarme

Trabalho em andamento

- Utilização de níveis de alarmes
  - Análise da concentração de alarmes e
  - Correlação temporal
- Separação dos fluxos de dados – Análise da Correlação espacial nos fluxos
- Análise de algoritmos para detecção de mudanças Abruptas e geração de alarmes.

Obrigado!