DANTE: DETECÇÃO DE ANOMALIAS E NOVIDADES EM SÉRIES TEMPORAIS COM REDES AUTO-ORGANIZÁVEIS

Leonardo Aguayo*, Guilherme A. Barreto*

*Universidade Federal do Ceará, Depto. Engenharia de Teleinformática Av. Mister Hull, S/N - CP 6007, CEP 60455-970, Campus do Pici, Centro de Technologia, Fortaleza, Ceará.

Emails: leonardo.aguayo@indt.org.br, guilherme@deti.ufc.br

Abstract— This paper introduces the DANTE project: **D**etection of **A**nomalies and **N**ovelties in **T**ime s**E**ries with self-organizing networks. The goal of this project is to evaluate self-organizing networks in the detection of anomalies/novelties in dynamic data patterns. For this purpose, we first describe three standard clustering-based approaches which uses well-known self-organizing neural architectures, such as the SOM and the Fuzzy ART algorithms, and then present a novel approach based on the Operator Map (OPM) network. The OPM is a generalization of the SOM where neurons are regarded as temporal filters for dynamic patters. The OPM is used to build local adaptive filters for a given nonstationary time series. Non-parametric confidence intervals are then computed for the residuals of the local models and used as decision thresholds for detecting novelties/anomalies. Computer simulations are carried out to compare the performances of the aforementioned algorithms.

Keywords— Operator map, Anomaly Detection, Time Series, Local Linear Models, Adaptive Filtering.

Resumo— Este trabalho apresenta o projeto DANTE: **D**etecção de **A**nomalias e **N**ovidades em séries **TE**mporais. O objetivo do projeto é avaliar o desempenho de diversas redes auto-organizadas ao detectar anomalias/novidades em padrões de dados dinâmicos. Para tanto, inicialmente descrevem-se três abordagens tradicionais de agrupamento (*clustering*) que utilizam arquiteturas auto-organizáveis, tais como os algoritmos SOM (*Self-Organizing Map*) e Fuzzy-ART, e em seguida apresenta-se uma nova abordagem baseada na rede Operator Map (OPM). A rede OPM é uma generalização da rede SOM, na qual os neurônios são usados como filtros temporais para padrões dinâmicos: utiliza-se o OPM para construir filtros adaptativos de abrangência local para uma dada série não-estacionária. Para realizar a detecção de anomalias, calculam-se intervalos de confiança não-paramétricos a partir dos resíduos obtidos a partir dos modelos locais. Várias simulações computacionais são realizadas a fim de comparar os desempenhos dos algoritmos supracitados.

Keywords— Mapa de Operadores, Detecção de Novidades, Séries Temporais, Modelos Lineares Locais, Filtragem Adaptativa.

1 Introdução

Técnicas de detecção de anomalias[1] constituem procedimentos computacionais projetados para lidar com o difícil problema de encontrar amostras de dados aparentemente inconsistentes com o conjunto de dados já modelado. Recentemente, observou-se um aumento no número de aplicações da rede SOM (*Self-Organizing Map*) neste tipo de problema (Sarasamma & Zhu 2006, Barreto et al. 2005, Lee & Cho 2005, Singh & Markou 2004), sendo a maioria delas com enfoque apenas em dados estáticos, i.e. dados para os quais a dimensão temporal não é uma fonte relevante de informação. Entretanto, dados provenientes de várias aplicações reais são ordenados no tempo, tipicamente na forma de medições sucessivas da magnitude de uma ou mais grandezas de interesse, dando origem a séries temporais. Na indústria, por exemplo, processos de monitoração envolvem a coleta da leitura contínua de diversos sensores, de modo a rastrear o estado do sistema monitorado (Zorriassatine et al. 2005, Jamsa-Jounela et al. 2003, Alhoniemi et al. 1999). No mercado financeiro, a série histórica de ações pode apresentar padrões que auxiliam o investidor a tomar decisões de curto ou longo prazo.

A detecção de anomalias em séries temporais é particularmente desafiadora devido à presença de características determinísticas, tais como tendência e sazonalidade, que podem mascarar o caráter de novidade presente nos dados. Processos inerentemente não-estacionários, tais como séries com mudança de regime, ainda impõem limitações adicionais na modelagem da série. Além disto, alguns tipos específicos de séries, tais como séries econométricas, podem possuir poucas amostras, restringindo a quantidade de dados disponíveis necessária para extrair informação sobre seu comportamento. Finalmente, aplicações nas quais o fator atraso é crítico, tais como detecção de falhas e segurança, requerem detecção de anomalias em tempo real. Abordagens tradicionais, tais como modelagem estatística paramétrica e testes de hipóteses (Markou & Singh 2003a) podem ser aplicadas com sucesso para modelar padrões estáticos (i.e. sem memória), visto que estas técnicas assumem algum grau de estacionariedade nos dados. Por um lado, a dinâmica de processos estacionários lineares pode ser capturada pela modelagem ARMA tradicional, e por outro lado, padrões não-lineares e não-estacionários, tais como séries caóticas, necessitam uma abordagem mais robusta em termos de aprendizado e capacidade computacional.

[1] Dependendo do campo de pesquisa, a detecção de anomalias pode ter várias designações, tais como detecção de novidades, detecção de espúrios ou detecção de falhas.

A aplicação de redes neurais artificiais (RNAs) mostra-se útil em casos de classificação, dada a capacidade das RNAs de atuar como identificadores não-lineares de sistemas, generalizando o conhecimento adquirido em dados desconhecidos. A maioria dos métodos baseados em RNAs empregam treinamento supervisionado, tais como as arquiteturas MLP e RBF (Markou & Singh 2003b, Fancourt & Principe 2004). Entretanto, em problemas de detecção de anomalias encontra-se tipicamente uma assimetria no tamanho dos dados de treinamento: dados já classificados como anormais podem ser custosos a serem coletados, ou até mesmo inexistentes. Uma solução plausível faz uso de algoritmos de *clustering* destinados encontrar subconjuntos de dados com estrutura temporal similar (Liao 2005). Entretanto, poucos algoritmos baseados em clustering para detecção de anomalias têm sido propostos, em particular variantes do algoritmo SOM. A maioria das abordagens baseadas em redes SOM usualmente convertem a série temporal em uma representação não-temporal (por exemplo, utilizando-se componentes espectrais via Transformada Discreta de Fourier) e a utiliza como entrada para a rede SOM (Wong et al. 2006).

Outra abordagem comum é utilizar linhas de atraso de comprimento fixo como entrada da rede, novamente convertendo a série temporal em uma representação espacial (Fu et al. 2001). Desde a década de 1990, diversas variações da rede SOM têm sido propostas com o intuito de apresentar desempenho superior à classificação estática, quando alimentadas com séries temporais (Barreto & Araújo 2001). Entretanto, tais SOMs temporais não foram sistematicamente utilizadas para o propósito de detecção de anomalias/novidades.

Do exposto, o propósito deste trabalho é entender a eficácia da utilização de variantes da rede SOM na detecção de anomalias em séries temporais. Com este intuito, inicialmente descrevem-se três abordagens tradicionais de agrupamento (*clustering*) que utilizam arquiteturas auto-organizáveis, tais como os algoritmos SOM (*Self-Organizing Map*) e Fuzzy-ART (Carpenter et al. 1991), e em seguida apresenta-se uma nova abordagem baseada na arquitetura *Operator Map* (OPM), introduzida no final dos anos 1980 por Lampinen & Oja (1989). Neste trabalho, utiliza-se o modelo OPM para construir filtros adaptativos locais adequados à modelagem de séries não-estacionárias. Intervalos de confiança não-paramétricos são calculados a partir dos resíduos dos modelos locais e utilizados como limiares de decisão para detecção de anomalias/novidades. O restante do trabalho está dividido na seguinte forma: na Seção 2, descrevem-se os algoritmos avaliados para detectar anomalias/novidades em séries temporais e ainda apresenta-se a a metodologia utilizada nas simulações. Na Seção 4, encontram-se os resultados numéricos, seguida de conclusões na Seção 5.

2 Clustering de Séries Temporais para Detecção de Anomalias

Nesta Seção, descrevem-se três abordagens utilizadas para detecção de anomalias em séries temporais, limitada à descrição de detecção baseada em protótipos. Assume-se que os algoritmos são treinados *on-line* assim que o dado é coletado. Os vetores de entrada são construídos a partir de uma janela deslizante de tamanho fixo. Assim, no instante t, o vetor de entrada é dado por

$$\mathbf{x}^+(t) = [x(t)\ x(t-1)\ \cdots\ x(t-p+1)]^T, \quad (1)$$

onde $p \geq 1$ é tamanho da janela. A atualização dos pesos da rede é permitida até um número máximo de passos, T_{max}. Os primeiros dois algoritmos são baseados na rede SOM, enquanto o terceiro pertence à família de arquitetura de redes ART (*Adaptive Resonance Theory*), o qual possui um mecanismo intrínseco de detecção de novidades, justificando sua inclusão na avaliação de desempenho.

2.1 SOM Tradicional

Realiza-se o treinamento de uma rede SOM utilizando-se como entrada o vetor $\mathbf{x}^+(t)$. Em seguida, determina-se o neurônio vencedor de acordo com a seguinte regra de seleção $i^*(t)$,

$$i^*(t) = \arg\min_{\forall i} \|\mathbf{x}^+(t) - \mathbf{w}_i(t)\|, \quad i = 1, \ldots, Q, \quad (2)$$

onde Q é o número de neurônios e t denota a iteração corrente do algoritmo. Atualizam-se os pesos correspondentes ao vencedor por intermédio da seguinte regra de aprendizado:

$$\mathbf{w}_i(t+1) = \mathbf{w}_i(t) + \eta(t) h(i^*, i; t)[\mathbf{x}^+(t) - \mathbf{w}_i(t)], \quad (3)$$

onde $h(i^*, i; t)$ é uma função gaussiana que controla o grau de alteração imposto aos pesos dos neurônios localizados na vizinhança do neurônio vencedor:

$$h(i^*, i; t) = \exp\left(-\frac{\|\mathbf{r}_i(t) - \mathbf{r}_{i^*}(t)\|^2}{\sigma^2(t)}\right), \quad (4)$$

em que $\sigma(t)$ define o raio da vizinhança na iteração t, enquanto $\mathbf{r}_i(t)$ e $\mathbf{r}_{i^*}(t)$ são respectivamente as coordenadas dos neurônios i e i^* no arranjo de saída. A taxa de aprendizagem $0 < \eta(t) < 1$ deve ser decrescente com o tempo, de modo a garantir a convergência do valor dos pesos dos neurônios para estados estáveis. Neste trabalho, utilizou-se $\eta(t) = \eta_0 \left(\eta_T/\eta_0\right)^{-(t/T_{max})}$, sendo η_0 um valor inicial para η, e η_T o valor após T_{max} iterações de treinamento. A variável $\sigma(t)$ decresce de maneira similar.

2.2 Modelo Kangas

Diversos algoritmos baseados na rede SOM têm sido propostos para realizar *clustering* em séries temporais, mas não utilizados para propósito de detecção de novidade. O modelo proposto por Kangas et al. (1990) é um dos mais simples disponíveis, e consiste em realizar uma filtragem IIR de primeira ordem no vetor de entrada $\mathbf{x}^+(t)$:

$$\overline{\mathbf{x}}(t) = (1-\lambda)\overline{\mathbf{x}}(t-1) + \lambda\mathbf{x}^+(t), \qquad (5)$$

em que $0 < \lambda < 1$ é o parâmetro de decaimento de memória. Apresenta-se o vetor filtrado $\overline{\mathbf{x}}(t)$ ao algoritmos SOM, o qual segue o procedimento usual de treinamento, dado pela Eq. (3).

2.3 Algoritmo Fuzzy-ART

Este trabalho também avalia o desempenho do algoritmo Fuzzy-ART (Carpenter et al. 1991) na detecção de anomalias em séries temporais, dada a sua simplicidade de implementação e baixo custo computacional. Apresenta-se o vetor de entrada $\mathbf{x}^+(t)$ a uma camada competitiva Q de neurônios, e seleciona-se o neurônio vencedor i^* com base na métrica T_{i^*}, tomada para o vencedor como a de valor mais alto entre todos os neurônios:

$$i^*(t) = \arg\max_{\forall i} \{T_i(t)\}, \qquad (6)$$

em que T_i é definido como

$$T_i(t) = \frac{|\mathbf{x}^+(t) \wedge \mathbf{w}_i(t)|}{\varepsilon + |\mathbf{w}_i(t)|}, \qquad (7)$$

tal que $0 < \varepsilon \ll 1$ é uma pequena constante positiva, e $|\mathbf{u}|$ é a norma L_1 do vetor $\mathbf{u}$. O símbolo $\wedge$ denota o operador mínimo que por componente do vetor, ou seja

$$x_j^+(t) \wedge w_{ij}(t) \equiv \min\left\{x_j^+(t), w_{ij}(t)\right\}. \qquad (8)$$

O próximo passo envolve o teste de ressonância. Se

$$\frac{|\mathbf{x}^+(t) \wedge \mathbf{w}_{i^*}(t)|}{|\mathbf{x}^+(t)|} \geq \rho, \qquad (9)$$

atualizam-se os pesos do neurônio vencedor $i^*(t)$ da seguinte forma:

$$\mathbf{w}_{i^*}(t+1) = \beta\left(\mathbf{x}^+(t) \wedge \mathbf{w}_{i^*}(t)\right) + (1-\beta)\,\mathbf{w}_{i^*}(t) \qquad (10)$$

em que as constantes $0 < \rho < 1$ e $0 < \beta < 1$ são chamados de *parâmetro de vigilância* e taxa de aprendizagem, respectivamente. Se o teste de ressonância para o neurônio vencedor corrente $i^*(t)$ falha, seleciona-se outro neurônio como vencedor, tipicamente o que possuir o segundo maior valor para $T_i(t)$. Se o testa ainda falhar, o processo se repete até que um dos neurônios $i^*(t)$ satisfaça Eq. (9). Se o teste falhar para todos os neurônios, o vetor de entrada é classificado como *novo* e adicionado à camada competitiva. O parâmetro ρ controla a sensibilidade do algoritmo a variações dos vetores de entrada. Se $\rho \to 1$, um número maior de protótipos é criado na camada competitiva. para $\rho \to 0$, o número de protótipos é menor.

2.4 Metodologia de Detecção

Diferentemente da rede Fuzzy-ART, os métodos previamente descritos, baseados na rede SOM, não possuem um mecanismo intrínseco de detecção de novidades. Entretanto, é prática comum (Sarasamma & Zhu 2006, Barreto et al. 2005, Alhoniemi et al. 1999) utilizar o erro de quantização

$$e_q(\mathbf{x}^+, \mathbf{w}_{i^*}; t) = \|\mathbf{x}^+(t) - \mathbf{w}_{i^*}(t)\|, \qquad (11)$$

como medida da proximidade de $\mathbf{x}^+(t)$ a uma representação estatística do comportamento normal codificado nos vetores de peso da rede SOM. Uma vez que a rede SOM tradicional (ou o modelo de Kangas) foi treinado, apresentam-se novamente os vetores para a rede. A partir dos erros de quantização resultantes, $\{e_q(\mathbf{x}^+, \mathbf{w}_{i^*}; t)\}_{t=1}^N$, calculam-se os limiares para a detecção de novidades. Para uma rede com treinamento bem-sucedido, a distribuição probabilística destes erros de quantização devem refletir o comportamento conhecido ou 'normal' da variável de entrada, cujo modelo temporal está sendo construído. Recentemente, diversos procedimentos destinados a calcular os limiares de decisão têm sido apresentados. A maioria deles baseia-se em técnicas estatísticas bem estabelecidas (Hodge & Austin 2004), mas aqui aplica-se a abordagem descrita em Barreto et al. (2005). Para um nível de significância α, busca-se um intervalo no qual encontra-se um percentual $100(1-\alpha)$ (por exemplo $\alpha = 0.05$) de valores de erro de quantização considerados normais. Assim, calculam-se os limiares inferior e superior $[\tau^-,\ \tau^+]$ como se segue:

- **Limite Inferior** (τ^-): Este é o $100\frac{\alpha}{2}$ percentil[2] da distribuição dos erros de quantização associados aos vetores de treinamento.
- **Limite Superior** (τ^+): Este é o percentil $100(1-\frac{\alpha}{2})$ da distribuição dos erros de quantização associados aos vetores de treinamento.

Uma vez computado o intervalo de decisão $[\tau^-,\ \tau^+]$, o comportamento anômalo da série temporal pode ser detectado *on-line* por intermédio da seguinte regra:

$$\begin{array}{ll} \text{SE} & e_q(\mathbf{x}^+, \mathbf{w}_{i^*}; t) \in [\tau^-,\ \tau^+] \\ \text{ENTÃO} & \mathbf{x}^+(t) \text{ é } \textbf{NORMAL} \\ \text{SENÃO} & \mathbf{x}^+(t) \text{ é } \textbf{ANORMAL} \end{array} \qquad (12)$$

[2] O percentil de uma distribuição de valores é um número N_α tal que o percentual $100(1-\alpha)$ das amostras é menor ou igual a N_α.

3 Abordagem Proposta

A componente principal do método proposto é a arquitetura OPM. Neurônios na rede OPM são tratados como operadores matemáticos, tipicamente denotados por $G(\cdot)$, representando algum tipo de filtro ou mapeamento para padrões temporais, Tais operadores usualmente contêm parâmetros ajustáveis, os quais podem ser atualizados de modo adaptativo e auto-organizado. Assim, um dado operador temporal pode eventualmente se tornar especializado em tratar uma certa faixa dinâmica de valores da série temporal de entrada. Mais especificamente, vamos assumir que no instante de tempo t uma data série temporal possa ser descrita pelo seguinte modelo global

$$x(t) = H\left(\mathbf{x}^-(t)\right) + \varepsilon(t) \tag{13}$$

em que $\mathbf{x}^-(t) = [x(t-1)\ x(t-2)\ \cdots\ x(t-p)]^T$ é um vetor contendo as últimas p amostras da série, $H(\cdot)$ é um mapeamento desconhecido (possivelmente não-linear), e $\varepsilon(t)$ é uma amostra de um processo ruído branco gaussiano de média zero e variância σ_ε^2. Vamos ainda assumir que o modelo global $H(\cdot)$ possa ser aproximado com precisão arbitrária por um conjunto de Q modelos locais G_i, $i = 1, \ldots, Q$, associados aos neurônios no modelo OPM. Como aplicação-alvo é a detecção de anomalias em séries temporais, está-se interessado em prover uma boa estimativa $\hat{x}(t)$ do estado corrente do sistema monitorado, $x(t)$, dado o vetor $\mathbf{x}(t)$ e os modelos locais $G_i(\cdot)$. Seja então $x_i(t)$ a estimativa do estado corrente, fornecida pelo neurônio i. Assim,

$$e_i(t) = x(t) - \hat{x}_i(t), \tag{14}$$

é o erro de predição associado ao neurônio i. Se o sistema está operando normalmente, espera-se que o erro de predição seja pequeno, dada a aproximação local do mapeamento $H(\cdot)$. Caso contrário, uma anomalia pode estar ocorrendo. Uma escolha comum para o filtro local G_i é dada por um modelo linear autoregressivo (AR). Neste caso, a estimativa devida ao neurônio i para o valor corrente da série temporal é dada por

$$\hat{x}_i(t) = \mathbf{w}_i^T(t)\mathbf{x}^-(t) = \sum_{j=1}^{n} w_{ij}(t)x^-(t-j) \tag{15}$$

em que $\mathbf{w}_i(t) = [w_{1i}(t)\ w_{2i}\ \cdots\ w_{pi}]^T$ é o vetor de coeficientes (pesos) associado ao neurônio i. O neurônio vencedor $i^*(t)$ é o que provê a melhor estimativa para $x(t)$. Em outras palavras, o neurônio vencedor no instante t é aquele com o menor valor absoluto para o erro de predição

$$i^*(t) = \arg\min_{\forall i}\{|x(t) - \hat{x}_i(t)|\} = \arg\min_{\forall i}\{|e_i(t)|\} \tag{16}$$

em que $|u|$ denota o valor absoluto para o escalar u. A quantidade $e_{i^*}(t) = x(t) - \hat{x}_{i^*}(t)$ é o erro de predição associado ao neurônio vencedor. A regra de atualização do neurônio i é uma equação similar à equação de algoritmos LMS, levemente modificada para incluir uma função vizinhança:

$$\mathbf{w}_i(t+1) = \mathbf{w}_i(t) + \eta(t)h(i^*, i; t)e_i(t)\mathbf{x}(t) \tag{17}$$

$$= \mathbf{w}_i(t) + \eta(t)h(i^*, i; t)[x(t) - \hat{x}_i(t)]\mathbf{x}(t) \tag{18}$$

tal que $h_{i^*,i}(t)$ é a função vizinhança como definido em Eq. (4). Uma rede OPM treinada com sucesso deve ajustar-se a Q modelos autoregressivos locais para uma dada série não-estacionária. Note-se que uma rede OPM com um único neurônio (i.e. $Q = 1$) é equivalente a um filtro adaptativo linear AR.

3.1 Detecção de Anomalias com Rede OPM

Para utilizar a rede OPM para detecção de anomalias, torna-se necessário definir um intervalo de decisão $[\tau^-, \tau^+]$. O cálculo dos limiares inferior e superior deste intervalo segue a mesma lógica da técnica apresentada na Seção 2.4, exceto pelo fato de que agora utilizam-se os erros de predição dos neurônios vencedores:

- **Limite Inferior** (τ^-): Este é o $100\frac{\alpha}{2}$ percentil da distribuição dos erros de predição $\{e_{i^*}(t)\}$.
- **Limite Superior** (τ^+): Este é o $100(1-\frac{\alpha}{2})$ percentil da distribuição dos erros de predição $\{e_{i^*}(t)\}$.

A regra de decisão para o método proposto pode ser escrito na seguinte forma:

$$\begin{array}{rl} \text{SE} & e_{i^*}(t) \in [\tau^-,\ \tau^+], \\ \text{ENTÃO} & x(t) \text{ é } \mathbf{NORMAL} \\ \text{SENÃO} & x(t) \text{ é } \mathbf{ANORMAL} \end{array} \tag{19}$$

4 Simulações

A viabilidade do método proposto é avaliada utilizando-se sinais de entrada derivados de quatro sistemas dinâmicos distintos, sendo três deles realizações de sistemas caóticos. O primeiro é composto da componente x das equações de Lorenz

$$\dot{x} = \sigma_L(y - x),\ \dot{y} = x(\alpha_L - z) - y,\ \dot{z} = xy - \epsilon_L z, \tag{20}$$

a qual exibe dinâmica caótica para $\sigma_L = 10$, $\alpha_L = 28$ e $\epsilon_L = 8/3$. O segundo e terceiro casos são derivados da série Mackey-Glass com diferentes atrasos τ:

$$\dot{x} = Rx(t) + P\frac{x(t-\tau)}{(1 + x(t-\tau)^{10})}, \tag{21}$$

com $P = 0{,}2$, R = -0,1 e $\tau = 17$ ou $\tau = 35$. O quarto caso é um processo linear autoregressivo de segunda ordem - $AR(2)$:

$$x(n+1) = 1,9x(n-1) - 0,99x(n-2) + n(t), \tag{22}$$

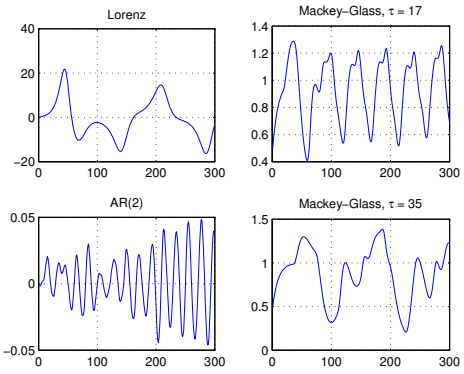

Figura 1: Amostras das séries temporais usadas na avaliação dos modelos.

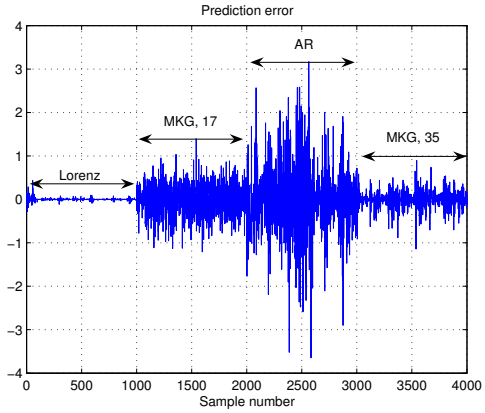

Figura 2: Erro de predição $e_{i^*}(t)$.

em que $n(t)$ é uma amostra de um processo ruído branco gaussiano com média nula e variância $\sigma_n = 10^{-3}$. A Figura 1 mostra 300 amostras de cada sinal.

O experimento de detecção de novidades foi projetado de modo a realizar a detecção de novidades *on-line* em um sinal anômalo, após treinar as redes com uma seqüência considerada normal. Este papel ficou associado à série de Lorenz, deixando as séries Mackey-Glass e o processo AR como representantes do comportamento anormal. Apenas para clareza da apresentação dos resultados, mostram-se as diferentes séries de teste em forma seqüencial: um conjunto de k amostras de cada série é usada como entrada para as quatro redes, seguida de k da próxima série, e assim por diante. A Figura 2 mostra os erros de predição $e_{i^*}(t)$ coletados do neurônio vencedor i^* para a rede OPM, quando as primeiras $k = 1000$ amostras consistem da série de Lorenz. É possível perceber (i) o relativamente baixo erro de predição para as primeiras k amostras, mostrando a capacidade de produção de um modelo global Eq. 13 a partir de modelos locais dados pelos G_{i^*}; e (ii) quando um padrão diferente é apresentado, o erro de predição é maior. Antes de aplicar a metodologia descrita na Seção 3, é ilustrativo observar a função distribuição cumulativa (CDF) dos erros de predição para a rede OPM. A Figura 3 mostra as CDFs para os erros $e_{i^*}(t)$ obtidos para as diferentes seqüências de teste, em que é possível verificar que o comportamento anormal resulta em distribuições com maior variância. Uma análise comparativa da performance das redes OPM, SOM, Kangas e Fuzzy-ART pode ser feira de maneira simples utilizando-se as estatísticas das percentagens de verdadeiros positivos e falsos positivos. Aqui, um verdadeiro positivo é a ocorrência de uma amostra $x(t)$ com valor anormal, quando o sinal de teste pertence a um padrão Mackey-Glass ou a um processo AR, e um falso positivo quando uma detecção incorreta ocorre na apresentação de uma amostra correspondente à série de Lorenz. O ponto com coordenadas (FP,TP) é um ponto no espaço ROC *Receiver Operating Characteristic*, utilizado pata identificar de maneira visual bons e maus classificadores. Por exemplo, um classificador binário perfeito deve ter as coordenadas (0,1). Agora, se alterarmos o percentil N_α, usado, o intervalo de decisão $[\tau^-,\ \tau^+]$ também é alterado, e consegue-se um conjunto de pontos no plano ROC, permitindo avaliar o desempenho dos detectores de novidade sob diferentes graus de tolerância para o erro de predição. Adicionalmente, diferentes configurações para os sinais de entrada e das redes foram utilizados, consistindo de variações em parâmetros gerais, tais como o tamanho da janela p, a variância de ruído σ_ε^2, o número de neurônios Q, além de variações em parâmetros específicos das redes, tais como o parâmetro de vigilância ρ e β da rede Fuzzy-ART, e o parâmetro λ da rede Kangas. A Figura 4 mostra um resultado típico do desempenho das redes, obtido para $Q = 40$ neurônios e uma janela de tamanho $p = 30$. Para o conjunto de dados usado neste trabalho, o melhor desempenho foi alcançado pelo modelo OPM, seguido de perto pelo modelo de Kangas e pela rede Fuzzy-ART. É interessante notar como a simples filtragem definida pela Eq. (5) resulta na grande diferença observada entre a rede Kangas e a rede SOM tradicional. A rede Fuzzy-ART também teve desempenho similar às redes OPM e Kangas, mesmo sem ter uma estrutura explícita para processar séries temporais. Seu bom desempenho pode ser explicado pelo fato de seu algoritmo consistir de um procedimento inerente à detecção de novidades, dado

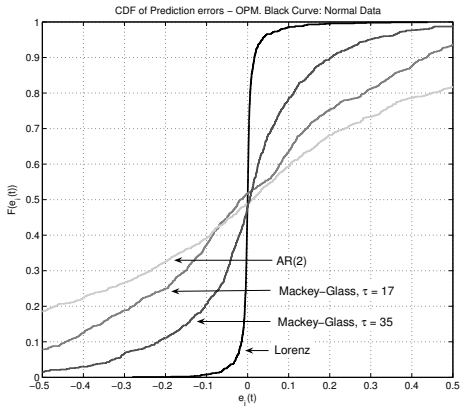

Figura 3: Distribuições cumulativas para os erros de predição.

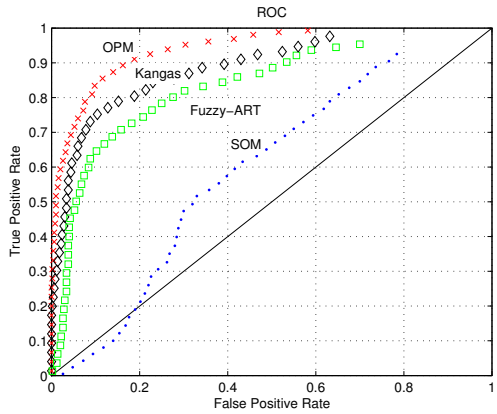

Figura 4: Curvas ROC para as redes avaliadas.

pela métrica de dissimilaridade dada pela Eq. (9). Finalmente, o método proposto aparece como um candidato viável à detecção de novidades, usando a metodologia definida na Seção 2.4. O algoritmo adaptativo e a estrutura de conexões permite a interpretação da rede OPM como um banco de Q filtros adaptativos, cujos pesos são ajustados para realizar a melhor aproximação local de sinal de entrada.

5 Conclusões

Neste trabalho, propôs-se um novo modelo de detecção de anomalias, baseado na arquitetura da rede OPM, uma generalização da rede SOM cujos neurônios podem ser vistos como filtros para padrões dinâmicos. A abordagem proposta utiliza o modelo OPM para criar filtros adaptativos locais para uma dada série não-estacionária, dos quais derivam-se intervalos de confiança não-paramétricos advindos dos erros de predição dos neurônios vencedores. Comparou-se a estratégia com outras arquiteturas conhecidas, tais como a rede SOM e a rede Fuzzy-ART. Trabalhos futuros envolvem o emprego de outras regras de atualização dos pesos na rede OPM, assim como a implementação adaptativa dos percentis α.

Agradecimentos: Os autores agradecem à CAPES/PRODOC pelo apoio financeiro.

Referências

Alhoniemi, E., Hollmén, J., Simula, O. & Vesanto, J. (1999). Process monitoring and modeling using the self-organizing map, *Integrated Computer Aided Engineering* **6**(1): 3–14.

Barreto, G. A. & Araújo, A. F. R. (2001). Time in self-organizing maps: An overview of models, *International Journal of Computer Research* **10**(2): 139–179.

Barreto, G. A., Mota, J. C. M., Souza, L. G. M., Frota, R. A. & Aguayo, L. (2005). Condition monitoring of 3G cellular networks through competitive neural models, *IEEE Transactions on Neural Networks* **16**(5): 1064–1075.

Carpenter, G. A., Grossberg, S. & Rosen, D. B. (1991). Fuzzy ART: Fast stable learning and categorization of analog patterns by an adaptive resonance system, *Neural Networks* **4**(6): 759–771.

Fancourt, C. L. & Principe, J. C. (2004). On the use of neural networks in the generalized likelihood ratio test for detecting abrupt changes in signals, *Proceedings of the 2000 IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN'00)*, Vol. 3, pp. 243–248.

Fu, T. C., Chung, F. L., Ng, V. & Luk, R. (2001). Pattern discovery from stock time series using self-organizing maps, *Workshop Notes of KDD2001 Workshop on Temporal Data Mining*, pp. 27–37.

Hodge, V. J. & Austin, J. (2004). A survey of outlier detection methodologies, *Artificial Intelligence Review* **22**(2): 85–126.

Jamsa-Jounela, S. L., Vermasvuori, M., Enden, P. & Haavisto, S. (2003). A process monitoring system based on the kohonen self-organizing maps, *Control Engineering Practice* **11**(1): 83–92.

Kangas, J. A., Kohonen, T. K. & Laaksonen, J. (1990). Variants of self-organizing maps, *IEEE Transactions on Neural Networks* **1**(1): 93–99.

Lampinen, J. & Oja, E. (1989). Self-organizing maps for spatial and temporal AR models, *Proceedings of the 6th Scandinavian Conference on Image Analysis (SCIA'89)*, Helsinki, Finland, pp. 120–127.

Lee, H.-J. & Cho, S. (2005). SOM-based novelty detection using novel data, *Lecture Notes on Computer Science* **3578**: 359–366.

Liao, T. W. (2005). Clustering of time series data - a survey, *Pattern Recognition* **38**(11): 1857–1874.

Markou, M. & Singh, S. (2003a). Novelty detection: a review - part 1: Statistical approaches, *Signal Processing* **83**: 2481–2497.

Markou, M. & Singh, S. (2003b). Novelty detection: A review - part 2: Neural network based approaches, *Signal Processing* **83**: 2499–2521.

Sarasamma, S. T. & Zhu, Q. A. (2006). Min-max hyperellipsoidal clustering for anomaly detection in network security, *IEEE Transactions on Systems, Man and Cybernetics* **B-36**(4): 887–901.

Singh, S. & Markou, M. (2004). An approach to novelty detection applied to the classification of image regions, *IEEE Transactions on Knowledge and Data Engineering* **16**(4): 1041–4347.

Wong, M., Jack, L. & Nandi, A. (2006). Modified self-organising map for automated novelty detection applied to vibration signal monitoring, *Mechanical Systems and Signal Processing* **20**(3): 593–610.

Zorriassatine, F., Al-Habaibeh, A., Parkin, R., Jackson, M. & Coy, J. (2005). Novelty detection for practical pattern recognition in condition monitoring of multivariate processes: a case study, *International Journal of Advanced Manufacturing Technology* **25**(9-10): 954–963.