DETECÇÃO DE ANOMALIAS EM FLUXOS DE REDES DE COMPUTADORES UTILIZANDO TÉCNICAS DE REDES NEURAIS E ESTIMADORES LINEARES

José Barbosa da Silva Filho

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia de Sistemas e Computação.

Orientador: Luís Felipe Magalhães de Moraes

Rio de Janeiro
Setembro de 2015

DETECÇÃO DE ANOMALIAS EM FLUXOS DE REDES DE COMPUTADORES UTILIZANDO TÉCNICAS DE REDES NEURAIS E ESTIMADORES LINEARES

José Barbosa da Silva Filho

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE) DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Examinada por:

Prof. Luís Felipe Magalhães de Moraes, Ph.D.

Prof. Claudio Luís de Amorim, Ph.D.

Prof. Márcio Portes de Albuquerque, D.Sc.

RIO DE JANEIRO, RJ – BRASIL
SETEMBRO DE 2015

Silva Filho, José Barbosa da

Detecção de Anomalias em Fluxos de Redes de Computadores Utilizando Técnicas de Redes Neurais e Estimadores Lineares/José Barbosa da Silva Filho. – Rio de Janeiro: UFRJ/COPPE, 2015.

XIV, 58 p.: il.; 29, 7cm.

Orientador: Luís Felipe Magalhães de Moraes

Dissertação (mestrado) – UFRJ/COPPE/Programa de Engenharia de Sistemas e Computação, 2015.

Referências Bibliográficas: p. 47 – 51.

1. Redes de Computadores. 2. Anomalias. 3. Inteligência Artificial. 4. Rede Neural. 5. Estimador Linear. I. Moraes, Luís Felipe Magalhães de. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia de Sistemas e Computação. III. Título.

A Deus e a minha Família
dedico o fruto de todas estas
horas de estudo e trabalho.

Agradecimentos

Agradecer deveria ser a ação mais realizada pelo homem, ao almejar atingir a sabedoria. Sendo assim não poderia esquecer de todos que contribuíram com este trabalho. Agradeço aos amigos Marcos Coutinho, Renato Silva e Renato Cerceau que dividiram preciosas horas de suas vidas, nos estudos, nas alegrias e que nos motivaram por toda esta jornada. E com grande apreço, aos companheiros de certezas e incertezas, Evandro Macedo e Vander Proença pelo inestimável apoio na *última milha corrida*.

Aos mestres que mostraram o caminho... Em especial ao professor Luís Felipe Magalhães de Moraes pelos ensinamentos e dedicada orientação; aos professores Luís Alfredo Vidal de Carvalho e Roberto Kopp pelos exemplos e apoio. Ao professor Márcio Portes de Albuquerque, pela sua dedicação, pacientes conselhos e muitas horas investidas na orientação final deste trabalho. Ao querido professor Ricardo Rhomberg Martins por ser mais que um professor, por ser mais que um amigo, ser a voz firme da oração no momento certo, aquele que sempre acreditou mesmo quando eu tive alguma dúvida em viver *o sonho*.

Sonhar... A faculdade de sonhar é inerente ao ser humano, reflexo e imagem da capacidade criadora de Deus. Viver o sonho, torná-lo real e concreto exige, porém, o trabalho árduo, dedicação e a humildade reconhecer suas limitações. Virtudes de caráter que foram aprendidas com meus pais José e Maria da Guia, com seus exemplos de vida. Ela, a mãe que soube me ensinar o valor do aprendizado desde meu primeiro lápis. Ele, o pai que foi o suporte durante tantos anos e ainda hoje seus exemplos de virtudes são meu *Norte* nos momentos de dúvidas e dificuldades...

Somadas ao apoio de minha esposa Eliana, que soube compreender as horas insones, as incertezas, as madrugadas e os fins de semana investidos nas simulações, códigos e cálculos... E que neste mar revolto de tensões que vivi, ainda me presenteou com a nossa pequena Sarah Marina...

Sarah, alegria de minha vida, seu sorriso de criança e amor incondicional, deram-me as forças para superar as dificuldades e relembrar a alegria de aprender.

DEUS, agradeço cada minuto a força e orientação que me deste através das vozes destes muitos mestres que estiveram em meu caminho. Sem ti, realização alguma teria sentido, trabalho algum teria mérito.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

DETECÇÃO DE ANOMALIAS EM FLUXOS DE REDES DE COMPUTADORES UTILIZANDO TÉCNICAS DE REDES NEURAIS E ESTIMADORES LINEARES

José Barbosa da Silva Filho

Setembro/2015

Orientador: Luís Felipe Magalhães de Moraes

Programa: Engenharia de Sistemas e Computação

Nesta dissertação, apresenta-se uma proposta de metodologia para a identificação de anomalias em fluxos de redes de computadores, com o uso de redes neurais artificiais (*Perceptron*) e estimadores lineares. A metodologia proposta foi verificada em uma rede de computadores real, a Rede-Rio de Computadores, a qual tem seu tráfego coletado e particionado em cinco séries discretas, utilizadas como base para métricas que definam, em conjunto, uma assinatura matemática em condições de normalidade. Os resultados são analisados e discutidos, sendo avaliada a efetividade real da metodologia proposta na identificação de anomalias simuladas, do tipo ciberataque. Por fim, como contribuição relevante, tem-se como legado o protótipo da ferramenta de monitoramento *on-line* de anomalias na Rede-Rio de Computadores, denominado **Anomalia RNA-Perceptron**, pelo Laboratório de Redes de Alta Velocidade - RAVEL do COPPE/UFRJ.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

ANOMALY DETECTION IN COMPUTER NETWORKS FLOWS USING TECHNIQUES OF NEURAL NETWORKS AND LINEAR ESTIMATORS

José Barbosa da Silva Filho

September/2015

Advisor: Luís Felipe Magalhães de Moraes

Department: Systems Engineering and Computer Science

In this dissertation, we have proposed a methodology for identifying anomalies in streams of computer networks, using artificial neural networks (Perceptron) and linear estimators. This Methodology is applied in an experimental laboratory, a real case of study: the Rede-Rio Computer Network; which has its traffic collected and is partitioned into five discrete series, used as basis for evaluation metrics that define a mathematical signature of normalcy. The results are analyzed and discussed as the proposed methodology actual effectiveness metric for identifying simulated anomalies, the type cyberattack. Finally, as relief contribution, we have a legacy prototype of the online anomalies monitoring tool, **Anomalia RNA-Perceptron**, applied to the Rede-Rio Computer Network monitoring by High Speed Networks Laboratory - RAVEL at COPPE/UFRJ.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

$\hat{y}_k$	Valor estimado de y no instante k, p. 9
$\langle \varepsilon_r \rangle$	Erro relativo médio, p. 10
ε	Erro de estimação, p. 10
$\varepsilon_n(k)$	Erro erro normalizado em y_k no instante k, p. 10
$\varepsilon_r(k)$	Erro relativo no instante k, p. 10
s	Desvio Padrão Amostral, p. 10
s^2	Variância Amostral, p. 10
w_i	Coeficiente do Estimador Linear, p. 9

Lista de Siglas

ANSI	American National Standards Institute, p. 39
ARMA	Modelo Autorregressivo com Médias Móveis, p. 44
ARX	Modelo Autorregressivo com Entradas Exógenas, p. 7
AR	Autorregressivo, p. 7
FAPERJ	Fundação de Amparo a Pesquisa do Rio de Janeiro, p. 2
IANA	*Internet Assigned Numbers Authority*, p. 11
IA	Inteligência Artificial, p. 37
IHM	Interface Homem-Máquina, p. 38
MATLAB	MATrix LABoratory, p. 13
PESC	Programa de Engenharia de Sistemas e Computação, p. 2
RAVEL	Redes de Alta Velocidade, p. 2
RFC	*Request for Comments*, p. 11
RNA	Rede Neural Artificial, p. 7
SISO	Entrada Simples (*Single Input*), Saída Simples (*Single Output*), p. 14
SMS	*Short Message System*, p. 38
ST	Série Temporal, p. 37

Capítulo 1

Introdução

Com a evolução acentuada das soluções de comunicação e arquitetura na área de redes de computadores, em parte devido ao crescimento e importância comercial da INTERNET, há um natural aumento da probabilidade de falhas sistêmicas e do crescimento exponencial das atividades maliciosas. Assim, com o objetivo do controle e administração do uso dos recursos compartilhados, faz-se necessária uma atividade de monitoramento eficaz das redes de computadores.

O monitoramento de um sistema, em sua essência, visa a identificação de desvios na operação normal deste e, se possível, definir o agente ou causa de tal desvio, possibilitando assim sua classificação e atuação corretiva posterior. A este desvio do padrão de operação normal se denomina anomalia do sistema, ou anomalia sistêmica. Logo, uma anomalia é caracterizada quando temos o desvio do comportamento padrão histórico de um conjunto de variáveis observáveis do sistema [NG (2006)].

No contexto de sistemas de redes de computadores, deseja-se que a atividade de monitoramento tenha especial foco na garantia da segurança da informação trocada, em termos de confiabilidade e sigilo. Também é importante que haja garantia da disponibilidade dos meios, antecipando incidentes de forma pró-ativa, gerando condições de minimizar os impactos nocivos destes incidentes no regime normal de trabalho em uma rede de computadores.

Nesta esfera, há um grupo em especial de anomalias, os ciberataques[1] (objeto do presente estudo), que possuem relação com as tentativas de ataque malicioso, a exemplo das definidas nos trabalhos de [DENNING (1987)] e [KRUEGEL e VIGNA (2003)].

[1]ciberataque: roubo de recursos/informações e/ou intrusão no sistema de rede causando prejuízos a operação.

Nos últimos cinco anos, a mídia tem registrado diversas ocorrências que podem ilustrar os prejuízos econômicos da interrupção, mesmo que parcial, dos serviços oferecidos em rede. Temos como exemplo o falha sistêmica descrita no artigo **O apagão de internet e telefonia causa transtornos na Região Sul** [LOPES *et al.* (2012)], fato ocorrido no Brasil em abril de 2012.

No plano mais específico de anomalias causadas com intenção maliciosa/criminosa, destaca-se o artigo **Hackers roubam mais de US$ 1 bilhão em ataques a bancos** [BBC-BRASIL (2015)]. No Brasil, ressalta-se o exemplo do recente ataque às prefeituras do Estado de São Paulo, apresentadas no artigo em hipermídia **Criminosos invadem sistema interno de computadores de prefeituras** [TAMURA *et al.* (2015)].

1.1 Motivação e Posicionamento do Trabalho

Ao longo das duas últimas décadas, diversos trabalhos na área de monitoramento e identificação de anomalias foram apresentados, em parte motivados pela importância econômica dos sistemas de rede de computadores na sociedade moderna.

Inicialmente, destaca-se a caracterização do tráfego da internet nas pesquisas de [CLAFFY (1994)], seguido pelos trabalhos de [BARFORD *et al.* (2002)], [ANDROULIDAKIS e PAPAVASSILOU (2008)], [HE *et al.* (2008)], [HONG *et al.* (2008)] e [ZHANI *et al.* (2008)] que propõem metodologias e modelos de solução para o problema de identificação de anomalias. Por fim, temos os trabalhos de [CELENK *et al.* (2010)], [GOGOI *et al.* (2011)] e [BARTOS *et al.* (2011)] que versam sobre a pesquisa, identificação, monitoramento e previsão de anomalias em fluxos de rede.

No contexto nacional, temos o trabalho de [ZARPELÃO (2010)], onde foi proposto um sistema de detecção de anomalias em redes de computadores baseado em três níveis de análise, somada as contribuições do Laboratório de Redes de Alta Velocidade (RAVEL[2]) da Universidade Federal do Rio de Janeiro, onde se destacam a pesquisa de [TÖPKE (2001)] sobre **Uma metodologia para caracterização de tráfego e medidas de desempenho em *Backbones IP***, o trabalho de [VILELA (2006)], o qual apresenta uma proposta de caracterizar o tráfego de uma

[2]O RAVEL integra o conjunto de Laboratórios de Pesquisa do Programa de Engenharia de Sistemas e Computação (PESC) do COPPE/UFRJ.

rede de computadores pela classificação de seus fluxos, e em especial a pesquisa de identificação visual de anomalias por uso de assinaturas [ABREU (2006)], onde o presente trabalho se propõe a expandir os horizontes, posicionando-se como uma técnica complementar a ser aplicada ao monitoramento da Rede-Rio de Computadores [REDERIO (2015)].

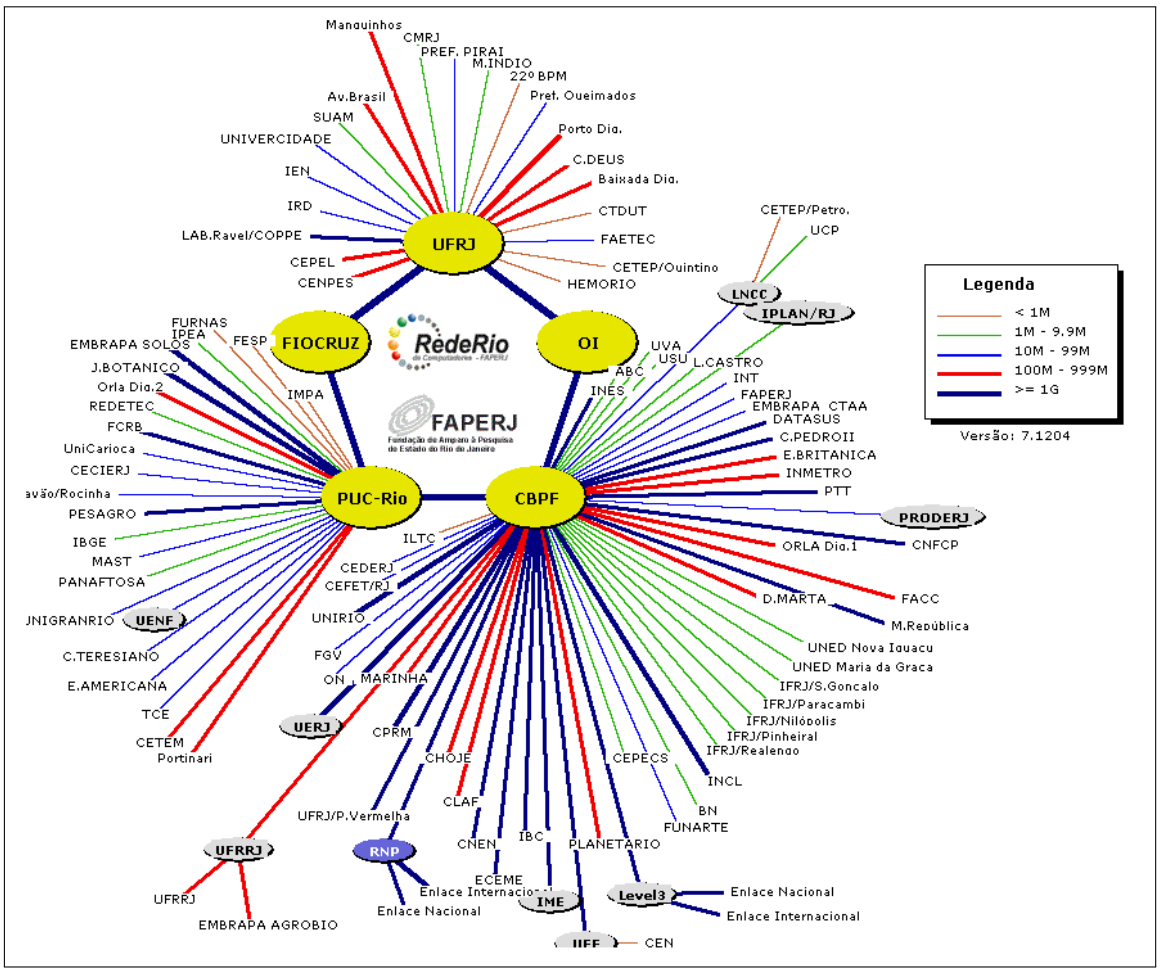

Figura 1.1: *Mapa Rede-Rio - Setembro de 2015* ([REDERIO (2015)])

1.2 Relevância e Objetivos

Apesar da significativa contribuição da solução de monitoramento visual de anomalias da Rede-Rio de Computadores, esta solução apresenta uma fragilidade a ser melhorada. As ações decorrentes do trabalho deste monitoramento são reativas e dependentes da avaliação e ação do operador de rede, ou seja, apesar da disponibilidade de grande quantidade de dados, ainda é necessária a supervisão humana constante para identificação de anomalias, as quais podem ocorrer em intervalos de tempo, nos quais não estejam sendo feitas observações pelo(s) gestor(es) da rede.

Faz-se desejada a criação de uma metodologia que permita o monitoramento e identificação semi-automatizados das anomalias, preferencialmente em intervalo de tempo real, isto sem gerar perturbações que possam comprometer o próprio processo de comunicação.

Definida, validada experimentalmente e convertida em ferramenta, esta metodologia poderá ser aplicada imediatamente no monitoramento da Rede-Rio de Computadores. Esta ferramenta contribuirá na identificação de anomalias em tempo real e permitira minimizar os impactos que a interrupção deste recurso gera no ambiente acadêmico.

Ressalta-se que esta ferramenta estará sujeita a duas diretrizes quase antagônicas: a alta eficiência na identificação/classificação e, tendo como contraponto, a necessidade de realizar esta tarefa em tempo hábil e com pouco consumo de processamento de máquina, evitando causar interferência no processo de comunicação.

No presente trabalho, a proposta primária é implementar o conjunto de ideias contido no artigo de [CELENK *et al.* (2010)], substituindo o método de detecção de anomalias original (avaliação da entropia em séries discretas, com o uso de estimadores ARMA e filtros digitais), por detecção utilizando redes neurais artificiais, configuradas como aproximadores de modelos autorregressivos de segunda ordem [AGUIRRE (2007)]; a partir da implementação de um protótipo de monitoramento de anomalias na Rede-Rio de Computadores com o método proposto, continuando a pesquisa proposta em [ABREU (2006)].

Propõe-se ainda:

- Estudar a modelagem matemática dos fluxos de dados em ambientes de rede Internet, referenciado nos trabalhos de [CLAFFY (1994)], [VILELA e DE MORAES (2005)] e [SANTOS (2009)];
- Apresentar e analisar os resultados obtidos na identificação de anomalias no fluxos de dados da Rede-Rio de Computadores;

1.3 Organização do Trabalho

Este trabalho foi estruturado em quatro capítulos, permitindo a leitura sequencial (recomendada) ou o acesso aos assuntos principais do estudo. Além deste capítulo de introdução temos:

No Capítulo 2, apresenta-se o resultado da pesquisa bibliográfica, compondo o referencial teórico e a metodologia aplicada para a hipótese do uso de redes neurais para identificação de sinais. O Capítulo 3 apresenta os resultados da identificação de anomalias, sua eficiência analisada e comparada ao trabalho similar de identificação de anomalias por séries temporais realizado no Laboratório RAVEL/UFRJ [(DA SILVA (2015)], bem como o protótipo construído e em pleno uso para a Rede-Rio de Computadores, baseado na metodologia e resultados obtidos neste trabalho de pesquisa; o Capítulo 4 é reservado para considerações finais, conclusões e perspectivas de trabalhos futuros. No Apêndice A, encontra-se o Manual de Usuário do Sistema de Identificação e Alerta de Anomalias.

Capítulo 2

Método Proposto e sua Fundamentação Teórica

Durante o estudo e revisão bibliográfica, foram selecionados alguns candidatos a modelo de solução para o problema de identificação de anomalias em redes de computadores. Dentre os quais, destacam-se os apresentados nas pesquisas de [BARFORD *et al.* (2002)], [KRISHNAMURTHY *et al.* (2003)], [ANDROULIDAKIS e PAPAVASSILOU (2008)], [HE *et al.* (2008)], [HONG *et al.* (2008)], [ZHANI *et al.* (2008)], [BARTOS *et al.* (2011)] e [WENFANG e CHI (2012)]. No critério de escolha adotado se considerou, qualitativamente, os resultados apresentados pelos métodos na identificação de anomalias em sistemas de comunicação de dados, ponderados pela facilidade de reprodução do método com os recursos disponíveis; bem como sua viabilidade de implementação prática.

Assim, os modelos de solução que se apresentaram como candidatos viáveis foram classificados em **Aprendizagem de Máquina** (Redes Neurais Artificiais e Redes Neurais Sem Peso) e **Análise de Sinais** (Séries Temporais com uso de estimadores), segundo a taxonomia de [GARCÍA-TEODORO *et al.* (2009)].

Como forma de avaliar as melhores ferramentas, e a sua possível ação combinada, definiu-se como metodologia de trabalho o ensaio de laboratório, onde se destacam a prototipação e análise dos resultados obtidos de forma experimental.

Durante a avaliação das técnicas, foram realizados alguns ensaios com o uso de uma rede neural sem peso do tipo *WISARD*, como definida em [ALEKSANDER *et al.* (1984)], aplicadas em conjunto com a ferramenta de identificação de anomalias no fluxo normal de dados da Rede-Rio de Computadores, produto do trabalho [ABREU (2006)]; tornando-se esta a primeira versão de ferramenta para uso na identificação de anomalias por inteligência artificial. Estes ensaios permitiram avaliar

a ferramenta, qualitativamente e quantitativamente, indicando como pontos positivos: a sua simplicidade de implantação e baixo custo computacional; e como ponto negativo que a metodologia por rede sem peso tem grande dependência da definição humana dos exemplos de normalidade (fase de treinamento).

Nestas condições de contorno, a técnica de rede neural sem peso não apresentou a robustez desejada às variações de assinaturas maliciosas diferentes das tratadas pela pesquisa de [ABREU (2006)], sendo abandonada em favor das Redes Neurais Artificiais com Peso.

2.1 Método Proposto

O técnica de identificação de anomalias utilizado neste trabalho é baseada na metodologia proposta na pesquisa [CELENK *et al.* (2010)], onde os autores utilizaram na detecção de anomalias estimadores ARMA, combinados à filtros digitais sobre a entropia de séries discretas, obtidas com base no tráfego de uma rede de computadores.

Propõe-se utilizar a mesma metodologia do artigo, até modelo de entrada de dados, substituindo a fase de detecção de anomalias dos autores pela previsão através de uma RNA-Perceptron (sem aplicação de filtros digitais). E a partir daí, avaliar o comportamento do erro de estimação relativo como métrica de identificação de anomalias.

2.1.1 Identificação por RNA-Perceptron

Nesta identificação por RNA-Perceptron, para efeitos de modelagem matemática, supõem-se que o tráfego e fluxos são aproximados a sinais discretos no domínio do tempo, os quais guardam relação e podem ser representados por **processos estocásticos estacionários em sentido amplo**, como na metodologia do artigo [CELENK *et al.* (2010)].

Premissas adotadas:

1. Os fluxos referentes aos dados em redes de computadores podem ser descritos como processos estocásticos;

2. O tráfego em canais de dados pode ser definido como resultado da soma de fluxos de dados agregados nos respectivos canais;

3. O tráfego e seus fluxos componentes, podem ser representados (parametrizados) em função do tempo contínuo ou discreto;

Neste contexto, o tráfego e qualquer composição de fluxos oriunda deste, podem ser estimados pelo modelo autorregressivo (AR[1]) e suas variantes, como definidos e estudados nos trabalhos [SCALASSARA (2005)], [AGUIRRE (2007)], [CELENK *et al.* (2010)] e [MACEDO (2015)] e admitem sua previsão e estudo por estimadores lineares discretos, a exemplo do **Estimador Discreto de Segunda Ordem** proposto em [LATHI (1998)].

Na abordagem do presente trabalho, será utilizado o modelo Perceptron de McCulloch-Pitts [MINSKY e PAPERT (1969)], que pode ser visualizado na Figura 2.1, convenientemente configurado como um estimador linear de segunda ordem:

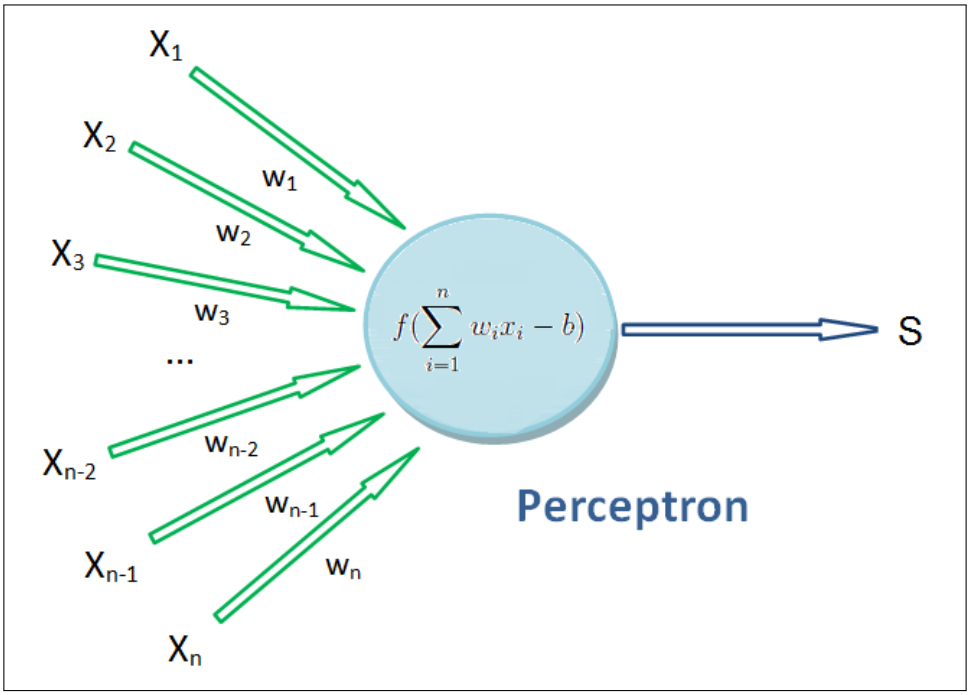

Figura 2.1: *Modelo Perceptron*

$$S = f(net) = f(\sum_{i=1}^{n} w_i x_i - b) \tag{2.1}$$

[1]AR: simplificação do modelo autorregressivo com entradas exógenas (ARX), onde não se consideram ruídos.

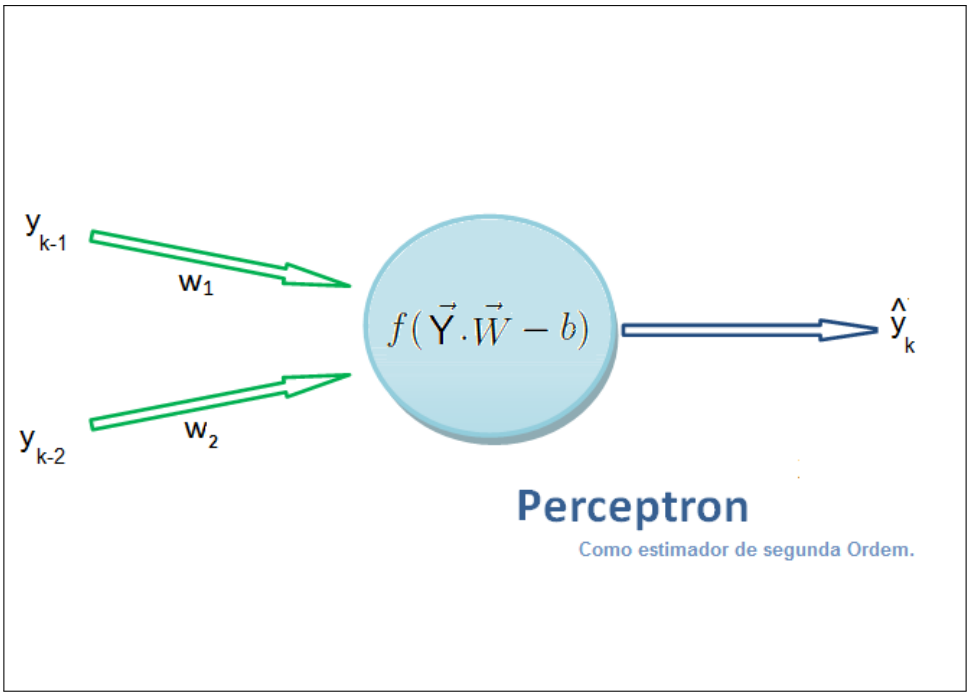

Figura 2.2: *Modelo Perceptron como estimador*

Por hipótese, no modelo do presente trabalho (Figura 2.2), tem-se:

- o vetor b, ou bias do sistema, inicializado como um vetor nulo;
- a função de ativação do perceptron será linear (*PureLin*).
- as entradas serão limitadas a duas, sendo o valor da série no instante k avaliado a partir as condições iniciais definidas pelos instantes $k-1$ e $k-2$;

Desta forma, o perceptron é modelado como um somador linear, onde w_i são os pesos da suas entradas:

$$\hat{y}_k = w_1 y_{k-1} + w_2 y_{k-2} \tag{2.2}$$

2.1.2 Métricas de Identificação

Identificado o modelo de comportamento da série discreta, pode-se estimar valores desta para qualquer instante de tempo futuro (com a restrição de $k \geq 2$), pois serão conhecidos os coeficientes da Equação do estimador linear (Equação 2.2), tornando-se a previsão apenas a solução numérica deste estimador no intervalo considerado. Este modelo se aproxima da série discreta real com uma margem de erro.

Para avaliar quantitativamente e qualitativamente este erro é importante estabelecer métricas, que serão utilizadas para determinar a eficiência do método na identificação das anomalias.

A primeira métrica de avaliação definida é o erro no instante observado (ε_k). Com ele, pode-se comparar o resultado estimado ($\hat{y_k}$), obtido a partir do modelo, com o dado real da série (y_k), para o instante k. É importante notar que o estimador do presente trabalho é definido como de segunda ordem, ou seja, apresenta a restrição de $k \geq 2$, logo $k \in \{2, 3, 4, ..., \infty\}$:

$$\varepsilon_k = \hat{y_k} - y_k \tag{2.3}$$

A partir deste, define-se o erro normalizado em y_k no instante k:

$$\varepsilon_n(k) = \frac{\hat{y_k} - y_k}{y_k} \tag{2.4}$$

E o erro relativo no instante k:

$$\varepsilon_r(k) = \left| \left(\frac{\hat{y_k} - y_k}{y_k} \right) \right| \tag{2.5}$$

Obtém-se o erro relativo médio ($\langle \varepsilon_r \rangle$) com base na Equação 2.6, sendo este definido para o intervalo de análise de cinco dias (ou 1440 amostras de cinco minutos de granularidade). Propõe-se este intervalo de avaliação a partir dos resultados de sazonalidade da pesquisa de [MACEDO (2015)].

$$\langle \varepsilon_r \rangle = \frac{1}{1440} \sum_{k=1}^{1440} \left| \left(\frac{\hat{y_k} - y_k}{y_k} \right) \right| \tag{2.6}$$

Define-se o desvio padrão amostral (s) do erro relativo médio, avaliado para o intervalo de cinco dias (ou 1440 amostras de cinco minutos de granularidade), como:

$$s = \sqrt{\frac{1}{1440} \sum_{k=1}^{1440} (\varepsilon_r(k) - \langle \varepsilon_r \rangle)^2} \tag{2.7}$$

E por extensão a variância amostral do erro relativo médio como s^2.

2.2 Identificação do Modelo

2.2.1 Captura e Extração de Dados

De forma análoga a proposta contida no trabalho de [CELENK *et al.* (2010)], implementa-se através do pacote de ferramentas *NFDUMP - Netflow processing tools* [HAAG *et al.* (2015)] a captura dos fluxos de rede[2], os quais são disponibilizados em disco, pelo servidor de monitoramento *IPTRAF*, com um intervalo de cinco minutos entre amostras.

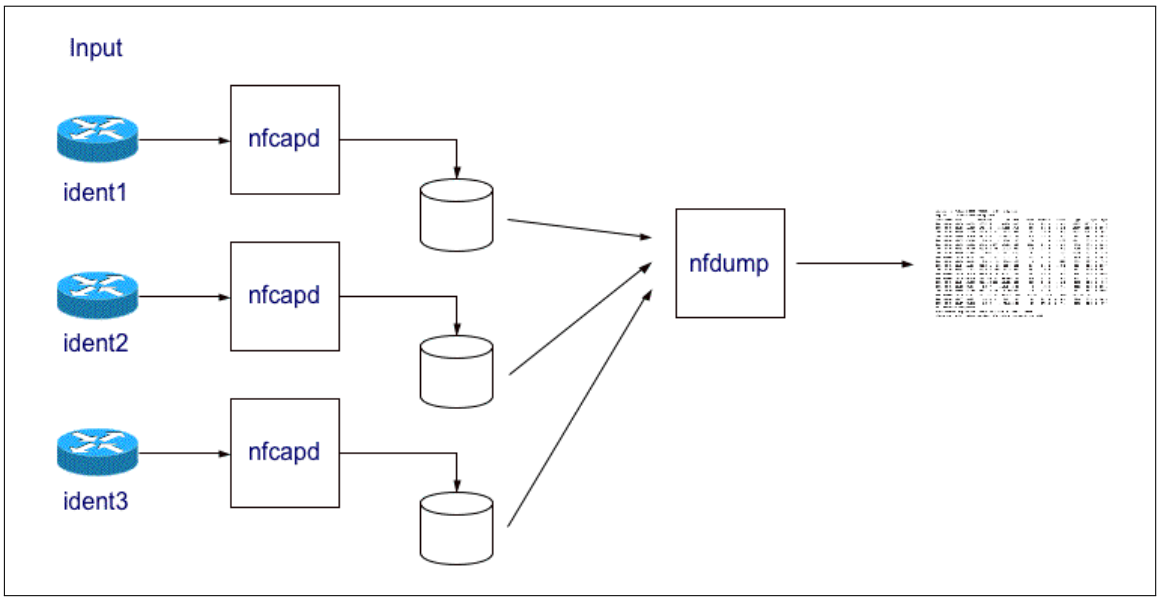

Figura 2.3: Estrutura do *Netflow* ([HAAG *et al.* (2015)])

O extrator de dados, escrito na linguagem C ANSI, foi implantado na plataforma de serviços do servidor IPTRAF. Sua função é totalizar a quantidade parcial de *bytes* trafegados pelas séries discretas, que compõem o conjunto de características avaliadas. Utiliza-se a classificação de portas da RFC6335 da IANA [COTTON *et al.* (2011)], para definir as séries discretas:

Tráfego (T_k):

É a principal série e define o Tráfego como a soma de todos os *bytes* indicados no *payload* dos fluxos no sentido origem para destino, no instante k, onde $k \in \{2, 3, .., N\}$;

[2]No estudo de caso, originados do roteador de borda da Rede-Rio de Computadores.

Média bytes/portas (M_k):

É definida como a soma de todos os *bytes* dividido pelo total de portas de origem, no fluxo. Sendo $BytesPorta_k(P)$ a quantidade de *bytes* na porta de origem **P**, no instante k, onde $k \in \{2, 3, .., N\}$. Definimos:

$$M_k = \frac{1}{(2^{16} - 1)} \sum_{P=1}^{(2^{16}-1)} BytesPorta_k(P)$$

Portas baixas (B_k):

É definida como soma de todos os *bytes* que tem origem em portas baixas (1-1023), no instante k, onde $k \in \{2, 3, .., N\}$;

Portas do servidor (S_k):

É definida como soma de todos os *bytes* que tem origem em portas de servidor (1024-49151), no instante k, onde $k \in \{2, 3, .., N\}$;

Portas dinâmicas (D_k):

É definida como a soma de todos os *bytes* que tem origem em portas dinâmicas (49152-65535), no instante k, onde $k \in \{2, 3, .., N\}$;

Onde **N** representa o tamanho do intervalo de amostras considerado.

Define-se o vetor de dados de entrada, $\overrightarrow{Y_k}$ que é obtido de acordo com a divisão dos fluxos das regiões de interesse (séries discretas) para a análise, sendo definido por:

$$\overrightarrow{Y_k} = \begin{bmatrix} T_k \\ M_k \\ B_k \\ S_k \\ D_k \end{bmatrix}$$

Nesta abordagem, é garantida a modularidade e robustez do método, permitindo lidar com o problema clássico do grande esforço computacional exigido nas análises deste tipo. Cada dimensão do vetor é avaliada por uma RNA-Perceptron independente e, se necessário de forma paralela. Isto resulta em aumento da velocidade de processamento e eficácia na identificação de anomalias. O primeiro resultado do aproveitamento das tecnologias de processamento concorrente e paralelo; e o segundo consequência do maior número de dimensões avaliadas simultaneamente.

2.2.2 Treinamento e Validação da RNA-Perceptron

Foi utilizado o período de coleta de dados entre 14 de junho de 2015 e 04 de agosto de 2015, onde o extrator de dados acumulou uma base histórica, composta pelas cinco séries temporais definidas anteriormente e que foram particionadas (individualmente) em três grupos sequenciais, de acordo com o proposto em [HAYKIN (1998)]:

Treinamento: São separados os primeiros 70% (setenta por cento) das amostras, para serem submetidos a RNA-Perceptron para seu treinamento.

Validação: São separados os 15% (quinze por cento) das amostras seguintes, para serem submetidos a RNA-Perceptron para sua validação.

Testes: São separados os últimos 15% (quinze por cento) das amostras, para serem submetidos a RNA-Perceptron para testes.

Para cada uma das séries temporais, individualmente particionadas, os dois primeiros grupos (validação e treinamento) são apresentados à respectiva RNA-Perceptron, implementada em MATLAB[3], como um perceptron de função de ativação linear, com o vetor de bias definido nulo e pesos inicialmente nulos. No treinamento, é utilizado o algoritmo denominado de **Propagação Reversa** (*Back-Propagation*, como definido em [B. WIDROW (1990)]).

No algoritmo de Propagação Reversa, a cada iteração, é calculado o erro entre o valor estimado e o valor de treinamento apresentado a rede neural artificial. Com base neste cálculo os pesos são reajustados seguindo a ordem da saída para entrada (de onde vem seu nome). O objetivo é tentar reduzir o valor do erro a um limiar mínimo, com os conjuntos de treinamento e validação. Ao fim do processo, espera-se que a rede acompanhe o comportamento da série apresentada.

Na forma definida no presente trabalho, a rede deverá conter em seus pesos neurais os valores estimados numericamente para os coeficientes ω_1 e ω_2 aplicáveis ao estimador discreto (Equação 2.2).

[3]O MATLAB é um conjunto de aplicativos destinado originalmente a realizar operações com matrizes. Foi criado por Cleve Moler no fim dos anos 1970, na Universidade do Novo México.

É importante ressaltar que:

- O grupo de testes foi reservado para avaliação e análise de eficiência da identificação com dados reais.

- Utiliza-se um perceptron por série discreta, sem interconexão entre os mesmos; ou seja, cada série é tratada como originária de sistema SISO independente e separado dos demais.

2.2.3 Análise Estatística

Com o uso da massa de testes (como definida na Seção 2.2.2), foram analisados os comportamentos de erro das séries discretas, com vistas a avaliar se existe algum padrão de comportamento, o que tornaria mais fácil o tratamento de dados e análise posterior. Um ponto importante para analise é caracterizar os intervalos de tempo utilizados:

Intervalo de Entrada: como foi adotado o estimador discreto autorregressivo de segunda ordem, exige-se duas amostras passadas (y_{k-1} e y_{k-2}) como parâmetros de avaliação, para estimar o valor atual da série ($\hat{y_k}$). Como a granularidade dos dados observados é de cinco minutos, define-se o intervalo de entrada de dados (valores passados) em dez minutos.

Intervalo de Análise: No trabalho de [MACEDO (2015)], verifica-se que o erro de identificação aumenta para a série do tráfego (T_k), conforme aumenta o lapso temporal entre intervalo de treinamento do modelo e o intervalo que é avaliado. De forma a minimizar este efeito, utiliza-se como limite de análise intervalos futuros de até cinco dias (ou 1440 amostras de cinco minutos de granularidade), permanecendo no limite superior de sazonalidade, ainda segundo o mesmo trabalho de pesquisa.

Por hipótese, espera-se que o erro relativo médio ($\langle \varepsilon_r \rangle$) venha a convergir em um valor constante (**Lei dos Grandes Números**), ou obedeça a alguma distribuição estatística previamente conhecida [LEON-GARCIA (1994)], quando observados em intervalos de análise suficientemente grandes.

Dentro deste contexto, e no intervalo de análise definido, por hipótese, será possível estimar o erro relativo do modelo no instante k ($\varepsilon_r(k)$), comparando-o ao grau máximo admissível de desvio do valor de sua média ($\langle \varepsilon_r \rangle$), na série avaliada. Caracteriza-se assim o comportamento de normalidade e, por exclusão, as anomalias (todo desvio que ultrapassar o limiar máximo arbitrado).

Capítulo 3

Resultados e Discussões

O presente capítulo está organizado em três seções. Na primeira apresenta-se os resultados obtidos nos testes realizados na Rede-Rio de Computadores (**Análise dos Dados da Rede-Rio**), durante o período compreendido entre o dia 14 de junho de 2015 e 04 de agosto de 2015.

Na segunda seção (**Análise Cross-Referenciada**), apresentam-se os resultados da análise e validação comparativa do método RNA-Perceptron com o trabalho de identificação de anomalias por séries temporais [DA SILVA (2015)], realizada para o período de 20 de julho de 2015 a 01 de agosto de 2015. E na última seção (**Ferramenta Anomalia RNA-Perceptron**), encontra-se o modelo conceitual do protótipo desenvolvido para monitoramento e identificação de anomalias na Rede-Rio de Computadores, bem o de exemplo de dois períodos atualizados de monitoramento (dia 13 de dezembro de 2015 às 23h 45min e dia 14 de dezembro de às 00h 20min).

Cabe ressaltar que as simulações foram conduzidas com o apoio computacional do software MATLAB versão 7.1, utilizado para análise e manipulação algébrica. Como plataforma um microcomputador com processador de 64 bits, AMD FX8100, 8 (oito) núcleos, 8 (oito) GB de Memória RAM, disco rígido de 1 (um) TB, com sistema operacional *WINDOWS 7*.

3.1 Análise dos Dados da Rede-Rio

De forma análoga ao modelo de divisão dos fluxos do tráfego, definido por [CELENK *et al.* (2010)], foram obtidas cinco séries temporais a partir dos fluxos capturados do Roteador de Borda da Rede-Rio de Computadores: **Tráfego (T_k)**, **Média bytes/portas (M_k)**, **Portas Baixas (B_k)**, **Portas Servidor (S_k)**, **Portas Dinâmicas (D_k)**. Estas séries foram submetidas individualmente a identificação pela RNA-Perceptron.

Após as fases de treinamento e validação (Seção 2.2.2), os coeficientes ω_1 e ω_2, são estimados de forma iterativa pelo algoritmo de **Propagação Reversa** (*Backpropagation*) [B. WIDROW (1990)]. A seguir, aplica-se os coeficientes estimados da série avaliada na Equação 2.2, determinando-se o modelo aproximado desta ($\hat{y}_k$).

Tabela 3.1: Séries identificadas na Rede-Rio de Computadores

Série Discreta	**Modelo Aproximado:** $\hat{y}_k$	$\langle \varepsilon_r \rangle$	s
Tráfego (T_k)	$0,8585y_{k-1} + 0,09793y_{k-2}$	0,002830	0,1093
Média (M_k)	$0,7813y_{k-1} + 0,1999y_{k-2}$	0,000432	0,0714
Portas Baixas (B_k)	$0,9417y_{k-1} + 0,01557y_{k-2}$	0,002294	0,1751
Portas Servidor (S_k)	$0,5131y_{k-1} + 0,3824y_{k-2}$	0,027906	0,6410
Portas Dinâmicas (D_k)	$0,6518y_{k-1} + 0,2847y_{k-2}$	0,011979	0,4190

Nas Seções 3.1.1 à 3.1.5, para cada série avaliada, apresenta-se as figuras de mérito (gráficos dos resultados):

- **Série Discreta:** é o resultado dos valores da série discreta em cinco dias escolhidos. Permite verificar se há uma similaridade periódica de comportamento;
- **Série Real (y_k) x Identificada ($\hat{y}_k$):** apresenta as curvas da série discreta real comparada à identificada pela RNA-Perceptron;
- **Histograma do Erro de Identificação Normalizado ($\varepsilon_n(k)$):** apresenta a distribuição do erro avaliado em intervalo de cinco dias;

Observa-se uma similaridade de comportamento com a distribuição normal em todos os histogramas de erro de identificação normalizado das séries (Figuras 3.3, 3.8, 3.13 ,3.18 e 3.23). Como resultado desta avaliação, propõe-se adotar o desvio padrão (Equação 2.7) como base de análise estatística do grau de anormalidade (anomalia) em um instante qualquer (k) sob avaliação.

Com esta proposição, define-se:

- **Grau de uma Anomalia:** como o número inteiro de desvios padrão (s), que o valor do módulo do erro relativo no instante k ($\varepsilon_r(k)$) se afasta de sua média histórica ($\langle\varepsilon_r\rangle$), isto na série avaliada. Adota-se a restrição, para fins de implementação computacional, que caso o número de desvios seja superior a três; este será arbitrado como três, de forma que o grau de anomalia pertença ao intervalo [0,3], onde zero é a normalidade;

E a partir desta nova métrica (Grau de uma Anomalia), define-se as figuras de mérito:

- **Normalidade x Anormalidade:** apresenta de forma sintética o percentual de amostras com algum grau de anomalia; comparadas ao percentual de amostras dentro da normalidade, no período de observação;
- **Graus de Anomalias:** apresenta de forma sintética a distribuição percentual do grau de anomalias; dentro da amostras consideradas anômalas;

3.1.1 Série Discreta: Tráfego (T_k)

Modelo Discreto Identificado:

$$y_k = 0,8585y_{k-1} + 0,09793y_{k-2}$$

Tabela 3.2: Série T_k: Pesos na RNA-Perceptron

Coeficiente	**Peso Neural**
ω_1	0,8585214451
ω_2	0,0979250898

Na Figura 3.1, tem-se o perfil da série em quatro dias distintos, na Figura 3.2, observa-se o perfil das série (y_k) comparada com o valor estimado pela RNA-Perceptron ($\hat{y_k}$), em um mesmo intervalo. A Figura 3.3 apresenta o histograma do erro normalizado da série (Equação 2.4), o qual permite avaliar o padrão de comportamento. E por fim, as Figuras 3.4 e 3.5 refletem a pesquisa de anomalias, na série considerada, no período compreendido entre dia 14 de junho de 2015 às 14h 40min e o dia 04 de agosto de 2015 às 13h 10min.

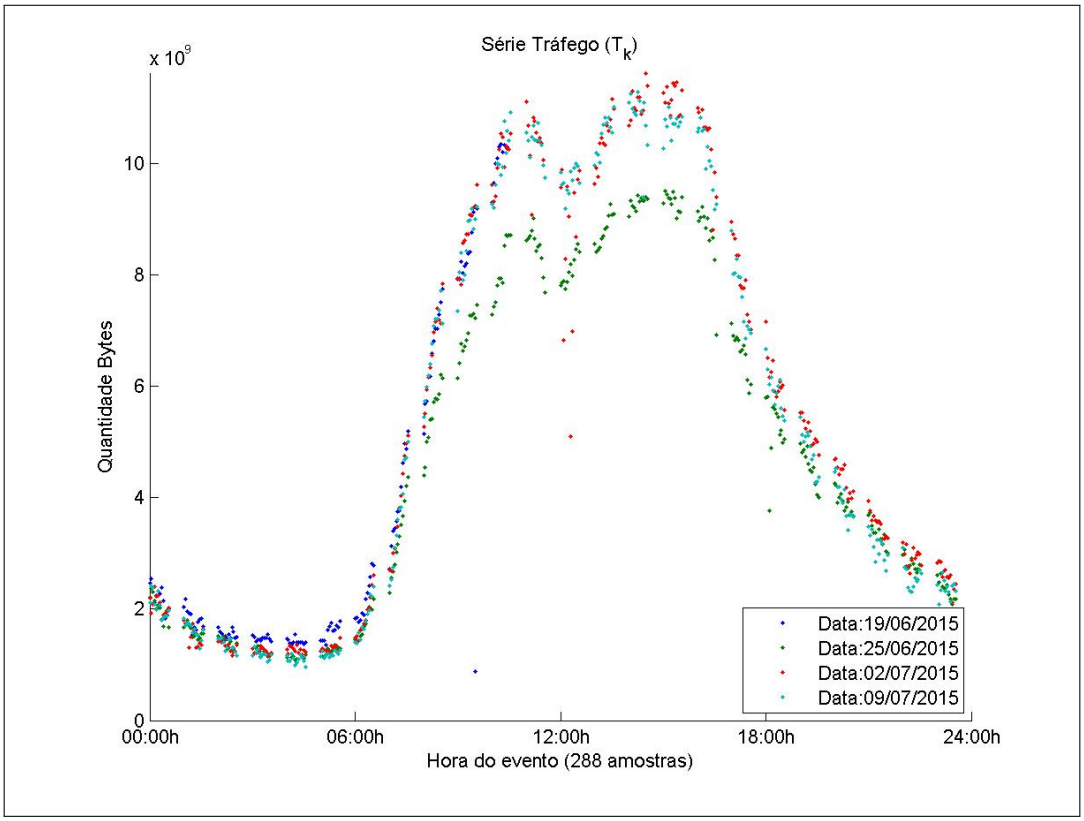

Figura 3.1: Série Discreta: Tráfego (T_k)

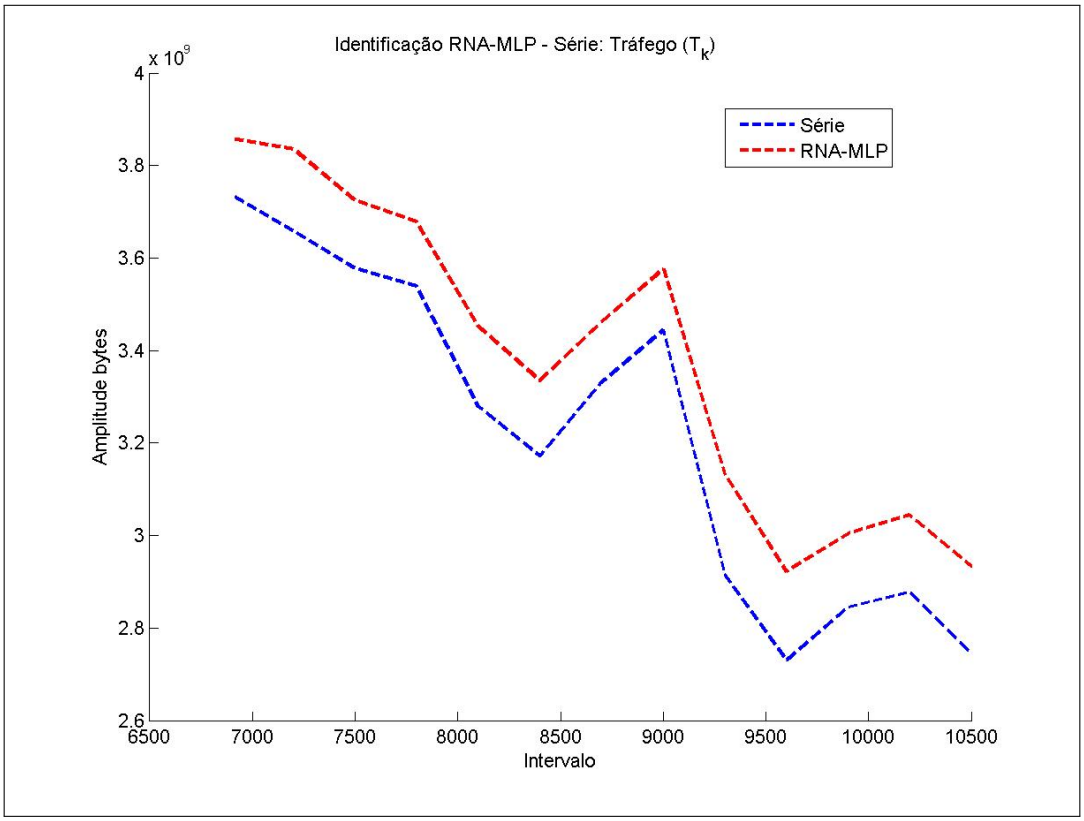

Figura 3.2: Série Tráfego (T_k): Real (y_k) x Identificada ($\hat{y}_k$)

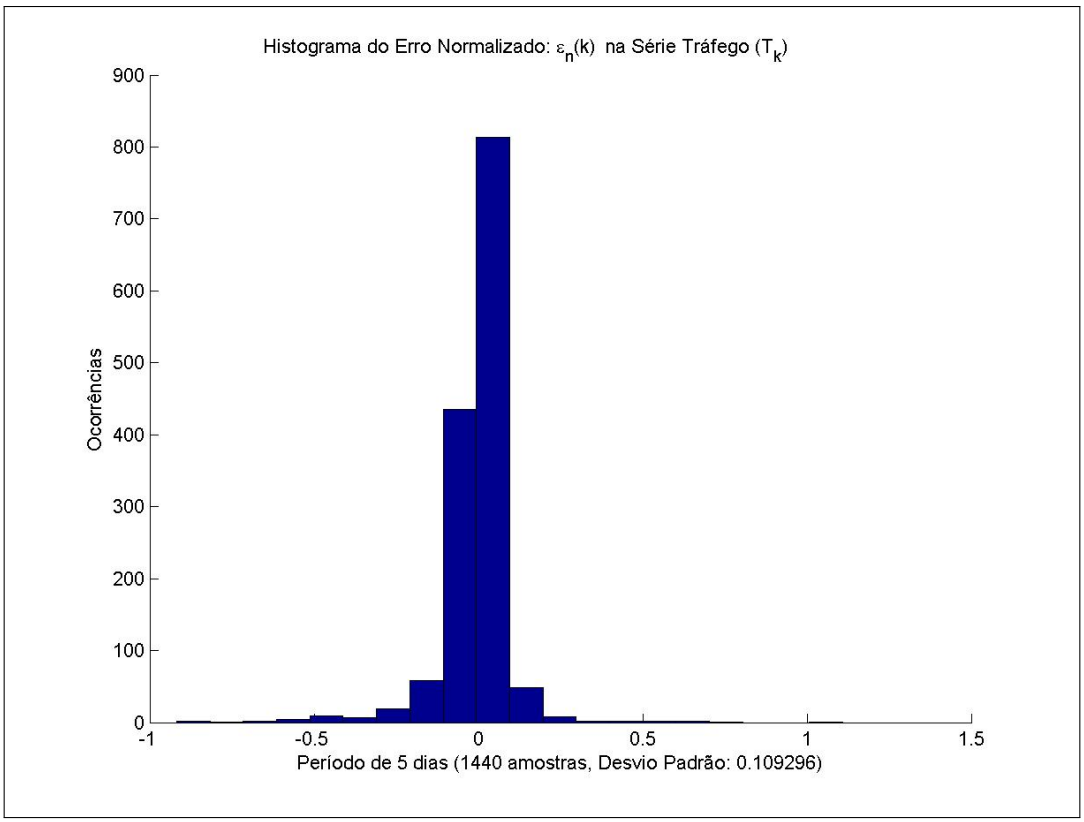

Figura 3.3: Série Tráfego (T_k): Histograma do erro ($\varepsilon_n(k)$) para 5 dias

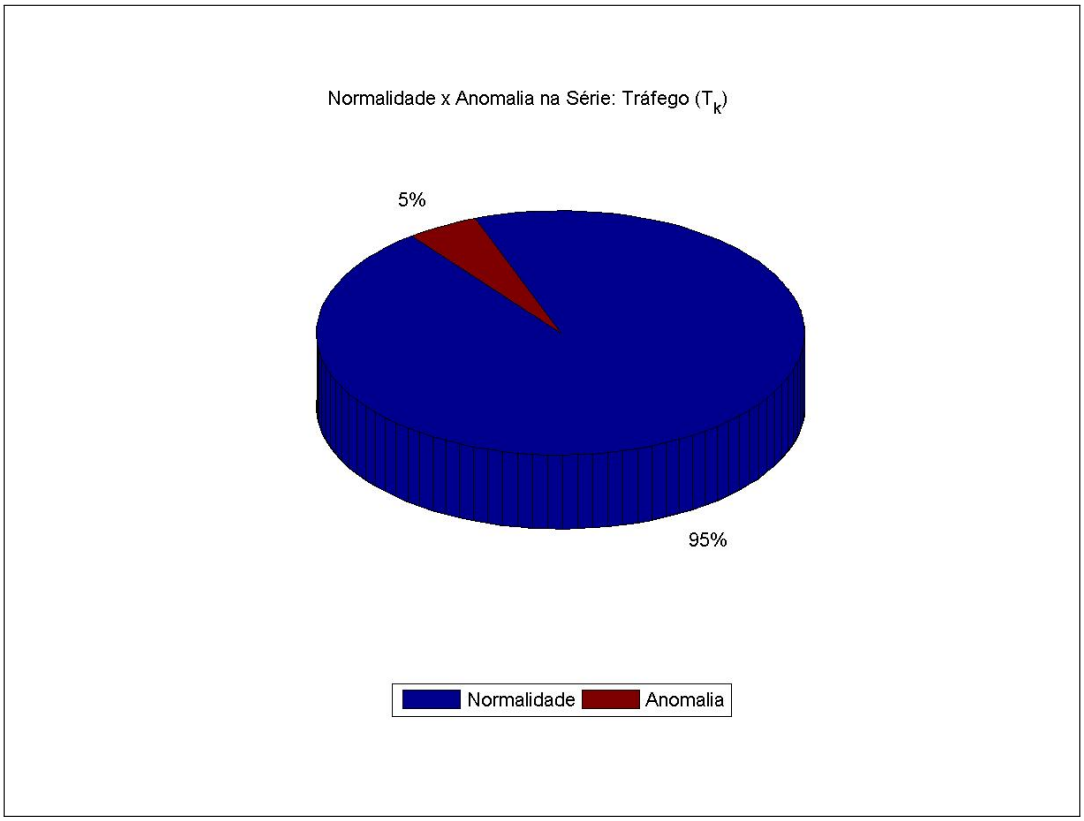

Figura 3.4: Série Tráfego (T_k): Normalidade x Anomalias

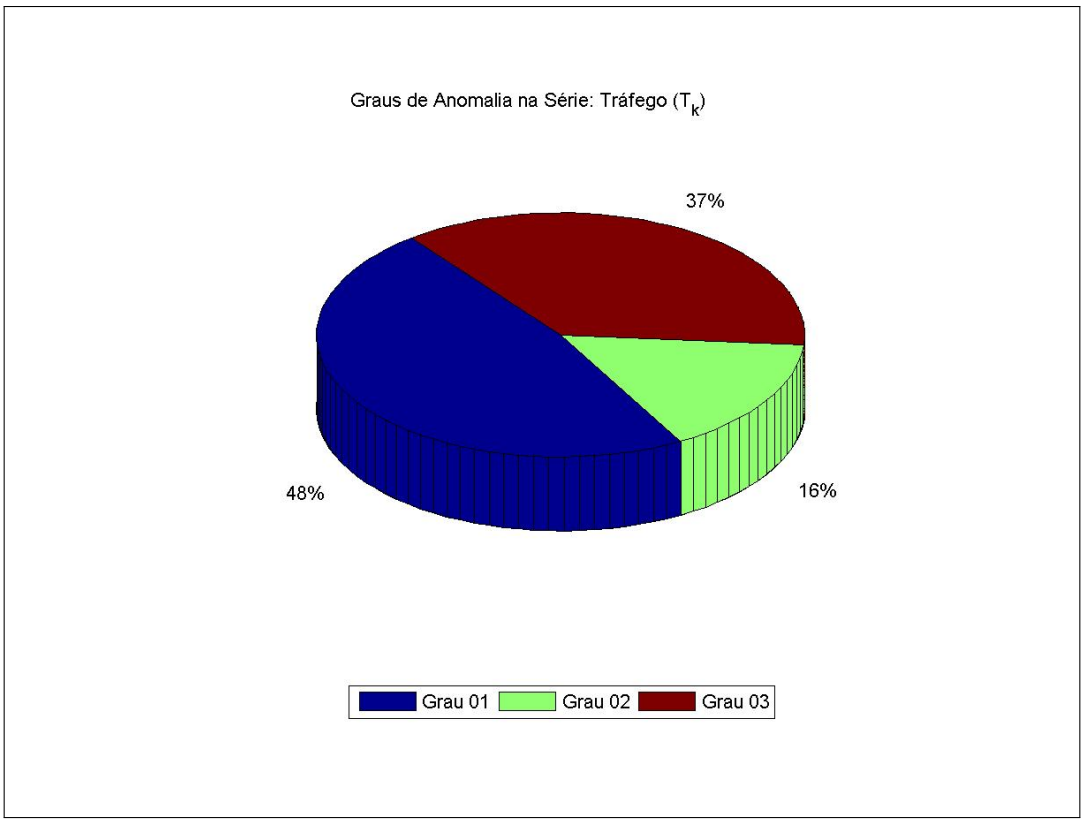

Figura 3.5: Série Tráfego (T_k): Graus de Anomalias

3.1.2 Série Discreta: Média bytes/portas (M_k)

Modelo Discreto Identificado:

$$y_k = 0,7813y_{k-1} + 0,1999y_{k-2}$$

Tabela 3.3: Série M_k: Pesos na RNA-Perceptron

Coeficiente	**Peso Neural**
ω_1	0,7813158983
ω_2	0,1999130122

Na Figura 3.6, tem-se o perfil da série em quatro dias distintos, na Figura 3.7, observa-se o perfil das série (y_k) comparada com o valor estimado pela RNA-Perceptron ($\hat{y_k}$), em um mesmo intervalo. A Figura 3.8 apresenta o histograma do erro normalizado da série (Equação 2.4), o qual permite avaliar o padrão de comportamento. E por fim, as Figuras 3.9 e 3.10 refletem a pesquisa de anomalias, na série considerada, no período compreendido entre dia 14 de junho de 2015 às 14h 40min e o dia 04 de agosto de 2015 às 13h 10min.

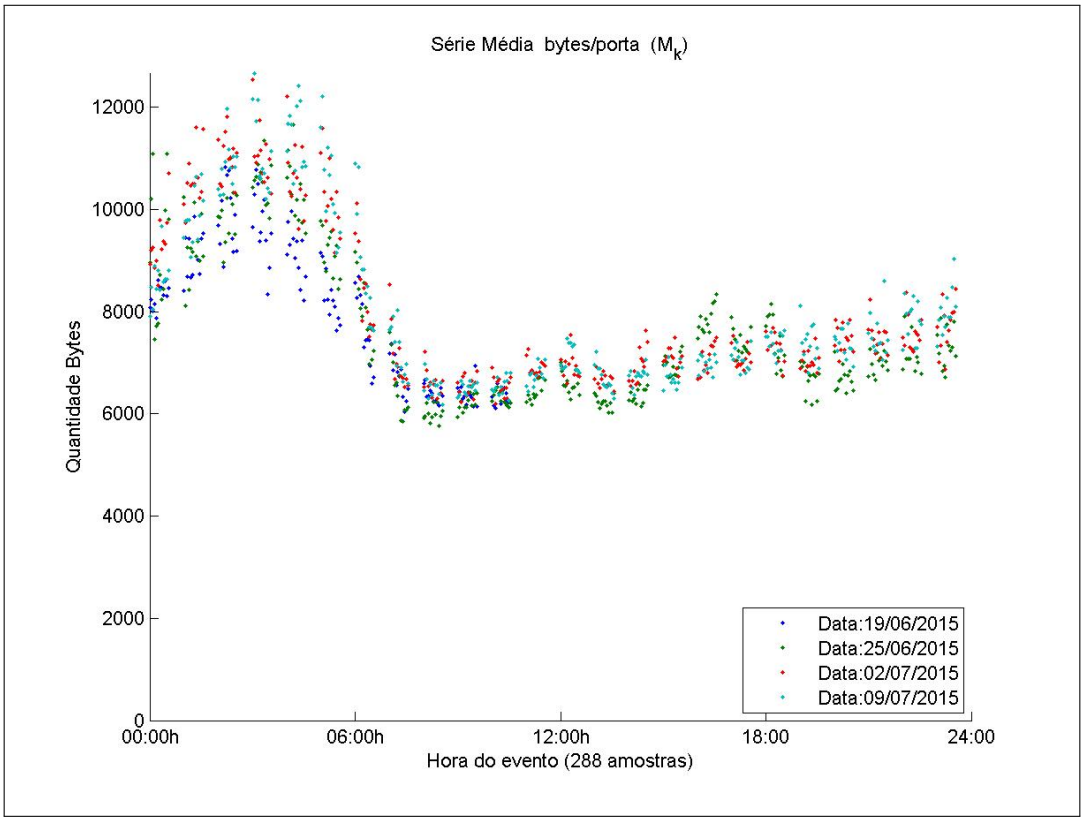

Figura 3.6: Série Discreta: Média bytes/portas (M_k)

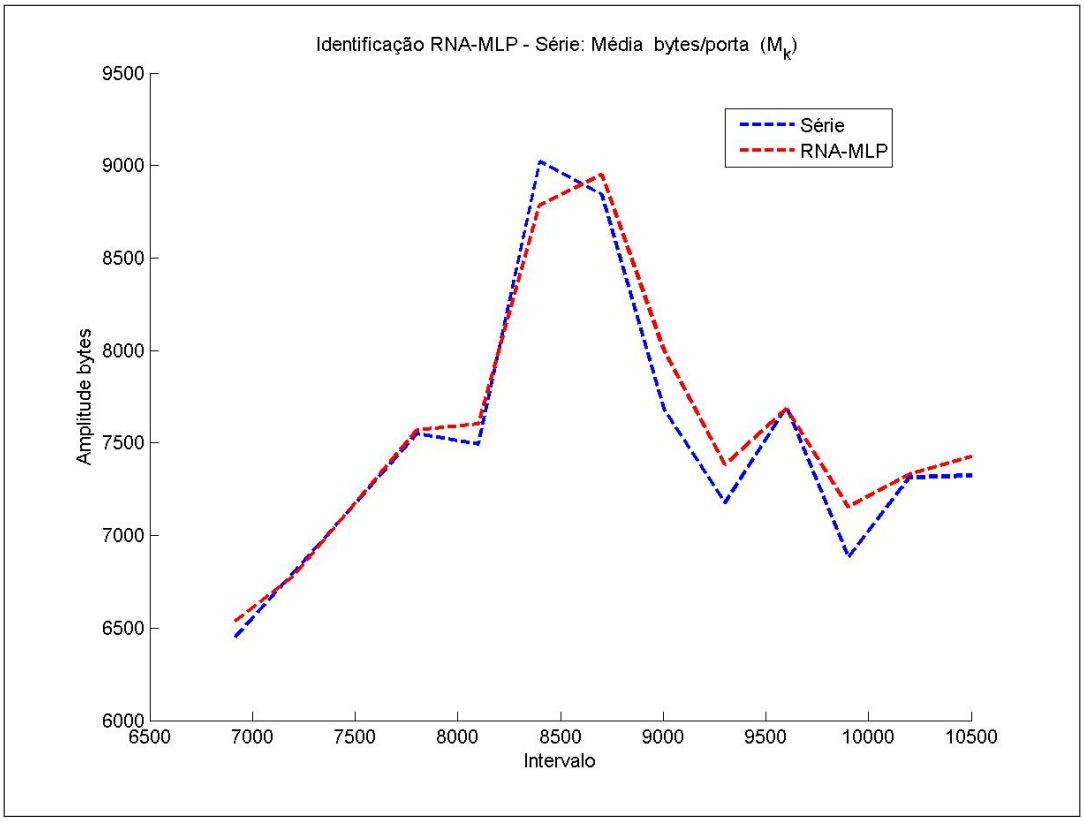

Figura 3.7: Série Média bytes/portas (M_k): Real (y_k) x Identificada ($\hat{y}_k$)

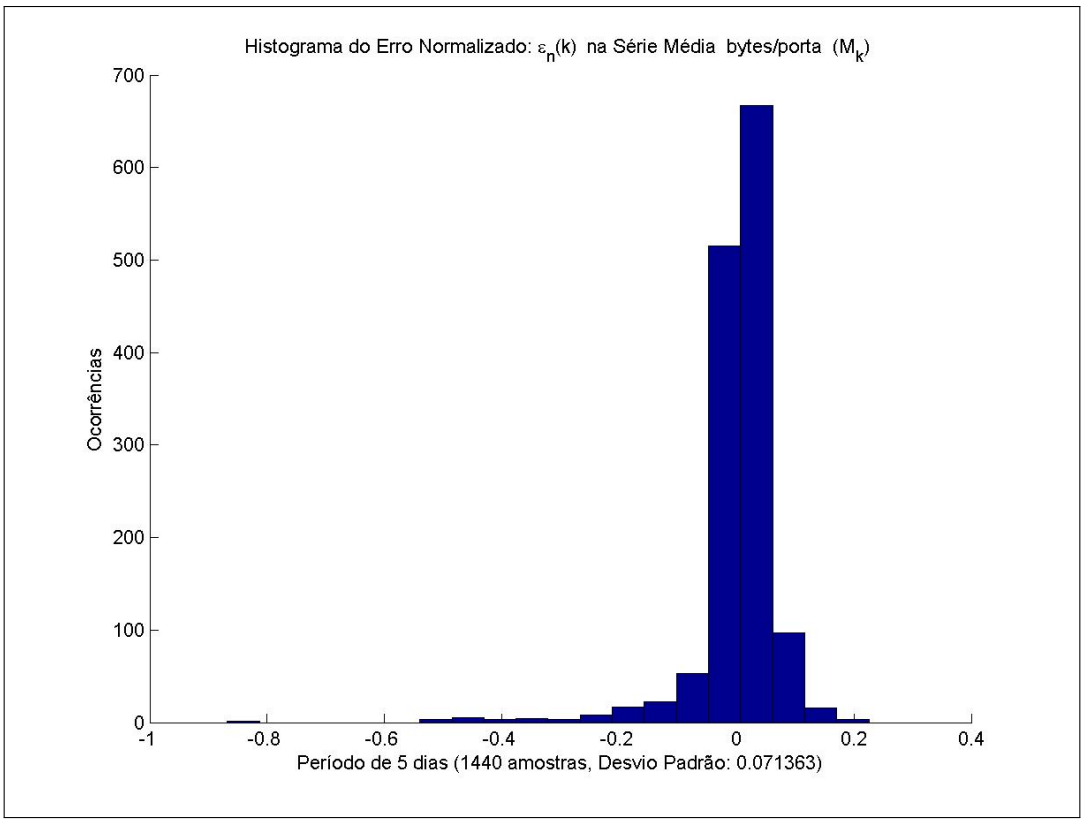

Figura 3.8: Série Média bytes/portas (M_k): Histograma do erro ($\varepsilon_n(k)$) para 5 dias

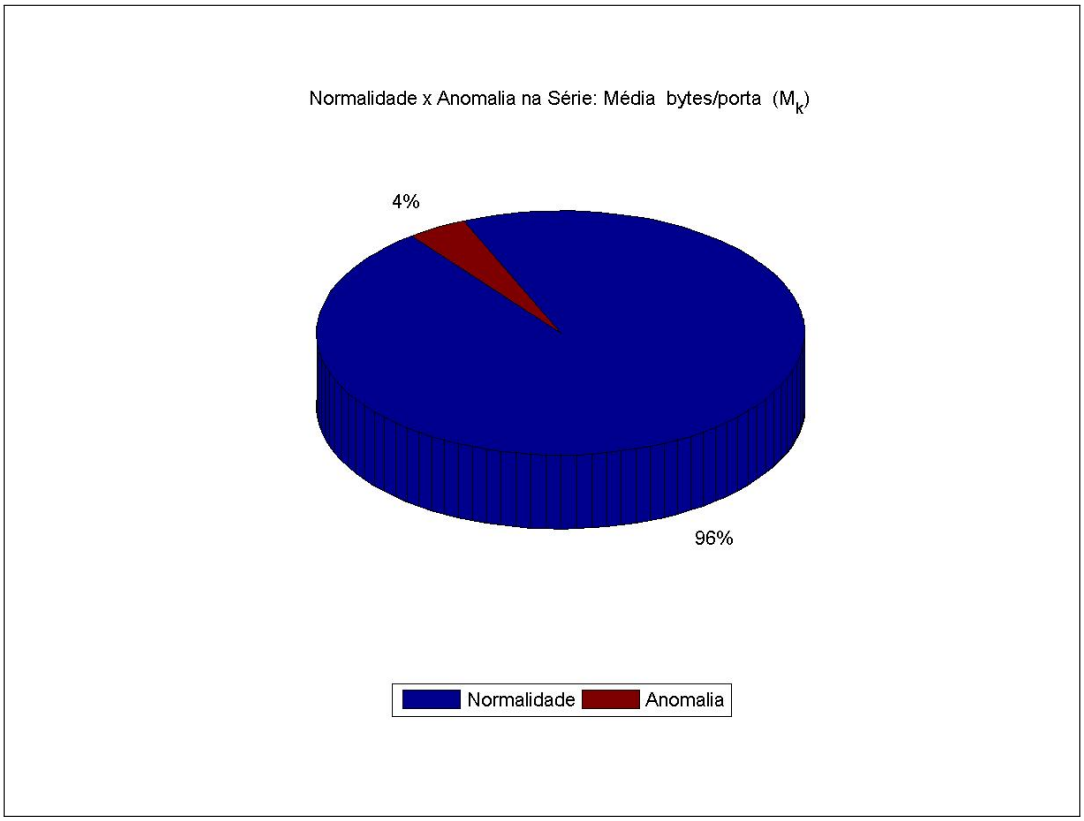

Figura 3.9: Série Média bytes/portas (M_k): Normalidade x Anomalias

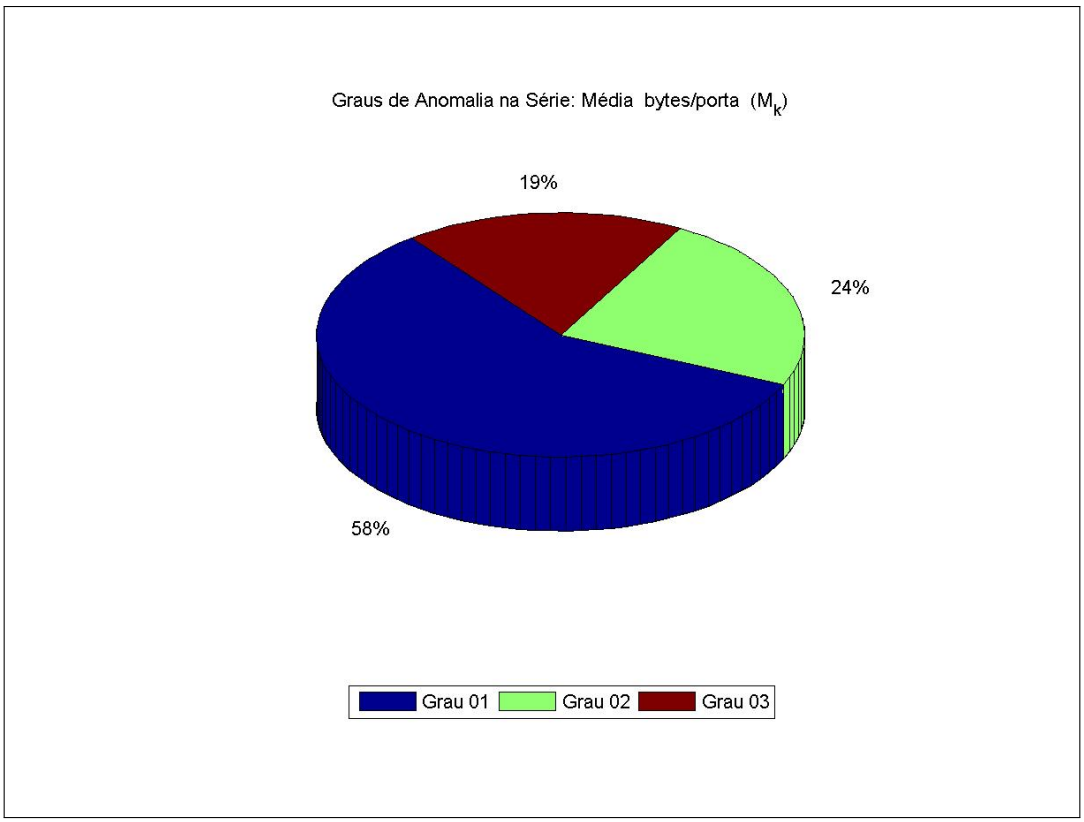

Figura 3.10: Série Média bytes/portas (M_k): Graus de Anomalias

3.1.3 Série Discreta: Portas Baixas (B_k)

Modelo Discreto Identificado:

$$y_k = 0,9417y_{k-1} + 0,01557y_{k-2}$$

Tabela 3.4: Série B_k: Pesos na RNA-Perceptron

Coeficiente	**Peso Neural**
ω_1	0,9416582356
ω_2	0,0155723936

Na Figura 3.11, tem-se o perfil da série em quatro dias distintos, na Figura 3.12, observa-se o perfil das série (y_k) comparada com o valor estimado pela RNA-Perceptron ($\hat{y_k}$), em um mesmo intervalo. A Figura 3.13 apresenta o histograma do erro normalizado da série (Equação 2.4), o qual permite avaliar o padrão de comportamento. E por fim, as Figuras 3.14 e 3.15 refletem a pesquisa de anomalias, na série considerada, no período compreendido entre dia 14 de junho de 2015 às 14h 40min e o dia 04 de agosto de 2015 às 13h 10min.

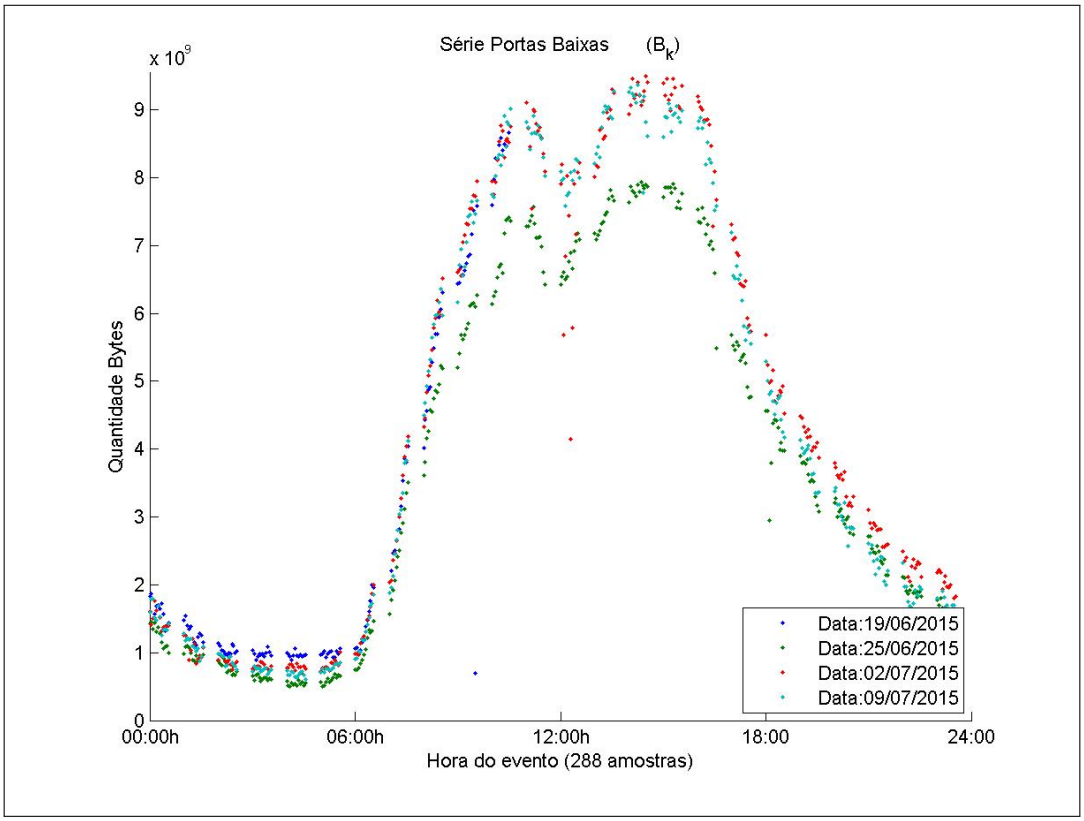

Figura 3.11: Série Discreta: Portas Baixas (B_k)

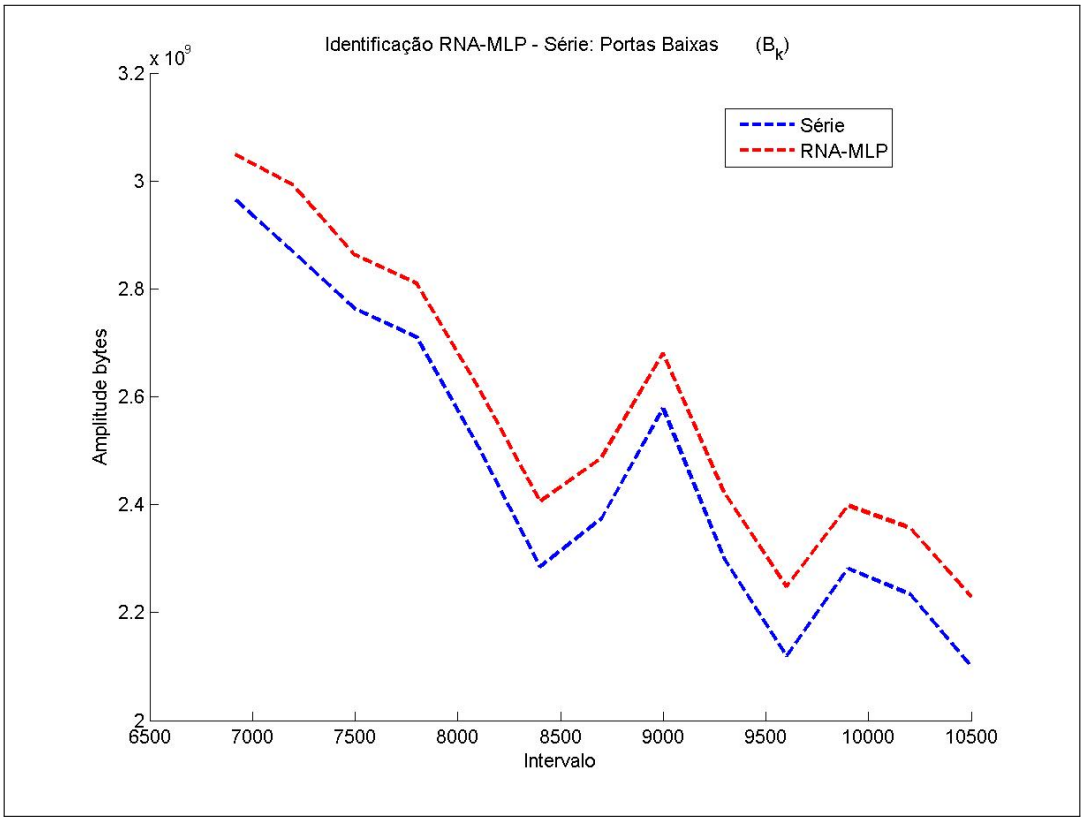

Figura 3.12: Série Portas Baixas (B_k): Real (y_k) x Identificada ($\hat{y}_k$)

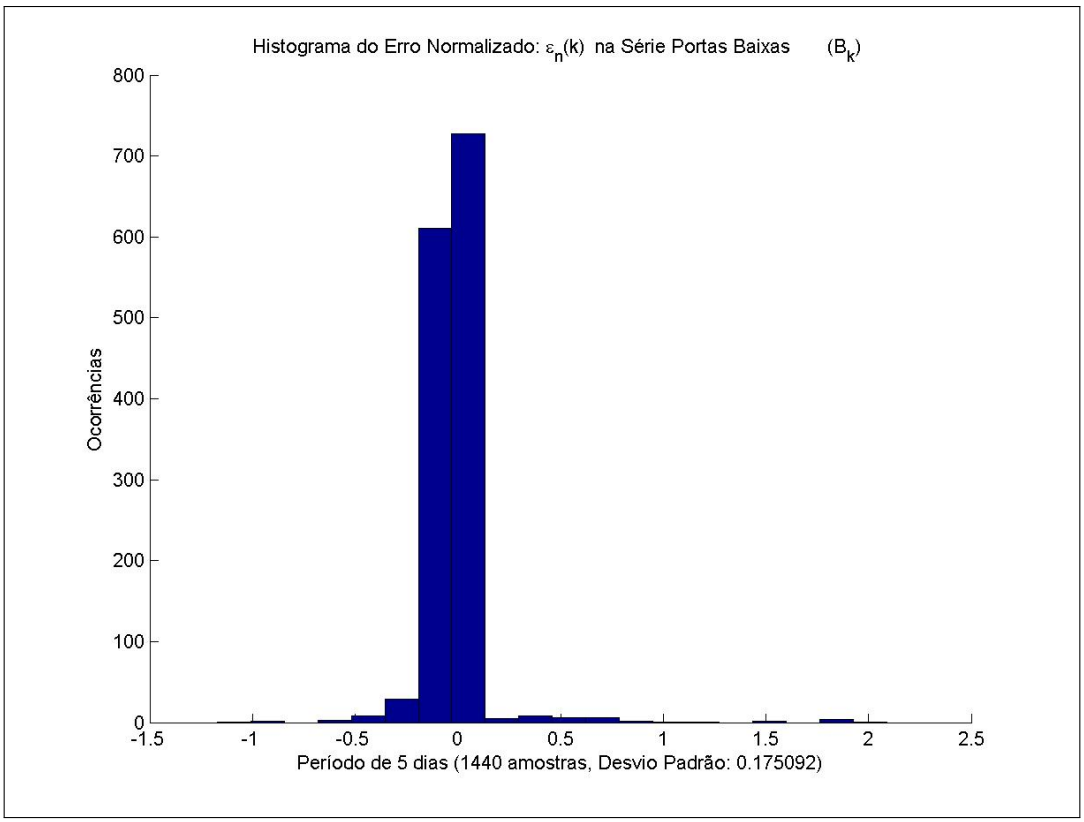

Figura 3.13: Série Portas Baixas (B_k): Histograma do erro ($\varepsilon_n(k)$) para 5 dias

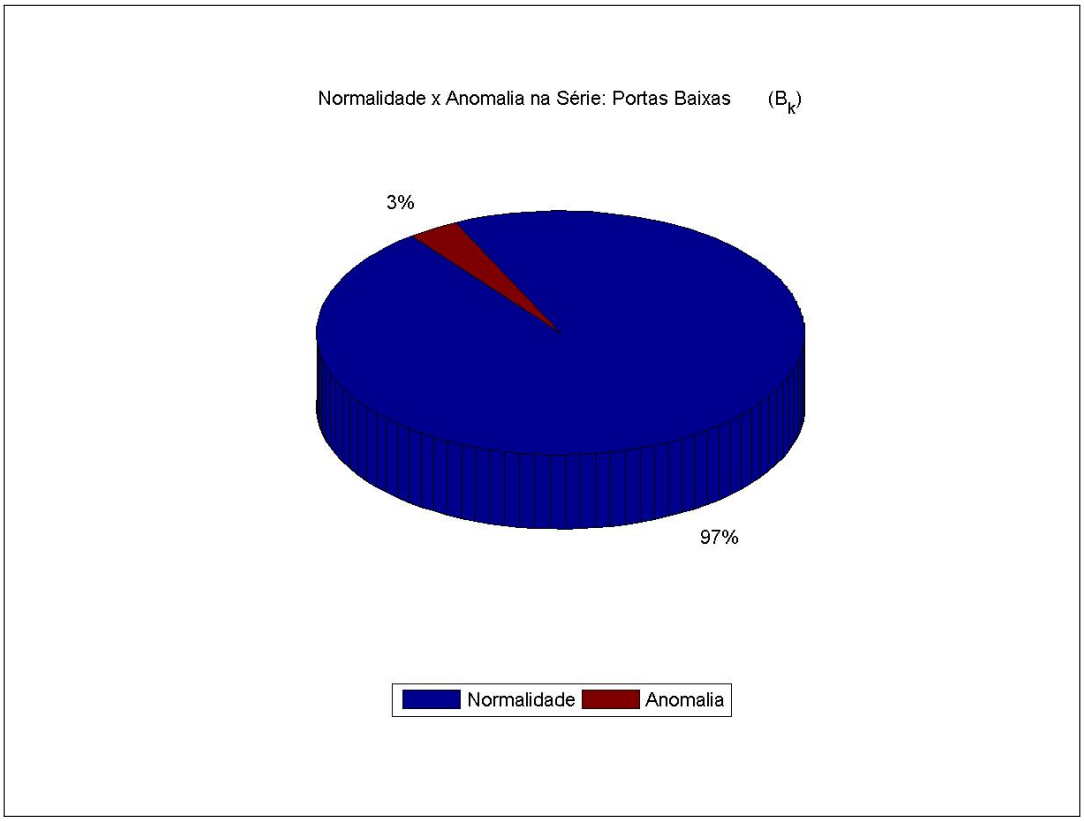

Figura 3.14: Série Portas Baixas (B_k): Normalidade x Anomalias

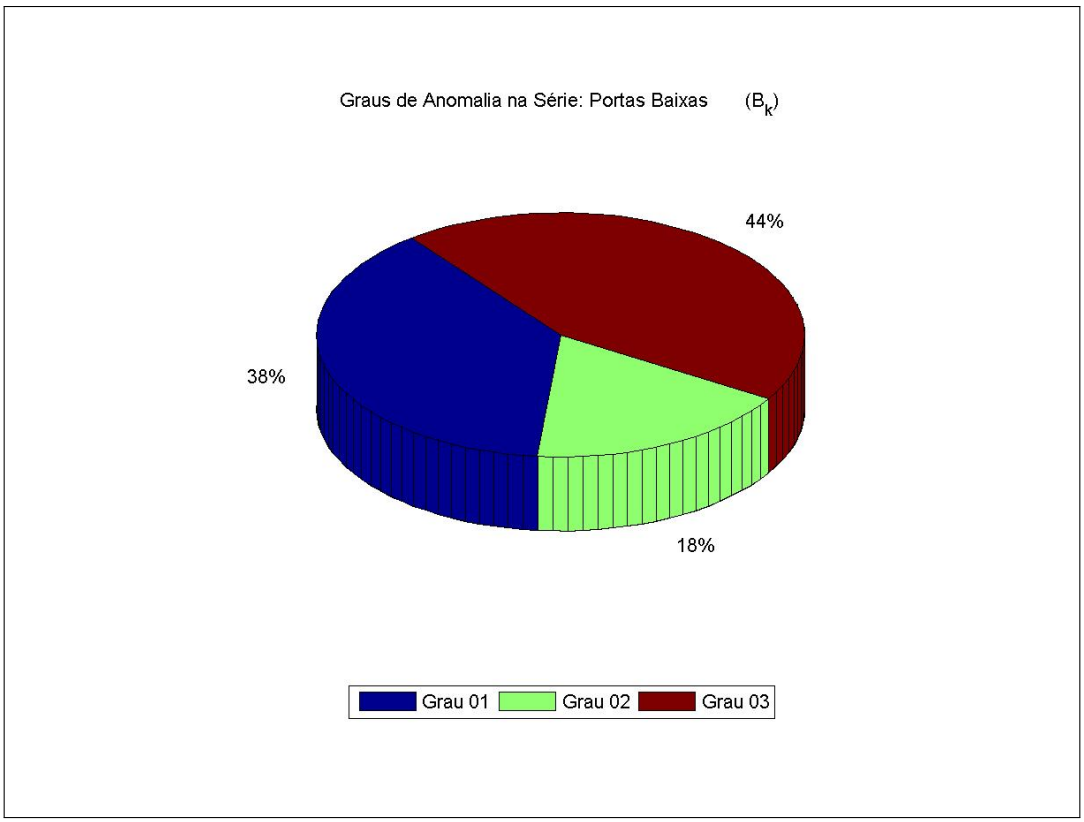

Figura 3.15: Série Portas Baixas (B_k): Graus de Anomalias

3.1.4 Série Discreta: Portas Servidor (S_k)

Modelo Discreto Identificado:

$$y_k = 0,5131y_{k-1} + 0,3824y_{k-2}$$

Tabela 3.5: Série S_k: Pesos na RNA-Perceptron

Coeficiente	**Peso Neural**
ω_1	0,5130916246
ω_2	0,3823794530

Na Figura 3.16, tem-se o perfil da série em quatro dias distintos, na Figura 3.17, observa-se o perfil das série (y_k) comparada com o valor estimado pela RNA-Perceptron ($\hat{y_k}$), em um mesmo intervalo. A Figura 3.18 apresenta o histograma do erro normalizado da série (Equação 2.4), o qual permite avaliar o padrão de comportamento. E por fim, as Figuras 3.19 e 3.20 refletem a pesquisa de anomalias, na série considerada, no período compreendido entre dia 14 de junho de 2015 às 14h 40min e o dia 04 de agosto de 2015 às 13h 10min.

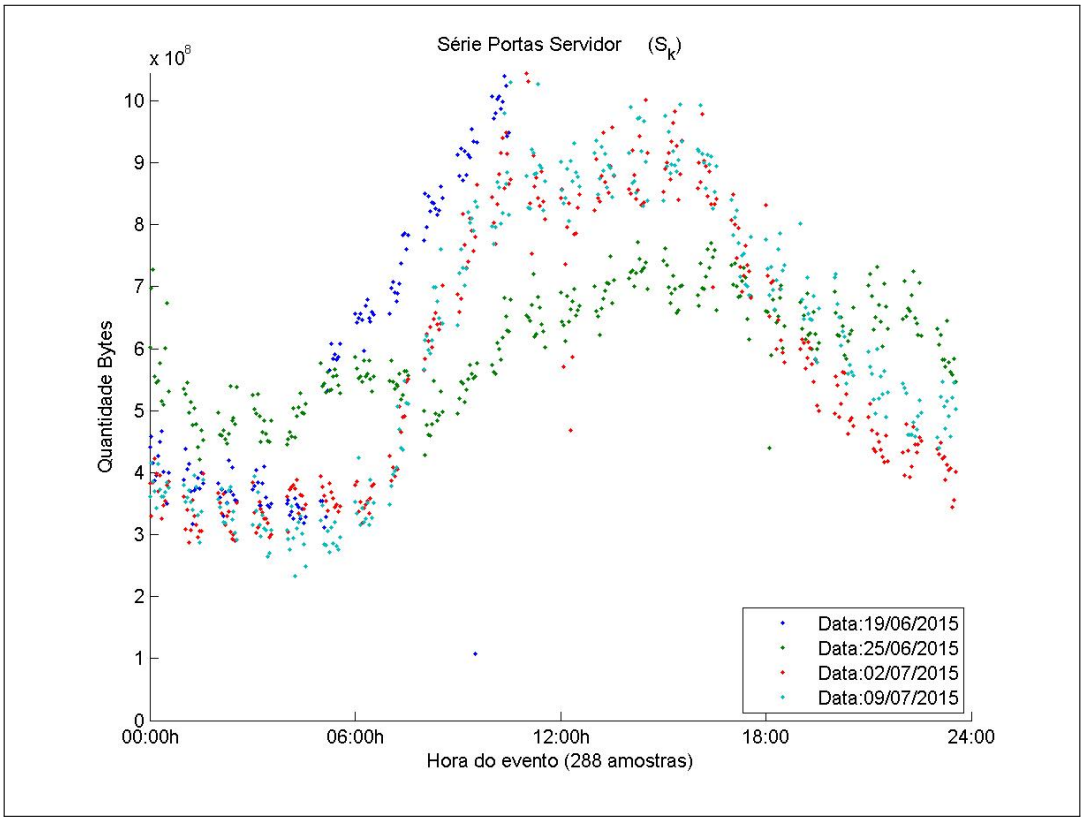

Figura 3.16: Série Discreta (S_k): Portas Servidor

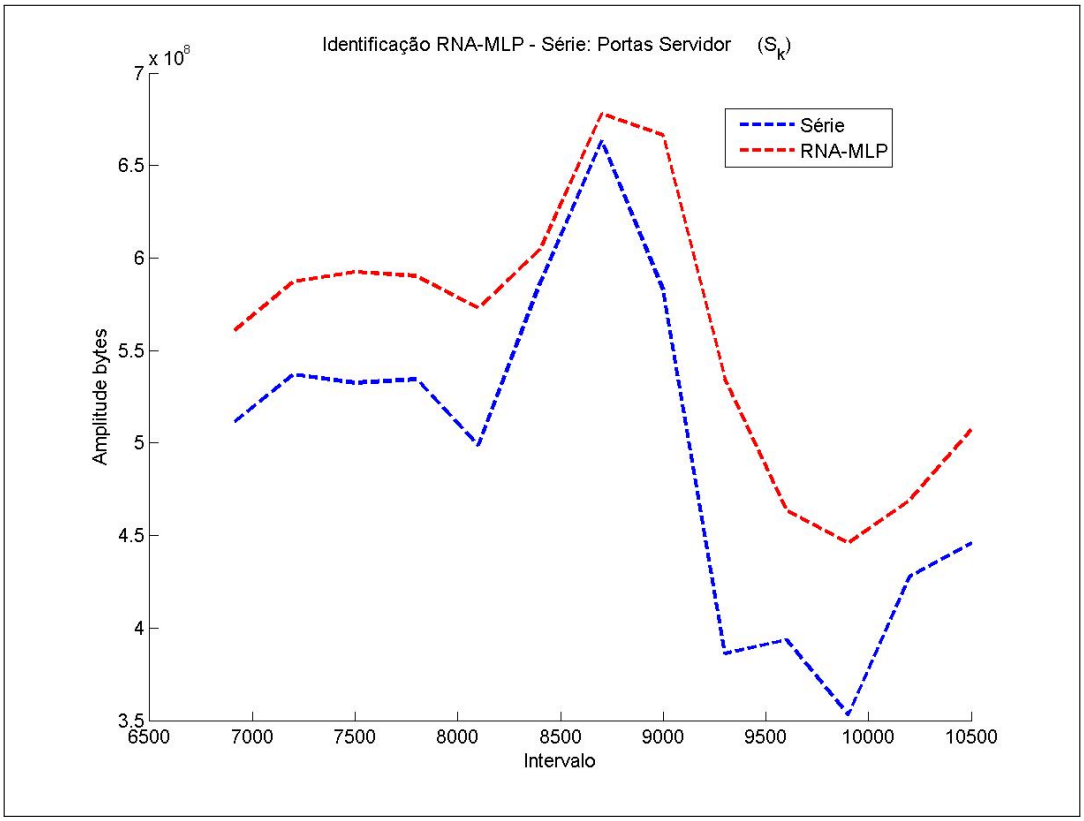

Figura 3.17: Série Portas Servidor (S_k): Real (y_k) x Identificada ($\hat{y}_k$)

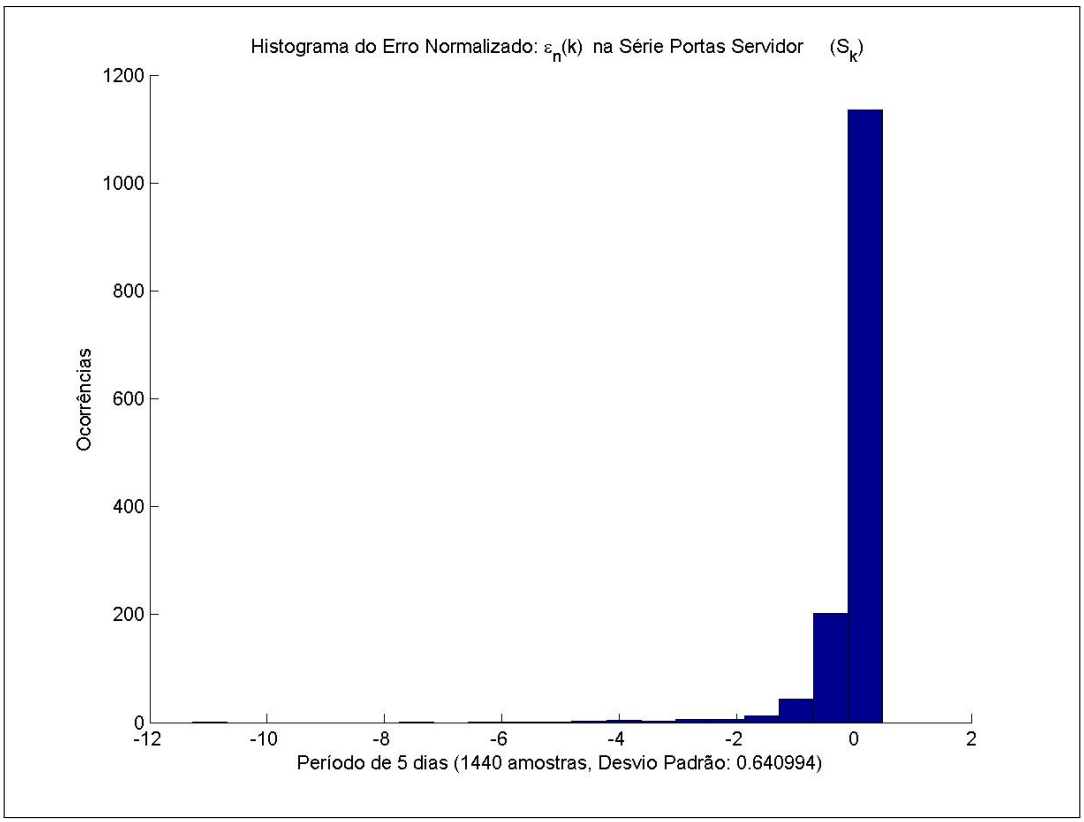

Figura 3.18: Série Portas Servidor (S_k): Histograma do erro ($\varepsilon_n(k)$) para 5 dias

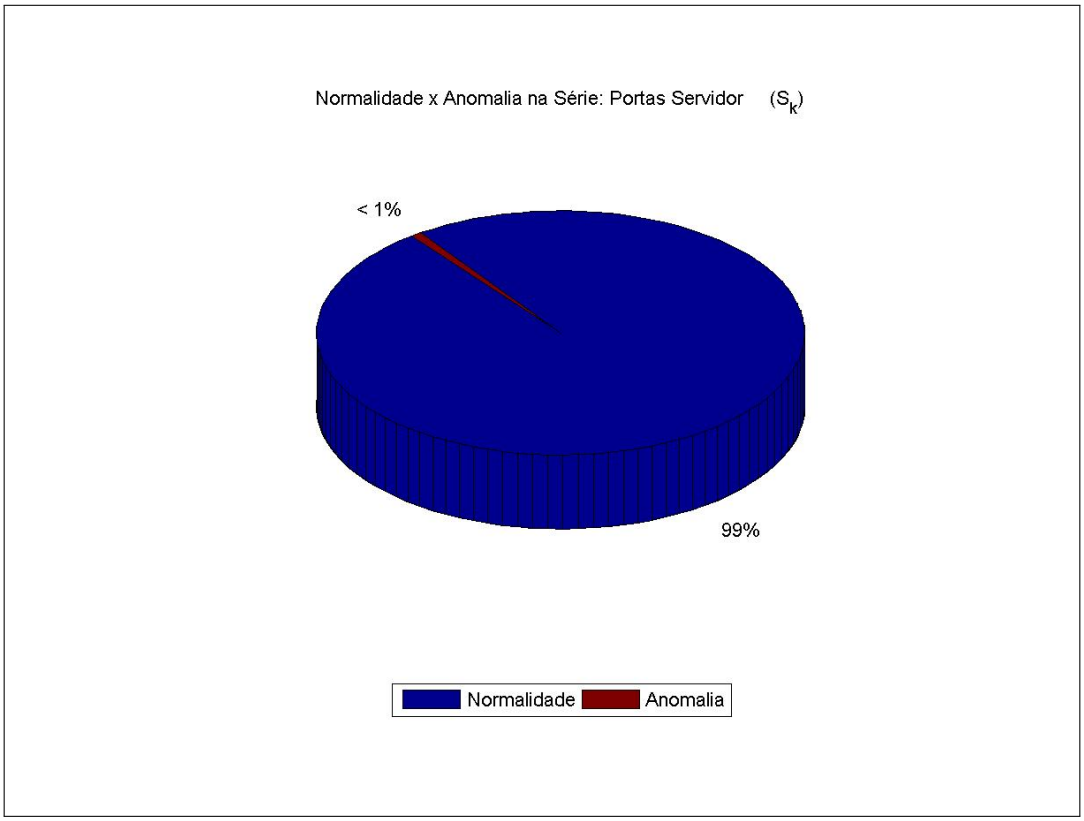

Figura 3.19: Série Portas Servidor (S_k): Normalidade x Anomalias

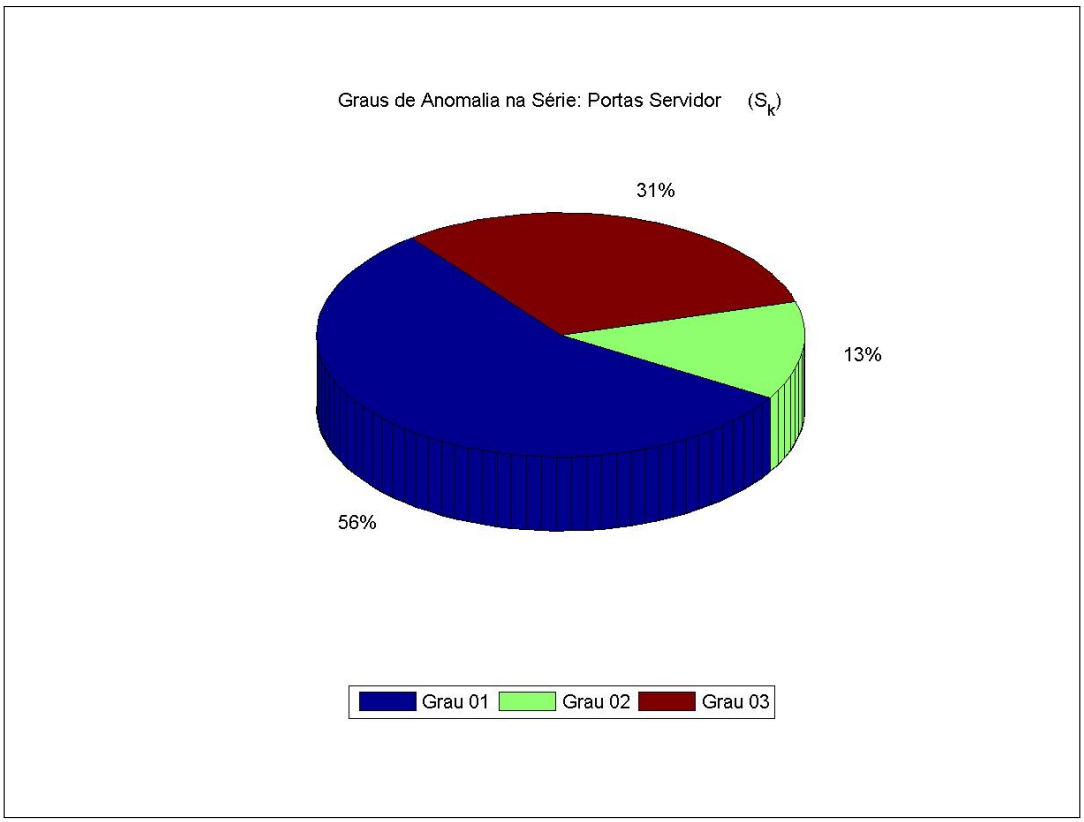

Figura 3.20: Série Portas Servidor (S_k): Graus de Anomalias

3.1.5 Série Discreta: Portas Dinâmicas (D_k)

Modelo Discreto Identificado:

$$y_k = 0,6518y_{k-1} + 0,2847y_{k-2}$$

Tabela 3.6: Série D_k: Pesos na RNA-Perceptron

Coeficiente	**Peso Neural**
ω_1	0,6518115918
ω_2	0,2847240979

Na Figura 3.21, tem-se o perfil da série em quatro dias distintos, na Figura 3.22, observa-se o perfil das série (y_k) comparada com o valor estimado pela RNA-Perceptron ($\hat{y_k}$), em um mesmo intervalo. A Figura 3.23 apresenta o histograma do erro normalizado da série (Equação 2.4), o qual permite avaliar o padrão de comportamento. E por fim, as Figuras 3.24 e 3.25 refletem a pesquisa de anomalias, na série considerada, no período compreendido entre dia 14 de junho de 2015 às 14h 40min e o dia 04 de agosto de 2015 às 13h 10min.

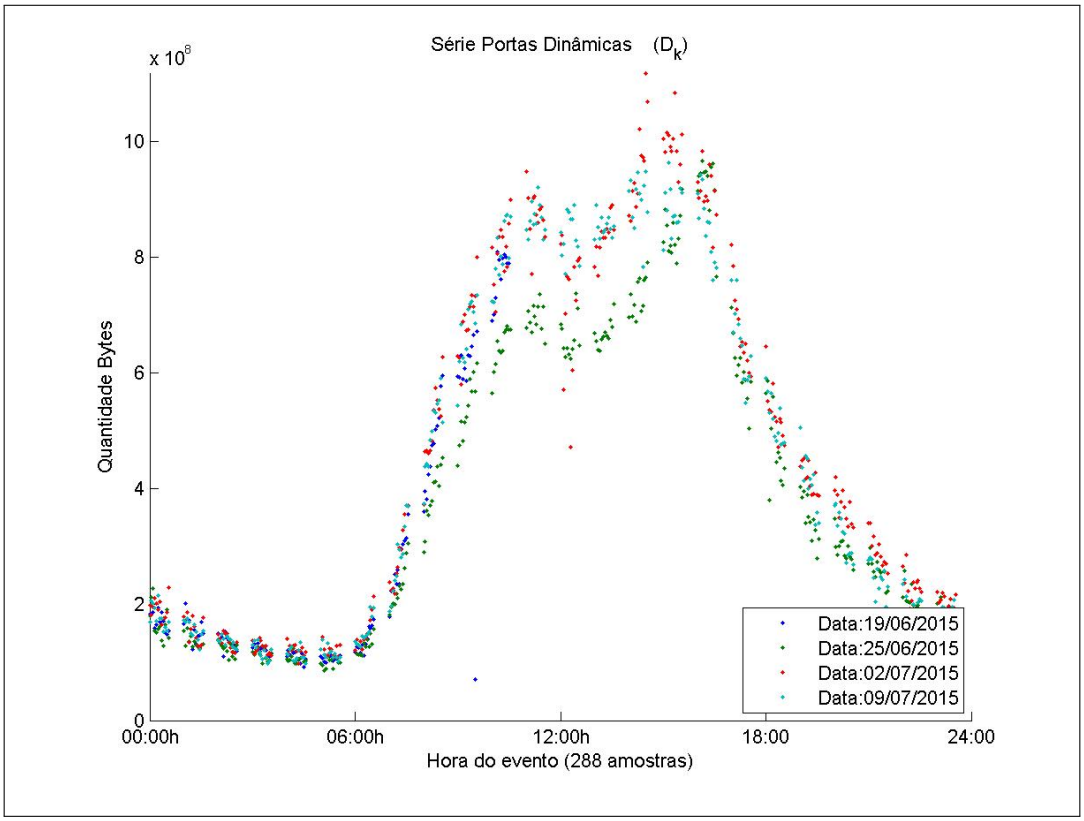

Figura 3.21: Série Discreta: Portas Dinâmicas (D_k)

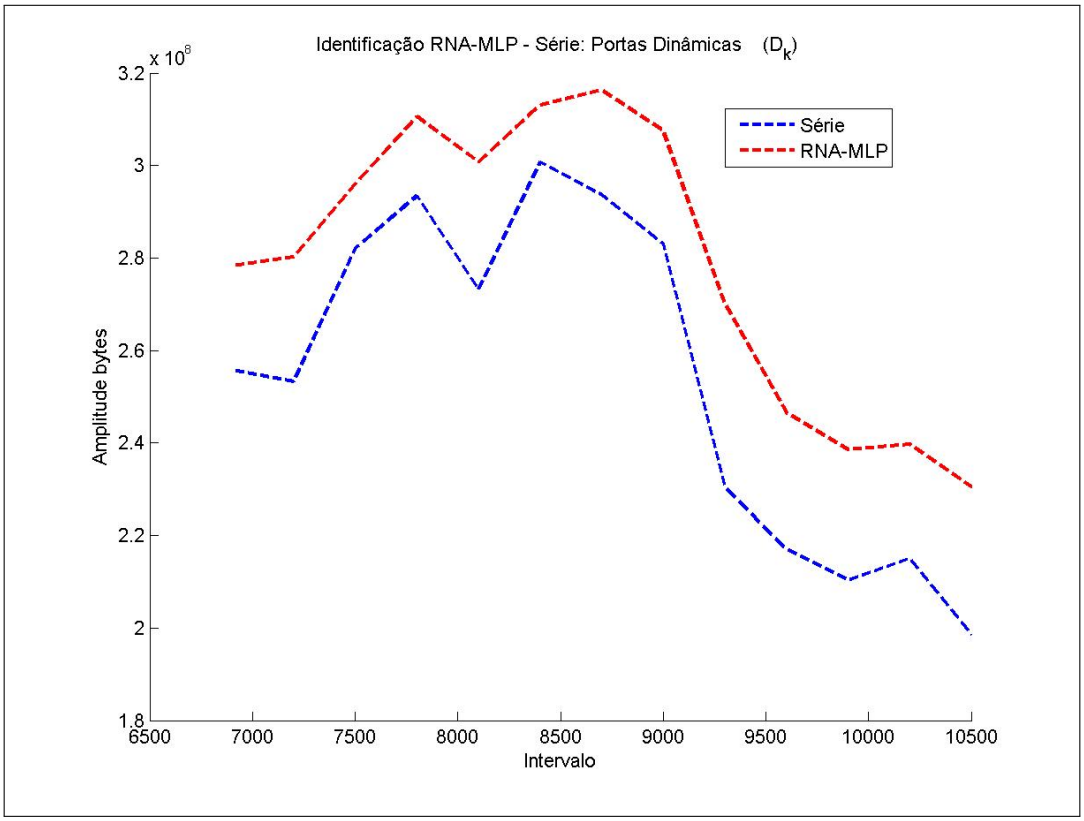

Figura 3.22: Série Portas Dinâmicas (D_k): Real (y_k) x Identificada ($\hat{y}_k$)

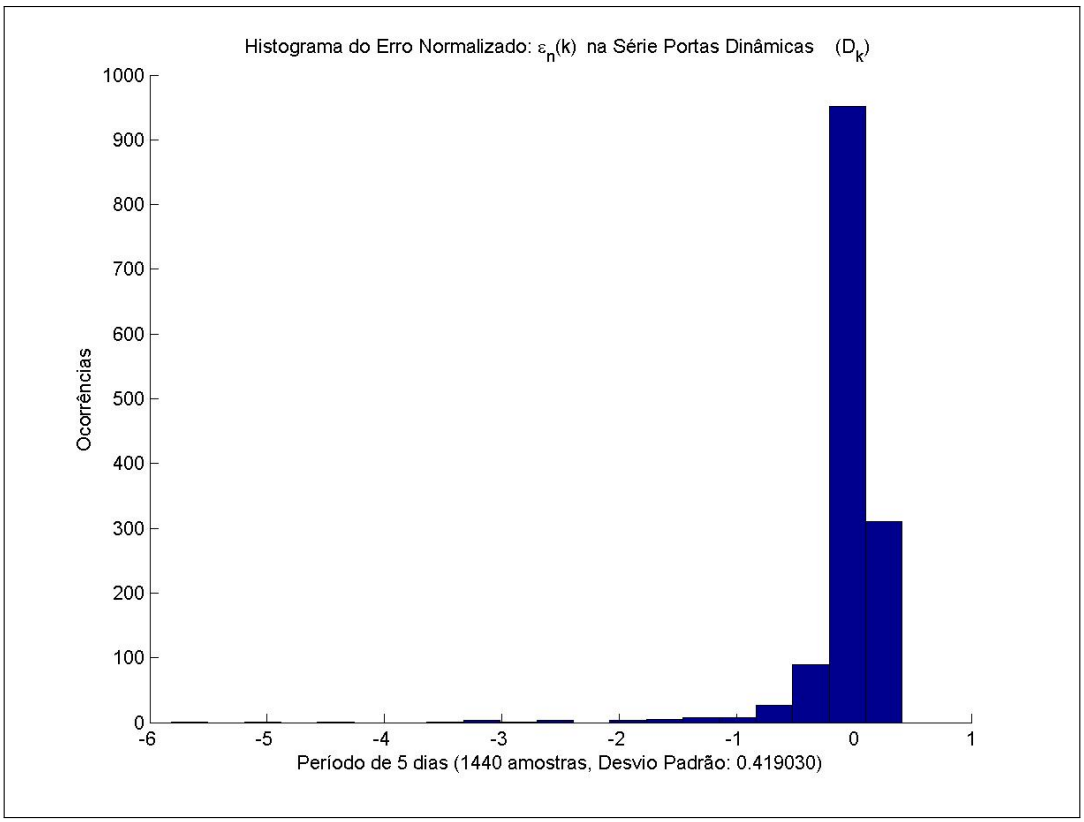

Figura 3.23: Série Portas Dinâmicas (D_k): Histograma do erro ($\varepsilon_n(k)$) para 5 dias

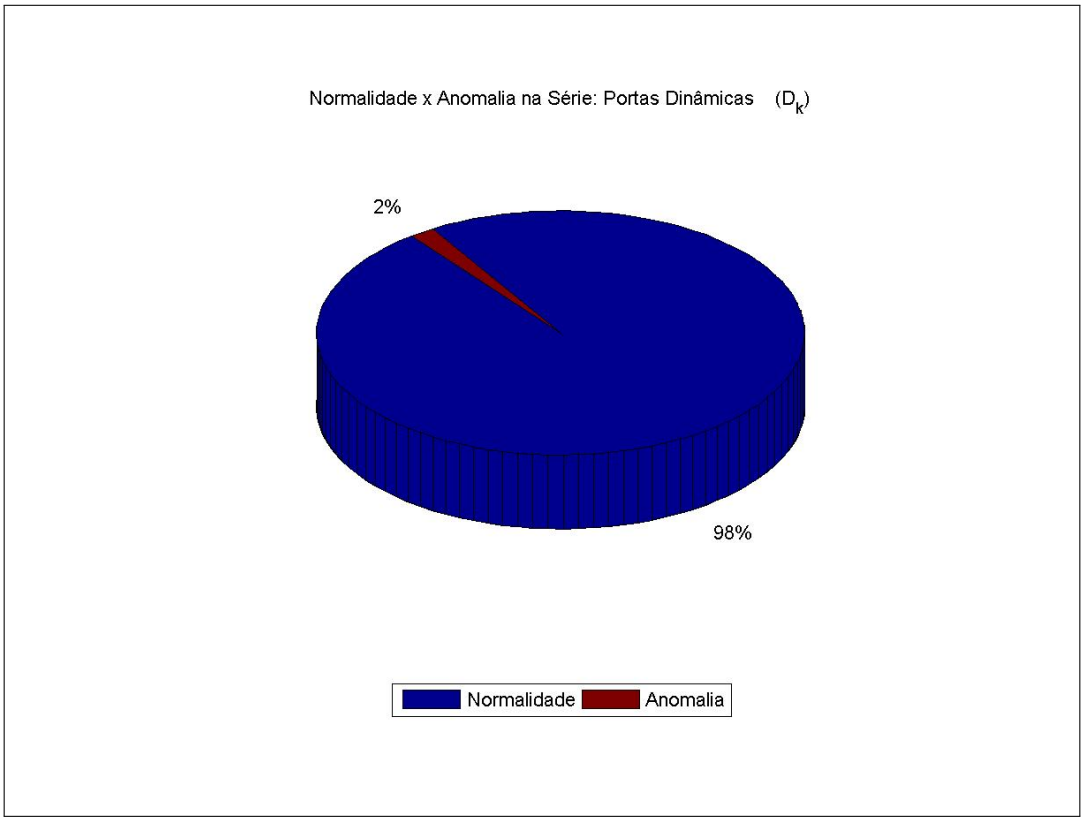

Figura 3.24: Série Portas Dinâmicas (D_k): Normalidade x Anomalias

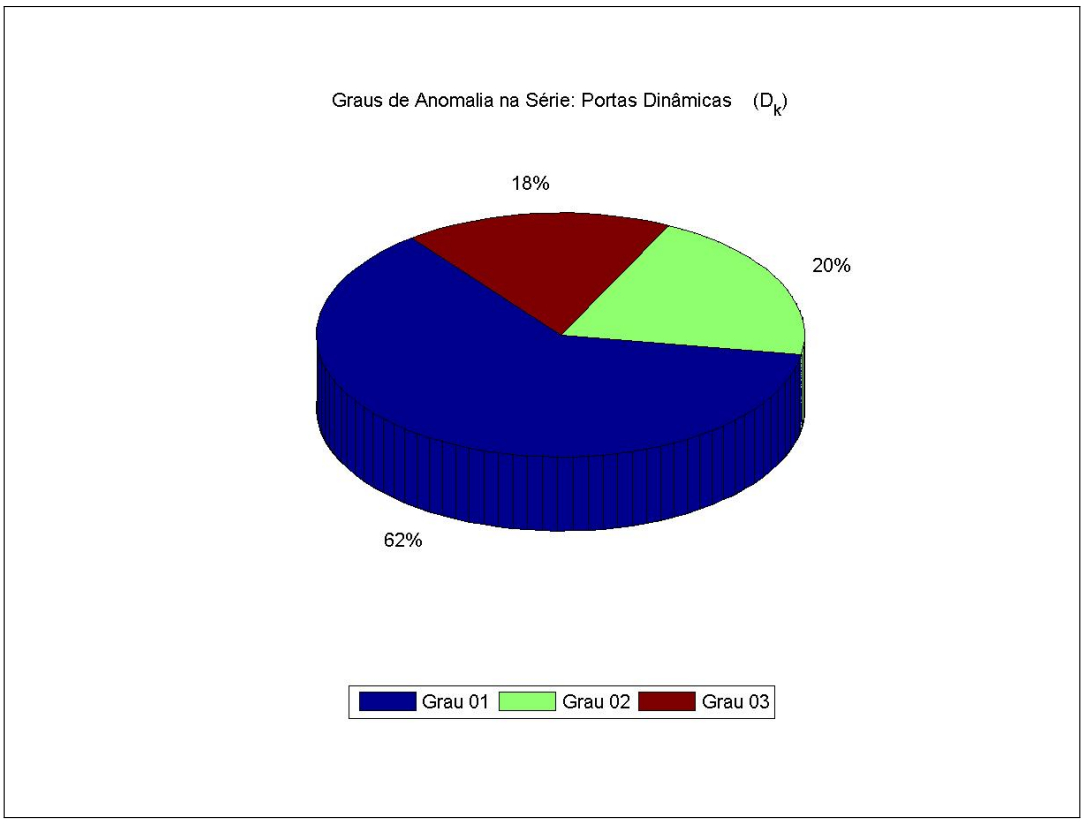

Figura 3.25: Série Portas Dinâmicas (D_k): Graus de Anomalias

3.1.6 Caracterizando intensidade de anomalias

Com vistas a destacar e tornar útil a informação das anomalias identificadas em cada uma das séries discretas, em que o fluxo de dados foi originalmente particionado, faz-se necessário estabelecer uma métrica de avaliação conjunta dos resultados.

Assim, com base na definição anterior de **grau de anomalia** (Seção 3.1), define-se por extensão:

- Intensidade de uma Anomalia: como a soma algébrica dos graus de anomalia observados em cada uma das séries, no mesmo instante de tempo discreto.

Logo, como os graus de anomalia foram classificados no intervalo [0,3], em cada uma das cinco séries avaliadas, a intensidade de uma anomalia varia no intervalo [0,15], sendo zero o indicador de normalidade do sistema. Cabe a ressalva que, pela natural continuidade desta pesquisa, poderá haver um refinamento desta métrica pela inserção de ponderações entre o valor de cada série.

Tabela 3.7: Caracterizando intensidade

Intensidade	**Intervalo**
Moderada	[1,4]
Forte	[5,9]
Muito Forte	[10,15]

Propõe-se para a Intensidade da Anomalia, a classificação em: **Moderada**, **Forte** e **Muito Forte** (Tabela 3.7). Na Figura 3.26 e na Tabela 3.8, apresenta-se esta dimensão de análise de anomalias para a Rede-Rio de Computadores, no período compreendido entre o dia 01 de Julho de 2015 às 00h 00min e o dia 31 de julho de 2015 às 23h 59min.

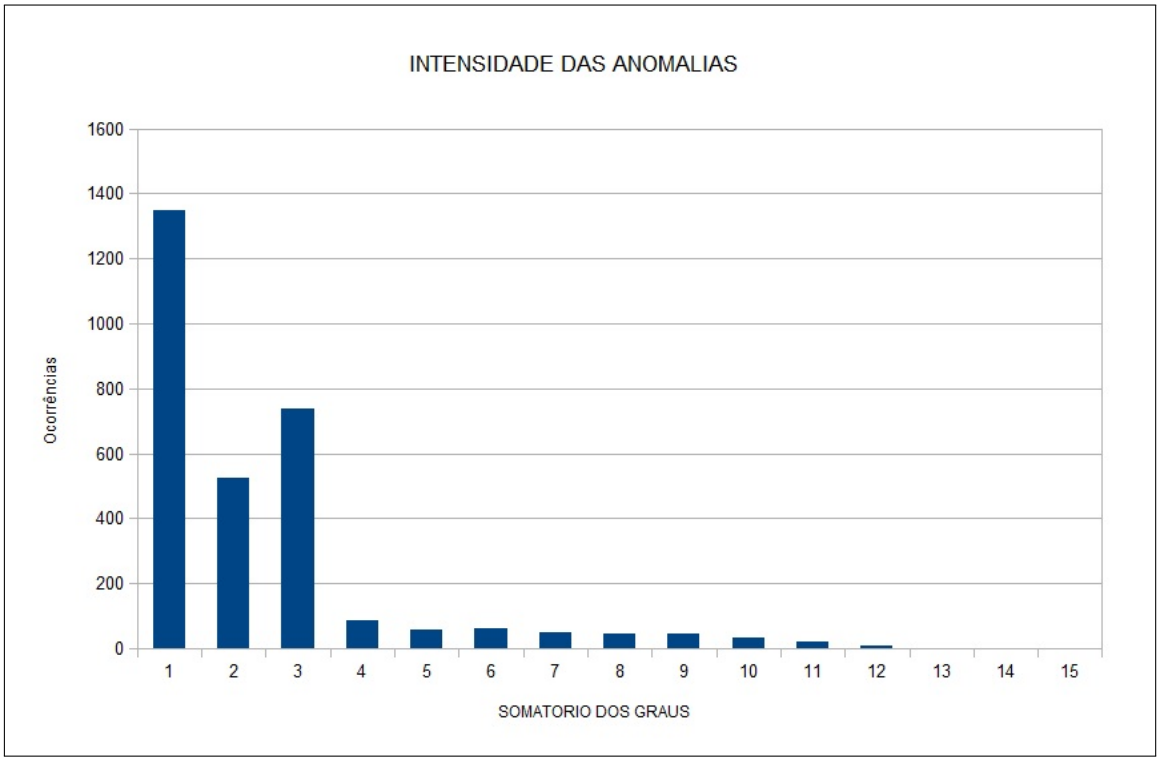

Figura 3.26: Intensidade Anomalias na Rede-Rio em Julho de 2015

Tabela 3.8: Intensidade de Anomalias na Rede-Rio de Computadores

Intensidade	**Quantidade**
1	1349
2	525
3	739
4	84
5	55
6	62
7	47
8	44
9	46
10	34
11	19
12	9
13	0
14	0
15	0

3.2 Análise Cross-Referenciada

Como método de avaliação da efetividade na identificação de anomalias maliciosas, estabeleceu-se um ensaio comparativo de resultados de laboratório com a técnica do trabalho de pesquisa de **Identificação de Anomalias em Fluxos de Rede Utilizando o Método de Previsão em Séries Temporais de HOLT-WINTERS** [DA SILVA (2015)], em curso no RAVEL/UFRJ.
Neste ensaio, consideram-se as seguintes premissas:

- O intervalo de análise em ambos os trabalhos coincidiram entre o dia 20 de julho de 2015 às 0h 00min e o dia 01 de agosto de 2015 às 12h 20min;
- Granularidade de fluxos com intervalos de 05 (cinco) minutos;
- Considerou-se na análise apenas as anomalias de intensidade **Forte** e **Muito Forte**, segundo a definição do presente trabalho;
- Disseminaram-se ataques de forma aleatória, criando anomalias adicionais de ciberataque na Rede-Rio de Computadores, definido como um grupo de controle[1].

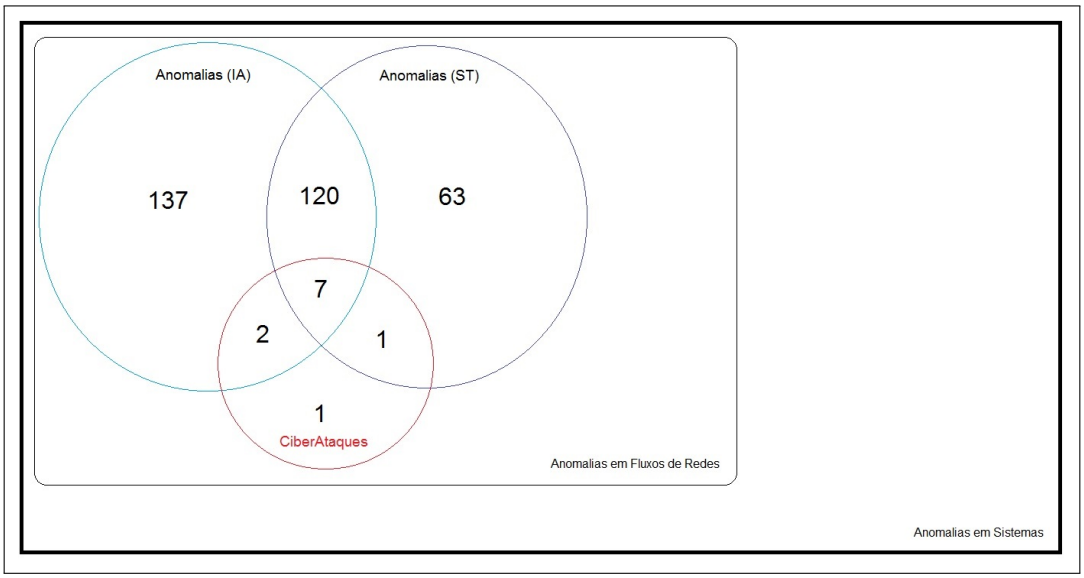

Figura 3.27: Análise Cross-Referenciada das Anomalias Identificadas

Tabela 3.9: Anomalias Identificadas

n(IA)	**n(ST)**	**n**$((IA) \cap (ST))$	**n**$((IA) \cup (ST))$	**n**$((IA) \cap (ST))$**%**	**n**(N_{IA})**%**	**n**(N_{ST})**%**
266	191	127	330	38,48	19,39	42,12

[1]Cabe registrar a colaboração do senhor Felipe Afonso Espósito, na atividade de disseminar o conjunto de controle, o qual só se tornou conhecido pela equipe do Laboratório RAVEL/UFRJ no momento de avaliação dos resultados.

Tabela 3.10: Análise Cross-Referenciada: Anomalias x Ataques

Conjunto Referenciado	**24 e 25/07**	**31 e 01/08**	**Total**	**Anomalia Grave**
n(IA)	23	28	51	9
n(ST)	27	17	44	8
n$((IA) \cap (ST))$	16	22	38	7
n(N_{IA})	11	0	6	1
n(N_{ST})	7	6	13	2
n(Ataques Simulados)				11
n(Falso Negativo)				1
n$((IA) \cup (ST))$	34	23	57	10
n$((IA) \cap (ST))$**%**	47,06	95,65	66,67	70,00
n(N_{IA})**%**	32,35	0,00	10,53	10,00
n(N_{ST})**%**	20,59	26,09	22,81	20,00
Efetividade(IA) %				81,82
Efetividade(ST) %)				72,73
Efetividade$((IA) \cap (ST))$ **%**				63,64
Efetividade$((IA) \cup (ST))$ **%**				90,91

Onde:

- **(IA):** Conjunto das anomalias identificadas pela técnica RNA-Perceptron;
- **(ST):** Conjunto das anomalias identificadas pela técnica de séries temporais [DA SILVA (2015)];
- **(**N_{IA}**):** Conjunto das anomalias identificadas pela técnica de séries temporais e não pela técnica RNA-Perceptron, e definido por $\{(ST) - (IA) \cup (ST)\}$;
- **(**N_{ST}**):** Conjunto das anomalias identificadas pela técnica RNA-Perceptron e não pela técnica de séries temporais, e definido por $\{(IA) - (IA) \cup (ST)\}$;
- **n(X) :** Número total de Elementos definindo no conjunto (X);
- **Efetividade(X)%** $= \dfrac{n(X)}{n(AtaquesSimulados)} \times 100$

Os resultados consolidados são apresentados na Tabela 3.9 e Figura 3.27, onde se verifica que há uma identificação positiva simultânea, por ambas as técnicas de 38,48 % (trinta e oito virgula quarenta e oito por cento) das anomalias do período; considerando o conjunto total de 330 (trezentos e trinta) anomalias identificadas por ambos os métodos (n$((IA) \cup (ST))$).

Avaliando os dados obtidos para o período, encontram-se dois intervalos onde há um aumento de 20,91% (vinte virgula noventa e um por cento) na intensidade das anomalias identificadas. O primeiro intervalo é definido entre o dia 24 de julho

de 2015 e 25 de julho de 2015 a e segunda definida entre o dia 31 de julho de 2015 e 01 de agosto de 2015. Formulou-se a hipótese que os ataques do grupo de controle foram disseminados nas datas em questão. Hipótese esta que, após receber a confirmação positiva, permitiu identificar um conjunto de dez anomalias-ataques do grupo de controle, e um falso negativo. Com este resultado, consolidado na

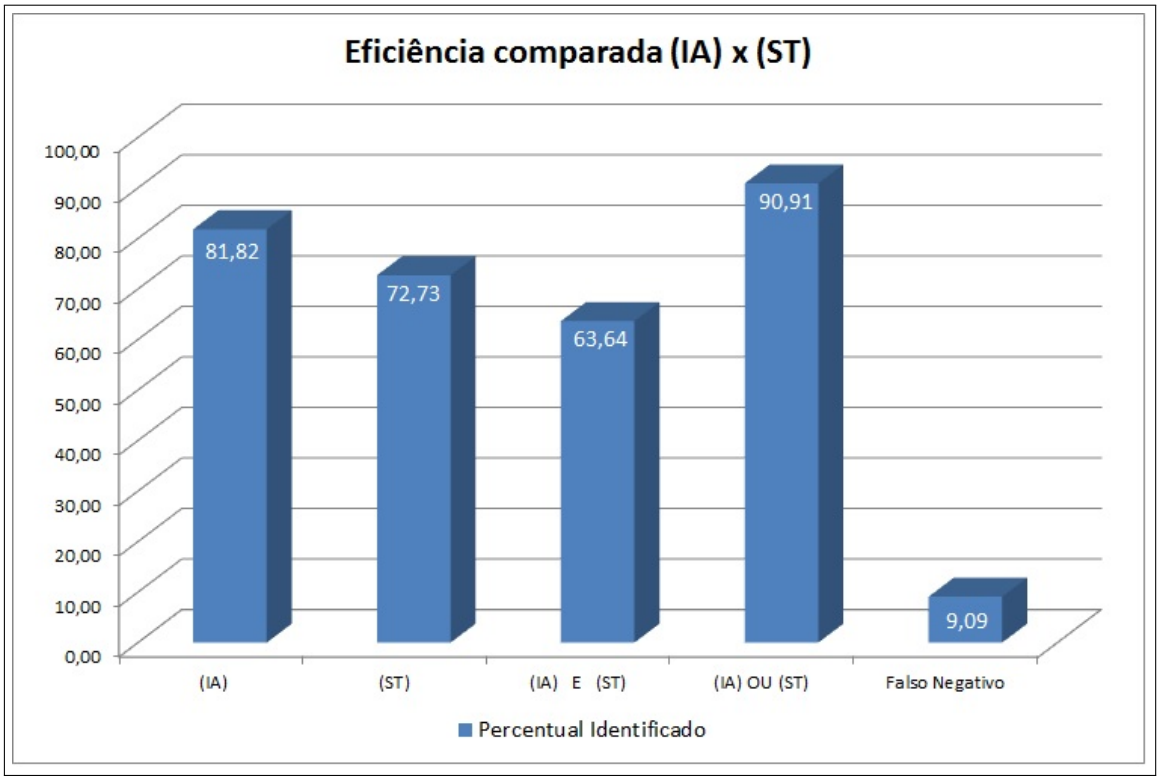

Figura 3.28: Análise Cross-Referenciada: Ataques

Tabela 3.10 e Figura 3.28, define-se a efetividade relativa de cada técnica abordada e, principalmente, valida-se a identificação de anomalias por RNA-Perceptron como uma a ferramenta eficiente que pode ser utilizada, em separado ou em conjunto, com outras técnicas de identificação de anomalias, em especial as anomalias originárias de ciberataques, ou seja, de cunho malicioso.

3.3 Ferramenta Anomalia RNA-Perceptron

Esta seção apresenta o protótipo de ferramenta de monitoramento (Figura 3.37) construída e em pleno uso pela Rede-Rio de Computadores, baseada na metodologia e resultados obtidos neste trabalho de pesquisa. Adota-se uma arquitetura modular e escalável, resumida na Figura 3.29, a qual permite a manutenção e evolução da ferramenta, conforme novos resultados forem acrescidos a esta pesquisa.

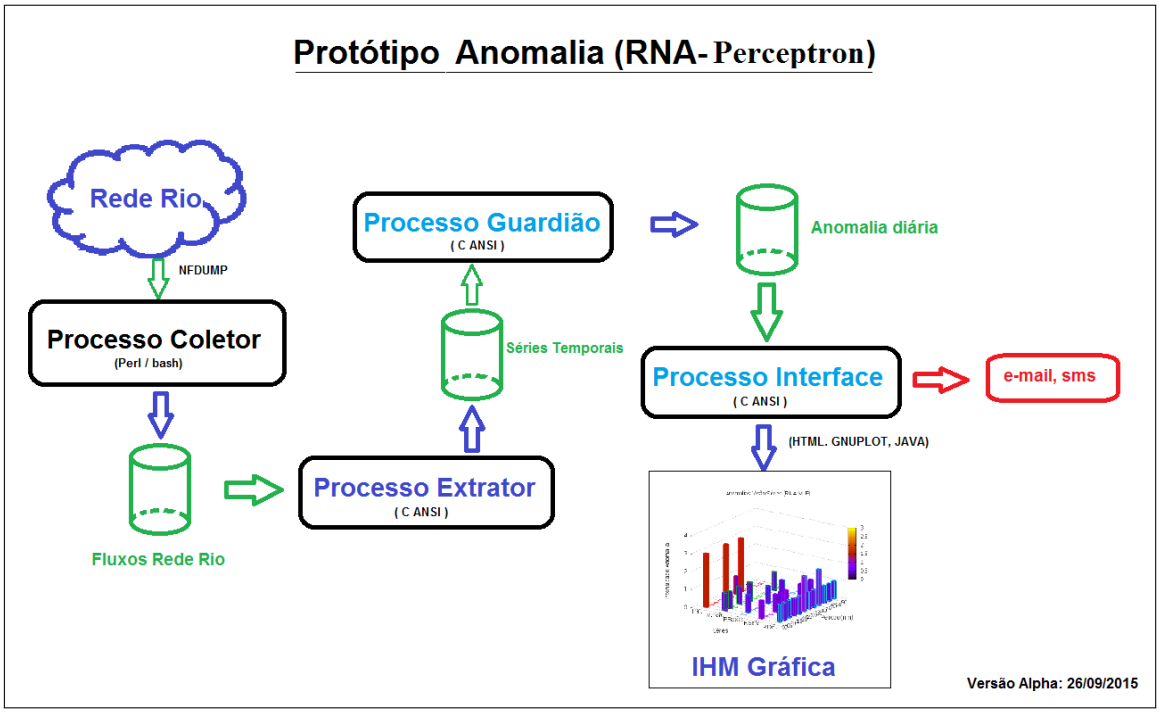

Figura 3.29: Modelo Conceitual da Ferramenta Anomalia RNA-Perceptron

3.3.1 Plataforma

A plataforma base da ferramenta aproveita os dados dos fluxos enviados pela Rede-Rio de Computadores, capturados de seu Roteador de Borda e já disponibilizados para as aplicações de **IPTRAF**[2] e **Anomalia** [ABREU (2006)]. Desta forma, foram minimizados a carga computacional de pré-processamento e armazenamento.

O código foi escrito em linguagem C ANSI adotando-se os conceitos de paralelismo de processos, o que permitirá seu porte futuro para uma plataforma que potencialize esta característica, indo além do ferramental básico oferecido pelo sistema operacional [TANENBAUM e WOODHULL (2010), KUKANOV e VOSS (2007)].

[2]Acessível em 25/10/2015 no sitio: http://iptraf.ravel.ufrj.br/

Tabela 3.11: Plataforma Anomalia RNA-Perceptron

Característica	Descrição
Software	C ANSI, PERL, GNUPLOT, HTML
Horas Codificação	198 horas (09/09/2015 à 26/09/2015)
Hardware	DELL PowerEdge T620
Processador	2 x Intel® Xeon® E5-2630 v2 2.60GHz, 15M Cache, 7.2GT/s QPI, Turbo, HT, 6C, 80W, Max Mem 1600MH, (6 cores / 12 threads)
Memória	32GB RDIMM
Disco	8 Discos rígidos de 600GB SAS, 15K RPM, 6 GBPS Hot-Plug de 3.5 Polegadas, em RAID 5, controladora H310/H710/H710P
Sistema Operacional	Ubuntu 14.04.3 LT (GNU/Linux 3.13.0-36-generic x86_64)

3.3.2 Monitoramento Exemplo

Nos gráficos seguintes, observam-se os resultados de dois períodos destacados como exemplo, o dia 13 de dezembro de 2015 às 23h 45min e o dia 14 de dezembro de 2015 às 00h 20min, onde se pode acompanhar o monitoramento da Rede-Rio de Computadores pela ferramenta de identificação de anomalias desenvolvida como parte do presente trabalho. Na Figura 3.36, apresenta-se um exemplo de *e-mail* de alerta enviado pelo protótipo.

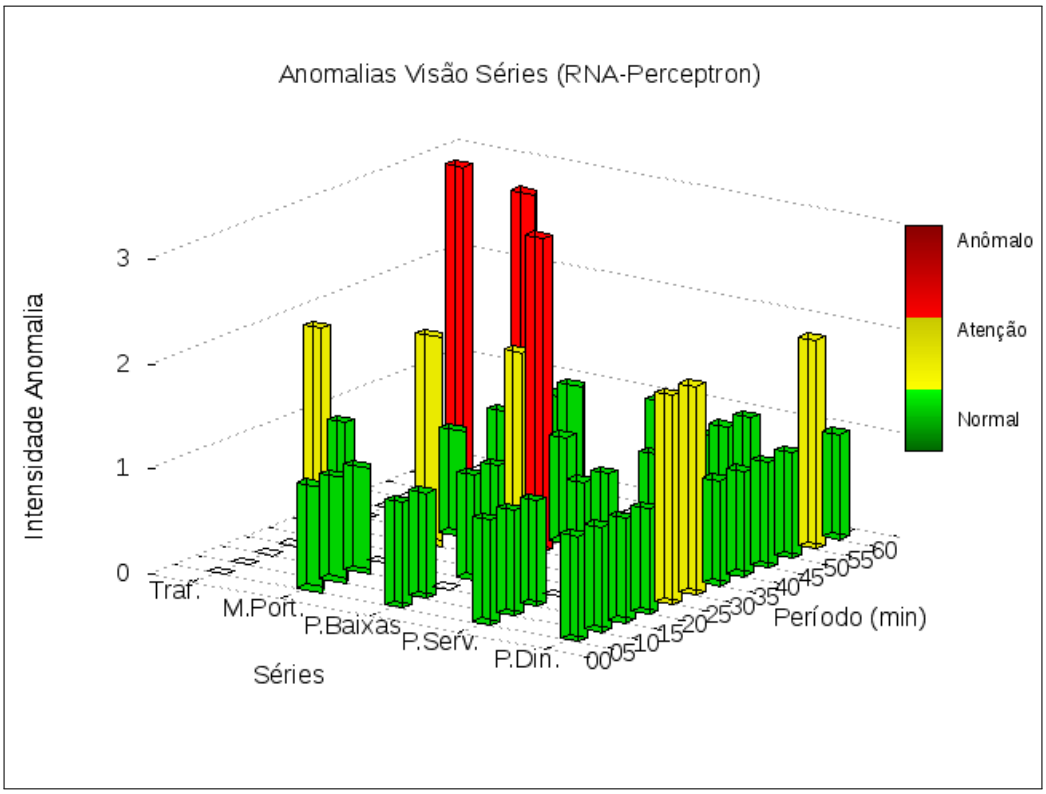

Figura 3.30: Anomalias, última hora, dia 13/12/2015 às 23h 45min

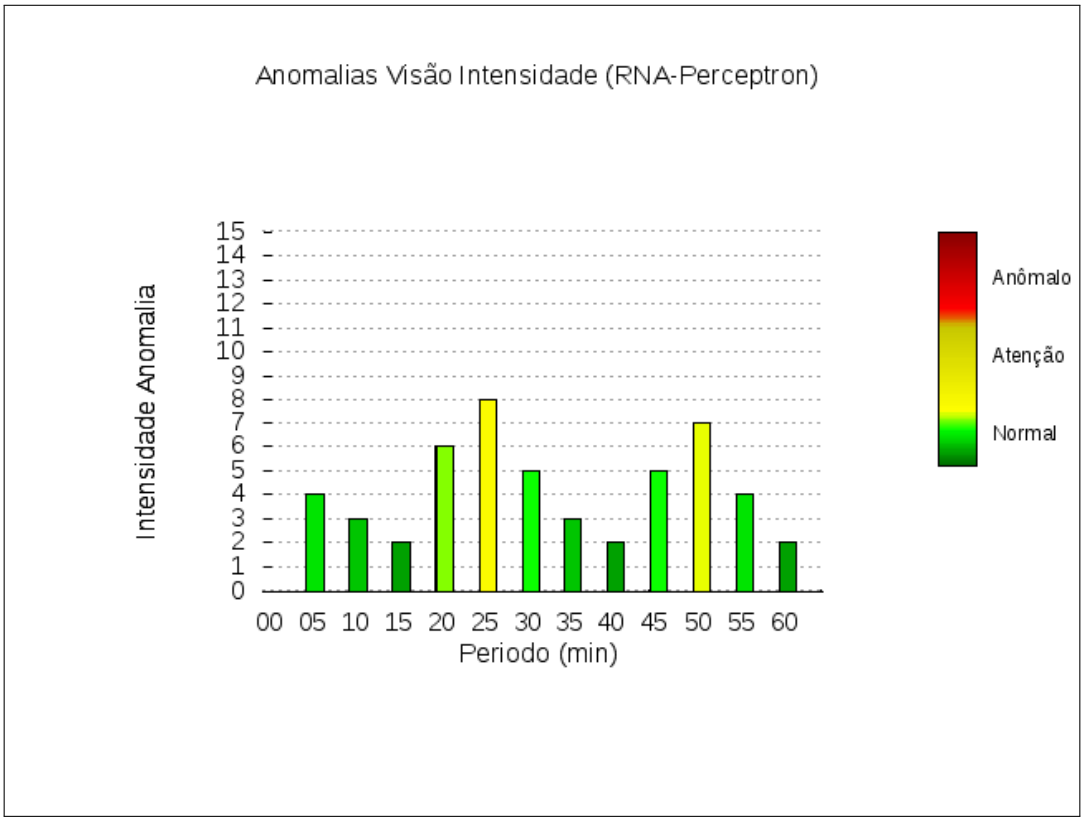

Figura 3.31: Intensidade de Anomalias, última hora, dia 13/12/2015 às 23h 45min

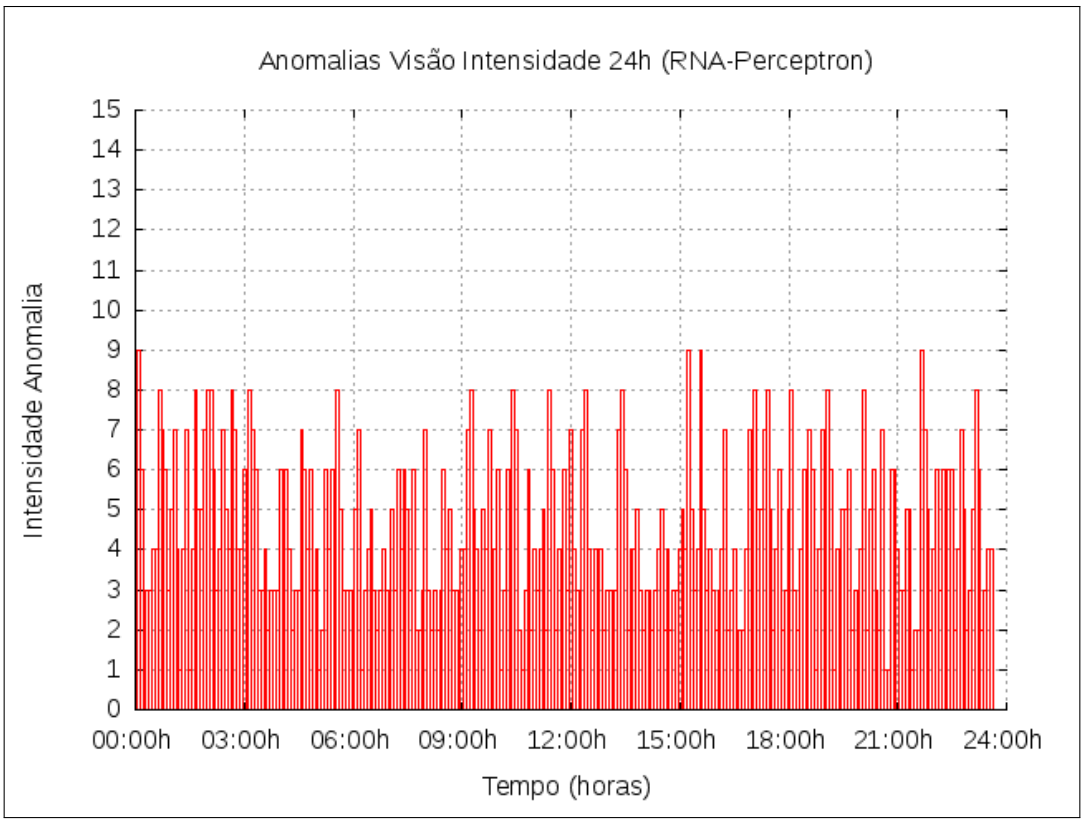

Figura 3.32: Intensidade de Anomalias em 24 horas, dia 13/12/2015 às 23h 45min

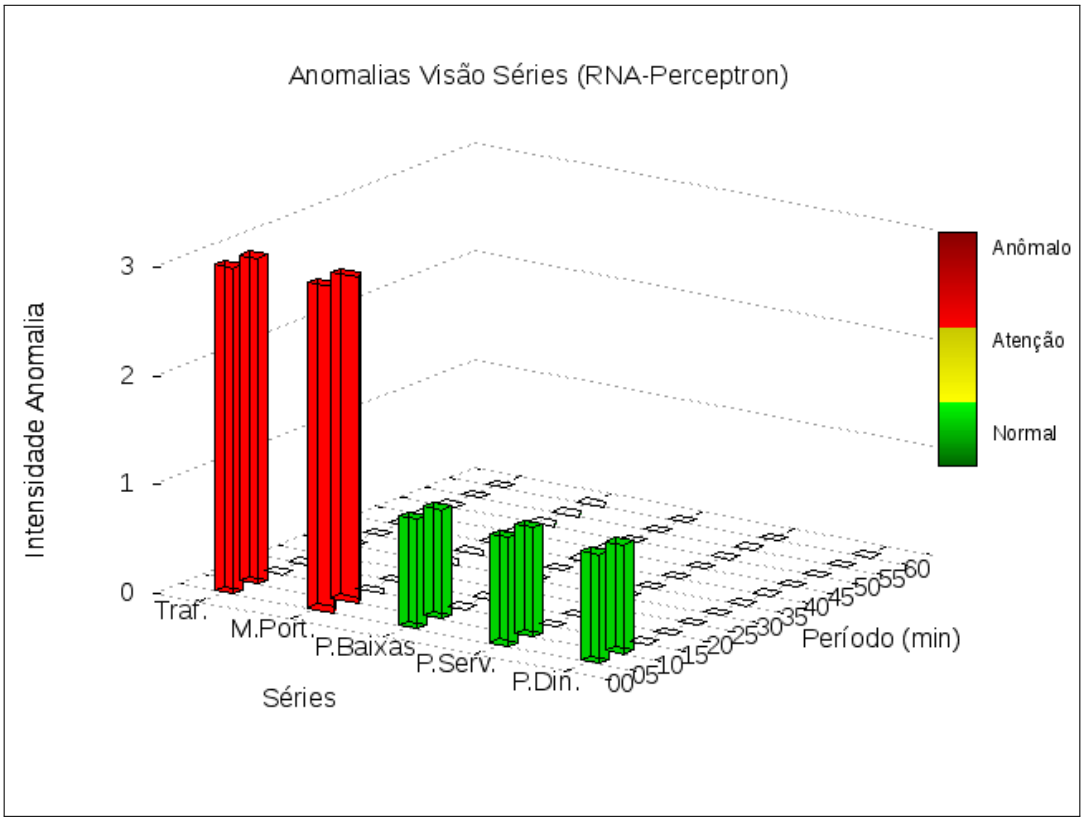

Figura 3.33: Anomalias, última hora, dia 14/12/2015 às 00h 20min

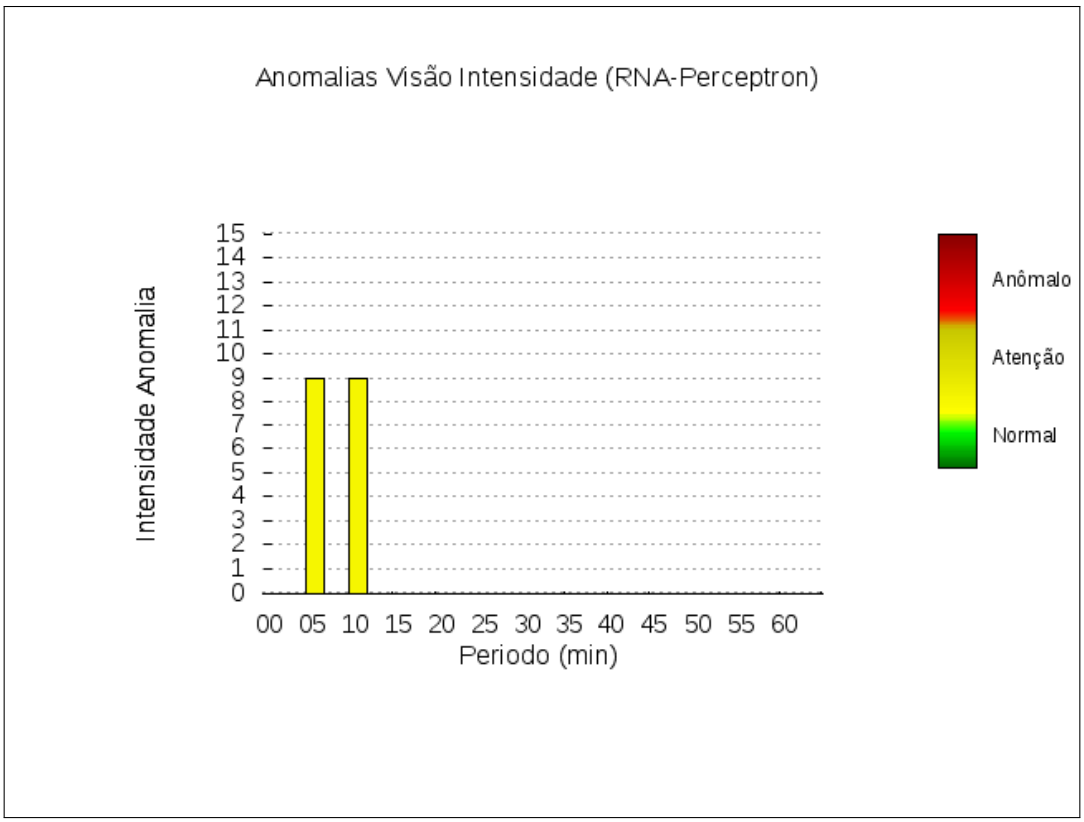

Figura 3.34: Intensidade de Anomalias, última hora, dia 14/12/2015 às 00h 20min

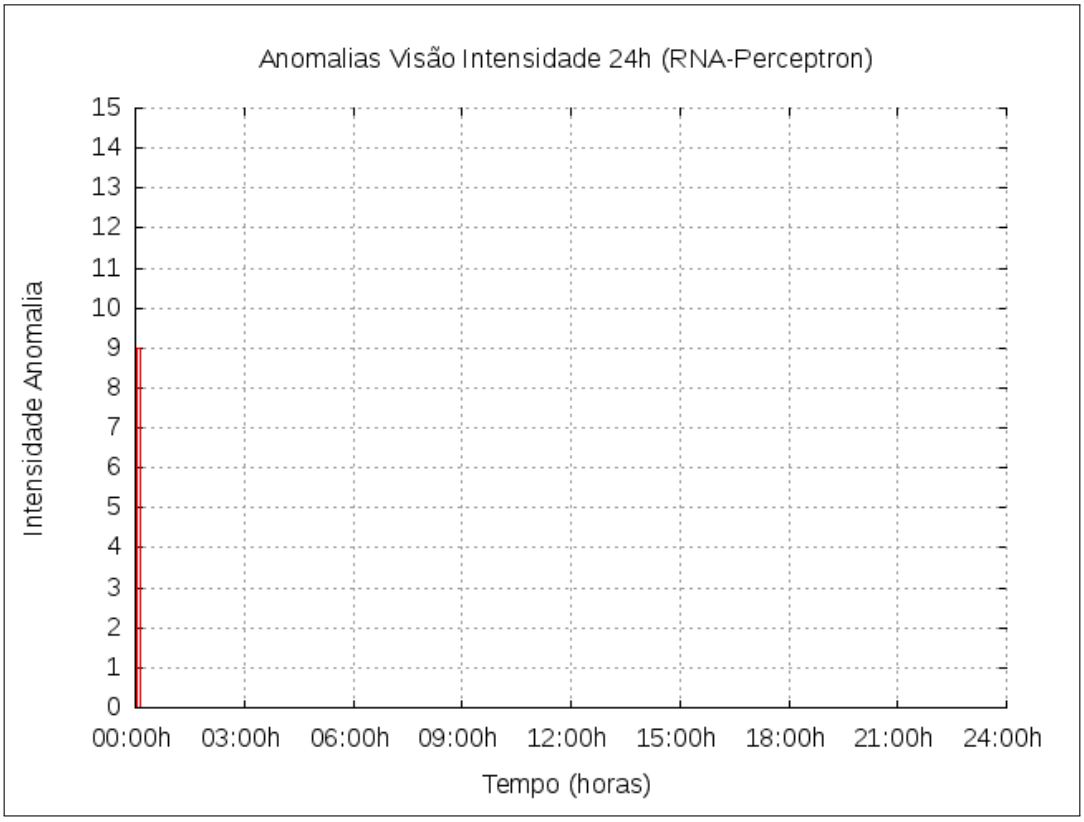

Figura 3.35: Intensidade de Anomalias em 24 horas, dia 14/12/2015 às 00h 20min

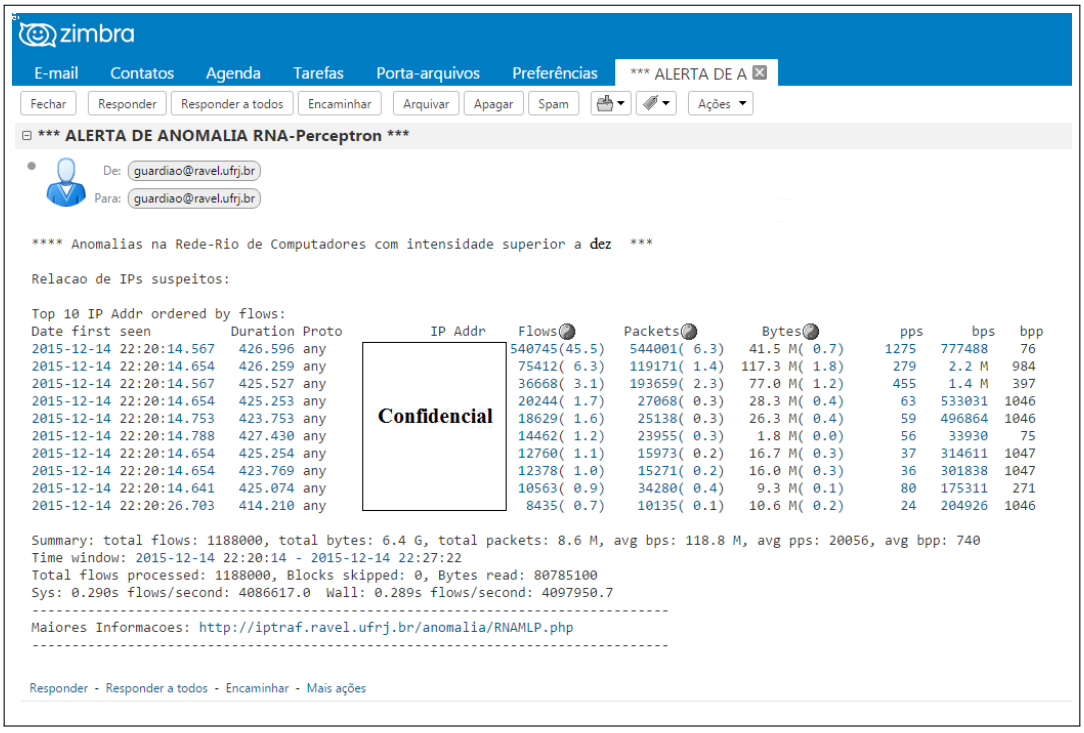

Figura 3.36: Exemplo *e-mail* de alerta de anomalia enviado

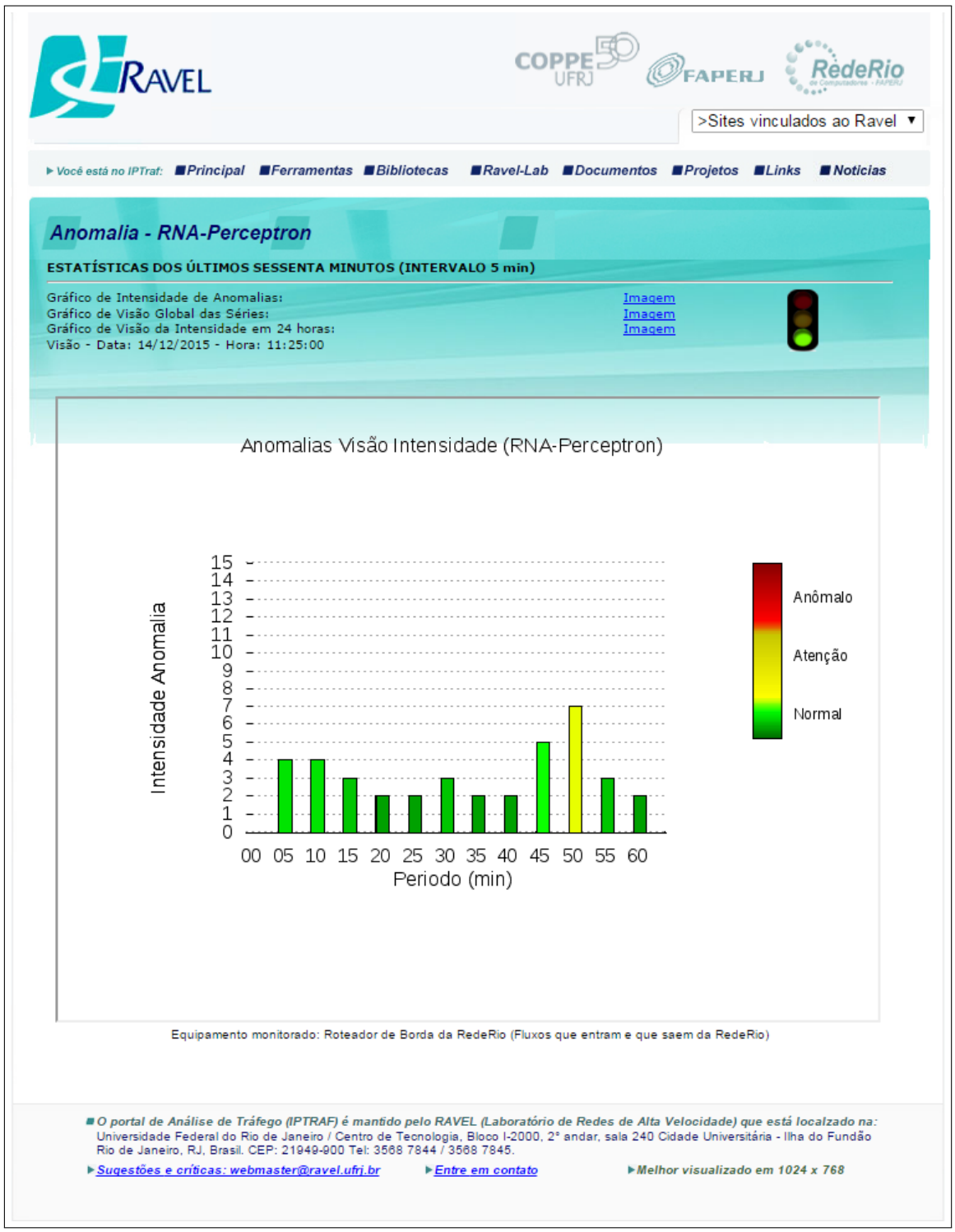

Figura 3.37: *Homepage* da Ferramenta Anomalia RNA-Perceptron

Capítulo 4

Conclusões e Perspectivas Futuras

Este trabalho teve como proposta estudar as anomalias em uma rede, baseado em cinco métricas aplicando o ferramental teórico de redes neurais artificiais e estimadores lineares.

Na construção do método de identificação de anomalias por Rede Neural Artificial (com peso), utilizou-se a metodologia definida no artigo [CELENK *et al.* (2010)], até modelo de entrada de dados, propondo uma alternativa à técnica de previsão de anomalias dos autores. No presente trabalho, a previsão é realizada através de uma RNA-Perceptron, enquanto no artigo é avaliada a entropia de séries discretas por um estimador ARMA combinado a filtros digitais. Em ambos os casos as técnicas de previsão são aplicadas a um conjunto de séries discretas, obtidas pelo particionamento de fluxos do tráfego de uma rede de computadores.

A opção em desmembrar o conjunto de fluxos que representa a série temporal de tráfego, a partir da partição destes fluxos em quatro séries distintas, permitiu aumentar a assertividade na identificação de anomalias. Como as quatro séries seguem uma classificação específica, sua observação permite uma avaliação direcionada, evitando um inter-relacionamento entre os dados quando observamos somente a série destinada ao tráfego. É importante notar que este particionamento não gerou aumento significativo na carga de processamento computacional imposta pelo método. Adicionalmente, outras formas de partições dos dados provenientes dos fluxos podem ser consideradas em estudos futuros: como exemplo inserir a visão do endereço de *IP* de origem e destino dos fluxos, e a aplicação de diferentes tipos de medidas de entropia.

Durante a pesquisa surgiram algumas dificuldades. Como exemplo a necessidade de redimensionamento do servidor utilizado na coleta, processamento, análise e visualização dos dados, em função do aumento da quantidade de fluxos oriundos do

roteador de borda da Rede-Rio de Computadores, após o aumento da capacidade dos enlaces. Esta modificação de plataforma implicou na necessidade de investir tempo adicional para adaptação da coleta dos fluxos, atividade que foi concluída em maio de 2015, limitando a quantidade de dados e nosso intervalo de análise aos meses de julho à agosto de 2015.

Como um dos pontos positivos do trabalho, destaca-se a validação experimental dos resultados da identificação RNA-Perceptron, através de grupos de controle sobre uma rede ativa, a Rede-Rio de Computadores, realizada de forma comparativa com o método desenvolvido em [DA SILVA (2015)]. Nesta avaliação, a metologia de identificação por RNA-Perceptron foi posta a prova e obteve uma efetividade de 81,82% (oitenta e um inteiros e oitenta e dois centésimos por cento) na identificação de anomalias do tipo ciberataque. Ressalva-se que este método pode trazer valores melhores se combinado com outra ferramenta. A exemplo, destaca-se a efetividade de 90,91% (noventa inteiros e noventa um centésimos por cento), quando combinadas à técnica de [DA SILVA (2015)] com o método de detecção por RNA-Perceptron, como apresentado na tabela 3.10.

Destaca-se ainda que a pesquisa, além de demonstrar a viabilidade do uso de redes neurais artificiais como ferramenta na identificação de anomalias em fluxos de redes, deixa como contribuições:

- Uma nova metodologia detecção e análise de anomalias usando Redes Neurais Artificiais (RNA-Perceptron), no âmbito do laboratório RAVEL/UFRJ;
- Modelos matemáticos de comportamento da Rede-Rio de Computadores;
- Bases de dados para análises e pesquisas futuras (tráfego, séries temporais);

Por fim, podem ser propostas as seguintes atividades que se abrem como perspectivas de pesquisas futuras ou trabalhos complementares:

- Avaliar os resultados da aplicação do método e métricas estabelecidas, em intervalo maior de dados (mínimo de um ano);
- Aplicação de outros modelos de redes neurais artificiais na identificação e classificação de anomalias, em especial modelos não lineares; comparando-se resultados, a exemplo das pesquisas de [YU (2004)], [ABRAMOVICH *et al.* (2007)] e [RAHROOH e SHEPARD (2009)];

- Avaliar a viabilidade de extensão do método para criação de uma ferramenta adaptativa, que pela redefinição dos parâmetros e re-identificação de modelos, aumentaria a robustez no processo de identificação de anomalias;

Destaca-se como contribuição para a pesquisa aplicada no âmbito do Programa de Engenharia de Sistemas e Computação do COPPE/UFRJ, a ferramenta *on-line* **Anomalia RNA-Perceptron**, implementada a partir da metodologia detalhada no presente trabalho; neste momento, plenamente funcional e monitorando as anomalias na Rede-Rio de Computadores (disponível no sitio http://iptraf.ravel.ufrj.br/anomalia/RNAMLP.php, em 04/01/2016 às 10h 45min).

Referências Bibliográficas

ABRAMOVICH, Y., SPENCER, N., TURLEY, M., 2007, "Time-Varying Autoregressive (TVAR) Models for Multiple Radar Observations", *Signal Processing, IEEE Transactions on*, v. 55, n. 4 (April), pp. 1298–1311. ISSN: 1053-587X. doi: 10.1109/TSP.2006.888064. Disponível em: <http://dx.doi.org/10.1109/TSP.2006.888064>.

ABREU, C., 2006, *Proposta e Implementação de Uma Ferramenta para Gerência de Segurança em Redes Baseada Numa Metodologia Usando Análise de Tráfego em Backbones IP*. Dissertação de mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

AGUIRRE, L. A., 2007, *Introdução à Identificação de Sistemas: Técnicas Lineares e Não-Lineares Aplicadas a Sistemas Reais*. 3 ed. Belo Horizonte, MG, Brasil, Editora UFMG. ISBN: 9788570415844.

ALEKSANDER, I., THOMAS, W., BOWDEN, P., 1984, "WISARD·a radical step forward in image recognition", *Sensor Review*, v. 4, n. 3, pp. 120–124. doi: 10.1108/eb007637. Disponível em: <http://dx.doi.org/10.1108/eb007637>.

ANDROULIDAKIS, PAPAVASSILOU, 2008, "Improving network anomaly detection via selective flow-based sampling", *Communications, IET*, v. 2, n. 3.

AUER, B., MAASS, 2001, "A regra de aprendizagem para perceptrons paralelos, do p-delta", *IEEE*.

B. WIDROW, M. L., 1990, "30 years of adaptive neural networks: Perceptron, madaline, and backpropagation", *Proc. IEEE*, v. 78, n. 9 (September), pp. 1415–1442.

BARFORD, P., KLINE, J., PLONKA, D., et al., 2002, "A Signal Analysis of Network Traffic Anomalies". In: *Proceedings of the 2Nd ACM SIGCOMM Workshop on Internet Measurment*, IMW '02, pp. 71–82, New York, NY, USA. ACM. ISBN: 1-58113-603-X. doi: 10.1145/637201.637210. Disponível em: <http://doi.acm.org/10.1145/637201.637210>.

BARTOS, K., REHAK, M., KRMICEK, V., 2011, "Optimizing flow sampling for network anomaly detection". In: *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pp. 1304–1309, July. doi: 10.1109/IWCMC.2011.5982728. Disponível em: <http://dx.doi.org/10.1109/IWCMC.2011.5982728>.

BBC-BRASIL, 2015, "Hackers roubam mais de US$ 1 bilhão em ataques a bancos", Edição do dia 16/fev/2015, capturado em 05/set/2015, Fevereiro. Disponível em: <http://bbc.in/1EH2s6i>.

CELENK, M., CONLEY, T., WILLIS, J., et al., 2010, "Predictive Network Anomaly Detection and Visualization", *Trans. Info. For. Sec.*, v. 5, n. 2 (jun), pp. 288–299. ISSN: 1556-6013. doi: 10.1109/TIFS.2010.2041808. Disponível em: <http://dx.doi.org/10.1109/TIFS.2010.2041808>.

CLAFFY, K. C., 1994, *Internet Traffic Characterization*. Tese de doutorado, Universidade da California, San Diego, CA, USA.

COTTON, M., EGGERT, L., TOUCH, J., et al., 2011, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", online, August. Disponível em: <http://www.ietf.org/rfc/rfc6335.txt>.

DA SILVA, V. L. P., 2015, *Identificacão de anomalias em fluxos de rede utilizando o método de previsão em séries temporais de Holt-Winters*. Dissertação de mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

DENNING, D. E., 1987, "An Intrusion-Detection Model". v. 13, pp. 222–232, Piscataway, NJ, USA, Feb. IEEE Press. doi: 10.1109/TSE.1987.232894. Disponível em: <http://dx.doi.org/10.1109/TSE.1987.232894>.

GARCÍA-TEODORO, P., DÍAZ-VERDEJO, J., MACIÁ-FERNÁNDEZ, G., et al., 2009, "Anomaly-based network intrusion detection: Techniques, systems and challenges", *Computers and Security*, v. 28, n. 1–2, pp. 18–28. ISSN: 0167-4048. doi: 10.1016/j.cose.2008.08.003. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404808000692>.

GOGOI, P., BHATTACHARYYA, D., BORAH, B., et al., 2011, "A Survey of Outlier Detection Methods in Network Anomaly Identification", *Comput. J.*, v. 54, n. 4 (abr.), pp. 570–588. ISSN: 0010-4620. doi: 10.1093/comjnl/bxr026. Disponível em: <http://dx.doi.org/10.1093/comjnl/bxr026>.

HAAG, P., OTHERS, 2015, "NFDUMP - Netflow processing tools", capturado em 25/out/2015, (licença: BSD License), Outubro. Disponível em: <http://sourceforge.net/projects/nfdump/>.

HAYKIN, S., 1998, *Neural Networks: A Comprehensive Foundation*. 2nd ed. Upper Saddle River, NJ, USA, Prentice Hall PTR. ISBN: 0132733501.

HE, L., YU, S., LI, M., 2008, "Anomaly Detection Based on Available Bandwidth Estimation". In: *Network and Parallel Computing, 2008. NPC 2008. IFIP International Conference on*, pp. 176–183, Oct. doi: 10.1109/NPC.2008.85. Disponível em: <http://dx.doi.org/10.1109/NPC.2008.85>.

HONG, W., ZHENGHU, G., QING, G., et al., 2008, "Detection Network Anomalies Based on Packet and Flow Analysis". In: *Networking, 2008. ICN 2008. Seventh International Conference on*, pp. 497–502, April. doi: 10.1109/ICN.2008.83. Disponível em: <http://dx.doi.org/10.1109/ICN.2008.83>.

KRISHNAMURTHY, B., SEN, S., ZHANG, Y., et al., 2003, "Sketch-based Change Detection: Methods, Evaluation, and Applications". In: *Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement*, IMC '03, pp. 234–247, New York, NY, USA, October. ACM. ISBN: 1-58113-773-7. doi: 10.1145/948205.948236. Disponível em: <http://doi.acm.org/10.1145/948205.948236>.

KRUEGEL, C., VIGNA, G., 2003, "Anomaly Detection of Web-based Attacks". In: *Proceedings of the 10th ACM Conference on Computer and Communications Security*, CCS '03, pp. 251–261, New York, NY, USA. ACM. ISBN: 1-58113-738-9. doi: 10.1145/948109.948144. Disponível em: <http://doi.acm.org/10.1145/948109.948144>.

KUKANOV, A., VOSS, M. J., 2007, "The Foundations for Scalable Multi-core Software in Intel Threading Building Blocks." *Intel Technology Journal*, v. 11, n. 4.

LATHI, B. P., 1998, *Modern Digital and Analog Communication Systems*. 3 ed. New York, NY, USA, Oxford University Press, Inc.

LEON-GARCIA, A., 1994, *Probability and Random Processes For Eletrical Engineering*. 2rd ed. Reading, MA, USA, Addison Wesley Longman (Pearson imprint). ISBN: 0321189639.

LOPES, E., BALDRATI, B., BATISTA, R., 2012, "Apagão de internet e telefonia causa transtornos na Região Sul", capturado em 04/set/2015, abril. Disponível em: <http://bit.ly/1OipXSR>.

MACEDO, E. L. C., 2015, *Previsão de Tráfego em Enlaces de Redes Utilizando Séries Temporais*. Dissertação de mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

MICHAELIS, H., WEISZFLOG, W., SILVA, A., et al., 1998, *Michaelis: moderno dicionário da língua portuguesa*. Dicionários Michaelis. São Paulo, SP, Brasil, Melhoramentos. ISBN: 9788506027592.

MINSKY, M., PAPERT, S., 1969, *Perceptrons: An Introduction to Computational Geometry*. Natick, M.I.T. Press.

NG, B., 2006, *Survey of anomaly detection methods*. Livermore, CA, USA, United States Department of Energy.

RAHROOH, A., SHEPARD, S., 2009, "Identification of nonlinear systems using {NARMAX} model", *Nonlinear Analysis: Theory, Methods And Applications*, v. 71, n. 12, pp. e1198–e1202. ISSN: 0362-546X. doi: 10.1016/j.na.2009.01.150. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0362546X09001461>.

REDERIO, 2015, "Histórico - Rede Rio de Computadores", capturado em 04/set/2015, Setembro. Disponível em: <http://www.rederio.br/site/node/3>.

SANTOS, A. F. P., 2009, *Identificação e Análise de Comportamentos Anômalos*. Tese de doutorado, LNCC, Rio de Janeiro, RJ, Brasil.

SCALASSARA, P. R., 2005, *Análise de Sinais de Ultra-som usando Decomposição Autorregressiva e Rastreamento de Polos*. Dissertação de mestrado, UEL, Londrina, PR, Brasil.

TAMURA, G., BONER, W., NACIONAL, E. J., 2015, "Criminosos invadem sistema interno de computadores de prefeituras", Edição do dia 03/set/2015, capturado em 05/set/2015, Setembro. Disponível em: <http://glo.bo/1M1yi04R>.

TANENBAUM, A. S., WOODHULL, A. S., 2010, *Operating Systems Design and Implementation*. 3 ed. New Jersey, USA, Prentice-Hall. ISBN: 9780131429383.

TÖPKE, C. R., 2001, *Uma Metodologia para Caracterização de Tráfego e Medidas de desempenho em Backbones IP*. Dissertação de mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

VILELA, G. S., 2006, *Caracterização de Tráfego Utilizando Classificação de Fluxos de Comunicação*. Dissertação de mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

VILELA, G. S., DE MORAES, L. F. M., 2005, "Caracterização de tráfego usando fluxos de comunicação." *Anais do 23º Simpósio Brasileiro de Redes de Computadores - XXIII SBRC*, (Maio). Disponível em: <http://iptraf.ravel.ufrj.br/Documentos/vilela_sbrc2005.pdf>.

WENFANG, Z., CHI, X., 2012, "Detection and Control of Anomaly Network Data Flows". In: *Computer Science Service System, 2012 International Conference on*, pp. 597–600, Aug. doi: 10.1109/CSSS.2012.154. Disponível em: <http://dx.doi.org/10.1109/CSSS.2012.154>.

YU, W., 2004, "Nonlinear system identification using discrete-time recurrent neural networks with stable learning algorithms", *Information Sciences*, v. 158, pp. 131–147. ISSN: 0020-0255. doi: 10.1016/j.ins.2003.08.002. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0020025503002032>.

ZARPELÃO, B. B., 2010, *Detecção de Anomalias em Redes de Computadores*. Tese de doutorado, UNICAMP, Campinas, SP, Brasil.

ZHANI, M., ELBIAZE, H., KAMOUN, F., 2008, "Analysis of prediction performance of training-based models using real network traffic". In: *Performance Evaluation of Computer and Telecommunication Systems, 2008. SPECTS 2008. International Symposium on*, pp. 472–479, June. Disponível em: <http://ojs.academypublisher.com/index.php/jnw/article/view/0409855865>.

Apêndice A

Manual de Usuário

Este Apêndice apresenta a versão atual do manual de usuário do sistema **Guardião**[1] , da qual a ferramenta Anomalia RNA-Percetron se configura como módulo. A versão mais atual do presente manual pode ser obtida na seção de documentos do sítio do servidor *IPTRAF* (http://iptraf.ravel.ufrj.br/).

A.1 Sistema Guardião

O sistema de identificação de anomalias Guardião é composto por dois módulos de detecção de anomalias. O primeiro módulo consiste em uma ferramenta de detecção de anomalias em redes de computadores, que se utiliza da análise de séries temporais com o método de previsão Holt-Winters [DA SILVA (2015)]. O segundo módulo é composto por uma ferramenta de detecção de anomalias utilizando Redes Neurais Artificiais (RNA-PERCEPTRON), aplicada na observação de cinco métricas analisadas a partir do tráfego de rede.

A.2 Módulo de Séries Temporais

O módulo baseado em séries temporais é fundamentado no trabalho de pesquisa de [DA SILVA (2015)], o qual aplica o método de previsão em séries temporais de Holt-Winters para realização das previsões de comportamento das métricas analisadas.

A interface gráfica Web da ferramenta desenvolvida a partir do trabalho mencionado pode ser encontrada no endereço abaixo:

http://iptraf.ravel.ufrj.br/anomalia/ANOMALIA-HW.php

[1] O presente Manual de Usuário é resultado do trabalho colaborativo de Evandro Macedo, José Barbosa da Silva Filho e Vander Proença da Silva, integrantes do laboratório RAVEL/UFRJ. Atualizado em 04 de janeiro de 2016

A interface, encontra-se dividida em duas partes. Na parte superior é possível escolher dentre as diversas séries temporais que foram processadas pelo módulo, contendo também um semáforo à direita, que representa o sistema de alarme, o qual será comentado mais adiante na seção específica (**Sistemas de alertas e alarmes**).

A parte inferior apresenta o gráfico do comportamento da série temporal referente à métrica selecionada. Neste gráfico são exibidos os dados da métrica real coletada e a aproximação calculada segundo o método aplicado pelo trabalho [DA SILVA (2015)].

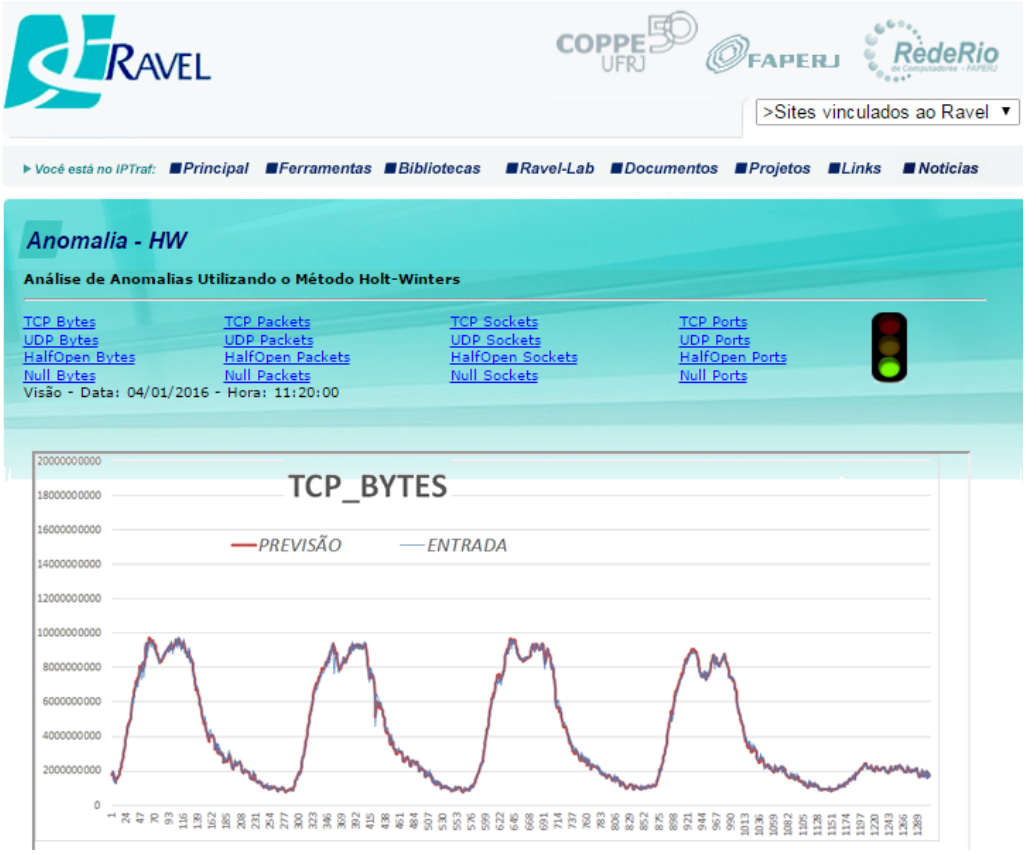

Figura A.1: Módulo Anomalia - Séries Temporais, dia 04/01/2016 às 11h 45min

A.3 Módulo de Redes Neurais

O módulo baseado em redes neurais é fundamentado no presente trabalho de dissertação, o qual aplica os conceitos de Inteligência Artificial para realização das previsões de comportamento das métricas analisadas.

No endereço abaixo, é possível encontrar a visualização do módulo de redes neurais, que também é composta de duas partes.

http://iptraf.ravel.ufrj.br/anomalia/RNAMLP.php

Na parte superior temos de igual forma o sistema de alarme, representado por um semáforo; e a seleção de três imagens (Figura A.2). Essas imagens correspondem aos gráficos de **intensidade de anomalias**, **uma visão global das séries observadas** e uma **visão da intensidade nas últimas 24 horas**. A parte inferior possui a visualização dos gráficos selecionados na parte superior.

Ao selecionar a primeira imagem, é visualizado o gráfico de intensidade de anomalias (Figura A.3), o qual fornece informações sobre o comportamento geral da rede ao longo do tempo.

Resumidamente, foram consideradas cinco métricas referentes ao comportamento da rede. É avaliada a diferença entre o comportamento do erro instantâneo e o comportamento do erro médio, definindo-se o desvio ou grau de anomalia. Este grau se encontra no intervalo de zero a três desvios padrões. Já a intensidade de anomalias é definida como a soma destes desvios para as cinco métricas analisadas, sendo subdivida nos intervalos: [0] Normal, [1-4] Moderada, [5-9] Forte e [10-15] Muito Forte.

Ao selecionar a segunda imagem se visualiza o gráfico de visão global das séries (Figura A.4), o qual informa o comportamento das séries com detalhes, para o intervalo de tempo considerado entre o instante atual até uma hora no passado. Esta imagem permite ao gestor da rede avaliar qual/quais séries estão com o comportamento anômalo, o que auxilia na tomada de decisão sobre o incidente.

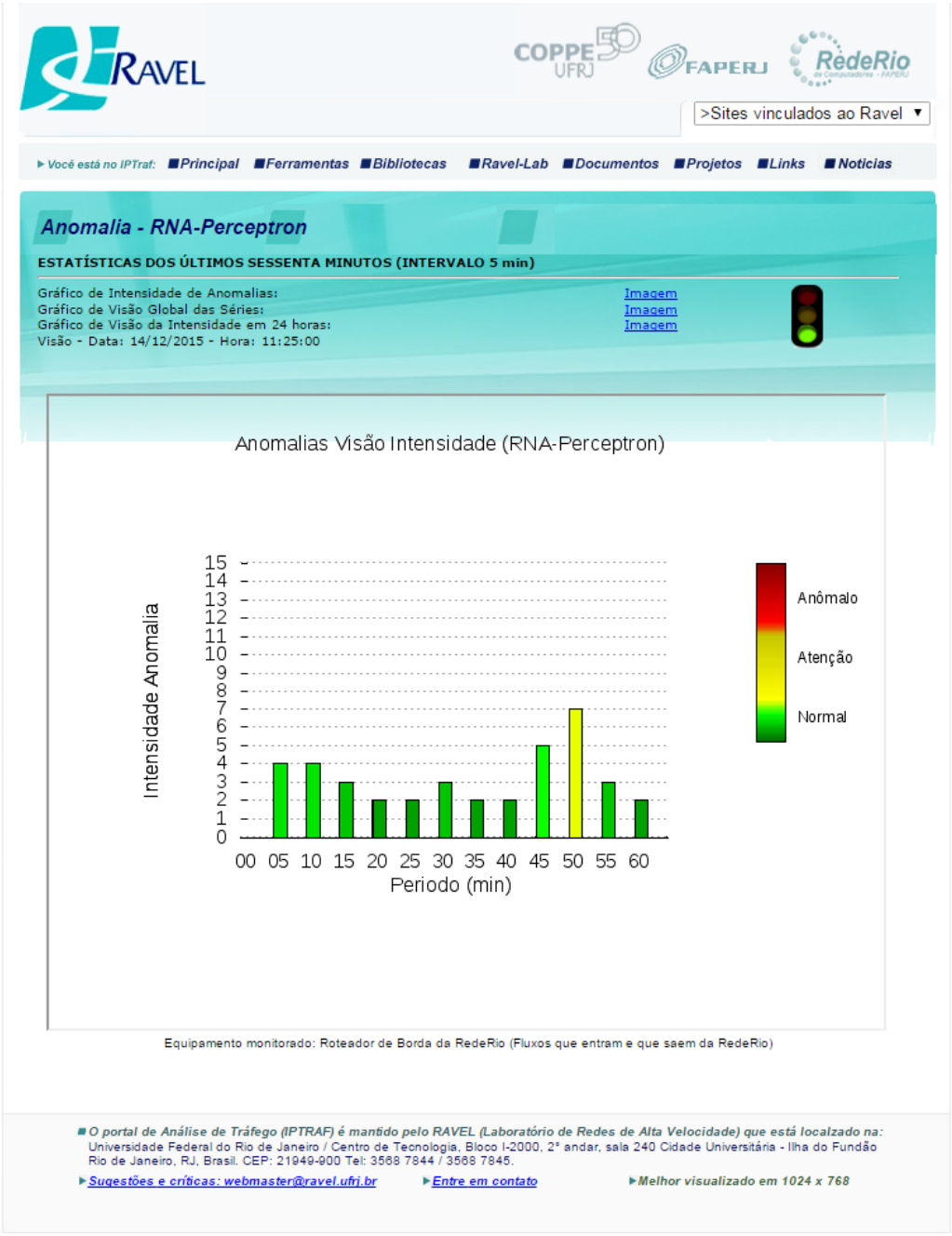

Figura A.2: Módulo Anomalia - Inteligência Artificial, dia 14/12/2015 às 11h 25min

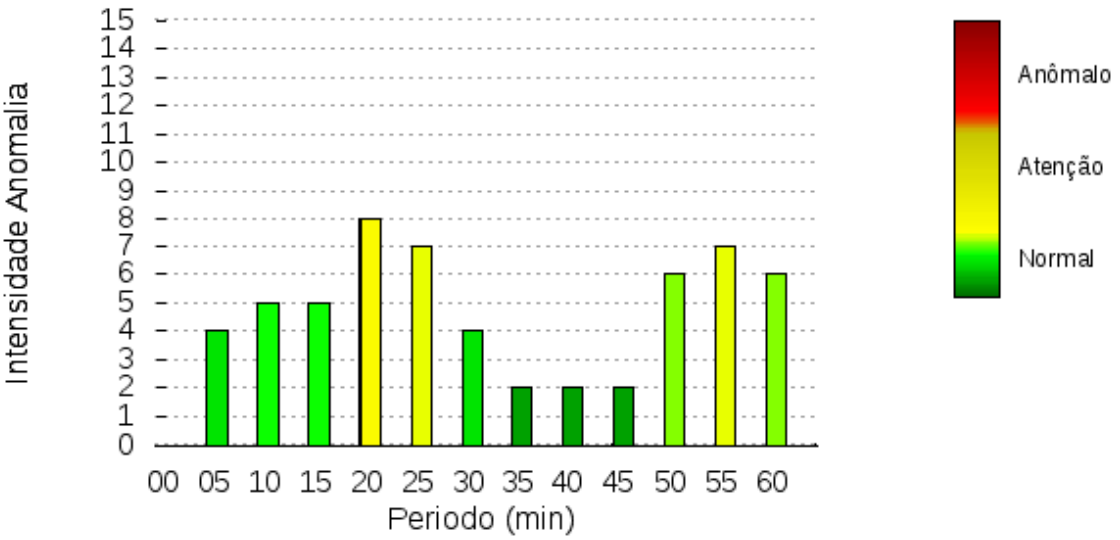

Figura A.3: Intensidade de Anomalias, dia 14/12/2015 às 11h 25min

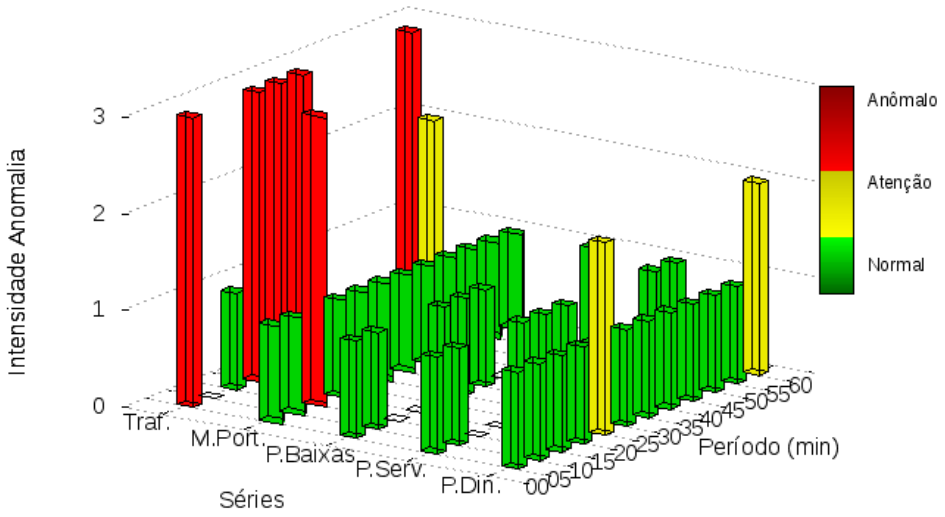

Figura A.4: Intensidade de Anomalias: por série, dia 14/12/2015 às 11h 25min

Ao selecionar a terceira imagem, é possível visualizar o gráfico de visão da intensidade em 24 horas (Figura A.5). Este gráfico apresenta um resumo da intensidade das anomalias ocorridas nas últimas 24 horas. Esta visão permite ao gestor de rede avaliar o comportamento de uma forma mais ampla, observando os momentos de maior intensidade de anomalias.

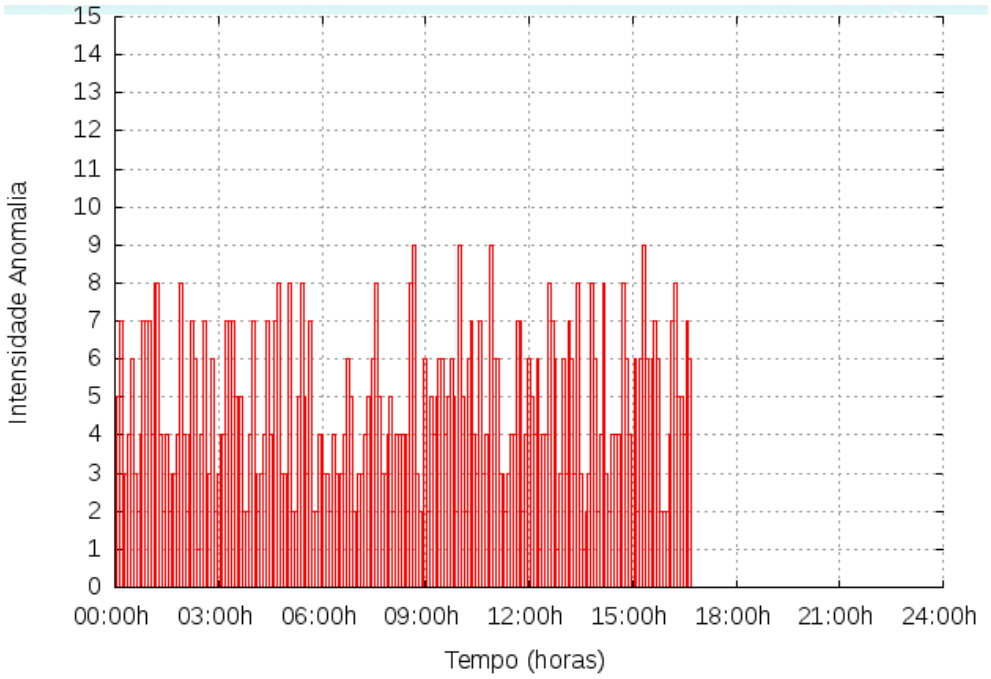

Figura A.5: Intensidade de Anomalias: últimas 24h, dia 14/12/2015 às 17h 05min

A.4 Sistema de alarmes e alertas

O sistema de alarmes e alertas é responsável por consolidar as informações provenientes dos dois módulos, permitindo assim ao operador de rede perceber de maneira rápida e simples as informações analisadas por ambos os módulos.

O sistema de alarmes possui três *status*:

- NORMAL - Representado por um semáforo verde;
- ALERTA - Representado por um semáforo amarelo;
- ALARME - Representado por um semáforo vermelho.

Quando ocorre a identificação de uma anomalia grave por um dos módulos, o sistema de alarmes e alertas é acionado, informando os operadores de rede cadastrados no sistema através de um *email/SMS* (Figura A.6) contendo as informações referentes ao alarme. Também são enviadas dados sobre alguns IP's suspeitos de serem as causas do alarme gerado.

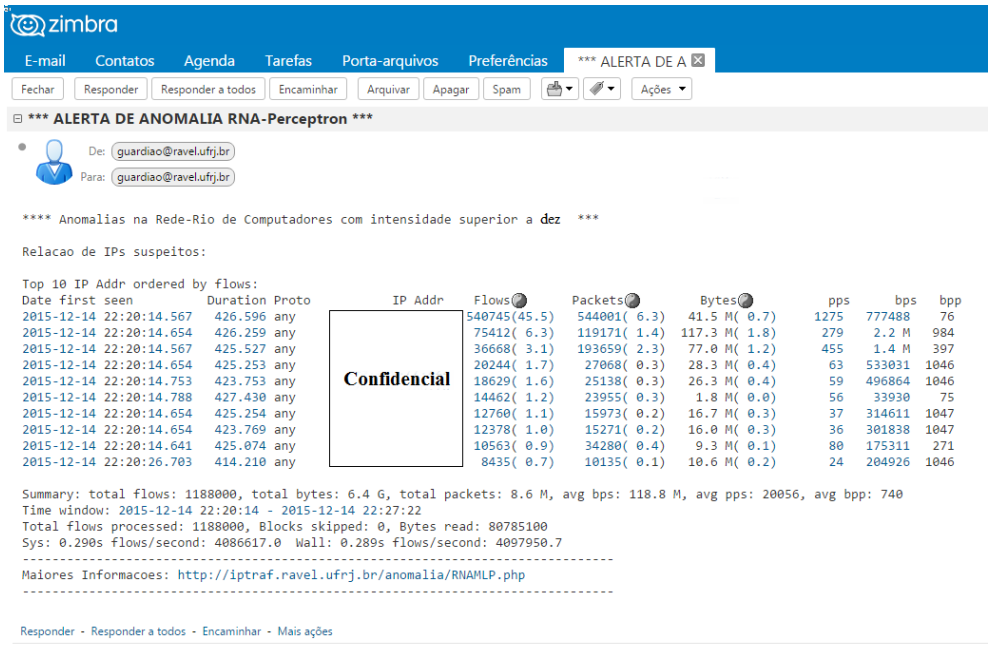

Figura A.6: Exemplo e-mail de alerta, dia 16/12/2016 às 17h 33min