SISTEMA GUARDIÃO

Manual de Usuário

Resumo

Neste documento é apresentada uma breve descrição das funcionalidades e da utilização do sistema integrado de detecção de anomalias em redes GUARDIÃO.

Versão 2.0 – 28/01/2020

Laboratório de Redes de Alta Velocidade – RAVEL/UFRJ

Sumário

Sistema Guardião

O sistema 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 baseada na análise dos fluxos de dados em séries temporais através do método de previsão de Holt-Winters. 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.

Módulo de Séries Temporais

O módulo baseado em séries temporais é fundamentado no trabalho [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 na aba de *plugins* da ferramenta de análise de fluxos.

---

http://iptraf.ravel.ufrj.br/ferramentas

A interface se encontra 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**, página 5).

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].

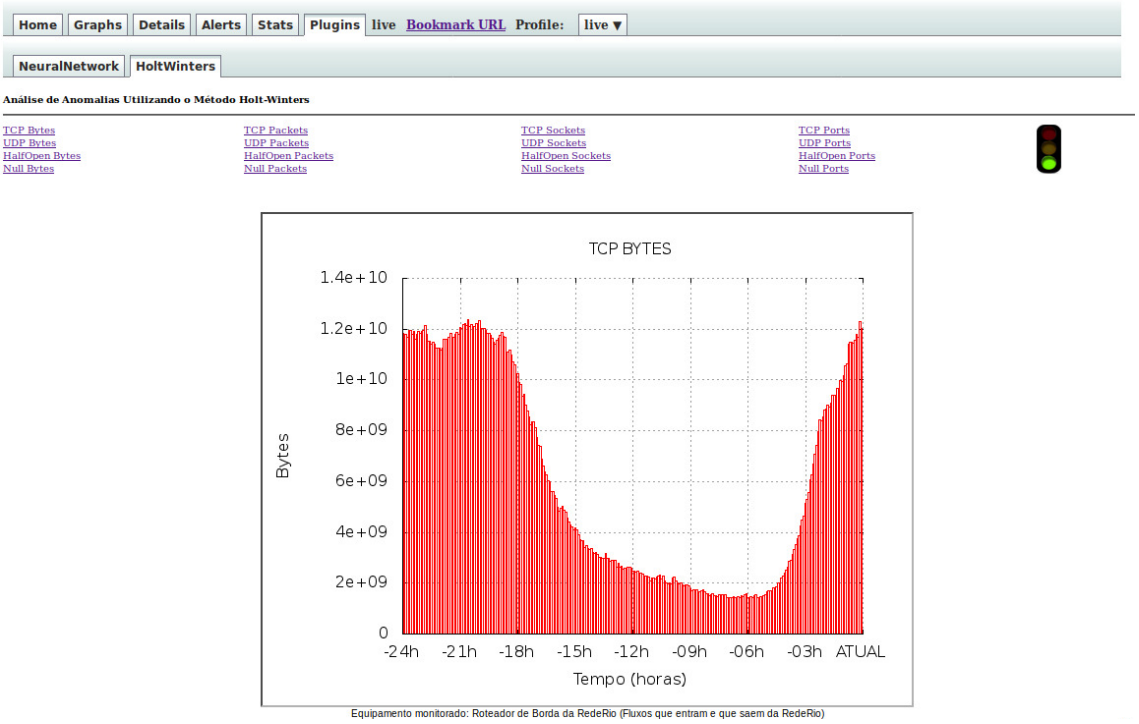


Figura 1: Interface gráfica Web do Módulo Anomalia baseado em Séries Temporais

Módulo de Redes Neurais

O módulo baseado em redes neurais é fundamentado no trabalho de [Silva Filho,2015], o qual aplica os conceitos de Inteligência Artificial para realização das previsões de comportamento das métricas analisadas.

No endereço abaixo, na aba de *plugins* da ferramenta de análise de fluxos, é possível encontrar a visualização do módulo de redes neurais, que também é composta de duas partes.

---

http://iptraf.ravel.ufrj.br/ferramentas

Na parte superior, temos de igual forma o sistema de alarme, representado por um semáforo; e a seleção de três imagens. 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.

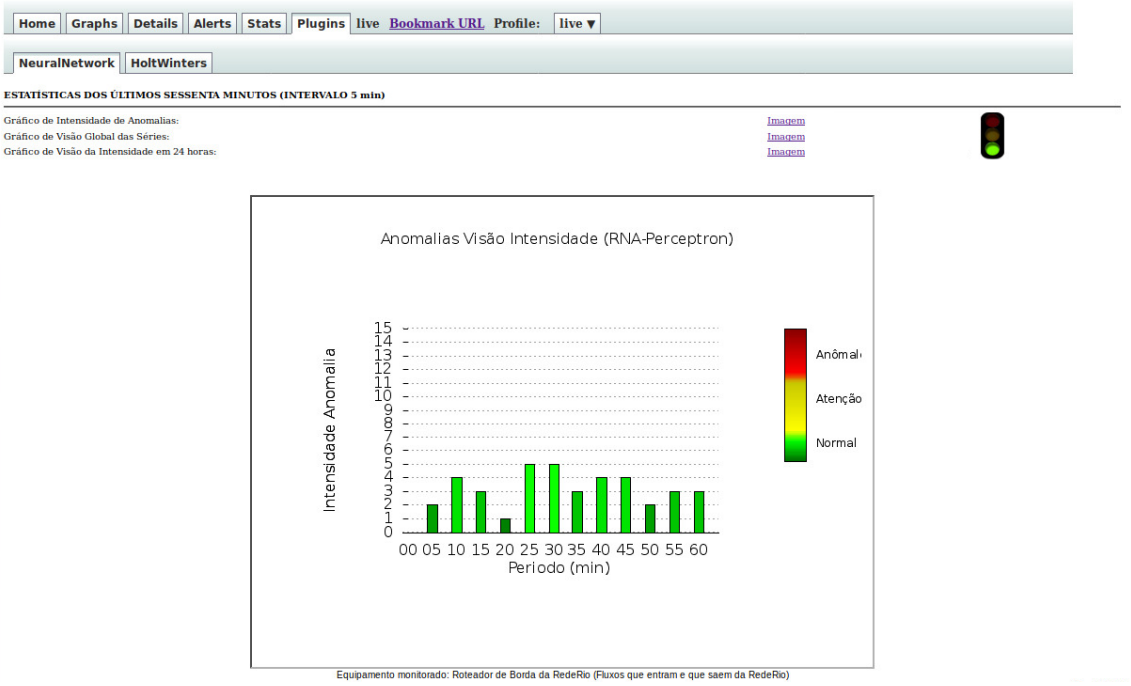


Figura 2: Interface gráfica Web do Módulo Anomalia baseado em Inteligência Artificial

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

Resumidamente, no trabalho [Silva Filho,2015] foram consideradas cinco métricas referentes ao comportamento da rede. É avaliada a diferença entre o comportamento do erro instantâneo e o comportamento 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
- [10-15] Muito Forte

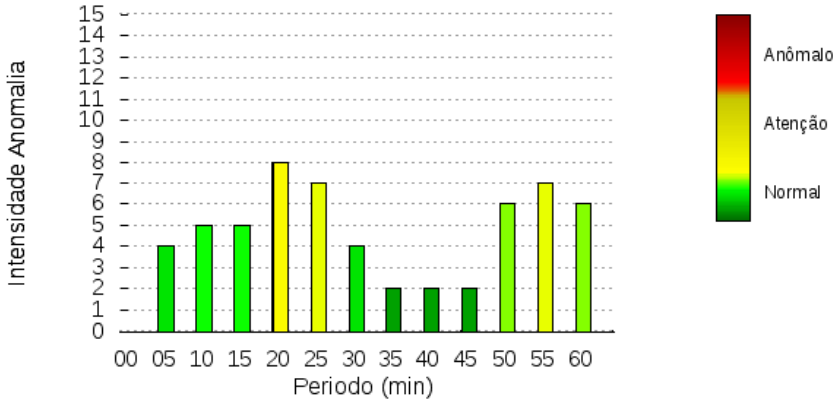


Figura 3: Exemplo de Intensidade de Anomalia com as cinco métricas acumuladas

Ao selecionar a segunda imagem, visualiza-se o gráfico de visão global das séries, o qual informa o comportamento da série 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.

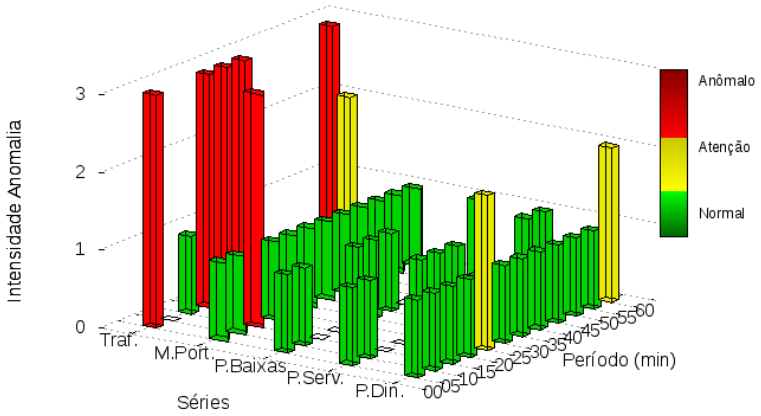


Figura 4: Exemplo de Intensidade de Anomalia para a série de cada métrica

Ao selecionar a terceira imagem, é possível visualizar o gráfico de visão da intensidade em 24 horas. 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.

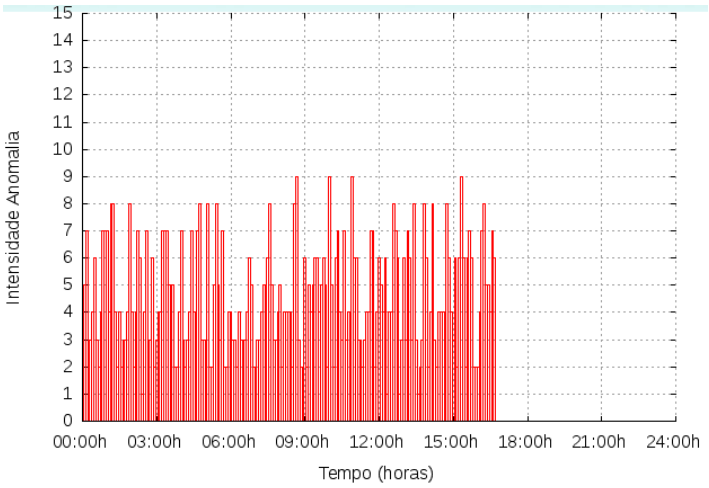


Figura 5: Exemplo Intensidade de Anomalias nas últimas 24 horas

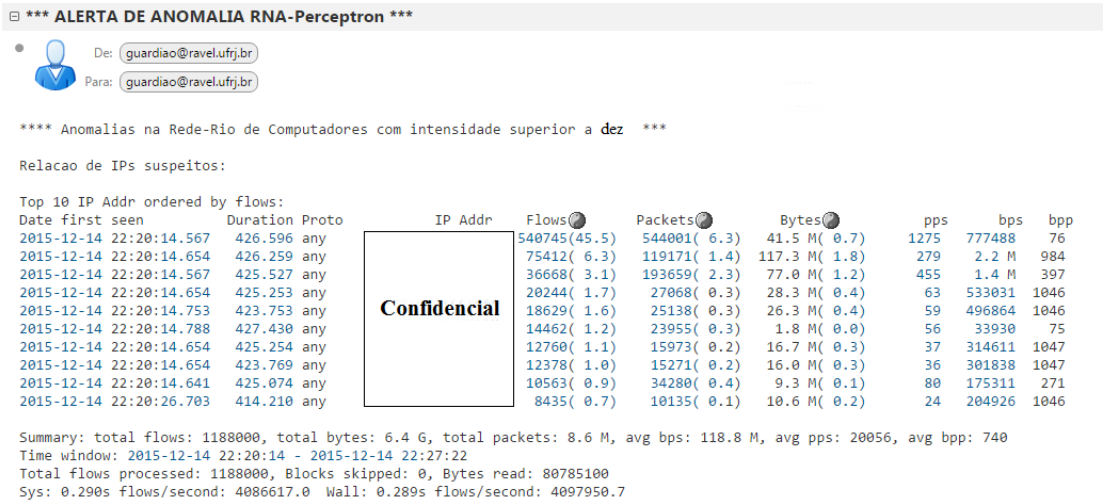
Sistema de alarmes e alertas

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 uma 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* contendo as informações referentes ao alarme. Também são enviadas informações sobre alguns IP's suspeitos de serem as causas do alarme gerado.



*** ALERTA DE ANOMALIA RNA-Perceptron ***

De: guardiao@ravel.ufrj.br
Para: guardiao@ravel.ufrj.br

**** Anomalias na Rede-Rio de Computadores com intensidade superior a dez ***

Relacao de IPs suspeitos:

Top 10 IP Addr ordered by flows:

Date first seen	Duration	Proto	IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2015-12-14 22:20:14.567	426.596	any	Confidencial	540745(45.5)	544001(6.3)	41.5 M(0.7)	1275	777488	76
2015-12-14 22:20:14.654	426.259	any		75412(6.3)	119171(1.4)	117.3 M(1.8)	279	2.2 M	984
2015-12-14 22:20:14.567	425.527	any		36668(3.1)	193659(2.3)	77.0 M(1.2)	455	1.4 M	397
2015-12-14 22:20:14.654	425.253	any		20244(1.7)	27068(0.3)	28.3 M(0.4)	63	533031	1046
2015-12-14 22:20:14.753	423.753	any		18629(1.6)	25138(0.3)	26.3 M(0.4)	59	496864	1046
2015-12-14 22:20:14.788	427.430	any		14462(1.2)	23955(0.3)	1.8 M(0.0)	56	33930	75
2015-12-14 22:20:14.654	425.254	any		12760(1.1)	15973(0.2)	16.7 M(0.3)	37	314611	1047
2015-12-14 22:20:14.654	423.769	any		12378(1.0)	15271(0.2)	16.0 M(0.3)	36	301838	1047
2015-12-14 22:20:14.641	425.074	any		10563(0.9)	34280(0.4)	9.3 M(0.1)	80	175311	271
2015-12-14 22:20:26.703	414.210	any		8435(0.7)	10135(0.1)	10.6 M(0.2)	24	204926	1046

Summary: total flows: 1188000, total bytes: 6.4 G, total packets: 8.6 M, avg bps: 118.8 M, avg pps: 20056, avg bpp: 740
Time window: 2015-12-14 22:20:14 - 2015-12-14 22:27:22
Total flows processed: 1188000, Blocks skipped: 0, Bytes read: 80785100
Sys: 0.290s flows/second: 4086617.0 Wall: 0.289s flows/second: 4097950.7

Figura 6: Exemplo e-mail de alerta enviado

Referências

DA SILVA, V. L. P., 2015, *Identificação 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.

SILVA FILHO, J. B. da, 2015, *Detecção de Anomalias em Fluxos de Redes de Computadores Utilizando Técnicas de Redes Neurais e Estimadores Lineares. Dissertação de mestrado*, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.