Detecção de Anomalias em Redes de Computadores

CONFERENCE PAPER · SEPTEMBER 2009

READS
128

6 AUTHORS, INCLUDING:

Bruno Bogaz Zarpelão
Universidade Estadual de Londrina
54 PUBLICATIONS **70** CITATIONS
SEE PROFILE

Lucas D. H. Sampaio
State University of Londrina
17 PUBLICATIONS **35** CITATIONS
SEE PROFILE

Taufik Abrao
Universidade Estadual de Londrina
177 PUBLICATIONS **413** CITATIONS
SEE PROFILE

Moisés F. Lima
Universidade Estadual de Londrina
10 PUBLICATIONS **30** CITATIONS
SEE PROFILE

Detecção de Anomalias em Redes de Computadores

Bruno B. Zarpelão, Leonardo S. Mendes, Taufik Abrão, Lucas D. H. Sampaio, Moises F. Lima e Mario L. Proença Jr.

Resumo- A detecção de anomalias é essencial para assegurar confiabilidade e segurança nas redes de computadores, que prestam serviços cada vez mais essenciais aos seus usuários. Neste trabalho é proposto um sistema de detecção de anomalias que utiliza algoritmos simples e eficientes para processar os dados coletados em diferentes objetos de gerência do protocolo SNMP *(Simple Network Management Protocol)*, e alertar o administrador de rede de maneira ágil sobre anomalias na rede monitorada. Testes foram realizados em um elemento da rede da Universidade Estadual de Londrina e os resultados foram satisfatórios.

Palavras-chave- Anomalias, GBA, Baseline, Alarmes.

Abstract- Anomaly detection is essential in order to ensure reliability and security in computer networks, which provide important services to their users. This work proposes an anomaly detection system that applies simple and efficient algorithms aiming to process the data collected in management objects of SNMP (Simple Network Management Protocol) protocol and to send alarms to the administrator signaling anomalies in the network. Tests were performed in an element from State University of Londrina network and the results were satisfactory.

Keywords- Anomalies, GBA, Baseline, Alarms.

I. INTRODUÇÃO

As tecnologias relacionadas às comunicações têm evoluído continuamente utilizando, por exemplo, redes Ethernet, redes IP, xDSL, redes sem fio, redes celular, HFC, FTTH e comunicação via satélite, para conectar computadores em diferentes lugares. Este cenário impulsiona a criação de novos negócios sobre esta malha de comunicação, principalmente sobre as redes corporativas, e conseqüentemente o desenvolvimento de novas aplicações computacionais financeiras, acadêmicas ou governamentais. Cada uma dessas aplicações trabalha com dados ou disponibiliza serviços os quais necessitam de uma garantia mínima de disponibilidade, qualidade e segurança durante suas operações [1][2].

Atualmente, estas aplicações não estão mais restritas às *intranets*, oferecendo a possibilidade de acesso remoto aos seus usuários por meio de VPNs, por exemplo, tornando estas redes mais suscetíveis a intrusões e ataques. Outro fator relevante relacionado à segurança das redes corporativas, é que freqüentemente elas estão abertas a novas conexões, a fim de disponibilizar recursos ou serviços para uma gama de usuários, entretanto devendo, proteger os recursos que são privados. Exemplos deste tipo de rede estão nas universidades, onde os alunos podem se conectar à rede da instituição, mas devem ser monitorados e possuir um acesso restrito aos recursos disponíveis por meio da mesma. Por isso, com o objetivo de complementar a segurança fornecida pelos *firewalls*, são desenvolvidos sistemas que possibilitam o monitoramento dos segmentos de rede e servidores. Eles procuram detectar, impedir e prevenir ataques na rede, sendo denominados *Intrusion Detection Systems* (IDS) [2][3].

Os IDSs presentes no mercado atual são em sua maioria baseados em assinaturas, o que os torna incapazes de detectar ataques novos ou desconhecidos, exigindo que suas bases de regras e assinaturas sejam atualizadas freqüentemente. A outra categoria de IDSs disponível inclui os sistemas baseados em detecção de anomalias. Por meio da coleta de dados de um segmento de rede ou servidor, eles modelam o seu comportamento normal, e a partir de técnicas estatísticas ou de redes neurais comparam este modelo com o tráfego real, classificando o resultado como normal ou anômalo [2][4]. Esta abordagem vem recebendo uma crescente atenção devido à sua capacidade de detectar novos ataques ou desconhecidos. No entanto, existem ainda alguns problemas em aberto, tais como as elevadas taxas de falsos positivos decorrentes da deficiência em distinguir comportamentos legítimos ou não anômalos de ataques [5].

Este trabalho apresenta um sistema de detecção de anomalias baseado em três pontos principais: (i) o modelo de caracterização de tráfego BLGBA (*Baseline* para o Gerenciamento de *Backbones* Automático) [6]; (ii) monitoramento da rede utilizando o protocolo de gerência SNMP (*Simple Network Management Protocol*) [7]; (iii) heurísticas para detecção e correlação de desvios de comportamento presentes em diferentes objetos SNMP comparados com o *baseline*.

O principal objetivo é diminuir a quantidade de dados que o administrador de rede tem de analisar, por meio de uma ferramenta simples de utilizar, que trate os dados observados sob várias perspectivas, proporcionando resultados simplificados para o administrador da rede. Para tanto, são monitorados diferentes objetos SNMP em cada segmento de rede. Os dados de cada objeto são caracterizados para formar o perfil de comportamento normal, que é comparado com os dados reais. Os desvios de comportamento identificados nos diferentes objetos SNMP são analisados em conjunto, segundo os relacionamentos existentes entre os objetos, para que seja confirmada a ocorrência da anomalia. O administrador de rede recebe um mapa da propagação da anomalia no elemento de rede, evitando que ele tenha que consultar em tempo real um grande conjunto de gráficos com dados de vários objetos de gerência.

B. B. Zarpelão e L. S. Mendes, Faculdade de Engenharia Elétrica e de Computação (FEEC), Universidade Estadual de Campinas (UNICAMP), Campinas, Brasil. E-mails: {bzarpe, lmendes}@decom.fee.unicamp.br.

M. L. Proença Jr. e M. F. Lima e Taufik A e Lucas D. H. S., Departamento de Computação, Universidade Estadual de Londrina (UEL), Londrina, Brasil. E-mails: {proenca, mflima, taufik, lucasdias}@uel.br

Este artigo está organizado da seguinte forma: Na seção 2 serão apresentados alguns trabalhos relacionados. A seção 3 detalha a proposta para detecção de anomalias. Na seção 4 são apresentados os testes realizados e os resultados obtidos. A conclusão do trabalho desenvolvido será apresentada na seção 5.

II. TRABALHOS RELACIONADOS

Vários pesquisadores tem se dedicado a propor abordagens para a detecção e a classificação de anomalias. Patcha e Min [2] apresentaram em seu trabalho um resumo contendo sistemas de detecção de anomalia e sistemas de detecção de intrusão propostos recentemente. Discutem ainda as tendências tecnológicas atuais para a detecção de anomalias e identificam os problemas e desafios abertos nesta área.

Kim e Reddy [3] propõem um sistema de detecção de anomalias que monitora os cabeçalhos dos pacotes. A abordagem utilizada consiste em monitorar o tráfego dos roteadores de saída de forma passiva em intervalos regulares . Dois tipos de mecanismos de detecção são aplicados: um *postmortem*, útil para engenharia de tráfego e análise de utilização de recursos e outro para detecção em tempo real. Os dados coletados são processados com a aplicação da transformada discreta de *wavelets*, com o objetivo de fornecer uma análise estatística eficaz. Este trabalho demonstra que a detecção baseada em perfis normais de comportamento, também utilizada em nosso trabalho, é de grande utilidade na detecção de anomalias desconhecidas. A contrário de Kim e Reddy, utilizamos dados coletados com o protocolo SNMP, que é conhecido como um padrão na gerência de redes e dispensa qualquer ferramenta específica, estando disponível em uma grande variedade de dispositivos.

He *et al.* [8] propõem uma abordagem de detecção de anomalias através do monitoramento da largura de banda disponível em *links* vitais da rede. Dentre as ferramentas existentes para detectar a largura de banda disponível, os autores utilizaram a PQLink, que ao contrário das outras ferramentas não requer acesso ao destino dos pacotes, conseguindo localizar links arbitrários e medir a disponibilidade de largura de banda. A detecção de anomalia baseada no PQLink se dá através da medição da variação da largura de banda disponível em um *link*. Através de simulações, os autores conseguiram comprovar que o PQLink é uma ferramenta estável, e que o método proposto para detecção de anomalia através da medição da largura de banda disponível em um *link* traz bons resultados. Mesmo assim, a proposta de [8] é suscetível a ocorrências de falsos positivos. Em nossa abordagem, o cruzamento de informações de diferentes objetos SNMP ajuda na verificação mais precisa da ocorrência da anomalia, evitando os falsos positivos.

Farraposo *et al.* [4] propõem um sistema que realiza o diagnóstico completo da anomalia. Além de identificar a ocorrência de uma anomalia, ele informa qual problema está ocorrendo e quais são os fluxos de tráfego responsáveis. O algoritmo se divide em três fases distintas. Na primeira, são analisadas duas janelas de dados diferentes onde busca-se detectar variações nos números medidos de pacotes, bytes e fluxos. Caso sejam identificadas variações, é aplicada a segunda fase do algoritmo, onde é realizada uma varredura em toda a rede para identificação de quais fluxos de dados são responsáveis pela anomalia. A última fase corresponde à identificação e classificação das anomalias, para as quais são criadas assinaturas. Esta abordagem, assim como a proposta em nosso trabalho, faz uso de algoritmos simples de maneira eficiente. A classificação das anomalias é baseada em assinaturas, impossibilitando a classificação de problemas ainda não cadastrados na base de conhecimento do sistema.

A proposta deste trabalho é utilizar dados coletados via protocolo SNMP para detectar anomalias. O protocolo SNMP é um padrão na gerência de redes IP, de forma que até dispositivos de rede mais simples oferecem suporte à sua utilização. Estes dados são analisados utilizando o modelo BLGBA e heurísticas, construindo uma solução amigável ao administrador de redes para o monitoramento da rede.

III. DETECÇÃO DE ANOMALIAS

Nesta seção serão detalhados os elementos do modelo proposto para detecção de anomalias. A figura 1 apresenta os elementos que compõem a solução e como eles interagem. Primeiramente, há um módulo responsável por coletar as informações das MIBs (*Management Information Bases*) e armazená-las em disco. Outro módulo fica responsável por analisar estas amostras e criar perfis de comportamento para cada dia da semana, armazenando-os em disco também. Para cada objeto SNMP analisado, há uma instância do Sistema de alarmes, que compara os dados coletados da MIB com o perfil de comportamento normal a fim de detectar desvios de comportamento. Todos os desvios de comportamento detectados são enviados para o Sistema de correlação, que os analisa decidindo se eles representam uma anomalia ou não. Caso a anomalia ocorra, um relatório é enviado ao administrador da rede.

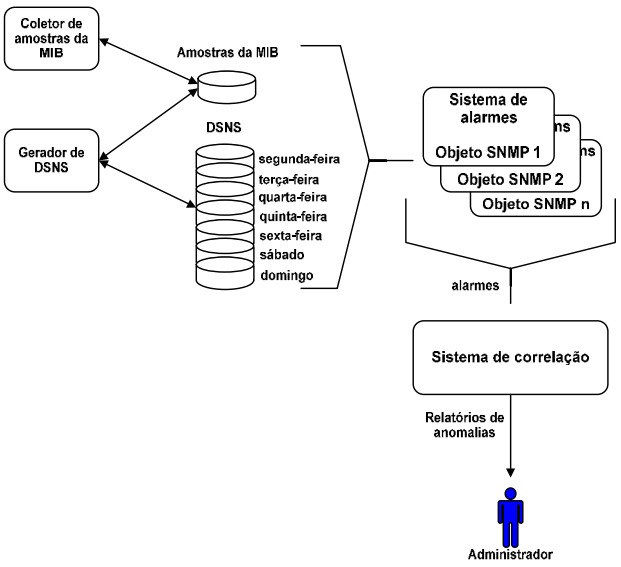

Fig. 1. Arquitetura do modelo proposto.

A. Caracterização do tráfego

O primeiro passo fundamental para que a detecção de anomalias seja realizada é definir o perfil de comportamento normal do objeto que será analisado, a partir de técnicas de caracterização de tráfego. A primeira dificuldade encontrada na caracterização do tráfego é a falta de consenso sobre qual

modelo é capaz de caracterizar o tráfego de rede de maneira eficiente. O tráfego de rede apresenta características auto-similares e um nível considerável de ruídos, além de fatores que tornam o seu comportamento dinâmico, como a variação do nível de utilização das redes em diferentes períodos do dia. Somente com o domínio do padrão de movimentação do tráfego da rede será possível realizar um diagnóstico de qualidade caso ocorram anomalias [1][6][9].

Neste trabalho, a caracterização de tráfego é realizada a partir da aplicação do modelo BLGBA no histórico de dados da rede, que resulta nos DSNS (*Digital Signature of Network Segment*). O modelo BLGBA e o DSNS foram propostos por Proença *et al.* [6]. O DSNS é o resultado da caracterização do tráfego. Ele pode ser definido como o conjunto básico de informações que constituem o perfil de operações normais dos dados observados em um objeto SNMP.

O comportamento do tráfego é formado em ciclos diários, distintos para diferentes dias da semana [10]. Esta característica se torna mais visível quando são comparados os tráfegos dos dias úteis com os fins de semana ou feriados. Os mecanismos de caracterização do tráfego devem estar preparados para lidar com estas situações. Neste trabalho, são gerados DSNS específicos para cada dia da semana, a fim de diminuir a quantidade de erros decorrentes da análise conjunta de dias com comportamentos tão diferentes como dias úteis e feriados. Além disso, cada segundo do dia também é analisado individualmente, para que o DSNS resultante respeite a variação do tráfego ao longo do dia. A coleta de dados segundo a segundo faz com que mais amostras sejam reunidas em um curto intervalo de tempo, oferecendo mais dados ao mecanismo de detecção de anomalias. Desta forma, as tomadas de decisão serão mais eficientes e ágeis. É importante observar que as coletas constantes podem causar sobrecarga na rede, e ações como separar o tráfego de gerência do restante do tráfego são importantes para garantir desempenho.

O DSNS é gerado segundo a segundo para um período de dias representado por N, que compõe o conjunto n_j, onde $j = (1, \ 2, \ \ldots, \ N)$. Cada um destes dias tem um conjunto de amostras coletadas, representadas por a_i, onde $i = (1, \ 2, \ \ldots, \ 86400)$, já que um dia tem 86400 segundos e as coletas das amostras são feitas segundo a segundo. Desta forma, os dados que formam o histórico analisado a partir da aplicação do modelo BLGBA pode ser representado por uma matriz ordenada com 86400 linhas e N colunas, como a apresentada na figura 2.

O algoritmo do BLGBA é baseado em uma variação do cálculo da moda, que leva em consideração as freqüências das classes inferiores e da classe modal. O algoritmo analisa a matriz da figura 2 linha a linha, separando os elementos em freqüências utilizando cinco classes e baseando-se na diferença entre o maior G_{aj} e o menor S_{aj} elementos de cada linha. Esta diferença dividida por 5 forma a amplitude h entre as classes, mostrada em (1):

$$h = \frac{(G_{aj} - S_{aj})}{5} \qquad (1)$$

O próximo passo é obter os limites L_{Ck} de cada uma das classes. Estes limites são calculados em (2), onde Ck representa a k-ésima classe *(k = 1...5)*.

$$L_{ck} = S_{aj} + (h * k) \qquad (2)$$

$$M_{ij} = \begin{pmatrix} a_{00001},n_1, \ a_{00001},n_2, \ \ldots, \ a_{00001},n_{n-1}, \ a_{00001},n_n \\ a_{00002},n_1, \ a_{00002},n_2, \ \ldots, \ a_{00002},n_{n-1}, \ a_{00002},n_n \\ a_{00003},n_1, \ a_{00003},n_2, \ \ldots, \ a_{00003},n_{n-1}, \ a_{00003},n_n \\ a_{00004},n_1, \ a_{00004},n_2, \ \ldots, \ a_{0004},n_{n-1}, \ a_{00004},n_n \\ \ldots \\ a_{86400},n_1, \ a_{86400},n_2, \ \ldots, \ a_{86400},n_{n-1}, \ a_{86400},n_n \end{pmatrix}$$

Fig. 2. Matriz com os dados que formam o histórico analisado para geração do DSNS.

O cálculo tem o propósito de obter o elemento que representa 80% das amostras analisadas. O Bl_i será definido como o maior elemento inserido na classe com freqüência acumulada maior ou igual a 80%. O objetivo é obter o elemento que estaria acima da maioria das amostras, respeitando o limite de 80%. A figura 3 ilustra a divisão de classes realizada pelo BLGBA para o cálculo do DSNS. O Bl_i é, portanto, o representante escolhido pelo BLGBA para cada linha analisada. Ao final da análise das 86400 linhas da matriz, temos um Bl_i para cada linha formando o DSNS resultante.

A figura 4 ilustra, na forma de histogramas, a movimentação diária para o objeto *ipInReceives* do servidor Proxy da Universidade Estadual de Londrina na semana de 29/03/2009 a 04/04/2009. Além da movimentação diária são apresentados os DSNS específicos para cada dia da semana. A movimentação real é apresentada em verde e vermelho, enquanto o DSNS é apresentado em azul. Um grande ajuste entre o tráfego real e o DSNS é observado.

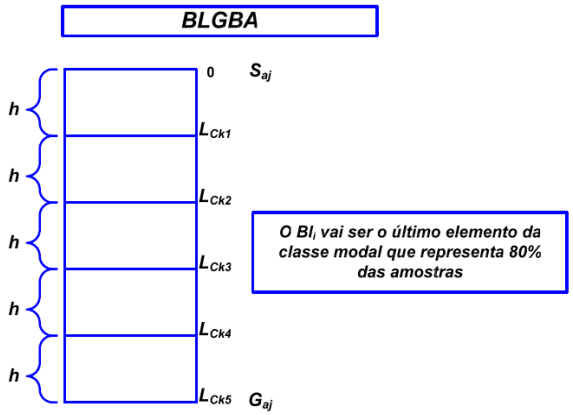

Fig. 3. Representação da divisão de classes para o calculo do DSNS.

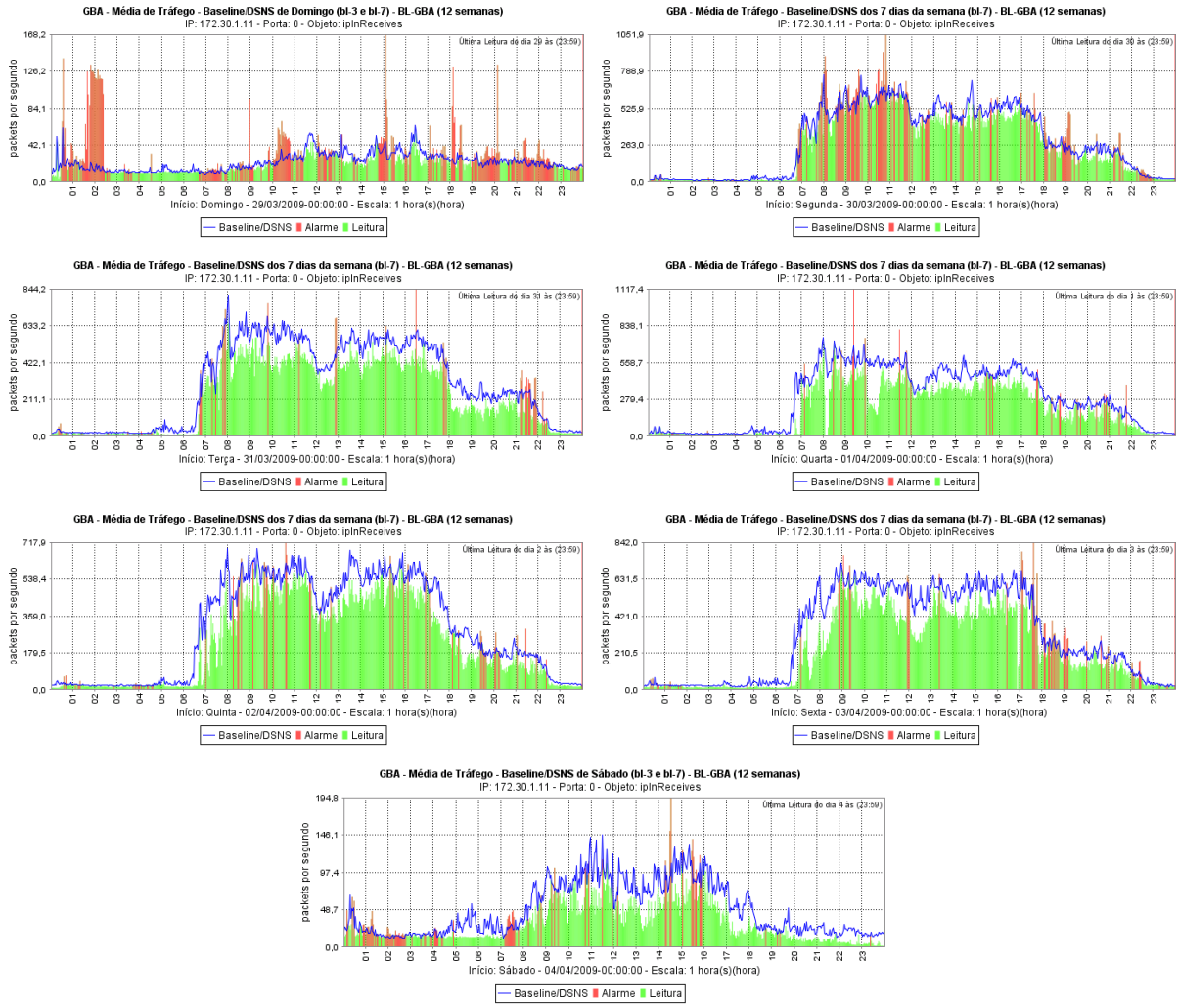

Fig. 4. Semana de tráfego no servidor Proxy, ipInReceives.

B. Sistema de Alarmes

O Sistema de alarmes é responsável por comparar os dados de um objeto SNMP ao seu respectivo DSNS, a fim de encontrar desvios de comportamento que são sinalizados por alarmes enviados ao Sistema de correlação.

O algoritmo do Sistema de alarmes é baseado no mecanismo de histerese e utiliza um parâmetro denominado δ para diminuir a possibilidade de geração de falsos positivos. A sua operação é orientada por três diferentes eventos. Inicialmente o DSNS é utilizado como limiar. Caso a leitura real tenha um valor maior que o valor respectivo do DSNS, um evento do tipo 1 é gerado. Com a identificação do evento 1, é iniciado um intervalo de tempo denominado intervalo de histerese. Neste intervalo o limiar é trabalhado de forma que seja identificada uma tendência de crescimento no trafego real analisado. Quando o evento 1 é identificado, o novo limiar passa a ser a leitura que ultrapassou o DSNS. Dentro do intervalo de histerese, toda vez que é encontrada uma leitura maior que o limiar corrente, ocorre a geração de um evento do tipo 2 e esta leitura passa a ser o novo limiar. Quando forem identificados um número de eventos 2 maior que o definido no δ dentro de um único intervalo de histerese, é gerado o evento 3 e um alarme. A figura 5 mostra o diagrama de estados que resume o funcionamento do algoritmo.

C. Sistema de correlação

O Sistema de correlação é responsável por reunir os alarmes gerados pelas diferentes instâncias do Sistema de alarmes e analisar se eles realmente estão relacionados a uma anomalia ou não.

A análise realizada é baseada em um grafo que representa as dependências entre os objetos SNMP monitorados. A forma utilizada para encontrar as relações entre os objetos SNMP foi o estudo de diagramas de Case [11]. Estes diagramas apresentam quais pontos do fluxo de dados de um elemento de rede são monitorados por cada objeto SNMP.

A figura 6 traz o grafo construído para objetos dos grupos *interface*, *ip* e *tcp* da MIB-II [12]. Cada vértice representa um objeto SNMP. No caso dos objetos *IfInOctets* e *ifOutOctets*, como há uma instância para cada *interface* monitorada no equipamento, há também um vértice para cada uma delas.

Para realizar a correlação, o monitoramento da rede é dividido em janelas fixas de cinco minutos. São analisados conjuntamente pelo Sistema de correlação os alarmes gerados dentro de uma mesma janela. Para executar a análise, é necessário definir quais objetos são possíveis pontos iniciais e finais de propagação da anomalia dentro do grafo de dependências. O algoritmo de busca em profundidade apresentado a seguir é então executado a fim de analisar os alarmes gerados em uma mesma janela de tempo para diferentes objetos SNMP.

ALGORITMO 1: BUSCA EM PROFUNDIDADE

Notação:

O_i *:* conjunto de objetos definidos como iniciais;

O_f *:* conjunto de objetos definidos como finais;

O_a: conjunto de objetos que apresentaram alarme na mesma janela de cinco minutos;

S *:* pilha utilizada na busca em profundidade

$C(o)$*:* função que retorna todos os objetos que são adjacentes ao objeto *o* e possuem alarmes gerados na mesma janela de cinco minutos que o objeto *o;*

PROGRAMA PRINCIPAL
01. INICIO
02. PARA cada $o \in (O_i \cap O_a)$ FAÇA
03. buscaProfundidade(*o*);
04. FIM PROGRAMA PRINCIPAL;
==========
05. PROCEDIMENTO buscaProfundidade(*o*)
06. INICIO
07. marcar *o* como visitado;
08. empilhar *o* em *S;*
09. SE ($o \in O_f$) ENTÃO
10. **anomalia detectada**;
11. PARA cada $(o' \in C(o))$ FAÇA
12. INICIO
13. SE *o'* não está marcado ENTÃO
14. buscaProfundidade(*o'*);
15. FIM PARA;
16. desempilhar *S*;
17. FIM PROCEDIMENTO;

IV. RESULTADOS

Testes foram realizados no servidor Proxy da Universidade Estadual de Londrina (UEL). Este elemento é responsável por intermediar o acesso de 5000 computadores da universidade à Internet, controlando o acesso a endereços não autorizados e operando como *cache* das páginas mais acessadas. Foi monitorada uma semana de tráfego, de 29/03/2009 a 04/04/2009.

Foram utilizadas duas métricas para avaliar o sistema de detecção de anomalias proposto: (i) taxa de detecção de anomalias, ou seja, de todas as anomalias ocorridas, quantas foram detectadas; (ii) a taxa de falsos positivos, definida como a razão entre a quantidade de notificações que não correspondem a uma anomalia e o total de notificações geradas.

Nos testes realizados, a taxa de detecção de anomalias foi de 78%. Em relação às notificações geradas, 13% do total delas eram falsas. Ambas as taxas obtidas são satisfatórias, principalmente pelas dificuldades existentes no período analisado. Várias anomalias foram formadas por picos de tráfego de poucos minutos, que poderiam ser facilmente confundidos com variações naturais de tráfego.

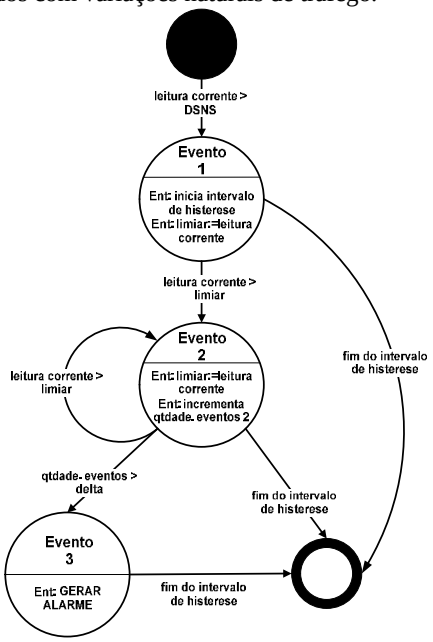

Fig. 5. Máquina de estados com algoritmo de histerese.

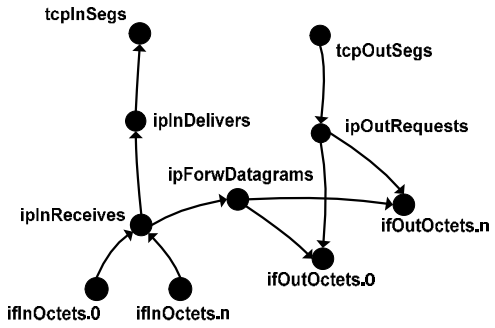

Fig. 6. Grafo com relacionamentos entre os objetos SNMP.

Analisando as anomalias detectadas no período, observa-se também que o sistema apresenta agilidade, facilitando uma ação corretiva do administrador que se antecipe à ocorrência de grandes impactos no bom funcionamento da rede.

A fim de ilustrar a operação do sistema, na figura 7 é apresentado um caso de uma anomalia identificada no dia 29/03/2009. Houve a ocorrência de um grande volume de tráfego, bem acima do previsto pelo DSNS para este horário, de maneira contínua durante 36 minutos, da 01h45 às 02h21. Antes deste período, à 01h35 se iniciaram alguns picos anormais de tráfego com durações curtas, que sinalizavam que mudanças não previstas no comportamento do tráfego poderiam ocorrer. À 01h37, o sistema de alarmes detectou a

anomalia, menos de dois minutos após o inicio dos primeiros movimentos anômalos. Foram gerados alarmes para três objetos, *ipInReceives*, *ipInDelivers* e *tcpInSegs*, definindo um caminho no grafo de dependências que levou o sistema a emitir a notificação. Outras notificações foram geradas até o fim da anomalia.

As notificações enviadas ao administrador de rede incluíram um mapa com a propagação da anomalia dentro do servidor Proxy, construído a partir dos objetos envolvidos e seus relacionamentos. Além de evitar a geração de falsos positivos, a análise realizada pelo Sistema de correlação reuniu os alertas emitidos nas perspectivas oferecidas pelo diferentes objetos SNMP monitorados, evitando que o administrador tenha que consultar gráficos com a movimentação de todos os objetos constantemente em busca de problemas.

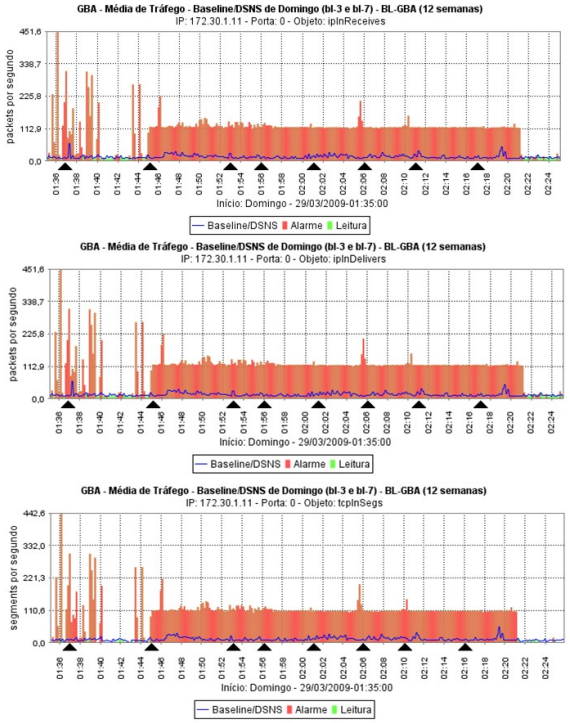

Fig. 7. Anomalia detectada no servidor Proxy em 29/03/2009.

V. CONCLUSÃO

Neste trabalho foi apresentado um sistema de detecção de anomalias que utiliza dados coletados com o protocolo SNMP, os perfis de tráfego gerados pelo modelo BLGBA e heurísticas para oferecer uma ferramenta eficiente ao administrador de rede, facilitando a sua tarefa de monitorar os servidores e segmentos em tempo real. O principal objetivo da proposta é processar os dados provenientes de vários objetos SNMP de forma a oferecer diagnósticos confiáveis sobre anomalias que estejam ocorrendo nos servidores e segmentos de rede monitorados.

Os resultados obtidos demonstram que a proposta é eficiente. É importante observar que os dados analisados apresentavam várias anomalias caracterizadas por picos curtos de tráfego, que podem ser confundidos com variações naturais de tráfego. Outro importante aspecto identificado na abordagem apresentada é a agilidade com que as anomalias foram detectadas.

Os trabalhos futuros trazem duas propostas principais. A primeira é a automatização da configuração do sistema de alarmes, visando atingir taxas passadas como objetivos pelos administradores de rede. A segunda diz respeito ao cruzamento dos diferentes mapas de propagação gerados pela ferramenta para emissão de diagnósticos sobre os problemas encontrados abrangendo a rede monitorada como um todo.

REFERÊNCIAS

[1] A. Asosheh e N. Ramezani. “A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification”. *WSEAS Transactions on Computers*, v. 7, n. 4, p. 281-290, 2008.

[2] A. Patcha e J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks*, v. 51, no. 12, p. 3448-3470, 2007.

[3] S. S. Kim e A. L. N. Reddy. “Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data”. *IEEE/ACM Transactions on Networking*, v. 16, n. 3, p. 562-575, 2008.

[4] S. Farraposo, P. Owezarski, e E. Monteiro. “A Multi-Scale Tomographic Algorithm for Detecting and Classifying Traffic Anomalies”. *Proceedings of IEEE International Conference on Communications 2007*, p. 363-370, 2007.

[5] L. Kuang e M. Zulkernine. “An anomaly intrusion detection method using the CSI-KNN algorithm”. *Proceedings of the 2008 ACM symposium on Applied computing*, p. 921-926, 2008.

[6] M. L. Proença Jr., C. Coppelmans, M. Bottoli, L. S. Mendes. “The Hurst Parameter for Digital Signature of network Segment”. *Proceedings of 11th International Conference on Telecommunications (ICT 2004)*, p. 772-781, 2004.

[7] W. Stallings *“SNMP, SNMPv2, SNMPv3, and RMON 1, 2 and 3”*. Addison-Wesley, 1998.

[8] L. He, S. Yu e M. Li. “Anomaly Detection Based on Available Bandwidth Estimation”. *Proceedings of IFIP International Conference on Network and Parallel Computing 2008*, p. 176-183, 2008.

[9] H. Hajji. “Statistical Analysis of Network Traffic for Adaptive Faults Detection”. *IEEE Transaction on Neural Networks*, v. 16, n. 5, pp. 1503-1063, 2005.

[10] P. Barford, J. Kline, D. Plonka and A. Ron, “A Signal Analysis of Network Traffic Anomalies”, *Proceedings of the ACM SIGCOMM Internet Measurement Workshop (IMW'02)*, pp. 71--82, 2002.

[11] J. D. Case and C. Partridge “Case diagrams: a first step to diagrammed Management Information Bases” *ACM SIGCOMM Computer Communication Review*, v. 19, p. 13-16, 1989.

[12] K. McCloghrie, M. Rose *“Management Information Base for Network Management of TCP/IP-based internet: MIB-II”*. RFC 1213, mar 1991.