Correlação de Objetos SNMP na Detecção de Anomalias em Servidores de Rede

Bruno B. Zarpelão[1], Leonardo S. Mendes[1], Maurício Bottoli[1], Gean D. Breda[1], Mario L. Proença Jr.[2]

Resumo **– Esse artigo apresenta um sistema de detecção de anomalias que pode ser dividido em três partes principais: (i) caracterização do tráfego usando o DSNS (*Digital Signature of Network Segment*) gerado pelo modelo BLGBA; (ii) detecção de desvios de comportamento nos objetos SNMP monitorados; (iii) correlação dos desvios de comportamento detectados para verificar a ocorrência das anomalias. Testes realizados em servidores de rede comprovaram a eficácia do sistema, demonstrando vantagens para a gerência de redes.**

Palavras-chave **– gerenciamento de redes, detecção de anomalias, alarmes, SNMP**

Abstract **– This paper presents an anomaly detection system that can be divided into three main parts: (i) traffic characterization using the DSNS (Digital Signature of Network Segment) generated by BLGBA model; (ii) detection of behavior deviations on the monitored SNMP objects; (iii) correlation of the behavior deviations detected to verify the occurrence of anomalies. Tests were realized on network servers and the system effectiviness was proved, demonstrating advantages to the network management.**

Keywords **– network management, anomaly detection, alarms, SNMP**

I. INTRODUÇÃO

Anomalias correspondem a situações atípicas onde as operações da rede se desviam de seu comportamento normal. Elas podem ser divididas em dois grupos principais: (i) O primeiro está relacionado à falhas e problemas de performance. Podem ser causados por sobrecarga a servidores de rede, mal funcionamento de equipamentos, congestionamentos, erros de softwares e de configuração (ii) O segundo inclui as anomalias relacionadas à segurança que envolvem ataques como *Denial of Service, worms* e invasões [1][6][7][13][16].

Independente do grupo ao qual a anomalia pertença, sua rápida detecção e solução interessam tanto aos administradores de rede como aos usuários finais. Sua não detecção pode ocasionar a degradação de recursos importantes ao funcionamento da rede sob o ponto de vista operacional e da qualidade dos serviços prestados [7].

A maioria das ferramentas de gerenciamento disponíveis comercialmente se limitam a apresentar os dados sobre a movimentação da rede, geralmente em forma de histogramas, que retratam o fluxo de informações de entrada e saída. Porém, elas deixam a identificação de comportamentos anômalos dependente exclusivamente dos conhecimentos empíricos adquiridos pelos administradores. As poucas ferramentas que realizam a análise sobre os dados coletados utilizam abordagens limitadas, oferecendo sistemas de alarmes simples baseados em limiares fixos pré-estabelecidos, que não se adaptam ao tráfego de redes às quais constantemente são incorporados novos serviços e usuários. Essas ferramentas detectam no máximo falhas mais graves como interrupção nos serviços de servidores e *links*, ignorando mudanças sutis em seu comportamento que, apesar de não causarem conseqüências drásticas à rede, podem implicar diretamente na confiabilidade dos serviços oferecidos [1][3][10][12][16].

O método de detecção de anomalias utilizado neste trabalho emprega uma técnica baseada na caracterização do tráfego, realizada a partir da análise estatística sobre o histórico de movimentação da rede. As anomalias são detectadas com a identificação de mudanças significativas no comportamento do tráfego monitorado, que sejam inconsistentes com o perfil de operação normal pré-estabelecido na caracterização do tráfego. As principais vantagens obtidas com o emprego desta técnica são a possibilidade de detectar anomalias desconhecidas e variantes das já conhecidas, além do fato do sistema não ficar restrito a um ambiente de rede específico [10][11].

Minimizar a geração de falsos positivos, ou alarmes falsos, é igualmente importante à rápida detecção de anomalias. Os falsos positivos, ou alarmes falsos, ocorrem quando mudanças normais no comportamento da rede são tomadas como eventos anômalos pelo sistema de detecção de anomalias. São considerados como efeito colateral da utilização de um método para detecção de anomalias. Se gerados com freqüência, os alarmes falsos podem desviar a atenção dos operadores encobrindo as notificações relacionadas a eventos verdadeiros, causando a desconfiança em relação ao sistema e fazendo com que este seja ignorado [1][5][12][13].

O tráfego de rede apresenta comportamentos diferenciados dependendo do horário do dia ou dia da semana. Normalmente, nos períodos noturnos, feriados e fins de semana, atinge níveis mais baixos quando comparados aos dias úteis e aos períodos correspondentes ao horário comercial [1][3][5][10]. É fundamental que o modelo utilizado na caracterização do tráfego seja eficiente ao prever essas mudanças de comportamento, a fim de evitar que elas

[1] Departamento de Comunicações, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, Brasil, e-mails: bzarpe@decom.fee.unicamp.br, lmendes@decom.fee.unicamp.br, bottoli@decom.fee.unicamp.br, gean@decom.fee.unicamp.br.

[2] Departamento de Computação, Universidade Estadual de Londrina, Londrina, Brasil, e-mail: proenca@uel.br.

Este trabalho foi apoiado pelo CNPq.

sejam confundidas com desvios causando a geração de falsos positivos.

A comparação entre o tráfego real e o perfil de operação normal estabelecido pela caracterização de tráfego também não é tarefa trivial. Diferentes propostas já foram apresentadas sobre quais desvios de comportamento caracterizam uma anomalia e devem ser reportados ao administrador de rede. Thottan e Ji [16] tratavam como anomalia apenas os eventos que resultavam em interrupção do serviço. Lakhina *et al.* [7] e Roughan *et al.* [13] chamaram a atenção à necessidade de detectar eventos que podem degradar a qualidade do serviço, mesmo que não haja a interrupção do mesmo. Em nosso trabalho, procuraremos alertar o administrador sobre situações que podem gerar, desde a degradação, até a interrupção dos serviços.

Um importante recurso a ser utilizado para aumentar a eficácia da detecção de anomalias é o monitoramento de diferentes objetos SNMP, procurando correlacionar os resultados obtidos nas análises realizadas em cada um deles. Dessa forma, alarmes gerados em objetos SNMP diferentes e que se refiram à mesma situação anômala, irão convergir para uma única notificação com poder semântico maior, evitando que os administradores de rede fiquem sobrecarregados por avisos redundantes [4][16].

O sistema de detecção de anomalias que desenvolvemos realiza a comparação entre o tráfego real e o perfil de operação normal esperado para o servidor ou segmento monitorado. Esta comparação é realizada dentro de um intervalo de histerese, aplicando a média dos resíduos resultantes dessa comparação na identificação de desvios de comportamento em cada objeto SNMP. Após realizada a comparação, os desvios são correlacionados para a detecção das anomalias. São apresentados resultados provenientes da aplicação desse sistema a servidores de rede da Universidade Estadual de Londrina.

Este trabalho é dividido da seguinte forma: na seção II serão apresentados alguns trabalhos relacionados à área da detecção de anomalias. A seção III descreve os servidores utilizados na obtenção dos resultados e apresenta os objetos SNMP monitorados. A seção IV trata dos conceitos acerca do modelo BLGBA e do DSNS, utilizados para a caracterização do tráfego. Na seção V será apresentado o sistema de detecção de anomalias com resultados de sua aplicação nos servidores utilizados. Por fim, na seção VI serão relacionadas algumas considerações finais e discussões sobre possíveis trabalhos futuros.

II. Trabalhos Relacionados

A necessidade de uma caracterização de tráfego eficaz para o sucesso na detecção de anomalias foi abordada por Hajji [3]. O modelo de caracterização de tráfego apresentado em seu trabalho exige que o conjunto de dados utilizado como histórico no estabelecimento do perfil de operação normal do tráfego seja puro. O modelo BLGBA, utilizado em nosso trabalho, apresenta como uma de suas vantagens a ausência de exigências desse tipo.

Como em nosso trabalho, as propriedades do protocolo de gerenciamento SNMP (*Simple Network Management Protocol*) [14] e da MIB-II (*Management Information Base*) [9] foram exploradas em [2], [8] e [16]. Cabrera *et al.* [2] apresentaram a possibilidade de se detectar ataques dos tipos *Distributed Denial of Service* utilizando dados provenientes de objetos SNMP. Li e Manikopoulos [8], por sua vez, abordaram a detecção de ataques do tipo *Denial of Service* fazendo uso de objetos SNMP. Thottan e Ji [16] utilizaram a correlação do comportamento de alguns objetos SNMP frente às anomalias para aumentar a eficácia do seu mecanismo de detecção.

Roughan *et al.* [13] trabalharam com as seguintes fontes de dados distintas: o protocolo de gerenciamento SNMP e o protocolo de roteamento BGP (*Border Gateway Protocol*). A partir da correlação entre desvios de comportamento encontrados nessas duas fontes de dados foi alcançada uma diminuição na taxa de falsos positivos.

Em [17], Wu e Zhang aplicaram a análise fatorial a um histórico do tráfego, de modo que todo o seu comportamento foi caracterizado em um pequeno conjunto de fatores formando o perfil de operação normal da rede. A comparação entre esse perfil estabelecido e o tráfego real visando a detecção de anomalias foi realizada a partir do cálculo da distância de Mahalanobis.

III. Servidores e Objetos SNMP Estudados

Com o objetivo de obter resultados concretos sobre as propostas envolvidas nesse trabalho, foi utilizado um ambiente real para testar o sistema de detecção de anomalias. Os servidores de rede da Universidade Estadual de Londrina utilizados para realização dos testes foram os seguintes:

- S_1: é o firewall da rede da Universidade Estadual de Londrina e concentra um tráfego de aproximadamente 3000 computadores para a Internet;
- S_2: é o principal servidor Web da Universidade Estadual de Londrina;
- S_3: é o servidor Proxy da Universidade Estadual de Londrina e conecta os seus 3000 computadores à Internet;

O monitoramento de um conjunto apropriado de objetos SNMP é necessário, tendo em vista a identificação de um maior número de comportamentos que as anomalias possam vir a apresentar. Neste trabalho foram escolhidos os seguintes objetos SNMP presentes na MIB-II [9]: ifInOctets (determina a quantidade de bytes recebidos por determinada interface do dispositivo monitorado), ipInReceives (determina a quantidade de pacotes IP recebidos pelo dispositivo) e o tcpInSegs (determina a quantidade de segmentos TCP recebidos pelo dispositivo).

IV. Caracterização do Tráfego: Modelo BLGBA e o DSNS

O DSNS (*Digital Signature of Network Segment*) pode ser definido como o conjunto de informações básicas que

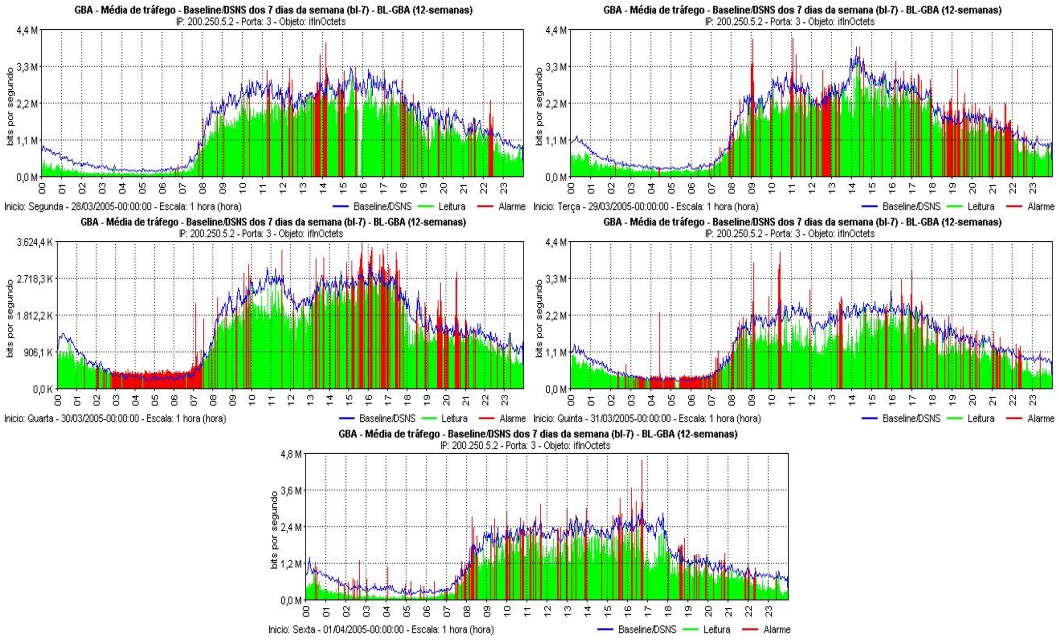

Fig. 4.1 Tráfego real e DSNS no S_1, ifInOctets

representam o perfil de operação normal do tráfego que flui por determinado servidor ou segmento de rede [10][11].

A coleta dos dados na MIB dos equipamentos de rede foi realizada pela ferramenta GBA (Gerenciamento de *Backbone* Automatizado). Ela foi escolhida por apresentar, em sua base de dados, informações relativas aos servidores da Universidade Estadual de Londrina pertencentes a um longo período, possibilitando a realização de testes em vários períodos do ano com diferentes características, como as férias escolares, por exemplo. A geração do DSNS foi baseada no modelo BLGBA, proposto por Proença *et al.* [10][11]. Esse modelo realiza uma análise estatística do histórico de dados coletados pelo GBA em um período que pode variar de 4 a 12 semanas visando a geração do DSNS. O modelo BLGBA é aplicado em coletas realizadas segundo a segundo, fazendo com que o DSNS gerado contenha uma estimativa para cada segundo de cada dia da semana, preservando as características do tráfego e sua evolução ao longo do tempo. Maiores detalhes sobre o DSNS e o modelo BLGBA podem ser encontrados em [10][11].

Com o intuito de ilustrar a utilização do DSNS gerado pelo modelo BLGBA, apresentamos a figura 4.1 que contém os dias úteis de uma semana de monitoramento do servidor S_1 com os respectivos DSNS. A linha azul nos gráficos representa os níveis de movimentação esperados a partir da estimativa encontrada no DSNS. As indicações de cor verde mostram que o tráfego real está abaixo do DSNS e as de cor vermelha significam que ele superou o DSNS, podendo representar assim um evento anômalo ou não. Ainda observando a figura 4.1, constata-se um grande ajuste entre o tráfego real e a estimativa contida no DSNS.

A figura 4.2 apresenta a variação do tráfego ao longo de um sábado no servidor S_2. O volume de tráfego é maior no início da madrugada, período destacado na figura 4.2 pela indicação (a), e após as 14h, período destacado na figura 4.2 pela indicação (b). Nestes horários, o *website* da Universidade Estadual de Londrina hospedado no servidor S_2, é mais acessado aos sábados. Foi observado que o DSNS gerado pelo modelo BLGBA prevê essas mudanças naturais na movimentação real de forma eficaz, eliminando a possibilidade de que elas sejam confundidas com desvios de comportamento.

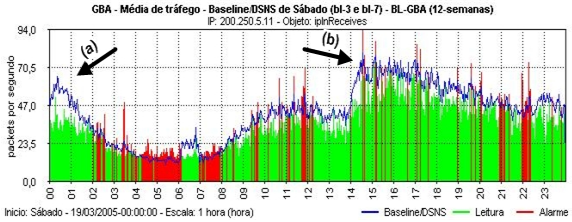

Fig. 4.2 Tráfego real e DSNS em sábado do servidor S_2, ipInReceives

V. DETECÇÃO DE ANOMALIAS

A identificação de eventos onde dados relativos à movimentação da rede estejam se desviando do comportamento normal estabelecido na caracterização de tráfego, aqui representado pelo DSNS, é um componente fundamental de um sistema de detecção de anomalias. Uma das dificuldades relacionadas a essa tarefa é que nem todos os eventos que apresentam desvio de comportamento necessitam ser reportados ao administrador de rede e cabe ao sistema de detecção de anomalias decidir quando emitir a notificação ou não.

Nosso primeiro objetivo nessa etapa do trabalho foi comparar os dados obtidos através dos objetos SNMP com os respectivos DSNS na busca por desvios significativos de comportamento. Esses desvios detectados em cada um dos objetos SNMP apresentam diferentes perspectivas sobre o evento em questão e a correlação entre eles, que é realizada

posteriormente, leva a um diagnóstico mais preciso indicando se houve ou não a anomalia.

A figura 5.1 apresenta o modelo de referência do *Sistema de detecção de anomalias*. Nele pode-se observar que a ferramenta GBA [10][11] é responsável pela coleta, armazenamento das amostras e geração dos DSNS. O *Sistema de detecção de anomalias* é formado pelo *Sistema de alarmes*, que realiza a comparação entre o tráfego real e o DSNS reportando os desvios detectados através de alarmes e pelo *Sistema de correlação*, que é encarregado de reunir esses alarmes e verificar se há correlação entre eles, com objetivo de detectar a ocorrência de uma anomalia.

O fato de vários alarmes oriundos da análise de diferentes objetos SNMP convergirem para uma única indicação de anomalia diminui a probabilidade de geração de falsos positivos e faz com que o volume de notificações referentes a cada anomalia seja bem menor, evitando que os administradores de rede fiquem sobrecarregados com avisos repetitivos.

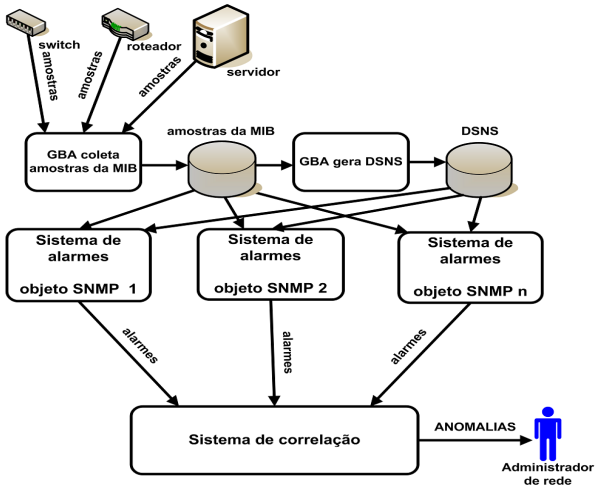

Fig. 5.1 Modelo de referência do *Sistema de detecção de anomalias*

O *Sistema de alarmes* tem por objetivo indicar a ocorrência do desvio de comportamento em um determinado objeto SNMP, gerando um alarme quando ocorrem de forma simultânea os três fatos apresentados a seguir:

- Fato 1: a amostra real analisada supera o limite estabelecido pelo DSNS.
- Fato 2: a amostra atual analisada ultrapassa a amostra anterior relativa à ocorrência do fato 1 dentro do intervalo de histerese *t*.
- Fato 3: a quantidade de ocorrências do fato 2 dentro do intervalo de histerese *t* supera o valor de $\boldsymbol{\delta}$.

A exigência da ocorrência desses três fatos para se caracterizar um desvio de comportamento significativo tem como objetivo evitar a geração de falsos positivos. Com a intenção de aumentar a confiabilidade do mecanismo, foi inserida mais uma variável ao contexto: a média dos resíduos resultantes da comparação entre a amostra real e o DSNS dentro do intervalo *t*. Na figura 5.2 é apresentado o autômato que representa o funcionamento do algoritmo empregado no *Sistema de alarmes* para identificação dos três fatos citados acima na comparação entre o tráfego real e o DSNS usando a média dos resíduos.

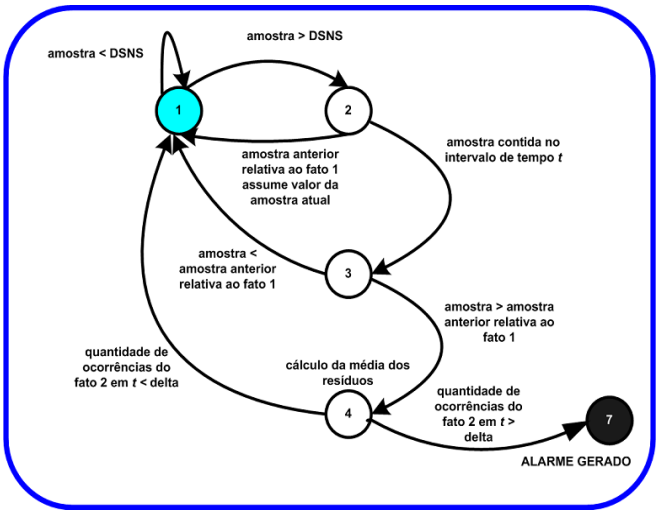

Fig. 5.2 Autômato do *Sistema de alarmes*

O intervalo de tempo *t* pode variar de 300 a 900 segundos (correspondendo a t_{min} e t_{max}, respectivamente, na fórmula (3) que será apresentada adiante). O valor de $\boldsymbol{\delta}$ se situa na faixa entre 130 e 390. Estas convenções foram definidas após grande quantidade de testes práticos e analíticos em diversas situações. Os valores dos parâmetros *t* e $\boldsymbol{\delta}$ variam conforme a média dos resíduos calculada dentro do próprio intervalo *t*, de modo que quanto menor a média do resíduo, maior será o intervalo *t* de análise e mais rígidos serão os parâmetros para geração dos alarmes. O objetivo é que o *Sistema de alarmes* analise os desvios menos incisivos por um tempo maior até se certificar que ele merece a geração de um alarme.

Os resíduos são normalizados segundo a fórmula (1), onde *amostra(i)* e *DSNS(i)* representam os valores da amostra real e o valor do DSNS respectivamente relativos ao instante *i* em que ocorre o fato 2.

$$residuo(i) = \frac{amostra(i)}{DSNS(i)} - 1 \qquad (1)$$

A média dos resíduos é calculada em cada uma das *n* ocorrências do fato 2, enquanto *n* menor que $\boldsymbol{\delta}$. A fórmula que determina a média é a seguinte:

$$media = \frac{\sum_{i=1}^{n} residuo(i)}{n} \qquad (2)$$

A fórmula (3) determina o valor do intervalo *t*:

$$t = t_{max} - \left[\left(\frac{media}{media_{max}} \right) * \left(t_{max} - t_{min} \right) \right] \qquad (3)$$

A fórmula (3) só é aplicada caso o valor de *media* seja inferior a 5 ($media_{max}$). Caso contrário, assume-se os valores mínimos possíveis para *t* e $\boldsymbol{\delta}$, que correspondem a 300 segundos e 130 respectivamente. A variação do $\boldsymbol{\delta}$ é baseada na variação de *t*.

Os alarmes gerados são enviados ao *Sistema de correlação* e não causam a notificação imediata do administrador, já que

eles não indicam a ocorrência de uma anomalia e sim de um desvio de comportamento em um objeto SNMP. Mesmo assim, a sinalização dos alarmes gerados fica disponível em arquivos de *logs* e em forma de gráficos referentes à movimentação da rede, para que os administradores possam fazer uma análise posterior mais precisa sobre os eventos ocorridos, caso seja necessário. Informações como momento de geração, quantidade e freqüência dos alarmes, valores do tráfego real e do DSNS e média dos resíduos normalizados podem ser úteis no planejamento da rede para que situações anômalas futuras passíveis de prevenção sejam evitadas.

A figura 5.3 apresenta as médias diárias de alarmes gerados pelo *Sistema de alarmes* para os servidores S_2, objetos ifInOctets, ipInReceives e tcpInSegs, e S_3, objetos ipInReceives e tcpInSegs, no último trimestre de 2004 e no primeiro trimestre de 2005.

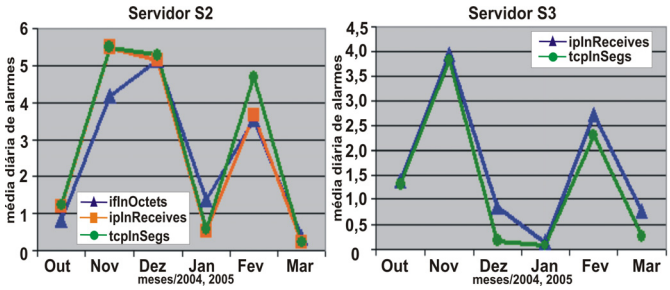

Fig. 5.3 Médias diárias de alarmes para o S_2 e o S_3

Esses gráficos mostram que as médias diárias de alarmes em diferentes objetos são semelhantes quando comparadas dentro de cada mês. No S_2, as médias do ifInOctets, do ipInReceives e do tcpInSegs são tão parecidas que as suas curvas se sobrepõe em alguns pontos do gráfico. Esses resultados indicam que os alarmes são gerados em diferentes objetos para as mesmas situações, levando à conclusão que há correlação no comportamento desses objetos frente às anomalias. Nos três servidores, constatou-se que a maioria das anomalias influencia na movimentação de pelo menos dois objetos. Esse fenômeno ocorreu principalmente nos servidores S_2 e S_3, que apresentam como característica a prestação de serviços diretos aos usuários mediante conexão TCP [15] e houve grande correlação entre o comportamento dos objetos ipInReceives e tcpInSegs. Para o S_2 em particular, o comportamento do objeto ifInOctets também apresentou correlação com o comportamento dos objetos ipInReceives e tcpInSegs. No S_1, caracterizado por prestar serviços importantes sob o ponto de vista operacional [15], há vários eventos correlacionados também, mas foi constatado que as anomalias se manifestam de maneira diferente em cada um dos objetos. Elas costumam ser mais perceptíveis no objeto ifInOctets e aparecerem de forma discreta no objeto ipInReceives.

Com base nessas conclusões, foi desenvolvida uma regra simples e eficaz de correlação dos desvios de comportamento detectados em cada um dos objetos SNMP. A anomalia é detectada quando há alarmes gerados em mais de um objeto SNMP no mesmo intervalo de tempo *t*. Essa regra também é fundamentada pelo fato de que dificilmente um falso alarme surge simultaneamente em mais de um objeto SNMP.

Na figura 5.4 são apresentados resultados provenientes da aplicação do *Sistema de detecção de anomalias* no servidor S_3 durante o mês de março de 2005. As médias diárias de alarmes para os objetos ipInReceives e tcpInSegs monitorados no servidor S_3 durante o mês de março de 2005 já havia sido apresentada na figura 5.3. Na figura 5.4 há um detalhamento dessa situação, onde são apresentados, dia a dia, os alarmes gerados pelo *Sistema de alarmes* e as notificações de anomalias realizadas pelo *Sistema de correlação*, ambos componentes do *Sistema de detecção de anomalias*. É possível observar que nos dias 2, 26, 28 e 29 alarmes foram gerados para somente um dos objetos e por isso não houve notificação de anomalia. Em geral, esses alarmes que não encontram correspondência em outro objeto SNMP dentro do mesmo intervalo de tempo são gerados para situações em que os desvios de comportamento não são relevantes e o mecanismo de correlação poupa o administrador de rede de ser notificado sobre tal situação sem importância.

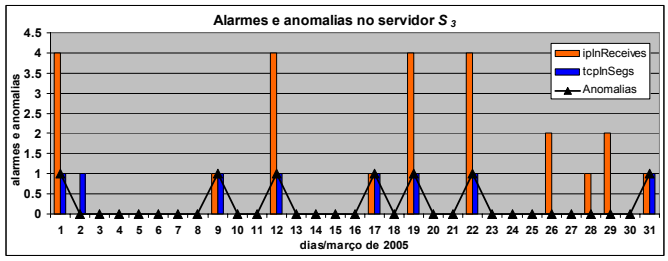

Fig. 5.4 Alarmes gerados e anomalias detectadas ao longo de março de 2005 no servidor S_3

Na figura 5.5 é mostrado um caso real de anomalia que ocorreu no servidor S_2 no dia 28/2/2005 devido à distribuição dos boletins de desempenho do vestibular 2005 da Universidade Estadual de Londrina, através do *website* da entidade, a partir das 18h. O grande número de requisições causou desvios de comportamento nos objetos ipInReceives e tcpInSegs, levando à geração de alarmes em ambos os objetos, que correlacionados resultaram na notificação relativa à anomalia.

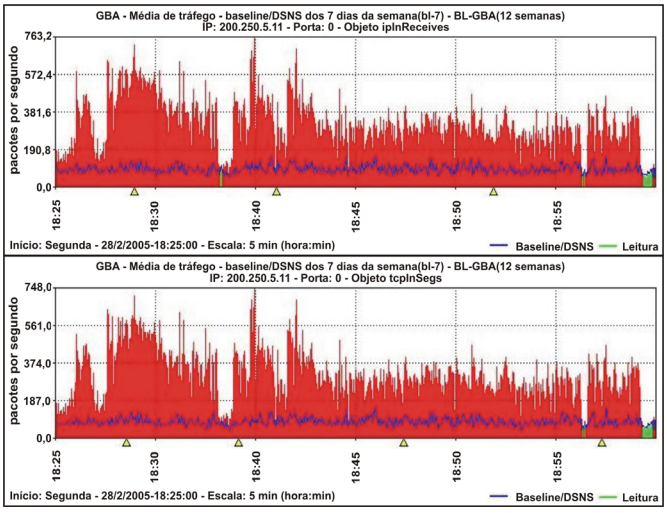

Fig. 5.5 Alarmes correlacionados e anomalia detectada no servidor S_2

Em cada um dos objetos SNMP apresentados na figura 5.5, é possível perceber a geração de alarmes apontando que havia um desvio significativo de comportamento tanto no objeto ipInReceives, como no objeto tcpInSegs. Diferenças bastante sutis entre o comportamento desses objetos frente à anomalia apresentada fizeram com que fosse gerado um alarme a mais no objeto tcpInSegs.

A anomalia começou a se intensificar por volta das 18h25 como é mostrado na figura 5.5. O *Sistema de alarmes* gerou o primeiro alarme para o objeto tcpInSegs antes das 18h30 e outro alarme para o objeto ipInReceives quase que simultaneamente. O *Sistema de correlação* recebeu esses dois alarmes gerados dentro do mesmo intervalo de tempo, aplicou a regra de correlação verificando a ocorrência da anomalia e notificou o administrador de rede. A emissão da notificação de anomalia apenas cinco minutos após o início da mesma permitiu que a busca pela solução do problema fosse providenciada rapidamente pelos administradores de rede.

VI. CONCLUSÕES

Neste trabalho pode-se confirmar novamente, assim como em [10] e [11], que os DSNS gerados pelo modelo BLGBA apresentaram bons resultados na caracterização de tráfego para objetos SNMP, cumprindo desta forma seu objetivo principal que é a criação de *baselines* para servidores e segmentos de rede. A eficácia da caracterização do tráfego é essencial para o bom desempenho do *Sistema de detecção de anomalias*, já que ela é o primeiro e fundamental passo que deve ser realizado em um sistema de detecção de anomalias.

Os alarmes gerados pelo *Sistema de alarmes* ficam disponíveis em *logs*, possibilitando que os administradores de rede examinem suas propriedades posteriormente à identificação dos desvios de comportamento. Desta forma, eles podem ser úteis na identificação de pontos críticos da rede para os quais devem ser buscadas soluções de forma a evitar a nova ocorrência de anomalias passíveis de prevenção, como por exemplo, congestionamentos advindos do excesso de carga em um servidor ou segmento.

As notificações de anomalias, emitidas pelo sistema logo após a correlação dos desvios de comportamento detectados, mostraram-se como um mecanismo fundamental na ajuda ao gerenciamento pró-ativo, permitindo que os administradores providenciem a rápida solução dos problemas e evitem que os serviços prestados pela rede sofram maiores conseqüências. A regra de correlação desenvolvida se mostrou bastante contundente para seu propósito de identificar a ocorrência de eventos correlatos em objetos SNMP, pertencentes a três diferentes grupos da MIB-II (*interface*, IP e TCP). Os resultados práticos comprovaram a sua eficácia, demonstrando ser este um caminho acertado para redução de falsos positivos.

Os trabalhos futuros incluem o aumento da variedade de objetos SNMP monitorados em cada um dos grupos da MIB-II abordados, buscando aumentar a correlação de comportamento entre eles para a diminuição dos falsos positivos. A localização da origem das anomalias, fornecendo um diagnóstico mais completo com objetivo de facilitar a determinação da causa e a solução do problema, também é outro trabalho que deve ser realizado.

REFERÊNCIAS

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

[2] J. B. D. Cabrera, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, R. K. Mehra. ***Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables – A Feasibility Study***. Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium on, p. 609-622, 14-18 maio 2001.

[3] H. Hajji ***Baselining Network Traffic and Online Faults Detection.*** IEEE International Conference on Communications, 2003 (ICC '03). v.: 1, p. 301-308, maio 2003.

[4] R. D. Gardner, D. A. Harle. ***Methods and Systems for Alarm Correlation.*** Global Telecommunications Conference, 1996 (GLOBECOM'96), v. 1, p. 136-140, nov. 1996.

[5] J. Jiang, S. Papavassiliou ***Detecting Network Attacks in the Internet via Statistical Network Traffic Normally Prediction*** Journal of Network and Systems Management, v. 12, p. 51-72, mar. 2004.

[6] B. Krishnamurthy, S. Subhabrata, Z. Zhang, Y. Chen ***Sketch-based Change Detection: Methods, Evaluation and Applications.*** Proceedings of the 3rd ACM SIGCOMM Internet Measurement Conference (IMC'03), p. 234-247, out 2003.

[7] A. Lakhina, M. Crovella, C. Diot ***Diagnosing Network-Wide Traffic Anomalies.*** ACM SIGCOMM Computer Communication Review, Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, v. 34, p. 219-230, ago 2004.

[8] J. Li, C. Manikopoulos. ***Early Statistical Anomaly Intrusion Detection of DOS Attacks Using MIB Traffic Parameters***. Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, p. 53-59, jun. 2003.

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

[10] Mario Lemes Proença Jr., C. Coppelmans, Maurício Bottoli, A. Alberti, Leonardo de Souza Mendes ***The Hurst Parameter for Digital Signature of Network Segment.*** 11th International Conference on Telecommunications (ICT 2004), 2004, Fortaleza. Springer-Verlag in the LNCS series. p. 772-781 ago 2004.

[11] Mario Lemes Proença Jr., C. Coppelmans, Maurício Bottoli, Leonardo de Souza Mendes ***Baseline to Help With Network Management***, ICETE 2004 – International Conference on E-business and Telecommunication Networks, Setubal – Portugal – 24-28 ago. 2004. Proceedings of ICETE, INSTICC Press, ISBN 972-8865-15-5, escolhido entre os best papers.

[12] X. Qin, W. Lee, L. Lewis, J.B.D. Cabrera ***Integrating Intrusion Detection and Network Management*** Network Operations and Management Symposium, 2002, p. 329-344, abril 2002

[13] M. Roughan, T. Griffin, Z. M. Mao, A. Greenberg, B. Freeman ***IP Forwarding Anomalies and Improving their Detection Using Multiple Data Sources*** Proceedings of the ACM SIGCOMM workshop on Network troubleshooting: research, theory and operations practice meet malfunctioning reality, p. 307-312, set. 2004.

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

[15] A. S. Tanembaum ***Computer Networks*** 4. ed. New Jersey: Prentice Hall, 2002.

[16] M. Thottan, C. Ji ***Anomaly Detection in IP Networks***. IEEE Transactions in Signal Processing, v. 51, n. 8, p. 2191-2204, ago. 2003

[17] N. Wu, J. Zhang ***Factor Analysis Based Anomaly Detection*** Proceedings of the 2003 IEEE, Workshop on Information Assurance, p. 108-115, jun. 2003.