Universidade Estadual de Londrina

MARCOS VINICIUS OLIVEIRA DE ASSIS

UM MODELO PARA DETECÇÃO DE ANOMALIAS QUE UTILIZA O MÉTODO DE PREVISÃO HOLT-WINTERS E ANÁLISE HEPTA-DIMENSIONAL DE FLUXOS IP

Londrina
2014

MARCOS VINICIUS OLIVEIRA DE ASSIS

UM MODELO PARA DETECÇÃO DE ANOMALIAS QUE UTILIZA O MÉTODO DE PREVISÃO HOLT-WINTERS E ANÁLISE HEPTA-DIMENSIONAL DE FLUXOS IP

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Mario Lemes Proença Jr.

Londrina
2014

Catalogação elaborada pela Divisão de Processos Técnicos da Biblioteca Central da Universidade Estadual de Londrina

Dados Internacionais de Catalogação-na-Publicação (CIP)

A848m Assis, Marcos Vinicius Oliveira de.
Um modelo para detecção de anomalias que utiliza o método de previsão Holt-Winters e análise hepta-dimensional de fluxos IP / Marcos Vinicius Oliveira de Assis. – Londrina, 2014.
129 f. : il.

Orientador: Mário Lemes Proença Junior.
Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação, 2014.
Inclui bibliografia.

1. Redes de computadores – Administração – Teses. 2. Redes de computadores – Anomalias – Teses. 3. Sistemas de transmissão de dados – Tráfego – Teses. 4. Redes de computadores – Medidas de segurança – Teses. 5. TCP/IP (Protocolo de rede de computação) – Teses. I. Proença Junior, Mário Lemes. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU 519.68.04

MARCOS VINICIUS OLIVEIRA DE ASSIS

UM MODELO PARA DETECÇÃO DE ANOMALIAS QUE UTILIZA O MÉTODO DE PREVISÃO HOLT-WINTERS E ANÁLISE HEPTA-DIMENSIONAL DE FLUXOS IP

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

_____

Prof. Dr. Mario Lemes Proença Jr
UEL – Londrina - PR

_____

Prof. Dr. Bruno Bogaz Zarpelão
UEL – Londrina - PR

_____

Prof. Dr. Sylvio Barbon Junior
UEL – Londrina - PR

_____

Prof. Dr. José Valdeni de Lima
UFRGS – Porto Alegre - RS

Londrina, 24 de fevereito de 2014.

Dedico este trabalho à toda minha família, por seu apoio, compreensão e incentivo incondicional em todos os momentos de minha vida; e a todos aqueles que visam o aperfeiçoamento pessoal por meio do conhecimento em qualquer área.

AGRADECIMENTOS

Agradeço primeiramente à Deus pela vida, por sempre me guiar em seus caminhos, pelos desafios que me foram proporcionados, pela força em mim despertada e pelas bençãos a mim direcionadas. Sem Ele nada disso seria possível.

Ao meu orientador prof. Dr. Mario Lemes Proença Jr. por todo seu apoio e orientação, pelas oportunidades ofertadas, pela confiança em meu trabalho e por sua compreensão, atenção e conselhos a mim direcionados, tornando possível meu crescimento intelectual, profissional e pessoal.

Aos professores Dr. Bruno B. Zarpelão, Dr. Sylvio Barbon Jr. e Dr. José Valdeni de Lima, os quais aceitaram de bom grado o convite de fazer parte da banca examinadora deste trabalho. Sou grato pela dedicação de tempo e esforço direcionada à avaliação deste texto, a qual com certeza contribuiu com o aumento de sua qualidade, bem como meu crescimento pessoal.

À minha esposa Natalie, pelo amor, compreensão, apoio e incentivo incondicional na conquista de meus objetivos e realizações pessoais. Agradeço por ser essa pessoa incrível, a qual me ensina algo novo todos os dias, e principalmente me direciona o maior amor do mundo, seja em momentos de conquistas ou derrotas. Sua alegria contagia meu coração e, ao seu lado, me sinto completo.

À minha mãe Renicler, por todos os valores e princípios ensinados, bem como pelo amor e apoio incondicional em todos os dias de minha vida. Sua presença e carinho, assim como seus conselhos foram, são e sempre serão essenciais para a minha formação como ser humano.

Ao meu pai Eunilson, também por todos os valores e princípios a mim repassados, em especial pelos exemplos de amor, força de vontade, determinação, dedicação, e por me ensinar com um homem deve agir com relação à sua família. Quando tiver filhos tenho certeza que serei um ótimo "pai de família" seguindo seus exemplos.

À minha avó Ingrácia e minha irmã Mariane, pela paciência e apoio nos momentos difíceis, mas principalmente por toda a alegria que proporcionam a minha vida, pelas conversas aleatórias, histórias antigas, brincadeiras e bagunças nas refeições, e por me apoiar em minhas decisões.

À Mestre Renata Balestrini, por sua dedicação e esmero ao ensino da arte tradicional de kung fu Hung Gar, por me permitir fazer parte dessa família, por me apresentar novas filosofias e pensamentos e, acima de tudo, por me guiar em minha busca ao

aperfeiçoamento pessoal em todas as áreas de minha vida.

A todos os professores que contribuíram para minha formação não somente durante o Mestrado, mas em todas as etapas de minha vida, por toda sua dedicação, paciência e sabedoria na execução dessa tarefa tão nobre e importante que é a educação.

À minha cunhada Mariane, pela dedicação de seu tempo na tradução e correção de diversos textos redigidos durante este Mestrado. Sem dúvidas seu cuidado e rigor foram essenciais para que os trabalhos produzidos por nosso grupo de pesquisa fossem vistos com outros olhos pelos revisores de conferências e revistas.

À minha tia Eunice, pela dedicação de seu tempo na revisão de português deste trabalho. Sem dúvidas, suas colocações e sugestões foram muito relevantes, contribuindo para a melhoria do texto como um todo.

Aos meus amigos e parceiros de grupo de pesquisa Luiz Fernando, Gilberto, Eduardo, Alexandro e Mário Adaniya por todas as conversas, discuções, risadas, "*rush's*" madrugada adentro, enfim pela amizade. Seu trabalho e dedicação foram essenciais para meu crescimento individual, me ensinando que o sucesso é resultado de trabalho duro, dedicação e principalmente companheirismo, visto que ninguém cresce sozinho.

Aos meus amigos Felipe, Guilherme e Bruno, por todo o apoio, incentivo e amizade dedicados a mim durante todo o tempo em que nos conhecemos. Em meio à incontáveis noites sem dormir, pressão e prazos apertados, os momentos que passamos juntos foram de suma importância para a conclusão deste trabalho.

À Universidade Estadual de Londrina e todos os seus componentes, os quais possibilitaram minha formação desde o ensino médio (por meio do Colégio Estadual José Aloísio de Aragão - Colégio de Aplicação), até minha Graduação e Mestrado em Ciência da Computação.

À CAPES pela concessão da bolsa de estudos.

"No coração do homem que controla seus pensamentos e emoções, nem sequer o tigre encontra espaço para introduzir suas garras ferozes".

Parte de um poema Shaolin.

ASSIS, Marcos Vinicius Oliveira de. **Um modelo para Detecção de Anomalias que utiliza o Método de Previsão Holt-Winters e análise Hepta-Dimensional de Fluxos.** 2014. 129 f. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2014.

RESUMO

Devido à crescente necessidade de maior agilidade nos processos de troca de informação, as redes de computadores estão constantemente se expandindo tanto em magnitude quanto na complexidade de seu gerenciamento. Um componente essencial destes processos é a detecção e identificação de anomalias. Embora existam diversos estudos nessa área, mecanismos de detecção de anomalias simples e eficientes ainda são necessários devido à escassez de abordagens adequadas a ambientes de rede de larga escala. Neste trabalho, é apresentado um sistema de detecção de anomalias que utiliza uma análise hepta-dimensional de fluxos IP por meio dos atributos: bits/s, pacotes/s, fluxos/s, endereços IP de origem e destino e portas de origem e destino. A base deste sistema é composta pelo método Holt-Winters *for Digital Signature* (HWDS), uma versão aprimorada do tradicional método Holt-Winters, o qual caracteriza o tráfego de cada uma das dimensões analisadas como forma de gerar assinaturas capazes de descrever o comportamento normal da rede, aqui denominado *Digital Signature of Network Segment using Flow analysis* (DSNSF). A baixa complexidade computacional da abordagem apresentada permite detecções mais rápidas de anomalias, mitigando o impacto causado em usuários finais. O sistema não apenas avisa ao administrador de redes sobre o problema, mas também provê informações importantes para identificá-lo e resolvê-lo. Para se mensurar a eficiência e precisão do sistema, diferentes cenários de testes foram analisados.

Palavras-chave: DSNSF. Holt-Winters. HWDS. Caracterização de tráfego. Gerenciamento de redes.

ASSIS, Marcos Vinicius Oliveira de. **A model for Anomaly Detection using the Holt-Winters Forecasting Method and Seven-Dimensional Flow analisys**. 2014. 129 p. Dissertation (Master´s degree in Computer Science) – Universidade Estadual de Londrina, Londrina, 2014.

ABSTRACT

Due to the increasingly need of more agility in information exchange, computer networks are continuously expanding both in magnitude and complexity of the management processes. An essential component of these processes is the anomaly detection and identification. Although there are several studies in this area, simple and efficient anomaly detection mechanisms are still required due to the lack of suitable approaches for large-scale network environments. In this research, we present an anomaly detection system using a seven-dimensional IP flow analysis through the attributes: bits/s, packets/s, flows/s, IP addresses of origin and destination and ports of origin and destination. The core of this system is composed by the Holt-Winters for Digital Signature (HWDS) method, an improvement of the traditional Holt-Winters, which characterizes the traffic of each one of the analyzed dimensions in order to generate profiles able to describe the network's normal behavior, here called Digital Signature of Network Segment using Flow analysis (DSNSF). The low complexity of the presented approach enables fast anomaly detection, mitigating the impact on final users. The system not only warns the network administrator about the problem, but also provides the necessary information to identify and solve it. To measure the efficiency and accuracy of the system, several different test scenarios were analyzed.

Key words: DSNSF. Holt-Winters. HWDS. Traffic characterization. Network management.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACO	*Ant Colony Optimization*
ARIMA	*Autregressive Integrated Moving Average*
BGP	*Border Gateway Protocol*
CC	Coeficiente de Correlação
desIP	*Destination* IP *Address*
desPort	*Destination Port*
DoS	*Denial of Service*
DSNS	*Digital Signature of Network Segment*
DSNSF	*Digital Signature of Network Segment using Flow analysis*
EWMA	*Exponentially Weighted Moving Average*
FSD	*Fractional Standard Deviation*
HW	Holt-Winters
HWDS	Holt-Winters *for Digital Signature*
IETF	Internet *Engineering Task Force*
IP	*Internet Protocol*
IPFIX	*Internet Protocol Flow Information eXport*
IPv6	Internet *Protocol version 6*
ISP	Internet *Service Provider*
LAN	*Local Area Network*
MIB	*Management Information Base*
MPLS	*Multi Protocol Label Switching*
NMSE	*Normalized Mean Square Error*
PCA	*Principal Component Analysis*
QoS	*Quality of Service*
RFC	*Request for Comments*
sMAPE	*Symmetric Mean Absolute Percentage Error*
SNMP	*Simple Network Management Protocol*
srcIP	*Source* IP *Address*
srcPort	*Source Port*
SVM	*Support Vector Machine*

LISTA DE SÍMBOLOS

t	Intervalo de tempo t.
k_t	Acúmulo de ponderações de equações EWMA ao longo do tempo *t.*
K	Valor da medição atual ou corrente em equações EWMA.
ρ	Coeficiente de suavização em equações EWMA.
y_t	Valor da série temporal no intervalo de tempo *t*.
y'_{t+1}	Previsão calculada para o intervalo de tempo *t*+1.
a	Parte que representa o *Baseline* nos métodos Holt-Winters e HWDS.
b	Parte que representa a Tendência Linear nos métodos Holt-Winters e HWDS.
c	Parte que representa a Sazonalidade nos métodos Holt-Winters e HWDS.
α	Coeficiente de suavização para o *Baseline* nos métodos Holt-Winters e HWDS.
β	Coeficiente de suavização para a Tendência Linear nos métodos Holt-Winters
e	HWDS.
γ	Coeficiente de suavização para a Sazonalidade e Intervalos de confiança do sistema.
s	Período do ciclo sazonal (periodicidade) da série temporal.
LI	Limite Inferior do intervalo de confiança dos DSNSFs gerados.
LS	Limite Superior do intervalo de confiança dos DSNSFs gerados.
δ	Fator escalar para a largura do intervalo de confiança.
d_t	Medida de desvio absoluto ou padrão, de acordo com a direção do erro ($d1_t$ e $d2_t$).
$\sigma(y')$	Desvio padrão da previsão (DSNSF) gerada.
$p(x_i)$	Distribuição de probabilidade de *x* para cada elemento *i*.
n_i	Número de ocorrência de elementos *i* no intervalo de tempo analisado.
N	Total de ocorrência de elementos no intervalo de tempo analisado.
$H(x)$	Entropia para o intervalo de tempo analisado.
m	Dados suavizados.
ω	Coeficiente de suavização para o método de Suavização Exponencial.
D	Vetor contendo os dados de DSNSFs.
T	Vetor contendo os dados do tráfego observado.
VP	Verdadeiros Positivos.

VN	Verdadeiros Negativos.
P	Resultados Positivos.
N	Resultados Negativos.

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a humanidade vive a era da informação, a qual se caracteriza pela agilidade, velocidade e facilidade na transmissão, compartilhamento e disseminação de conhecimento por meio de processos digitais completamente baseados em redes de computadores. Devido à convergência dos processos de comunicação para a Internet, essas redes se encontram sob um contínuo, crescimento necessário para suportar novos usuários, serviços e aplicações. Embora a evolução de tecnologias físicas de rede seja atualmente capaz de garantir essa escalabilidade, o gerenciamento dessas redes de larga escala ainda é uma tarefa complexa devido principalmente ao esforço computacional necessário pelo aumento de processamento e quantidade de dados de monitoramento.

O gerenciamento de redes de computadores é comumente executado de forma manual por parte dos administradores de rede, os quais analisam gráficos e informações estatísticas a procura de padrões comportamentais para possibilitar a detecção e identificação de ataques ou falhas. Essa abordagem é ineficaz, trabalhosa e sujeita a erros, o que tende a prejudicar a qualidade dos serviços providos pela rede. Dessa forma, são necessárias novas ferramentas de gerenciamento de rede, capazes de automaticamente analisar a rede e identificar proativamente problemas e padrões comportamentais anômalos. Este novo paradigma é conhecido como Gerenciamento Autônomico [1, 2, 3], o qual possibilita o aumento da confiabilidade e disponibilidade de redes de computadores, permitindo que administradores de rede possam rapidamente identificar e corrigir problemas.

Outra abordagem de gerenciamento de redes cada vez mais utilizada em diversos modelos e ferramentas [4, 5, 6, 7] é a análise de fluxos IP. Ao contrário da abordagem que emprega o *Simple Network Management Protocol* (SNMP) [8], este tipo de análise é capaz de disponibilizar uma ampla gama de informações por meio dos coletores NetFlow [9], IPFIX [10] e sFlow [11], tais como o número de *bytes* e pacotes, protocolos, endereços IP, número de portas, entre outros [12].

Entre os estudos e ferramentas que já utilizam análise de fluxos no gerenciamento de redes de computadores e detecção de anomalias, sua maior parte é baseada na análise de apenas um atributo disponibilizado por este novo paradigma de gerenciamento [13, 14]. Segundo Molnar *et al.* [15], a utilização de múltiplos atributos de fluxos correlacionados enriquece os processos de gerenciamento de redes de computadores melhorando os resultados finais na detecção e identificação de anomalias. Além disso, diversos estudos [16, 17, 18] são baseados na análise da rede em janelas de tempo (intervalos)

de cinco minutos. Essa tradicional abordagem vem se tornando impraticável na atualidade devido ao aumento das taxas de transmissão suportadas por redes de larga escala. Em uma rede 10 *Gigabit* Ethernet, por exemplo, em 5 minutos até 3 *Terabits* de dados podem ser comprometidos. Dessa forma, abordagens mais ágeis e capazes de detectar e identificar rapidamente problemas nas redes de computadores são necessárias para auxiliar no seu gerenciamento.

Este trabalho apresenta um sistema de detecção de anomalias baseado em uma análise hepta-dimensional de fluxos IP, utilizando os seguintes atributos: *bits*/s, pacotes/s, fluxos/s, endereços IP de origem e destino e portas de origem e destino. O sistema analisa simultaneamente as sete dimensões (atributos) em janelas de tempo de um minuto, detectando e identificando diferentes tipos de anomalias, gerando alarmes específicos e identificando suas possíveis causas. O sistema apresentado é dividido em dois módulos principais: o Módulo de Detecção e o Módulo de Informação.

O Módulo de Detecção é responsável pela análise autonômica das sete dimensões de fluxos IP anteriormente mencionadas. Essa análise inclui: processos de tratamento dos dados, tais como a transformação de dimensões qualitativas em dados quantitativos por meio da utilização da Entropia de Shannon [19] e a redução da granularidade de dados provida pela técnica de Suavização Exponencial [20]; e detecção de anomalias por meio de uma abordagem híbrida capaz de detectar assinaturas (padrão comportamental) de anomalias específicas e comportamentos anormais desconhecidos. Para que isso seja possível, o sistema é baseado na caracterização de tráfego [21]. O sistema apresentado caracteriza o comportamento normal da rede em cada uma das sete dimensões analisadas, gerando sete diferentes assinaturas que representam um dia normal. Essas assinaturas são chamadas *Digital Signature of Network Segment using Flow analysis* (DSNSF), ou Assinatura Digital de Segmento de Rede utilizando análise de Fluxos, e representa o núcleo do sistema de detecção de anomalias apresentado. Para realizar este processo de caracterização de tráfego, é apresentada e utilizada uma versão aperfeiçoada do método estatístico de previsão Holt-Winters [22], denominado Holt-Winters *for Digital Signature* (HWDS), ou Holt-Winters para Assinaturas Digitais. O método HWDS foi projetado especificamente para a geração de assinaturas digitais de redes, provendo uma abordagem de baixa complexidade computacional juntamente com uma maior eficiência que o método tradicional.

O módulo de Informação é responsável por prover informações relevantes sobre a anomalia detectada ao administrador de redes por meio do uso de duas diferentes

abordagens: a Visão Global, uma visão hepta-dimensional do comportamento da rede em um intervalo de tempo específico; e a classificação dos principais usuários, que provê o endereço IP de origem e destino, porta de origem e destino e protocolos com maior frequência de ocorrência no intervalo de tempo analisado. Essas informações auxiliam o administrador de redes no processo de tomada de decisões, reduzindo seu tempo de reação e consequentemente mitigando o impacto da anomalia aos usuários finais da rede.

Para avaliar e mensurar a performance do sistema apresentado, diferentes cenários de análises foram utilizados. O primeiro deles analisa os DSNSFs criados pelos métodos Holt-Winters e HWDS relativos à caracterização de tráfego de uma rede de larga escala, utilizando dados reais coletados na Universidade Estadual de Londrina, e avalia os resultados relativos à detecção de anomalias utilizando dados reais e anomalias específicas simuladas. O segundo cenário de testes avalia os resultados obtidos na caracterização de tráfego e detecção de anomalias em uma rede de baixa/média escala, utilizando dados reais coletados na Universidade Tecnológica Federal do Paraná - Campus Toledo, e apresenta a flexibilidade do sistema quanto à adição de novas assinaturas de anomalias.

Dentre as principais contribuições deste trabalho, pode-se destacar:

- Método HWDS: Proposta a implementação de uma versão aprimorada do tradicional método Holt-Winters que melhora os resultados da caracterização de tráfego;
- Análise Hepta-Dimensional de Fluxos IP: O sistema analisa simultaneamente 7 dimensões de fluxos IP em intervalos de 1 minuto, visando atender a demanda de redes de larga-escala;
- Entropia de Shannon e Suavização Exponencial: O sistema apresentado utiliza essas técnicas na conversão de dimensões ou atributos de fluxos IP qualitativos para quantitativos, e na diminuição da granularidade do tráfego avaliado, respectivamente;
- Detecção e Identificação de anomalias: Além de ser capaz de detectar anomalias em redes com precisão, o sistema apresentado provê informações relevantes sobre a anomalia detectada, permitindo a provável identificação de sua causa;
- Escalabilidade e flexibilidade: O sistema é aplicável aos ambientes de baixa, média ou larga escala, e é flexível a adições de novas assinaturas de anomalias (padrões comportamentais anômalos).

Este trabalho se encontra dividido da seguinte forma: no Capítulo 2 serão apresentados trabalhos relacionados ao tema de pesquisa desenvolvido, no Capítulo 3 serão apresentados os conceitos de gerenciamento de redes com enfoque na análise de fluxos IP. No Capítulo 4 será apresentado o sistema de detecção de anomalias apresentado, e no Capítulo 5 serão apresentados os resultados de performance e eficiência obtidos por este sistema. Finalmente, no Capítulo 6 são apresentadas as conclusões deste trabalho, bem como sugestões para trabalhos futuros.

2 TRABALHOS RELACIONADOS

Neste capítulo, serão apresentados trabalhos relacionados à pesquisa desenvolvida, os quais apresentam e utilizam conceitos importantes para o desenvolvimento deste trabalho, tais como o gerenciamento de redes através da análise de fluxos IP, gerenciamento autonômico, caracterização de tráfego e detecção de anomalias.

Nos últimos anos, a utilização de fluxos IP nos processos de análise e gerenciamento de redes de computadores tem aumentado significativamente, gradualmente substituindo abordagens e ferramentas baseadas na tecnologia SNMP (*Simple Network Management Protocol*). Essa transição ocorre principalmente devido à grande quantidade de informações disponíveis por meio da análise de fluxos IP, a qual provê dados detalhados sobre todos os processos de comunicação da rede analisada.

Em Kashihara *et al.* [23], os autores apresentam um sistema de gerenciamento de largura de banda para arquiteturas de rede com garantia de qualidade de Serviço (QoS) por meio da análise de fluxos IP. Neste trabalho, os autores analisam o sistema proposto quanto a capacidade de estimativa da utilização de largura de banda, a performance obtida por meio de sua utilização e fatores de escalabilidade necessários para a análise de centenas de fluxos IP.

Em Chen *et al.* [24], os autores utilizam a abordagem de análise de fluxos IP em sistemas concorrentes. Utilizando os fluxos coletados, os autores apresentam uma ferramenta capaz de detectar estados e ações inacessíveis. Os autores destacam que a análise de fluxos, em conjunto com técnicas de gráficos de acessibilidade, é reconhecida como a abordagem mais precisa e popular na solução deste tipo de problema.

Em Molnar *et al.* [15], os autores utilizam três diferentes atributos (ou dimensões) de fluxos IP, aplicando-os simultaneamente a um processo de caracterização do tráfego da rede analisada. Além de provar a existência de correlação entre as dimensões analisadas, os autores destacam que esse tipo de abordagem multidimensional enriquece os processos de gerenciamento de redes de computadores.

Dentre as diferentes abordagens utilizadas por ferramentas de gerenciamento de redes e detectores de anomalias, a caracterização de tráfego é uma das mais utilizadas. Essa preferência é decorrente de sua grande eficácia: a criação de um perfil capaz de descrever o comportamento normal da rede ou segmento de rede analisado facilita os processos de detecção e identificação de possíveis anomalias, sejam elas decorrentes de ataques ou falhas.

Em Kanda *et al.* [14], os autores apresentam a possibilidade da utilização de padrões de comunicação baseados em fluxos como uma abordagem viável na detecção de anomalias, analisando separadamente os diferentes *hosts* (computadores) da rede. Assim, os autores caracterizam o tráfego de hosts infectados por vírus do tipo *worm* (verme), criando um perfil que descreva o comportamento desse tipo de anomalia, facilitando sua posterior detecção. Os autores destacam que essa abordagem é capaz de detectar anomalias sutis, as quais dificilmente são detectadas por meio da análise de volume de tráfego.

Qin *et al.* [25] apresentam um método baseado em separação por *blind search* (busca cega) na detecção de tráfego considerado anômalo. Para tal, os autores utilizam uma abordagem baseada na caracterização de tráfego, decompondo o tráfego em dois componentes principais: o tráfego de rotina e o anômalo. Por meio dessa separação, os autores são capazes de caracterizar o comportamento normal dos usuários da rede (tráfego de rotina) e detectar diferentes tipos de comportamento anômalo, tais como varreduras, *flooding*, entre outros.

Em Dewaele *et al.* [26], os autores apresentam uma abordagem de detecção de anomalias em redes baseada na geração de perfis. Por meio da utilização em conjunto de *sketches* e modelagem de distribuição marginal não Gaussiana, é criado um perfil que representa o comportamento normal ou de referência da rede, o que possibilita a extração comportamentos anômalos.

Embora a detecção de anomalias em redes de computadores seja um tema amplamente estudado, este campo de estudo ainda se encontra em aberto. Isso ocorre principalmente devido à complexidade desta tarefa, a qual vem se acentuando com o aumento das redes de computadores a nível mundial, o que consequentemente aumenta sua complexidade de gerenciamento. Diversas abordagens vêm sendo aplicadas nessa área ao longo dos anos tais como heurísticas, as baseadas em processos estatísticos, mineração de dados, entre outras.

Um dos trabalhos mais importantes dessa área, o qual também foi um dos pioneiros nesse campo de pesquisa, foi desenvolvido por Lakhina *et al.* [17]. Nele, os autores utilizam uma técnica chamada PCA (*Principal Component Analysis*) na detecção de anomalias genéricas em redes de computadores, método amplamente utilizado na redução da dimensionalidade de conjuntos de dados.

Em Park *et al.* [21], os autores propõem uma abordagem de detecção de anomalias de intrusão baseada na contínua caracterização do comportamento normal de

usuários em fluxos de dados. Neste trabalho, os autores destacam a importância da caracterização do tráfego nos processos de detecção de anomalias.

Em Shon *et al.* [27], os autores utilizam uma versão aprimorada de uma técnica conhecida como SVM (Máquina de Vetor de Suporte) na classificação de comportamentos anômalos na rede. Por meio dessa abordagem, os autores são capazes de detectar ataques cibernéticos do tipo *zero-day* (ataques com comportamento ainda desconhecidos por ferramentas de detecção de anomalias), tais como *worms* e *spywares* (softwares de espionagem).

Em Siris *et al.* [28], os autores investigam diferentes algoritmos de detecção de anomalias na detecção de ataques do tipo SYN *flooding*, os quais são o tipo mais comum de ataque de negação de serviço (DoS). Os autores destacam que diversos tipos de ferramentas e mecanismos de detecção de anomalias são capazes de detectar tipos específicos de anomalias e comportamentos maliciosos. Por meio da utilização de abordagens estatísticas anomalias genéricas podem ser detectadas, o que aumenta drasticamente a eficiência dos processos de gerenciamento de redes.

Uma abordagem ou paradigma que vem sendo discutido de forma crescente para ferramentas de gerenciamento de rede, tais como detectores de anomalias, é o Gerenciamento Autonômico. Através da automação do processo de análise de rede, a eficiência e precisão do sistema de detecção de anomalias podem aumentar consideravelmente.

Em Xiong *et al.* [7], os autores propõem algoritmo autonômico inovador de detecção aleatória antecipada (*random early detection* - RED) denominado *Novel Proportional and Differential* RED (NPD-RED). Este método é capaz de autonomicamente controlar a largura de banda de pontos de acesso sem fio, considerados "gargalos" da vazão de redes de computadores, através do gerenciamento de fila ativa.

Já em Tcholtchev *et al.* [29], os autores propõem um inovador algoritmo baseado em uma Cadeia de Markov escalável para o isolamento *on-line* de falhas em redes autonômicas. Em outras palavras, a abordagem proposta pelos autores possibilita que falhas de rede possam ser autonomicamente detectadas e identificadas através do disparo de alarmes e alertas de falhas.

Em Song *et al.* [30], os autores propõem uma abordagem autonômica de detecção de anomalias em redes de computadores. Neste trabalho, a abordagem proposta é capaz de automaticamente ajustar e otimizar os parâmetros de uma SVM (Máquina de Vetor de Suporte) sem a necessidade de quaisquer ajustes por parte do administrador de rede.

Uma característica essencial em sistema e ferramentas modernas de detecção de anomalias é a baixa complexidade computacional da abordagem utilizada. Isso ocorre devido à necessidade de soluções mais ágeis e leves em redes de larga-escala, ambientes de alta agregação de tráfego que necessitam cada vez mais de técnicas de gerenciamento eficientes, as quais garantam que a qualidade dos serviços prestados pela rede seja mantida. Seguindo essa tendência, o método estatístico de previsão Holt-Winters vem sendo amplamente utilizado em problemas relacionados à caracterização de tráfego de rede nos últimos anos devido à sua grande eficiência de predição e baixo custo computacional.

Em Brutlag [31], o autor utiliza o método Holt-Winters na caracterização de tráfego e detecção de anomalias baseado na utilização da tecnologia SNMP. O autor se baseia na utilização de intervalos de confiança, calculados por meio de equações do tipo EWMA, para detectar comportamentos que diferem do esperado na rede analisada.

Em Les Cottrell *et al.* [32], os autores analisam quatro diferentes abordagens para solucionar falhas do tipo fim-a-fim e de performance. Os métodos discutidos foram: Holt-Winters, o algoritmo Plateau, e as técnicas de Kosmogorov-Smirnov e Mark Burgess. Após a realização de testes de performance para cada um destes métodos, os autores concluíram que o método Holt-Winters se saiu melhor que os outros devido à sua capacidade ímpar de incorporação de tendências sazonais em suas predições.

Em Shuying *et al.* [33], os autores aplicam o método Holt-Winters em conjunto com a distância de Kullback-Leibler e a entropia de Shannon na detecção de anomalias em redes. Essa abordagem é baseada na utilização de fluxos IP, utilizando quatro diferentes informações de fluxos para os processos de caracterização do comportamento normal da rede e detecção de comportamentos anômalos.

Em Tikunov *et al.* [34], os autores utilizam o método Holt-Winters na predição do comportamento normal de redes móveis. Os autores testaram a aplicação deste método em um ambiente real de uma rede móvel comercial, e apresentam os resultados de performance obtidos por meio deste teste. Segundo os autores, os testes apontaram que o método atingiu bons resultados, ou seja, a previsão por ele gerada representa com precisão o comportamento normal observado.

Como se pode observar por meio dos trabalhos citados, este é um grande campo de pesquisa que, embora amplamente abordado nos últimos anos, continua em aberto devido à complexidade de se desenvolver sistemas eficientes e simples o suficiente para suportar sua aplicação em ambientes de alta agregação de tráfego. É importante ressaltar que o presente trabalho faz parte de uma linha de pesquisa iniciada por Proença *et al.* [35], onde a

caracterização de tráfego é utilizada na geração de *Digital Signatures of Network Segment* (DSNS), tornando possível a detecção de anomalias. Neste trabalho, os autores introduzem a caracterização de tráfego para cada dia da semana separadamente, abordagem denominada *bl*-7, utilizando a tecnologia SNMP. A partir dessa pesquisa, diferentes abordagens foram desenvolvidas, dentre as quais pode-se destacar o trabalho de Adaniya *et al.* [36], onde os autores utilizam a geração de DSNSs em conjunto com a heurística *Firefly Harmonic Clustering* na detecção de anomalias por meio da tecnologia SNMP. Zacaron *et al.* [37] introduziu a análise de fluxos IP na geração de assinaturas digitais, utilizando *Digital Signatures of Network Segment using Flow analysis* (DSNSF) na detecção de anomalias em conjunto com o processo de clusterização do método K-*means*.

Seguindo essa linha de pesquisa, este trabalho tem como objetivo apresentar um sistema que une a grande eficiência e baixo custo computacional do método HWDS, uma versão aprimorada do método Holt-Winters, que obtém melhores resultados na caracterização de tráfego, com uma análise de fluxos IP multidimensional, abordagem inovadora em contraste com modelos anteriores.

3 GERENCIAMENTO DE REDES

As redes de computadores desempenham um papel fundamental na sociedade atual, sendo a base da maioria dos processos de comunicação e possibilitando o compartilhamento de informações de forma ágil e simplificada. Diversos tipos de aplicativos e serviços amplamente utilizados nos últimos anos precisam estar conectados para funcionar plenamente, o que consequentemente aumenta o número de pessoas (usuários) e dispositivos conectados o tempo todo. A convergência destes serviços para o paradigma orientado à conexão (Internet) está diretamente relacionada ao constante crescimento das redes de computadores na atualidade. As redes mais acessadas são relativas principalmente a grandes provedores de serviços ou organizações, tais como universidades, empresas corporativas, servidores de computação em nuvem e provedores de serviço de Internet (ISP's), os quais são ambientes conhecidos como redes de larga escala devido à grande agregação de tráfego suportada.

O gerenciamento de redes de larga escala é um problema amplamente discutido [4, 6]. O constante crescimento em escala dessas redes consequentemente aumenta a complexidade de sua análise, o que dificulta o processo de detecção de anomalias. Convencionalmente, administradores de redes utilizam ferramentas de gerenciamento baseadas no protocolo SNMP. Essas ferramentas têm sido utilizadas por muitos anos devido à simplicidade provida por essa abordagem e a diversidade de ferramentas disponíveis no mercado que as utilizam, dentre as quais podemos citar o Cacti [38] e o NTop [39].

Nos últimos anos, a análise de fluxos IP vem ganhando espaço entre as abordagens de gerenciamento de redes devido à ampla gama de informações providas por este tipo de análise. Fluxos IP disponibilizam diversos tipos de informações, tais como número de pacotes transportados, quantidade de bits, endereços IP de origem e destino, portas de origem e destino, protocolos, entre outros, os quais enriquecem o processo de gerenciamento de rede, disponibilizando ao administrador de redes uma visão mais completa do funcionamento das redes de computadores. Dentre ferramentas que utilizam essa abordagem, podemos destacar o NTop [39] e o NFSen [40].

Neste capítulo serão abordadas as principais características do protocolo SNMP e da análise de fluxos, os quais são considerados as principais abordagens utilizadas em ferramentas de gerenciamento e análise de redes na atualidade.

3.1 *SIMPLE NETWORK MANAGEMENT PROTOCOL* (SNMP)

O SNMP é um protocolo amplamente utilizado tanto na literatura quanto no mercado em soluções de gerenciamento de objetos específicos (informações de gerenciamento) de redes de computadores, tais como roteadores, *switches*, entre outros. Padronizado pela IETF, comunidade internacional responsável pela padronização de protocolos relacionados à evolução da Internet, em 1990 por meio do RFC 1157 [41], este protocolo ainda hoje é utilizado em ferramentas de gerenciamento de redes devido à sua simplicidade de funcionamento. Dentre as diversas ferramentas de gerenciamento de redes baseadas na utilização do protocolo SNMP, pode-se citar as ferramentas Cacti [38] e NTop [39].

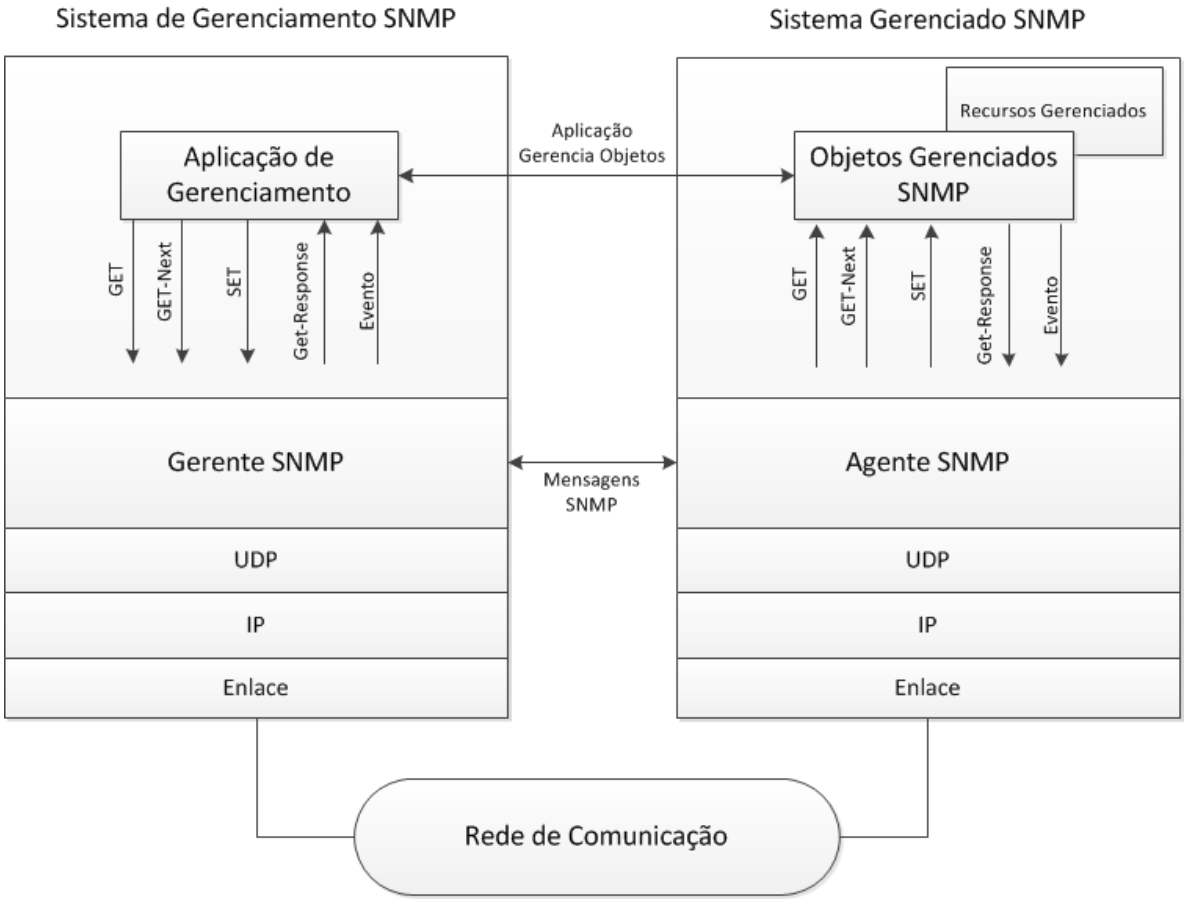
O protocolo SNMP tem seu funcionamento baseado em um modelo denominado "gerente/agente" [8]. Este modelo consiste basicamente de um gerente, um sistema gerenciado, um banco de dados com informações de gerenciamento e protocolo de gerenciamento de rede. Cada qual possui suas devidas funções:

- Gerente: Responsável por prover uma interface de comunicação entre o sistema gerenciado e administrador de redes. O gerente executa diversas funções de gerenciamento, tais como a gravação da velocidade de transmissão de uma interface específica de um *switch*, ou medir o tráfego de dados em uma interface LAN remota;
- Sistema gerenciado: Este sistema consiste em todos os processos agentes de dispositivos gerenciados pelo Gerente na rede analisada. Os processos agentes realizam operações de armazenamento e envio de informações dos dispositivos gerenciados, tais como roteadores, *switches*, servidores, entre outros;
- Banco de dados: Neste modelo, bancos de dados são denominados "Base de Informações de Gerenciamento" (*Management Information Base* - MIB). Eles estão presentes tanto no sistema gerenciado (armazenamento de informações de gerenciamento de dispositivos individuais) quanto no gerente (armazenamento de informações de gerenciamento do segmento de rede analisado);
- Protocolo de gerenciamento de rede: Este protocolo é responsável pela comunicação entre o gerente, os objetos gerenciados e seus agentes, processo organizado pelo protocolo SNMP.

O protocolo SNMP possui o termo simplificado em seu nome devido ao fato de que os agentes necessitam de um software mínimo, onde a maior parte do processamento de análise de gerência e armazenamento é de responsabilidade do dispositivo de gerenciamento (Gerente) [8].

O funcionamento básico desse protocolo pode ser observado na Figura 3.1, a qual ilustra todos os comandos de gerenciamento suportados pelo protocolo, bem como o processo de comunicação entre Gerente e Sistema gerenciado:

Figura 3.1 - Funcionamento básico do SNMP.



Como se pode observar, para garantir a simplicidade do protocolo de gerenciamento, apenas um conjunto limitado de comandos é suportado. Dentre eles, os comandos Get, GetNext e Set são responsáveis por solicitar ou alterar o valor de uma ou mais variáveis de objetos, e são executados pelo Sistema de Gerenciamento (Gerente). Por outro lado, o Sistema gerenciado apenas responde a essas solicitações para finalizar o processo de comunicação. Além disso, o Sistema Gerenciado é capaz de enviar uma notificação de evento específico para o Gerente por meio de mensagens denominadas *traps*, as quais podem

anunciar alterações físicas no dispositivo gerenciado, quando o limite de um determinado contador em uma variável de objeto for ultrapassado, entre outros.

Outra característica do protocolo SNMP que pode ser observada por meio da Figura 3.1 é o processo de comunicação entre Gerente e Sistema gerenciado. Como observado, a tecnologia SNMP utiliza o protocolo UDP (camada de transporte) para transporte de seus dados por meio de redes IP (camada de redes). Além disso, o protocolo SNMP precisa de um protocolo de camada de enlace, tal como Ethernet ou Token Ring para transportar os dados de gerenciamento através da rede. Como o protocolo UDP não é orientado a conexão, ou seja, não é estabelecida uma conexão entre *hosts* de origem e destino antes da transmissão dos dados, não se pode garantir a entrega dos pacotes transmitidos, embora sua retransmissão seja possível.

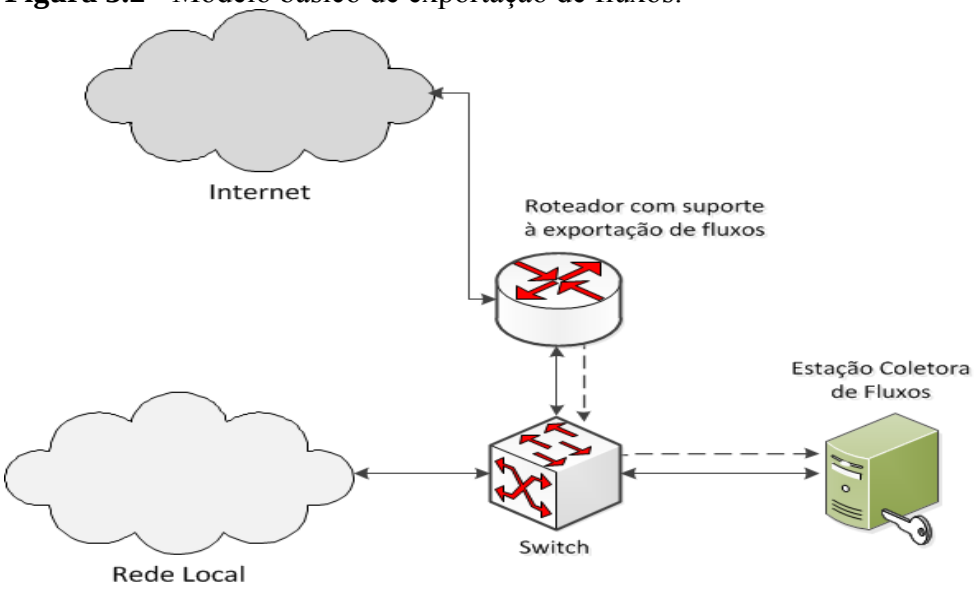
3.2 FLUXOS IP

A popularização de redes IP, acompanhada pelo constante surgimento de novas ferramentas e aplicativos baseados nessa tecnologia, proporcionam um aumento significativo na complexidade de análise e gerenciamento de redes modernas. Além disso, a frequência de ocorrência e intensidade de *cyber* ataques vem aumentando constantemente ao longo dos anos, causando cerca de U$ 1,5 bilhão em prejuízo no ano de 2012 [42]. Estes ataques têm se demonstrado cada vez mais complexos, utilizando novas abordagens na execução de ataques já conhecidos, tais como DoS e DDoS, para burlar sistemas de segurança convencionais. Assim, novas abordagens de gerenciamento de redes são necessárias para auxiliar administradores de redes nos processos de análise e segurança de redes modernas. A análise de fluxos IP foi desenvolvida como forma de proporcionar uma nova abordagem de gerenciamento, a qual disponibiliza ao administrador de redes e ferramentas de análise informações detalhadas sobre os processos de comunicação que utilizam o segmento de rede analisado. A utilização de fluxos IP em operações de gerenciamento de redes tem se tornado cada vez mais presente em diversos campos de aplicação, tais como caracterização de tráfego, engenharia de tráfego, monitoramento de qualidade de serviços, entre outros [12].

A definição de fluxos IP, segundo Trammell *et al.* [12], é a definição adotada pelo IETF na padronização do protocolo de exportação de fluxos IPFIX, o qual será abordado posteriormente. Segundo essa definição, registros de fluxos representam uma conexão entre dois *sockets* que caracterizam um processo de comunicação. Para tal, os pacotes transmitidos são analisados, e um fluxo é caracterizado quando pacotes partilham um

determinado conjunto de características, tais como endereços IP de origem e destino, portas de destino, entre outros. Ainda segundo a definição apresentada, registros de fluxos devem apresentar pelo menos endereços de destino, hora e informações de volume dos dados transferidos.

Figura 3.2 - Modelo básico de exportação de fluxos.



A coleta de fluxos IP em redes de computadores pode ser classificada em dois grupos principais: A coleta nativa e a adaptada. Na coleta nativa os dispositivos de redes tais como *switches* ou roteadores possuem suporte nativo à geração e exportação de fluxos IP por meio de um determinado protocolo. Um esquema de um ambiente de coleta nativa de fluxos IP pode ser observado na Figura 3.2. Como observado, uma rede local se conecta a um *switch*, o qual também está conectado a um servidor coletor de fluxos e a um roteador com suporte à exportação de fluxos. Como existe o suporte nativo de exportação de fluxos por parte do roteador mencionado, a configuração de exportação de fluxos ocorre diretamente por meio das configurações específicas deste dispositivo. Uma vez configurado, o dispositivo analisa o tráfego que passa por ele, e realiza os processos de medição (análise e montagem de fluxos IP) e exportação para uma máquina coletora (linha pontilhada), a qual se responsabiliza pela análise, processamento e armazenamento dos fluxos recebidos.

A coleta adaptada ocorre em situações nas quais os dispositivos presentes na rede analisada não possuem suporte nativo à exportação de fluxos. Neste caso, como destacado em [43], realiza-se o espelhamento de uma porta do switch analisado para um servidor específico, o qual executa uma aplicação responsável por receber, analisar e montar

os registros de fluxos IP com base nos pacotes recebidos. Essa aplicação também se torna responsável por exportar os fluxos gerados a uma máquina coletora.

Como se pode notar por meio da análise de ambos os processos, o processo de geração de fluxos, o qual ocorre antes de sua análise por uma máquina coletora, é dividido em três principais fases:

- Observação: Captura dos pacotes que trafegam pelo dispositivo;
- Medição: Análise dos pacotes capturados, bem como a montagem dos registros de fluxos que os representam;
- Exportação: Transmissão dos fluxos gerados a uma máquina coletora, responsável pela análise, processamento e armazenamento destes fluxos.

Independente do método de coleta empregado na análise de fluxos IP da rede analisada, estes três processos devem ser executados para a geração de fluxos IP.

A análise de fluxos IP é uma abordagem conhecida pela riqueza de informações disponibilizadas sobre o tráfego da rede analisada. A Figura 3.3 ilustra uma amostra composta por dez fluxos e seus respectivos atributos (básicos) utilizando o protocolo de exportação sFlow. Como pode ser observado, os atributos presentes em uma análise básica são: Data, composto de dia (ano-mês-dia) e hora de início do fluxo, duração, protocolo de camada de transporte utilizado, endereços IP e portas de origem e destino, número de pacotes transportados, volume de tráfego em bytes e número de fluxos.

Figura 3.3 - Exemplos de fluxos do tipo SFlow

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2012-10-09 00:00:02.517	0.000	TCP	177.99.161.90:22323	->	189.90.67.67:80	256	18944	1
2012-10-09 00:00:02.517	0.000	TCP	204.45.65.58:80	->	189.90.65.11:2797	256	389632	1
2012-10-09 00:00:02.517	0.000	TCP	201.94.222.197:3911	->	189.90.65.119:554	256	17408	1
2012-10-09 00:00:06.511	0.000	TCP	205.251.223.107:80	->	189.90.65.11:7677	256	389632	1
2012-10-09 00:00:06.511	0.000	TCP	173.194.27.112:80	->	189.90.65.11:11463	256	389632	1
2012-10-09 00:00:06.511	0.000	TCP	201.20.204.33:64290	->	189.90.67.66:80	256	18944	1
2012-10-09 00:00:06.511	0.000	TCP	157.56.229.75:80	->	189.90.65.11:21653	256	56576	1
2012-10-09 00:00:06.511	0.000	TCP	94.102.56.186:1935	->	189.90.76.111:4618	256	367104	1
2012-10-09 00:00:10.511	0.000	TCP	184.28.2.224:443	->	189.90.72.21:52772	256	18944	1
2012-10-09 00:00:10.511	0.000	TCP	69.171.227.65:80	->	189.90.65.11:12337	256	375552	1
2012-10-09 00:00:10.511	0.000	TCP	177.183.224.126:52365	->	189.90.67.66:80	256	17408	1
2012-10-09 00:00:15.511	0.000	TCP	189.115.45.205:49922	->	189.90.67.66:80	256	17408	1
2012-10-09 00:00:15.511	0.000	UDP	216.239.32.10:53	->	189.90.65.11:16857	256	33280	1
2012-10-09 00:00:15.511	0.000	TCP	200.163.216.220:49466	->	189.90.65.119:554	256	17408	1

Nos tópicos a seguir serão abordados os principais protocolos de exportação de fluxos IP existentes na atualidade: Netflow, IPFix e sFlow.

3.2.1 Netflow

O protocolo Netflow é uma tecnologia de monitoramento de tráfego inicialmente desenvolvida por Darren e Bruins [44] no ano de 1996 na empresa Cisco. Com o constante aumento na complexidade de análise de redes, os autores propuseram este protocolo como forma de auxiliar os processos de análise e gerenciamento. É importante ressaltar que este protocolo é um padrão proprietário da Cisco e, dessa forma, apenas equipamentos produzidos por essa empresa possuem suporte de exportação no formato Netflow para a maior parte das versões deste protocolo, com exceção de suas versões 5 e 9.

O funcionamento básico da análise de fluxos, apresentado na seção anterior, é o mesmo utilizado pelo protocolo Netflow, uma vez que essa tecnologia introduziu o paradigma da análise de fluxos. De forma simplificada, os dispositivos de rede com suporte a Netflow observam os pacotes que chegam a cada uma de suas interfaces, capturando estatísticas de tráfego por fluxos. Então, um repositório de fluxos, denominado *flow cache*, é criado, agregado e exportado (de acordo com as configurações de tempo) para uma máquina responsável pela análise e utilização destes fluxos nos processos de gerenciamento de redes [45].

O *flow cache* é criado pelo primeiro pacote de um fluxo de dados. Este *cache* é mantido enquanto pacotes similares de fluxos continuam chegando, os quais possuem uma ou mais características em comum com o pacote inicial, tal como endereços IP de origem e destino, porta de destino, protocolo de transporte utilizado, entre outros. Dado um critério de parada, o *flow cache* é encerrado, sendo exportado periodicamente (com base em configurações específicas) para máquinas coletoras.

Como mencionado, é necessário um critério de parada para que um *flow cache* não aumente indefinidamente. O Netflow especifica diferentes critérios de parada ou encerramento de fluxos, os quais são:

- Ociosidade: Critério de parada que ocorre em situações onde um determinado fluxo se encontra em estado de ociosidade, ou seja, nenhum pacote que se enquadre nas características destes fluxos chega em um determinado tempo. O tempo padrão de espera em ociosidade é 15 segundos;
- Atividade: Mesmo que um determinado fluxo nunca entre em estado de ociosidade, é preciso liberar os dados armazenados na *cache* em

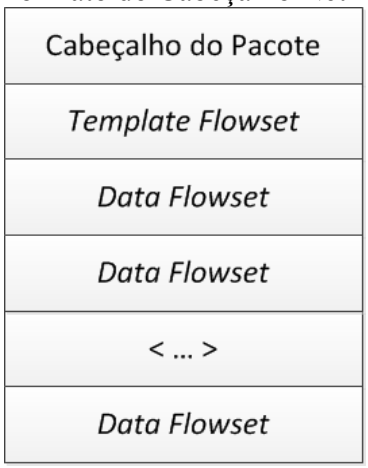
algum momento. Dessa forma, mesmo em atividade, é definido um tempo máximo de espera, o qual por padrão é de 30 minutos;

- Cache cheio: Critério de parada que ocorre quando o *cache flow* se encontra cheio, não podendo adicionar nenhuma nova informação. Dessa forma, diferentes medidas são tomadas pelo protocolo Netflow, dentre as quais podemos destacar duas diferentes abordagens. A primeira é a análise e expiração de fluxos mais antigos presentes na *cache*. A segunda, baseada na análise de fluxos que utilizam o protocolo TCP no transporte, expira fluxos os quais possuem *flags* RST ou FIN.

Após este critério de parada, os fluxos expirados são armazenados para que sejam exportados no próximo intervalo de exportação de fluxos.

O formato do cabeçalho de exportação do Netflow, ou seja, a organização das informações capturadas, é fixo na maior parte das versões dessa tecnologia. As versões de Netflow de 1 a 8 trazem um modelo ou *template* de cabeçalho fixo, enquanto a versão 9 introduz o conceito de *template* personalizável [45]. Nessa última versão, essa flexibilidade foi adicionada como forma de proporcionar uma melhor integração da tecnologia Netflow com MPLS, IPv6 e BGP, bem como registros de aplicações personalizadas de usuários. Além disso, é importante ressaltar que as versões mais populares deste protocolo são a 5 e a 9, amplamente utilizadas por dispositivos de rede na atualidade. A Figura 3.4 ilustra o formato do cabeçalho do protocolo Netflow versão 9:

Figura 3.4 - Formato do Cabeçalho NetFlow versão 9.



Como se pode observar, o cabeçalho é formado primeiramente por um cabeçalho de pacote, o qual identifica o protocolo Netflow juntamente de sua versão, um campo denominado *Template Flowset*, ou modelo de exportação, e *N* campos denominados *Data Flowset*, ou dados de conjunto de fluxos. O *Template Flowset* contém a configuração de exportação dos dados de fluxos capturados, ou seja, determina quais atributos de fluxos serão exportados. O número de campos *Data Flowset* é determinado por essa configuração, visto que este último tipo de campo apenas contém as informações de fluxos propriamente ditas.

3.2.2 sFlow

O protocolo sFlow, nome que pode ser definido como uma abreviação para *sampling flow* (amostragem de fluxos), é um protocolo de montagem e exportação de fluxos que, como o próprio nome sugere, utiliza técnicas de amostragem na análise dos dados observados. Essa abordagem é utilizada quando o volume de tráfego de dados é muito elevado, ou seja, em redes de larga escala nas quais a quantidade de informações analisadas é muito elevada. De forma geral, o sFlow é uma tecnologia baseada na utilização de amostragem simples randômica, a qual é suportada por diversos fabricantes de dispositivos de redes, tais como Alcatel, Force10, Extreme, Hitachi e HP por meio da incorporação de agentes sFlow em *switches* e roteadores [45].

Inicialmente desenvolvido pela empresa InMon Inc., este protocolo foi formalmente padronizado pelo IETF por meio do RFC 3176 [46]. Este documento descreve detalhadamente a estrutura e funcionamento do sFlow, definindo mecanismos de amostragem tais como o sFlow Agente e os formatos de amostragem suportados, estruturas que serão descritas no decorrer deste capítulo.

Sua abordagem baseada em amostragem possibilita que a rede seja analisada de forma completa sem a necessidade da análise de todos os pacotes observados. Dentre as principais características deste protocolo, pode-se destacar:

- Escalabilidade: A principal característica do protocolo sFlow é sua escalabilidade, visto que é capaz de analisar e gerar registros de fluxos de redes de larga escala (10 a 100 Gb/s). Além da escalabilidade relacionada à taxa de transmissão da rede, este protocolo suporta a análise de milhares de dispositivos paralelamente por meio de uma única unidade coletora sFlow, o que demonstra sua escalabilidade em relação ao tamanho dessas redes;

- Acurácia: O protocolo sFlow possui a capacidade de, mesmo com a utilização de métricas de amostragem, representar com precisão os processos de comunicação oriundos da observação de pacotes por parte da unidade coletora;
- Custo computacional: O agente sFlow, necessário para a análise, montagem e exportação de fluxos em *switches* e roteadores, é muito simples de ser implementado, não adicionando custo computacional significativo a estes dispositivos;
- Exportação: O protocolo sFlow possibilita a exportação de fluxos minuto a minuto, permitindo uma visualização mais ágil das informações coletadas por mecanismos de gerenciamento de redes ou outras ferramentas baseadas na análise de fluxos.

Segundo o RFC 3176 [46], o sistema de monitoramento do protocolo sFlow é composto de um Agente sFlow, o qual é incorporado em dispositivos de rede tais como *switches* e roteadores, e um coletor sFlow ou central de análise de dados. Segundo [45], o Agente sFlow é um processo de software que combina contadores de interfaces e amostragem de fluxos em datagramas sFlow, os quais são enviados para os coletores sFlow por meio da utilização do protocolo UDP.

O protocolo sFlow trabalha com duas formas de amostragem dos dados observados para a diminuição da quantidade de dados analisados. A primeira delas é denominada *Statistical packet-based sampling of switched flows*. Nessa abordagem de amostragem, o agente sFlow se utiliza de um contador que é decrementado a cada pacote que chega na interface. Uma vez que este contador chega a zero é realizada uma amostra, ou seja, um pacote é capturado e adicionado à montagem de fluxos. Por exemplo, diz-se que a amostragem utilizada pelo protocolo sFlow é 1:256 (1 por 256) quando a cada 256 pacotes que chegam na interface analisada, um deles é adicionado à análise de fluxos, representando os 256 que foram descartados.

A segunda abordagem de amostragem utilizada pelo sFlow é denominada *Time-based sampling of network interface statistics*. Essa abordagem objetiva a utilização de um contador para a realização periódica de sondagem (ou *polling*) nos Agentes sFlow. Assim, um intervalo de sondagem máximo é atribuído para o agente, mas o mesmo possui total acesso a essas configurações, podendo livremente alterar este valor como forma de incrementar a eficiência de cenários específicos. Segundo o RFC 3176 [46], ambas as

abordagens de amostragens são utilizadas de forma combinada em datagramas sFlow, sendo elas projetadas como parte de um sistema integrado.

Atualmente o protocolo sFlow se encontra na versão 5, a qual foi disponibilizada no ano de 2004. Segundo [11], uma das principais diferenças dessa versão em relação às versões anteriores está ligada ao datagrama sFlow, a qual permitem que diferentes fornecedores personalizem alguns campos que possuem suporte à extensão.

3.2.3 IPFIX

Mesmo representando uma alternativa efetiva de abordagem para o gerenciamento de redes, o Netflow continua sendo proprietário da Cisco Systems. Baseado no funcionamento de sua nona versão, a IETF (*International Engineering Task Force*) desenvolveu o IPFIX (*Internet Protocol for Information Export*), uma padronização da coleta de fluxos em redes de computadores. Essa padronização ocorreu inicialmente por meio do RFC 3917 [47], e vem sendo gradativamente adotada por fabricantes de dispositivos de redes, o que simplifica os processos de exportação de fluxos IP para aplicações que as utilizam, tais como sistemas de gerenciamento de redes. De modo geral, o IPFIX pode ser definido como um padrão que determina qual será o formato da informação de fluxo IP coletado que será recebido pelo processo coletor.

A descrição do padrão IPFIX proposto pela IETF é apresentada em diversos documentos, denominados RFCs. Com o passar dos anos, novas funcionalidades e características vão sendo desenvolvidas e descritas em novos RFCs, os quais apresentam melhorias à tecnologia anteriormente proposta. Isso permite à tecnologia um amadurecimento essencial para sua utilização em larga escala em ambientes diversificados, objetivo principal de uma padronização. O IPFIX é composto de 20 diferentes RFCs, sendo que o primeiro foi publicado em outubro de 2004 e o mais atual em março de 2012. A grande maioria dos RFCs propostos descreve características específicas do funcionamento do IPFIX, como o suporte a exportação de fluxos bidirecionais e a "anonimização" de endereços de origem/destino dos fluxos. A Tabela 3.1 aborda todos os RFCs relativos ao IPFIX encontrados na base de dados do IETF [10].

Conforme abordado anteriormente, o IPFIX foi desenvolvido com o objetivo da padronização da forma com que a extração de fluxos IP é realizada. Sendo assim, deve-se possuir suporte para todos os tipos de dispositivos e sistemas de gerenciamento, ou seja, o IPFIX é flexível o bastante para ser utilizado em dispositivos e sistemas de diferentes

fabricantes sem perda de performance ou funcionalidade. Além disso, as conexões presentes entre as etapas de Exportação e Importação de dados segue uma relação *n* para *m*, ou seja, um processo de exportação é capaz de enviar dados para diversos processos coletores, da mesma forma que um processo coletor pode receber fluxos de diversos processos de exportação.

Tabela 3.1 - RFCs que descrevem a tecnologia IPFIX

NÚMERO	TÍTULO	DATA	STATUS
RFC 6526	*IPFIX PER STREAM CONTROL TRANSMISSION PROTOCOL (SCTP) STREAM*	MARÇO 2012	PADRÃO PROPOSTO
RFC 6313	*EXPORT OF STRUCTURED DATA IN IPFIX*	JULHO 2011	PADRÃO PROPOSTO
RFC 6235	*IP FLOW ANONYMIZATION SUPPORT*	MAIO 2011	EXPERIMENTAL
RFC 6183	*IPFIX MEDIATION: FRAMEWORK*	ABRIL 2011	INFORMACIONAL
RFC 5982	*IPFIX MEDIATION: PROBLEM STATEMENT*	AGOSTO 2010	INFORMACIONAL
RFC 5815	*DEFINITIONS OF MANAGED OBJECTS FOR IPFIX*	ABRIL 2010	PADRÃO PROPOSTO
RFC 5655	*SPECIFICATION OF THE IPFIX FILE FORMAT*	OUTUBRO 2009	PADRÃO PROPOSTO
RFC 5610	*EXPORT TYPE INFORMATION FOR IPFIX INFORMATION ELEMENTS*	JULHO 2009	PADRÃO PROPOSTO
RFC 5477	*INFORMATION MODEL FOR PACKET SAMPLING EXPORTS*	MARÇO 2009	PADRÃO PROPOSTO
RFC 5476	*PACKET SAMPLING (PSAMP) PROTOCOL SPECIFICATIONS*	MARÇO 2009	PADRÃO PROPOSTO
RFC 5473	*REDUCING REDUNDANCY IN IPFIX AND PSAMP REPORTS*	MARÇO 2009	INFORMACIONAL
RFC 5472	*IPFIX APPLICABILITY*	MARÇO 2009	INFORMACIONAL
RFC 5471	*GUIDELINES FOR IPFIX TESTING*	MARÇO 2009	INFORMACIONAL
RFC 5470	*ARCHITECTURE FOR IPFIX*	MARÇO 2009	INFORMACIONAL
RFC 5153	*IPFIX IMPLEMENTATION GUIDELINES*	ABRIL 2008	INFORMACIONAL
RFC 5103	*BIDIRECTIONAL FLOW EXPORT USING IPFIX*	JANEIRO 2008	PADRÃO PROPOSTO
RFC 5102	*INFORMATION MODEL FOR IPFIX*	JANEIRO 2008	PADRÃO PROPOSTO
RFC 5101	*SPECIFICATION OF THE IPFIX PROTOCOL FOR EXCHANGE OF IP TRAFFIC FLOW INFORMATION*	JANEIRO 2008	PADRÃO PROPOSTO
RFC 3955	*EVALUATION OF CANDIDATE PROTOCOLS FOR IPFIX*	OUTUBRO 2004	INFORMACIONAL
RFC 3917	*REQUIREMENTS FOR IPFIX*	OUTUBRO 2004	INFORMACIONAL

Para que todas essas etapas possam ser efetuadas com sucesso, a IETF padronizou o formato do pacote de fluxos utilizado pelo IPFIX. É um modelo genérico, com grande capacidade de adaptação, o qual é composto basicamente de um cabeçalho fixo e conjuntos característicos. O cabeçalho sempre contém o número da versão do protocolo IPFIX utilizado, marcações de tempo de inicio e fim do fluxo, o tamanho da mensagem transmitida, um número sequencial (detecção de falhas) e um ID relativo ao local de coleta do fluxo. Já os conjuntos característicos representam os diferentes tipos de dados transportados pelo pacote, e são eles:

- Conjunto de Dados;
- Conjunto de Modelos;
- Conjuntos de opções de Modelo.

Os Conjuntos de dados são responsáveis pelo armazenamento das informações capturadas propriamente ditas. São compostos de sub-campos denominados Registros de Dados, os quais possuem as informações relativas aos parâmetros estipulados no Conjunto de Modelos (abordado em seguida). Os conjuntos de dados estão diretamente relacionados aos conjuntos de modelos, sendo que o tamanho e a posição desses registros são designados por estes modelos. Dessa forma, os registros de fluxos IP coletados se tornam inúteis sem a presença de conjuntos de modelos, os quais relacionam as informações capturadas.

Os Conjuntos de Modelos são responsáveis pela definição dos modelos de estrutura em que os dados do fluxo IP coletados serão organizados. Assim como os Conjuntos de dados, são compostos de sub-cambos denominados Registros de Modelos, os quais definem a forma com que cada um dos diferentes registros de dados são interpretados. Em outras palavras, os registros de modelos são os responsáveis por dar significado às informações presentes no conjunto de dados. Os modelos são compostos por um cabeçalho e uma seqüência de registros denominados Elementos de Informação, os quais possuem uma descrição de cada um dos dados presentes no conjunto de dados. Os modelos sempre possuem em seu cabeçalho um ID que o identifique e um número relativo à quantidade de Elementos de Informação presentes. Estes, por sua vez, são compostos de outros dois campos: um ID que identifica o dado relativo à esse campo e o tamanho desse dado.

Os conjuntos de opções de Modelo possuem uma estrutura semelhante à dos conjuntos de Modelos. São compostos de sub-campos denominados Registros de opções de Modelo, os quais são caracterizados por definir a forma que um determinado campo de um registro de dados será interpretado, ou seja, sua estrutura fundamental. Assim como os conjuntos de modelos, os registros destes conjuntos são constituídos por um identificador, um número relativo ao número de campos presentes e um adicional denominado contador de escopos. Escopos são estruturas semelhantes aos Elementos de Informação, com o diferencial de conter dados relativos aos campos dos Modelos ao invés de referenciar os dados, sendo considerados estruturas de Metadados, ou seja, que armazenam informações relativas à outras informações.

A Tabela 3.2 ilustra o formato de um pacote IPFIX de exemplo, onde é possível se observar o cabeçalho, os dados relativos aos Conjuntos de Modelos e Conjuntos de Dados:

Tabela 3.2 - Exemplo de pacote IPFIX

	BITS 0..15	**BITS 16..31**
CABEÇALHO	VERSION = 0X000A	MESSAGE LENGTH = 64 BYTES
	EXPORT TIMESTAMP = 2005-12-31 23:59:60	
	SEQUENCE NUMBER = 0	
	OBSERVATION DOMAIN ID = 12345678	
CONJUNTOS DE MODELOS	SET ID = 2 (TEMPLATE)	SET LENGTH = 20 BYTES
	TEMPLATE ID = 256	NUMBER OF FIELDS = 3
	TYP = SOURCEIPV4ADDRESS	FIELD LENGTH = 4 BYTES
	TYP = DESTINATIONIPV4ADDRESS	FIELD LENGTH = 4 BYTES
	TYP = PACKETDELTACOUNT	FIELD LENGTH = 4 BYTES
	SET ID = 256 (DATA SET USING TEMPLATE 256)	SET LENGTH = 28 BYTES
CONJUNTOS DE DADOS	RECORD 1, FIELD 1 = 192.168.0.201	
	RECORD 1, FIELD 2 = 192.168.0.1	
	RECORD 1, FIELD 3 = 235 PACKETS	
	RECORD 2, FIELD 1 = 192.168.0.202	
	RECORD 2, FIELD 2 = 192.168.0.1	
	RECORD 2, FIELD 3 = 42 PACKETS	

3.3 ANÁLISE COMPARATIVA: SNMP E FLUXOS IP

Neste capítulo foram abordadas as duas principais tecnologias utilizadas em ferramentas de gerenciamento de redes na atualidade: a tecnologia SNMP e os Fluxos IP. A tecnologia SNMP vem sendo amplamente utilizada desde seu desenvolvimento, principalmente pelo fato de que essa abordagem é simples e eficaz. Ainda hoje, diversos software têm como base essa tecnologia, tais como o Cacti [38] e o NTop [39]. Entretanto, a análise de fluxos IP, a qual pode utilizar os protocolos de exportação NetFlow, sFlow ou IPFIX, vêm se popularizando tanto na literatura quanto no mercado como uma abordagem alternativa e poderosa nos processos de análise e monitoramento de redes.

A tecnologia SNMP funciona com base na utilização de Agentes, os quais devem ser instalados nos dispositivos gerenciados e que disponibilizam informações a uma estação gerente por meio da resposta de mensagens GET e GETNEXT, por exemplo. Todo o processo de gerenciamento disponibilizado por meio dessa tecnologia é baseado na utilização de contadores, os quais podem estar relacionados a diferentes interfaces, armazenando tais informações no próprio objeto gerenciado em uma base de dados denominada MIB.

Na abordagem de gerenciamento de redes por meio da análise de Fluxos IP a metodologia de coleta de informações se diferencia. Seja qual for o protocolo de exportação utilizado (NetFlow, sFlow ou IPFIX), a análise de fluxos IP não necessita da instalação de quaisquer agentes nos objetos gerenciados. Nessa abordagem, o protocolo de exportação é configurado em um dispositivo de rede (roteador, *switch*, *firewall*, etc.), normalmente que agregue o tráfego de toda a rede ou de um setor específico. Dessa forma, todo o tráfego que representa os processos de comunicação da rede analisada que for transmitido através desses equipamentos é analisado, amostrado (se for o caso), transformados em fluxos IP e exportados para uma estação coletora. Essa estação se responsabiliza pelo armazenamento dos fluxos recebidos e, na maioria dos casos, pela disponibilização desses dados para ferramentas específicas de gerenciamento de redes.

Quando as duas tecnologias são comparadas, diversas diferenças podem ser observadas. Num primeiro momento, uma característica que se destaca bastante é a necessidade da execução de um processo Agente em todos os dispositivos que devem ser gerenciados pela tecnologia SNMP. Em uma situação onde se deseja monitorar a utilização da Internet de dispositivos individuais pertencentes a um segmento de rede se faz necessária a instalação de processos Agentes em cada um dos dispositivos analisados. Na análise de fluxos IP, basta instalar um dispositivo com suporte a um dos protocolos de exportação discutidos no *gateway* ou saída padrão dessa rede. Dessa forma, o dispositivo é capaz de gerar fluxos IP relativos a todos os processos de comunicação que passam por ele, ou seja, todos os processos de comunicação dos dispositivos pertencentes à rede analisada com dispositivos externos (Internet, por exemplo).

Além disso, outra característica importante que se destaca entre as tecnologias SNMP e de fluxos IP é a gama de informações providas, bem como a forma com que essas informações são disponibilizadas pelos protocolos para os processos de gerenciamento. Como destacado, a tecnologia SNMP é baseada na utilização de contadores, os quais representam a maior parte das informações armazenadas pelos dispositivos em suas MIBs e disponibilizados para a estação gerente. Para o gerenciamento de tráfego de volume

essas informações são essenciais, e suprem toda a necessidade de ferramentas de gerenciamento baseadas em tal análise. Entretanto, com a popularização da Internet, as redes vêm crescendo de forma constante tanto em magnitude quanto na complexidade de sua análise. Em redes de larga-escala, ambientes de alta agregação de tráfego, o gerenciamento e identificação de falhas, ataques e outras anomalias vem se tornando uma tarefa cada vez mais complexa de ser executada através de abordagens baseadas apenas na análise de volume de tráfego. Os fluxos IP trazem uma ampla gama de informações sobre todo o comportamento da rede: não somente informações quantitativas, tais como volume de bytes, número de pacotes, duração do fluxo ou número de fluxos que compõem um processo de comunicação, mas também informações qualitativas, tais como endereços IP de origem e destino e portas de origem e destino de dispositivos que se comunicam e o protocolo de camada de transporte utilizado neste processo.

Como forma de simplificar este processo de comparação entre as tecnologias abordadas, a empresa Paessler, uma desenvolvedora de tecnologias de análise e gerenciamento de redes, disponibilizou em [48] uma tabela comparativa. Essa tabela ilustra as principais diferenças do ponto de vista específico da ferramenta PRTG dessa empresa, mas destaca alguns aspectos que podem ser observados em qualquer situação. A Tabela 3.3, ilustra uma versão resumida da fonte citada [48], destacando as informações mais relevantes do ponto de vista geral.

Tabela 3.3 - Diferenças entre SNMP e NetFlow

	SNMP	**NetFlow**
Tráfego pode ser filtrado	Não	Sim
Diferencia utilização de banda por protocolo ou IP	Não	Sim
Possibilita a criação de listas TOP (protocolos, conexões, etc)	Não	Sim
Filtragem da utilização de banda por porta física da rede	Sim	Não
Largura de banda utilizada para o monitoramento	Pequena	Depende do Tráfego

Como pode ser observado, a empresa citada utiliza o protocolo NetFlow como padrão de comparação. Como esse protocolo não possui suporte a amostragem, a banda utilizada para monitoramento pode ser elevada em redes de larga escala. Nesses casos recomenda-se a utilização dos protocolos sFlow e IPFIX, os quais possuem suporte de amostragem.

4 SISTEMA DE DETECÇÃO DE ANOMALIAS

Com o constante crescimento das redes de computadores na atualidade, principalmente as de larga escala, tais como redes de grandes empresas, governamentais, hospitalares e de provedores de serviço de Internet, a necessidade de novas ferramentas de gerenciamento capazes de detectar e identificar anomalias é cada vez maior. Essas ferramentas devem ser capazes de analisar uma grande quantidade de tráfego de dados de forma ágil e eficaz, tarefa cada vez mais complexa.

Este capítulo tem como objetivo a descrição da ferramenta de detecção de anomalias proposta e desenvolvida neste trabalho. Essa ferramenta tem como objetivo a análise de fluxos IP, a detecção e a identificação de anomalias em redes de larga escala, utilizando uma abordagem inovadora que analisa de forma autônoma sete diferentes dimensões (atributos) de fluxos IP simultaneamente.

4.1 CARACTERIZAÇÃO DE TRÁFEGO

Para possibilitar essa análise, o sistema se baseia em um dos paradigmas mais utilizados e bem aceitos em ferramentas e abordagens de detecção de anomalias na atualidade, tanto na literatura quanto no mercado: a caracterização de tráfego. Neste paradigma, o sistema de detecção primeiramente analisa o comportamento normal da rede, se utilizando de métodos estatísticos, heurísticos ou de mineração de dados na criação de um padrão ou perfil que descreva o comportamento normal da rede analisada. Como abordado anteriormente, a análise de fluxos IP disponibiliza uma ampla gama de informações relativas aos processos de comunicação das redes de computadores. Dessa forma, pode-se gerar múltiplos perfis que representam o comportamento normal da rede, cada um descrevendo um atributo ou dimensão específico. O sistema aqui descrito analisa de forma simultânea sete diferentes dimensões de fluxos, gerando sete diferentes perfis de redes, aqui denominados *Digital Signature of Network Segment using Flow analysis* - DSNSF (ou, da tradução literal, Assinatura Digital de Segmento de Rede utilizando análise de Fluxos). As dimensões analisadas representam tanto volume de tráfego quanto informações qualitativas referentes aos processos de comunicação transmitidos através da rede analisada, sendo elas: bits/s, pacotes/s, fluxos/s, endereços IP de origem e destino e portas de origem e destino.

Conforme discutido anteriormente, o sistema descrito deve ser capaz de unir a eficiência de análise, traduzida pela alta taxa de alarmes reais (anomalias detectadas)

disparados em conjunto com a baixa taxa de ocorrência de falsos alarmes, e a agilidade de abordagens com baixo custo computacional, justificada pela alta quantidade de dados processados oriundos de redes de larga escala. A caracterização de tráfego é o processo base do sistema apresentado, sendo o processo com maior custo computacional inerente de todo o sistema. Isso se dá devido ao fato de que, nessa etapa, ocorre todo o processamento real dos dados utilizados no processo de análise, detecção e identificação de anomalias. Dessa forma, faz-se necessária a utilização de um método simples, ágil e eficaz na caracterização de tráfego deste sistema: o Holt-Winters *for Digital Signature* - HWDS (Holt-Winters para Assinaturas Digitais). Este método é uma versão aprimorada do tradicional método estatístico de previsão Holt-Winters (HW), o qual possibilita a obtenção de melhores resultados (previsões) na geração de assinaturas digitais (DSNSFs).

4.1.1 *Exponentially-Weighted Moving Average* (EWMA)

Antes de introduzir os conceitos relativos à utilização dos métodos HW e HWDS na caracterização de tráfego, é necessário compreender o funcionamento de equações do tipo *Exponentially-Weighted Moving Average* (EWMA) [20], ou segundo Brutlag [31], a suavização exponencial. A EWMA é uma técnica estatística simples (estimador), o qual realiza uma soma ponderada entre o valor atual e um valor relativo ao acúmulo dessas ponderações ao longo do tempo analisado. Dessa forma, pode-se estimar o valor do próximo intervalo de tempo analisado com base nos intervalos anteriores. Equações do tipo EWMA são representadas na seguinte forma:

$$k_{t+1} = \rho K_t + (1-\rho) k_t \quad (1)$$

onde k_t é o acúmulo das ponderações ao longo do tempo t, K_t é o valor da medição atual ou corrente, ρ é uma variável denominada "coeficiente de suavização", a qual deve necessariamente pertencer ao intervalo $0 < \rho < 1$, e k_{t+1} é o valor relativo à previsão calculada.

Dessa forma, a principal característica de equações do tipo EWMA é a soma ponderada, possibilitada por meio do coeficiente de suavização aqui representado por ρ. Essa constante é responsável por indicar o peso que os dados atuais possuem, com relação a dados históricos, no cálculo da previsão do próximo valor. Tipicamente, são utilizados valores

baixos para a constante que representa o coeficiente de suavização, uma vez que dados históricos possuem maior peso no cálculo de previsões que valores atuais. Além disso, equações do tipo EWMA são conhecidas como suavizações exponenciais devido ao fato de que o peso dos dados passados decai exponencialmente em relação à uma nova predição ao longo do tempo, a medida que tais dados vão se tornando mais antigos.

As equações do tipo EWMA são muito utilizadas em diversos campos, inclusive na área da computação na predição de valores temporais devido à sua simplicidade e eficiência. Entretanto, em casos onde existe a presença de periodicidade e tendência de crescimento/decrescimento essa equação não é aplicável. No caso específico deste trabalho, os dados analisados são relativos a dias completos de monitoramento de rede, os quais possuem tendências de crescimento e periodicidade, uma vez que cada horário do dia possui um comportamento de tráfego característico. Dessa forma, nestes casos recomenda-se a utilização do método estatístico de previsão Holt-Winters [31].

4.1.2 Holt-Winters (HW)

O método estatístico de previsão Holt-Winters [22] foi desenvolvido por Charles C. Holt e Peter R. Winters no ano de 1960 com o objetivo de auxiliar no cálculo da previsão de vendas de varejo. Os autores observaram que a utilização de equações EWMA não se aplicava à essa situação devido ao fato de que estes ambientes possuem tendência de crescimento linear, além da presença de periodicidade, ou seja, períodos do ano em que as vendas possuem um comportamento característico. Dentre esses períodos pode-se destacar, por exemplo, o mês de Dezembro, onde o número de vendas aumenta significativamente, e Fevereiro, quando existe uma queda brusca neste número.

Segundo Goodwin [49], mesmo após mais de 50 anos de seu desenvolvimento, o método Holt-Winters continua sendo amplamente utilizado principalmente devido à sua simplicidade. Mesmo quando aplicado a uma grande quantidade de dados, este método é capaz de disponibilizar previsões precisas. Segundo o autor, o método possui baixos requisitos de armazenamento de informação, ou seja, não é necessário o armazenamento de um amplo banco de dados para a geração da próxima previsão. Além disso, o método Holt-Winters é facilmente automatizado devido à simplicidade de suas operações, baseadas em equações do tipo EWMA. Por fim, outra vantagem do método está na sua capacidade adaptativa, uma vez que o Holt-Winters é capaz de se adaptar e incorporar alterações e mudanças em padrões relativos a tendências de periodicidade e linear nas vendas.

Ainda segundo Goodwin [49], ao longo dos anos o método Holt-Winters tem sido adaptado para utilização nas mais diversas áreas do conhecimento, as quais não foram originalmente analisadas por seus criadores. Na área da computação, mais especificamente na análise e gerenciamento de redes de computadores, a primeira utilização deste método foi apresentada por Brutlag [31] no ano de 2000. Em seu trabalho, o autor utilizou o método Holt-Winters na caracterização do tráfego normal de uma rede de computadores ainda utilizando os contadores de volume disponíveis por meio da tecnologia SNMP. Depois deste trabalho, diversos autores [33, 34] vêm utilizando o Holt-Winters na caracterização de tráfego de redes nos mais variados ambientes (corporativas, móveis, de larga escala, etc.) devido à eficácia de sua predição e sua simplicidade e baixo custo computacional.

De forma resumida, o método Holt-Winters pode ser definido como um modelo estatístico de previsão aplicado a séries temporais caracterizadas por meio da presença de tendência linear e periodicidade (sazonalidade). Suas operações são baseadas no modelo de suavização exponencial (EWMA), o que garante a simplicidade e adaptação a mudanças anteriormente mencionadas. O funcionamento deste método é realizado por meio da divisão dos dados analisados em três partes, cada uma sendo representada por uma equação do tipo EWMA. Essas partes são [22]:

- *Baseline*: Tendência base que representa o comportamento da série temporal analisada. É representada pela variável *a*;
- Tendência Linear: Tendência de crescimento ou decrescimento linear apresentado pela série temporal analisada. É representada pela variável *b*;
- Sazonalidade: Tendência sazonal, ou seja, relativa à periodicidade apresentada pela série temporal analisada. É representada pela variável *c*.

É importante ressaltar que *Baseline* neste contexto representa apenas a tendência base da previsão na série temporal analisada. É comum em trabalhos relacionados à caracterização de tráfego que este termo seja utilizado para designar o perfil ou assinatura que descreva o comportamento normal de rede. Entretanto, este termo é definido na literatura [22, 31] como a equação EWMA que representa a tendência base da previsão e, portanto, iremos manter essa nomenclatura. Neste trabalho, sempre que for necessária a utilização de um termo para designar um perfil ou assinatura que represente o comportamento normal de rede será utilizada a sigla DSNSF (*Digital Signature of Network Segment using Flow analysis*).

No método Holt-Winters, a previsão y'_{t+1}, obtida através do valor corrente y_t, é dada pela seguinte equação:

$$y'_{t+1} = a_t + b_t + c_{t+1-s} \quad (2)$$

Na equação (2), a variável t indica o intervalo de tempo analisado, s indica o período do ciclo sazonal (periodicidade) da série temporal, y_t é o valor da série temporal no intervalo de tempo t e y'_{t+1} é a previsão calculada para o intervalo de tempo t+1. As três partes que compõem o cálculo dessa previsão são obtidas através das equações:

$$a_t = \alpha\,(y_t - c_{t-s}) + (1 - \alpha)\,(a_{t-1} + b_{t-1}) \quad (3)$$

$$b_t = \beta\,(a_t - a_{t-1}) + (1 - \beta)\,b_{t-1} \quad (4)$$

$$c_t = \gamma\,(y_t - a_t) + (1 - \gamma)\,c_{t+1-s} \quad (5)$$

Como se pode observar, as equações acima descritas são da mesma forma da Equação (1), sendo caracterizadas como do tipo EWMA. Como analisado na seção anterior, essas equações são caracterizadas por uma divisão em duas partes, cada qual recebe um peso no resultado final. Este peso é definido por meio da utilização das constantes α, β e γ, possibilitando a criação de previsões mais suaves.

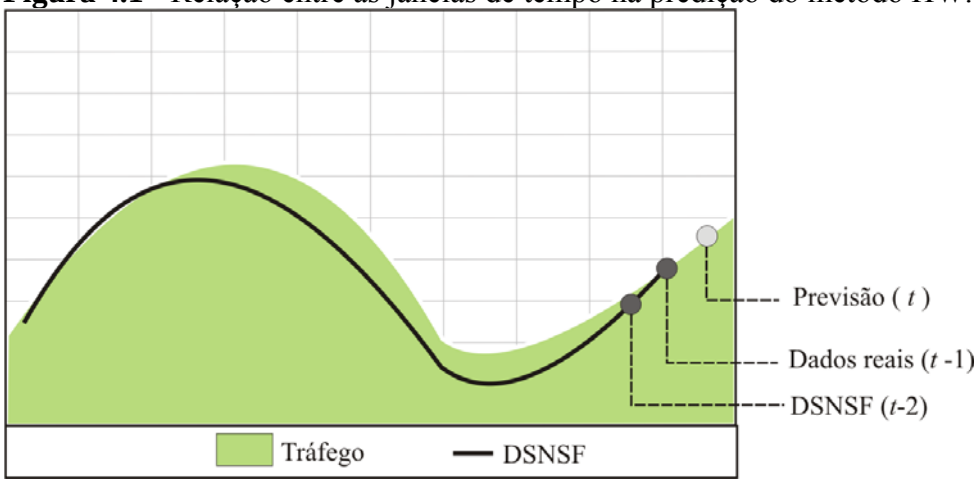
Os valores designados para as constantes α, β e γ influenciam diretamente o comportamento da previsão gerada. Essas constantes são denominadas coeficientes de suavização, e seus valores devem necessariamente pertencer ao intervalo $0 < \alpha, \beta, \gamma < 1$. Essa capacidade de ajuste permite a obtenção do DSNSF mais rápida ou lentamente, de acordo com os requerimentos específicos do segmento de rede analisado.

Para a utilização do método Holt-Winters na criação de DSNSFs, os coeficientes de suavização devem possuir valores pequenos, ou seja, próximos de zero [31]. Neste tipo específico de aplicação (caracterização de tráfego), a velocidade de convergência da previsão (DSNSF) não deve ser rápida devido ao fator de adaptabilidade do método com relação a *outliers*, ou seja, comportamentos de rede que diferem do normal. Quanto mais rápida essa conversão, maior influência *outliers* terão na geração de DSNSFs, diminuindo a eficiência do modelo na caracterização do tráfego normal do segmento de rede analisado. Dessa forma, ao se atribuir valores pequenos aos coeficientes de suavização, o método Holt-

Winters atribui um maior peso para dados históricos, suavizando o impacto causado por mudanças oriundas do novo conjunto de dados analisados.

Outra característica importante do método Holt-Winters é que, com exceção da constante *c* (tendência sazonal), não é necessário armazenar os valores relativos às constantes *a* (*baseline*) e *b* (tendência linear) calculados nas últimas iterações do método. Assim, para o cálculo da previsão para o ponto *t* o algoritmo utiliza as informações de previsão já existentes, calculadas no instante $t-2$ para prever o comportamento de $t-1$ (DSNSF), em conjunto com as informações do período $t-1$. A Figura 4.1 ilustra essa relação, onde os pontos mais escuros ilustram os períodos de tempo utilizados para o cálculo da previsão, representada pelo ponto mais claro.

Figura 4.1 - Relação entre as janelas de tempo na predição do método HW.



4.1.3 Holt-Winters *for Digital Signature* (HWDS)

Visando atingir melhores resultados relativos à criação do DSNSF, foi proposta e utilizada uma versão aprimorada do método Holt-Winters tradicional, denominada Holt-Winters *for Digital Signature* (HWDS), ou Holt-Winters para Assinaturas Digitais. Dessa forma, foram implementadas modificações nas equações que descrevem os componentes *baseline* e tendência linear do modelo tradicional, apresentados pelas Equações (3) e (4), respectivamente. Para se alcançar uma melhor adaptação do comportamento normal (DSNSF) dos segmentos analisados, uma abordagem similar à utilizada pelo componente de tendência sazonal, Equação (5), é implementada. Assim, ao invés de se utilizar os intervalos de tempo imediatamente anteriores ao analisado para o cálculo da previsão, são utilizados intervalos de tempo iguais ao corrente, com o diferencial de serem relativos ao período

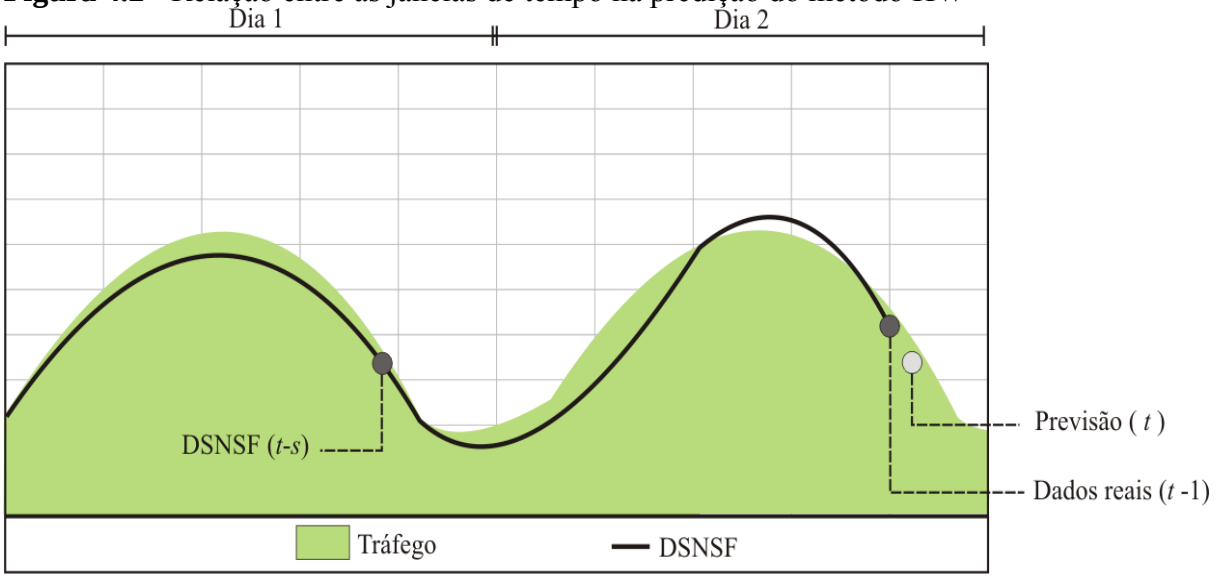
sazonal anterior. Essa alteração pode ser observada nas novas equações que representam o *baseline* e a tendência linear para o método HWDS:

$$a_t = \alpha\,(y_t - c_{t-s}) + (1 - \alpha)\,(a_{t-s} + b_{t-s}) \quad (6)$$

$$b_t = \beta\,(a_t - a_{t-s}) + (1 - \beta)\,b_{t-s} \quad (7)$$

Por meio dessa nova abordagem, para o cálculo da previsão para o ponto t o algoritmo utiliza as informações de dados reais, obtidos em $t-1$, em conjunto com as informações de DSNSF de mesmo intervalo de tempo, com o diferencial de pertencer ao período sazonal anterior, ou seja, no ponto $t-s$. A Figura 4.2 ilustra essa nova relação, onde os pontos mais escuros ilustram os períodos de tempo utilizados para o cálculo da previsão, representada pelo ponto mais claro ao final.

Figura 4.2 - Relação entre as janelas de tempo na predição do método HW



Essa modificação permite que a suavização seja realizada com intervalos de tempo que representam a mesma janela de tempo, ao contrário do método tradicional que utiliza intervalo da série temporal imediatamente anterior ao analisado para o cálculo da predição. Em termos de dados reais, cada janela de série temporal representa uma janela de tempo no dia analisado.

Por exemplo, para que seja possível o cálculo da predição do comportamento da janela de tempo que representa o horário das 14h em uma análise que separa o dia em janelas de tempo de 5 minutos, o método Holt-Winters utilizaria dados

relativos às 13h55min. Por outro lado, o método HWDS utilizaria os dados relativos à uma janela de tempo que representa o horário das 14h, porém relativo ao período sazonal anterior, ou seja, ao dia anterior.

A mudança proposta e implementada é justificada pois, em dias similares, janelas temporais iguais tendem a ser semelhantes, o que não ocorre com janelas temporais consecutivas de uma mesma série temporal. Essa medida melhora os resultados obtidos no processo de criação de DSNSFs.

A geração de DSNSF utilizando o método HWDS ocorre dinamicamente, ou seja, o DSNSF gerado passa por alterações a cada novo dia processado pelo método. Dessa forma, os dados utilizados são relativos a dois tipos de entrada para o cálculo da previsão de como o próximo dia deve se comportar: os dados do dia atual e o DSNSF (previsão e valores dos componentes *a, b* e *c*) gerado para o dia anterior. Em outras palavras:

$$DSNSF_{amanha} = HWDS(Dados\_Reais_{hoje}, DSNSF_{ontem})$$

Essa característica permite que o método se adapte a mudanças comportamentais do segmento de rede analisado de forma simplificada, sem a necessidade da realização de quaisquer ajustes adicionais no método.

Como discutido anteriormente, os coeficientes de suavização possuem um papel fundamental no cálculo das previsões utilizando o método Holt-Winters. Essa característica é mantida no método HWDS, onde essas constantes devem possuir valores pequenos para tornar as modificações assimiladas pelo DSNSF após o processo de predição mais suave.

4.1.4 Intervalos de Confiança

De acordo com Brutlag [31], a utilização de intervalos de confiança ou limites é uma eficiente abordagem para a detecção de anomalias a qual indica um intervalo onde variações são consideradas normais. Entretanto, a abordagem descrita pelo autor é simétrica, ou seja, as distâncias entre a estimativa e os limites inferior e superior são iguais. Essa característica permite a classificação de comportamentos anômalos como normais em redes onde variações são predominantemente inferiores ou superiores que as estimativas realizadas. Neste trabalho é proposta uma abordagem assimétrica para a geração de intervalos de confiança, onde os limites superior e inferior são calculados separadamente:

$$LI = y'_t - \delta d1_t$$
$$LS = y'_t + \delta d2_t \quad (8)$$

Na Equação (8), os limites superior (LS) e inferior (LI) são calculados utilizando a previsão ou estimativa (DSNSF) y'_t, um fator escalar δ para a largura do intervalo de confiança variando no intervalo $2 < \delta < 3$ [31], e pela medida de desvio d, a qual pode ser calculada de duas formas:

$$d_t = \gamma(|\, y_t - y'_t \,|) + (1 - \gamma)\, d_{t-s} \quad (9)$$
$$d_t = \gamma(\ \sigma(y'_t)\ ) + (1 - \gamma)\, d_{t-s} \quad (10)$$

Se o valor de y_t é superior ou igual ao valor da previsão y'_t, $d1_t$ é atualizado utilizando a equação (9) e $d2_t$ é atualizado utilizando a equação (10). Caso contrário, se o valor y_t é inferior ao valor da previsão y'_t, $d1_t$ é atualizado usando a equação (10) e $d2_t$ é atualizado usando a equação (9). Em outras palavras, os intervalos onde o erro é predominantemente superior são atualizados com o desvio absoluto do intervalo e o limite oposto é atualizado por meio do desvio padrão (σ) da previsão.

Figura 4.3 - Algoritmo 1: HWDS utilizado na criação de DSNSF.

Algorithm 1 – HWDS utilizado na criação do DSNSF

Require: Conjunto de dados de fluxos das sete dimensões coletados de um banco de dados histórico; valores pre-definidos para os coeficientes de suavização.

Ensure: μ: Vetor representando o atributo de fluxo analisado para um dia, o qual é dividido em 1440 intervalos de 1 minuto. Em outras palavras, são os valores do DSNSF gerado para o próximo dia.
LI, LS: Limites Inferior e Superior ou intervalos de confiança.

1: **for** $i = 1$ to 1440 **do**
2: Cálculo do baseline para i (6)
3: Cálculo da tendência linear para i (7)
4: Cálculo da tendência sazonal para i (5)
5: Cálculo da previsão para $i + 1$ (2)
6: Cálculo dos limites Superior e Inferior (8)
7: $LS_i \leftarrow$ limite superior
8: $LI_i \leftarrow$ limite inferior
9: $\mu_i \leftarrow$ previsão calculada
10: **end for**
11: **return** μ, LS, LI

O funcionamento básico do método HWDS pode ser observado no Algoritmo presente na Figura 4.3.

4.1.5 Métodos de Preparação dos Dados

Conforme abordado anteriormente, o sistema apresentado utiliza a análise de fluxos IP para o monitoramento, detecção e identificação de anomalias, por meio de uma abordagem inovadora que utiliza sete diferentes dimensões ou atributos de fluxos. Essas dimensões são submetidas a um processo de caracterização de tráfego por meio de sua aplicação ao método HWDS, sendo elas: bits/s, pacotes/s, fluxos/s, endereços IP de origem e destino e portas de origem e destino.

As dimensões bits/s, pacotes/s e fluxos/s são métricas quantitativas, as quais possibilitam a geração de gráficos de movimento de tráfego (e, consequentemente, a criação de DSNSFs) do dia analisado sem quaisquer processos de tratamento sobre esses dados. As dimensões restantes (Endereços IP de origem e destino e portas de origem e destino) são métricas qualitativas que descrevem os dispositivos que participam nos processos de comunicação, bem como as portas utilizadas para isso.

Para possibilitar a utilização das quatro dimensões qualitativas no processo de caracterização de tráfego de rede, o cálculo da Entropia de Shannon [19] é aplicado. Isso possibilita a análise comportamental da rede por meio dos graus de concentração ou dispersão dos elementos nas dimensões utilizadas. Quanto maiores os valores de entropia obtidos em uma análise, mais dispersa se encontra a distribuição analisada, enquanto baixos valores de entropia indicam uma alta concentração de elementos na distribuição. Dessa forma, calcula-se a distribuição de probabilidade de cada intervalo de tempo analisado para as 4 diferentes dimensões por meio da equação:

$$p(x_i) = \frac{n_i}{N} \tag{11}$$

Na Equação (11), $p(x_i)$ é a distribuição de probabilidade de x para cada elemento i, obtido através do número de ocorrência n_i desses elementos dividido pelo número total de ocorrências N no intervalo de tempo analisado. Assim, a entropia deste intervalo pode ser calculada através da equação:

$$H(x) = -\sum_{i}^{N} p(x_i) \cdot \log_2 p(x_i) \tag{12}$$

Além disso, o intervalo de tempo de análise utilizado no processo de caracterização de tráfego é de 1 minuto, o que representa uma abordagem mais ágil de análise e detecção de comportamentos anômalos na rede. Dessa forma, essa abordagem utiliza um total de 1440 diferentes intervalos (janelas de tempo) que representam o comportamento do dia analisado. Diversos trabalhos [16, 17, 18] na literatura utilizam intervalos de 5 minutos em seus processos de detecção de anomalia devido ao fato de que essa abordagem reduz a granularidade dos dados analisados, facilitando a caracterização de tráfego e, consequentemente, diminuindo o número de alarmes falso-positivos (alarmes disparados erroneamente). Entretanto, essa abordagem clássica vem se tornando cada vez mais impraticável devido ao aumento nas taxas de transmissão de redes de larga escala. Em uma rede 10 Gigabit Ethernet, por exemplo, em 5 minutos, até 400% mais dados (3 Terabits) podem ser comprometidos em comparação com a abordagem de 1 minuto (0.6 Terabits). Dessa forma, para que seja possível a análise da rede em intervalos de 1 minuto, utiliza-se a Suavização Exponencial [20] para reduzir a granularidade dos dados por meio de equação:

$$m_1 = x_0 \, , \; t = 0$$
$$m_t = \omega \, (y_t) + (1 - \omega) \, m_{t-1}, \; t > 1 \tag{13}$$

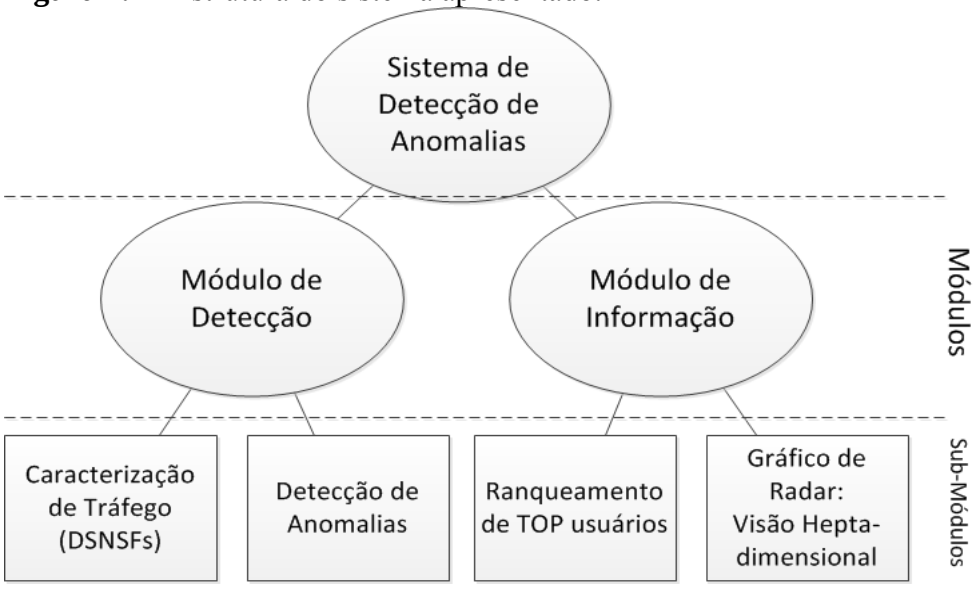
Nessa equação, m representa os dados suavizados, y são os dados não tratados, t é o intervalo de tempo analisado, variando de 1 a 1440, e ω é o coeficiente de suavização. A utilização da técnica de Suavização exponencial não descaracteriza os dados suavizados que representam o comportamento normal da rede, preservando todas as suas tendências de crescimento e decrescimento. Ela apenas reduz a granularidade da série temporal analisada, eliminando a ocorrência de picos abruptos nos movimentos de tráfego gerados. Os testes apresentados na seção 5.2.1, comprovam por meio de avaliações de performance específicas que a utilização dessa técnica não compromete os dados analisados de forma alguma.

4.2 DETECÇÃO E IDENTIFICAÇÃO DE ANOMALIAS

A detecção de anomalias apresentada neste trabalho é baseada na análise e caracterização do tráfego com relação a sete diferentes dimensões de fluxos, conforme discutido na seção 4.1. Essa abordagem explora a riqueza de informação disponibilizada por meio da análise de Fluxos IP de redes de modo a tornar os processos de caracterização e a detecção de anomalias mais preciso e eficaz.

Além do recurso de detecção de anomalia, este sistema provê a administradores de rede informações relevantes para auxiliar na solução do ataque ou falha detectado. Estes dados diminuem a complexidade de análise da anomalia, aumentando a confiabilidade e a disponibilidade da rede, bem como a velocidade do processo de tomada de decisão, mitigando o impacto causado na rede e em seus usuários finais. Dessa forma, o sistema apresentado pode ser dividido em 2 módulos: o Módulo de Detecção e o Módulo de Informação. O primeiro é responsável pelos processos de caracterização de tráfego e detecção de anomalias, e o segundo disponibiliza informações relevantes sobre a anomalia detectada. A Figura 4.4 resume a estrutura do sistema:

Figura 4.4 - Estrutura do sistema apresentado.



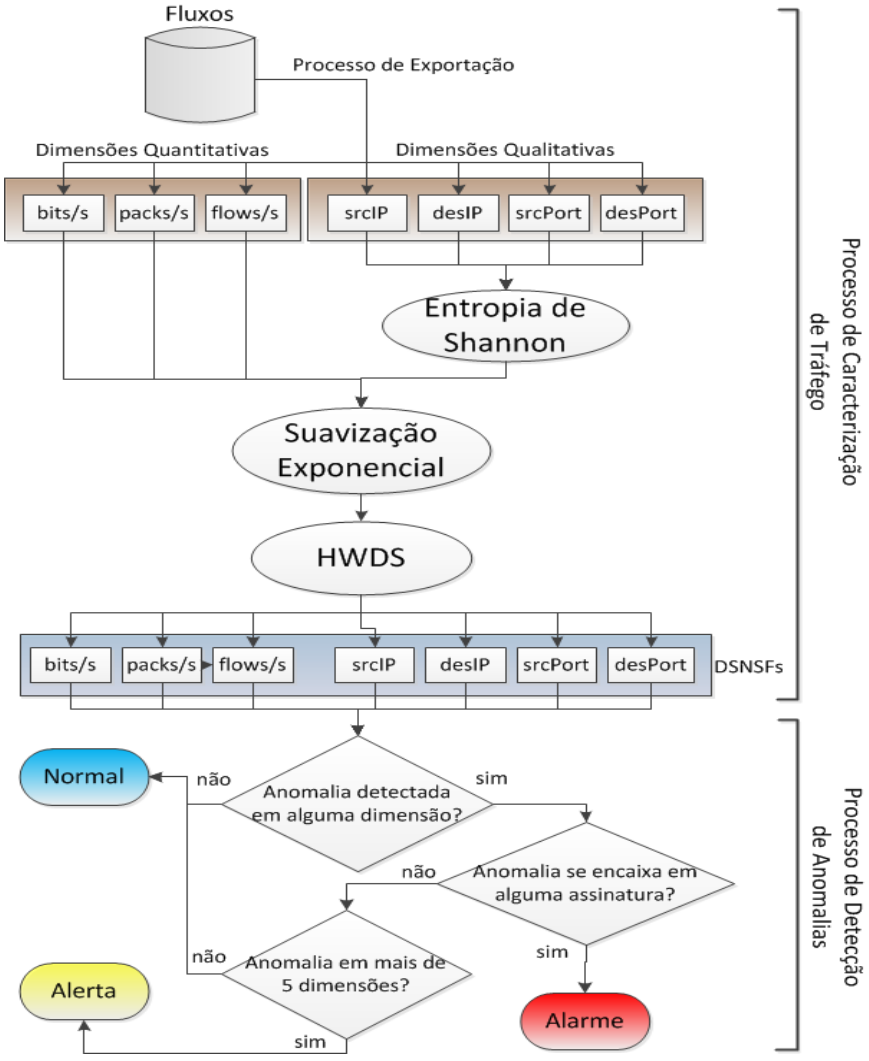
4.2.1 Módulo de Detecção

Este módulo é responsável pelos processos de caracterização de tráfego e detecção de anomalias no segmento de rede analisado. É importante ressaltar que, no modelo de gerenciamento de redes proposto, os processos deste módulo são realizados de forma

inteiramente autonômica, sem qualquer interferência do administrador de redes. O diagrama de funcionamento deste módulo é apresentado na Figura 4.5.

Como se pode observar, os métodos e procedimentos descritos na seção 4.1 são parte essencial do Módulo de Detecção. O primeiro processo envolve a exportação dos registros de fluxos coletados em arquivos. Neste passo, dados relativos às dimensões analisadas são extraídos por meio do aplicativo NFDump [9] em arquivos separados, de modo que estes possam ser submetidos ao processo de caracterização de tráfego (geração de DSNSFs). Conforme descrito na seção 4.1.5, os atributos (ou dimensões) de fluxos bits/s, pacotes/s e fluxos/s são métricas quantitativas que possibilitam a geração de gráficos de movimento dos dias analisados sem qualquer tratamento nos dados. As dimensões analisadas restantes (Endereços IP e portas de origem e destino) são métricas qualitativas que descrevem os dispositivos que participam em processos de comunicação. Dessa forma, essas quatro dimensões são tratadas por meio da técnica Entropia de Shannon, descrita pela Equação (12).

Figura 4.5 - Diagrama de funcionamento do Módulo de Detecção.



Ainda conforme a seção 4.1.5, a abordagem utilizada pelo sistema apresentado, caracterizada pela utilização de janelas de análise de 1 minuto, possui elevada granularidade dos dados. Essa característica diminui a eficácia do processo de caracterização de tráfego, o que pode comprometer a eficiência do sistema como um todo. Para solucionar este problema sem aumentar o intervalo de análise, os dados de todas as dimensões são submetidos à técnica de Suavização Exponencial, descrita pela Equação (13).

Após os processos de preparação dos dados, as sete dimensões de fluxos são submetidas ao método HWDS, descrito na Figura 4.3, o qual é responsável pela geração de DSNSFs e intervalos de confiança (*thresholds*) para cada um deles. Como a geração de DSNSFs pelo método HWDS ocorre de forma dinâmica, o sistema requer apenas dados históricos relativos à um dia anterior e o último DSNSF gerado. Assim, para cada novo dia submetido ao sistema de detecção de anomalias, sete DSNSFs são gerados para descrever o comportamento do próximo dia.

Após a geração de DSNSFs para cada uma das sete dimensões analisadas (caracterização de tráfego), o processo de detecção de anomalias se inicia. Diferentes tipos de anomalias se comportam de maneiras diferentes, o que dificulta o processo de detecção e identificação de anomalias em sistemas tradicionais baseados em poucos (ou mesmo apenas um) atributos de fluxo. Com a riqueza de informação provida pela análise hepta-dimensional, o sistema apresentado utiliza duas diferentes abordagens no processo de detecção de anomalias: a geração de Alertas e a geração de Alarmes por meio de assinaturas. O conceito de anomalia utilizado neste trabalho engloba qualquer comportamento que se encontra fora dos intervalos de confiança gerados a partir dos DSNSF em qualquer dimensão. Para simplificar a explicação do processo de detecção de anomalias, este conceito é dividido em "anomalias locais", desvios comportamentais em uma única dimensão, e "anomalias globais", que são anomalias geradas pela combinação de diferentes anomalias locais, as quais disparam Alertas e Alarmes no sistema.

Essas duas abordagens são predominantemente similares, detectando comportamentos anômalos e disparando avisos sobre o problema para o administrador de redes. Sua diferença está no tipo de detecção: alarmes detectam anomalias que possuem uma assinatura registrada no sistema (comportamento conhecido), enquanto alertas identificam anomalias ainda desconhecidas para o sistema. A incorporação de novas assinaturas comportamentais de anomalias no sistema é discutida na seção 4.2.2.

Alertas são anomalias globais cujo comportamento ainda é desconhecido pelo sistema. Essas anomalias não se enquadram em nenhuma das assinaturas

comportamentais existentes no sistema. A geração de Alertas ocorre quando 5 ou mais das dimensões analisadas (no nosso caso são sete) apresentam anomalias no mesmo intervalo de tempo. A escolha deste número é justificada na seção 5.2.2, onde são apresentados resultados quantitativos que comprovam a maior eficácia do sistema utilizando essa quantidade de dimensões.

Alarmes são anomalias globais que possuem assinatura comportamental conhecida pelo sistema, sendo capazes de diretamente identificar a anomalia de acordo com este comportamento. A geração de Alarmes no sistema ocorre quando o padrão comportamental da anomalia global detectada em um intervalo de tempo através das sete dimensões analisadas se enquadra na assinatura de algum ataque ou falha conhecido pelo sistema.

4.2.2 Módulo de Informação

Este módulo é responsável por prover a administradores de rede informações relevantes sobre a anomalia detectada, também permitindo a identificação de anomalias ainda desconhecidas por meio da criação de novas assinaturas no sistema.

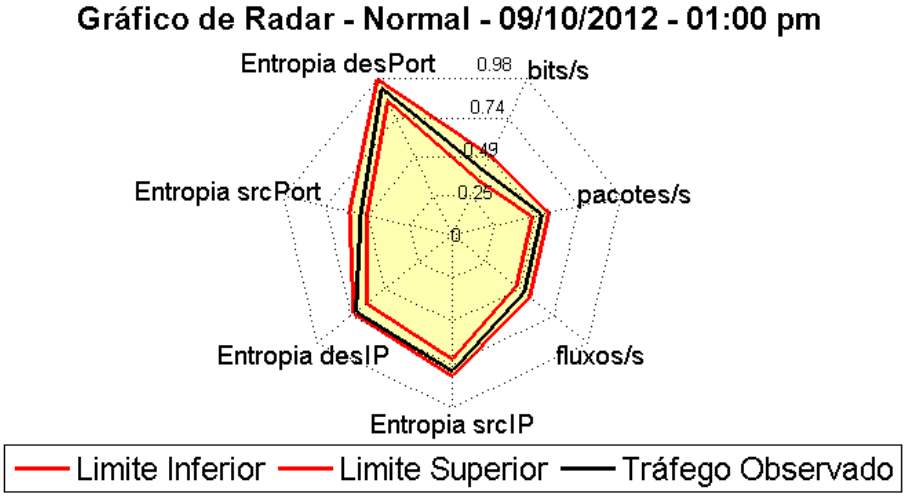
As informações e dados disponibilizados por meio deste módulo aumentam a efetividade do processo de tomada de decisões por parte do administrador de redes, consequentemente diminuindo o impacto de ataques ou falhas aos usuários finais da rede. Esses dados são providos através de duas abordagens principais: o classificação de principais usuários (usuários mais frequentes) e a análise global de um intervalo de tempo individual (intervalo de 1 minuto analisado).

O classificação de principais usuários disponibiliza ao administrador de redes os endereços IP de origem e destino, portas de origem e destino e protocolos que possuem maior frequência de ocorrência no intervalo de tempo analisado. Para cada um destes atributos, são apresentados os três elementos de maior frequência, assim como suas porcentagens de ocorrência relativas ao intervalo de tempo avaliado. O processo de coleta dessas informações ocorre juntamente com o cálculo da Entropia de Shannon das dimensões qualitativas descritas anteriormente. Como este cálculo utiliza a frequência de ocorrência (distribuição de probabilidade) dos diferentes elementos que compõem os intervalos de tempo analisados, o armazenamento dessa informação não adiciona nenhum custo computacional relevante ao sistema. As informações apresentadas auxiliam na identificação de o que está causando o problema, quem o está causando, em que porta o problema está ocorrendo, onde

especificamente a rede está sendo afetada, a proporção do impacto causado e quais medidas podem ser tomadas para concertar o problema ou interromper o ataque.

A análise global provê ao administrador de redes um gráfico do estado das sete dimensões avaliadas simultaneamente para um mesmo intervalo de tempo. Através da utilização de um Gráfico de Radar, duas linhas que representam os limites inferior e superior calculados com base nos DSNSFs das dimensões analisadas, bem como uma terceira linha que representa o comportamento da rede, são apresentadas. Este gráfico possibilita a identificação de anomalias locais, onde é possível verificar se o comportamento da rede excedeu ou foi inferior ao esperado. Através da análise global, alertas gerados pelo sistema podem ser identificados, possibilitando que o administrador de redes atualize o sistema com a nova assinatura de anomalia. A Figura 4.6 apresenta um exemplo da análise global em um intervalo de tempo classificado como normal, referente ao dia 9 de Outubro de 2012.

Figura 4.6 - Gráfico de Radar: Visão Hepta-Dimensional de um intervalo normal.



4.3 COMPLEXIDADE COMPUTACIONAL DO SISTEMA

Esta seção tem como objetivo a análise de complexidade do sistema proposto, verificando o custo computacional de sua execução para comprovar sua aplicabilidade em redes de larga escala e sua eficiência e agilidade com relação a seus processos de gerenciamento. Devido à composição do sistema apresentado em diversas partes, sua complexidade será introduzida de forma gradual. O processo de exportação de fluxos é executado pela aplicação NFDump e, por isso, não será considerado nessa análise.

O sistema apresentado analisa um segmento de rede específico em sete diferentes dimensões, aqui representadas por *D*. Dessa forma, todos os cálculos executados pelo processo de caracterização de tráfego devem ser executados *D* vezes.

Para se transformar as informações qualitativas de fluxos (endereços IP e portas de origem e destino) em dados quantitativos, a Entropia de Shannon é aplicada. Este cálculo varia de 1 até o número de diferentes entradas no intervalo de tempo analisado, gerando um valor de Entropia para os 1440 intervalos de tempo que representam um dia. Dessa forma, sua complexidade pode ser representada por E^2.

Para reduzir a granularidade dos dados analisados, a técnica de Suavização exponencial é aplicada, a qual calcula um valor suavizado para todos os 1440 intervalos de tempo que representam um dia. Sua complexidade é aqui representada por *S*.

Finalmente, o processo de caracterização de tráfego executado pelo método HWDS (e também pelo Holt-Winters, já que ambos possuem complexidade igual) é linear, calculando a previsão para cada um dos 1440 intervalos de tempo analisados. Assim, sua complexidade é representada por *H*. O processo de detecção de anomalias é caracterizado por operações de comparação individuais, as quais não utilizam quaisquer laços e, dessa forma, não adicionam complexidade computacional significativa.

A complexidade geral do sistema é a junção de todos os sub-processos executados e aqui descritos. Portanto, sua complexidade pode ser representada como $\theta\,(DE^2SH)$, a qual é assintoticamente uma complexidade quadrática. Levando em consideração a quantidade de dados analisados e informações providas, essa é considerada uma complexidade computacional baixa.

O ambiente de testes sobre o qual as avaliações de performance foram realizadas é um computador com processador Intel de 3.0 GHz, 4 GB de memória RAM, uma configuração de um computador pessoal comum na atualidade. Neste ambiente de testes, o sistema pode analisar dois meses de dados em menos de cinco minutos, e a análise hepta-dimensional de dias individuais foi executada em menos de 30 segundos para fluxos IP com amostragem de pacotes. Para fluxos IP sem amostragem de pacotes o sistema pode analisar dois meses de dados em menos de 10 minutos, e a análise hepta-dimensional de dias individuais é executada em menos de 1 minuto. Essa configuração é considerada de baixo desempenho em comparação com configurações utilizadas em servidores gerenciados por administradores de redes de larga escala, o que demonstra a aplicabilidade do sistema apresentado em redes de alta agregação de tráfego.

5 TESTES E RESULTADOS

Neste capítulo serão apresentados os resultados obtidos por meio de testes de validação de performance sobre o sistema descrito neste trabalho. Para tal, foram utilizados diferentes cenários de testes, visando comprovar a eficiência deste sistema em diferentes perspectivas. A disposição dos cenários será realizada da seguinte forma:

- Cenário 1: Aplicação do sistema apresentado em um ambiente de alta agregação de tráfego, visando avaliar sua performance em uma rede de larga escala por meio da utilização de dados reais;
- Cenário 2: Aplicação do sistema em um ambiente de baixa a média agregação de tráfego, objetivando avaliar sua performance em redes menores por meio da utilização de dados reais.

Além disso, algumas das técnicas e abordagens utilizadas pelo sistema, tais como a utilização da suavização exponencial e a abordagem de geração de alertas, são discutidos qualitativamente, objetivando comprovar sua eficiência e justificar sua utilização.

Entretanto, antes de apresentar os resultados obtidos nos cenários mencionados, é necessária uma breve discussão sobre as técnicas de mensuração de performance utilizadas.

5.1 TÉCNICAS UTILIZADAS

Nesta seção serão apresentadas as técnicas de mensuração de performance utilizadas para avaliar os resultados obtidos nos cenários de testes. É importante ressaltar que todas as técnicas abordadas são amplamente utilizadas na literatura nos processos de validação de performance de diferentes abordagens de gerenciamento de redes.

5.1.1 Caracterização de Tráfego

A caracterização de tráfego é uma etapa essencial para o processo de detecção de anomalias utilizado pelo sistema aqui descrito. Por meio dessa abordagem o comportamento normal da rede ou segmento de rede analisado é mapeado, gerando um perfil ou assinatura que o descreva. Esse perfil é denominado *Digital Signature of Network Segment using Flow analysis* (DSNSF), e representa o núcleo de todo o sistema. Em outras palavras, se

o DSNSF não for suficientemente eficaz para descrever o comportamento normal do ambiente de rede analisado, todo o processo de análise e detecção de anomalias é comprometido.

As técnicas aqui descritas são responsáveis por mensurar a eficácia dos DSNSFs gerados com base em importantes fatores ou características para o processo de caracterização de tráfego. Entre estes fatores, se encontram o nível de concordância entre o DSNSF e o movimento real da rede, o erro ou a distância entre eles e a dispersão da previsão. Nos tópicos a seguir, as técnicas utilizadas na validação de performance da caracterização de tráfego serão detalhadas.

5.1.1.1 Coeficiente de correlação (CC)

O Coeficiente de Correlação, também conhecido como covariância normalizada ou apenas correlação, é uma métrica utilizada para se mensurar o grau de similaridade entre duas variáveis aleatórias, ou seja, o quão relacionadas as duas variáveis são. Em análises de performance relacionadas à caracterização de tráfego, essa métrica é utilizada como forma de se identificar a correspondência entre o DSNSF gerado e o tráfego real observado. De forma simplificada, essa métrica indica se o DSNSF gerado acompanha as tendências de crescimento e decrescimento do movimento gerado pelo tráfego real observado, ilustrando se o método utilizado no processo de caracterização de tráfego é eficiente ou não na descrição comportamental da rede. Para se calcular o coeficiente de correlação entre duas variáveis aleatórias, utiliza-se a seguinte equação:

$$CC = \frac{\sum_{i=1}^{n} (D_i - \overline{D}) * (T_i - \overline{T})}{\sqrt{\sum_{i=1}^{n} (D_i - \overline{D})^2 * \sum_{i=1}^{n} (T_i - \overline{T})^2}} \tag{14}$$

A Equação (14) descreve o cálculo do Coeficiente de Correlação para variáveis aleatórias discretas, ou seja, as variáveis D e T do exemplo possuem valores discretos. Estes podem ser acessados por um índice i, computacionalmente falando, tal que i = 1, 2, 3, ..., n. No caso, D e T representam vetores contendo os dados do DSNSF e do tráfego observado, respectivamente.

Tabela 5.1 - Possíveis resultados da métrica CC.

CC	Significado
1	As variáveis aleatórias são completamente iguais (X=Y)
0	As variáveis aleatórias são completamente diferentes (X!=Y)
-1	As variáveis aleatórias são opostamente iguais (X = -Y)

Os resultados apresentados por meio dessa métrica variam de -1 a 1, cada valor representando uma relação diferenciada entre as variáveis aleatórias analisadas. A Tabela 5.1 ilustra essas relações em conjunto com seus respectivos valores. Como pode ser observado, no ambiente de caracterização de tráfego, onde as variáveis aleatórias testadas são o DSNSF gerado e o movimento real de tráfego observado, o resultado ótimo para o coeficiente de correlação é o valor 1, onde a previsão foi exatamente igual ao tráfego real observado. Dessa forma, quanto mais próximo de 1 o resultado deste teste, melhor ajustado se encontra o DSNSF com o tráfego da rede em relação às tendências de crescimento e decrescimento do movimento. Além disso, é importante ressaltar que em ambientes de rede que possuem uma granularização de dados muito elevada, ou seja, o movimento gerado pelo tráfego observado é composto por picos abruptos, o resultado deste teste pode ser influenciado negativamente, o que não implica que o DSNSF gerado não seja eficiente. Isso ocorre em redes ou segmentos de rede pequenos, onde a utilização atípica de um único usuário pode interferir diretamente no comportamento do movimento de tráfego, ou em abordagens de análise de rede que dividem a série temporal em intervalos muito pequenos.

5.1.1.2 Erro quadrático médio normalizado (NMSE)

A segunda métrica utilizada é o Erro quadrático médio normalizado, do inglês *Normalized Mean Square Error* (NMSE) [50]. Essa métrica objetiva a validação da diferença entre valores esperados e os valores que foram realmente obtidos. Em um ambiente de testes voltado para a análise de performance de um método para a caracterização de tráfego, como é o caso, este método tem como objetivo medir o quão distante o DSNSF gerado se encontra, na média normalizada, do movimento real de tráfego observado.

Para se calcular o NMSE entre duas séries temporais, no caso o DSNSF e o movimento real observado, utiliza-se a seguinte equação:

$$NMSE = \frac{1}{n}\sum_{i=1}^{n}\frac{(D_i - T_i)^2}{\overline{D}\overline{T}} \tag{15}$$

Assim como na Equação (14), as variáveis *D* e *T* representam vetores discretos com índice variando de 1 até *n*. Além disso, essas variáveis são vetores contendo os valores que representam o DSNSF e o movimento de tráfego observado, respectivamente.

Ao contrário do coeficiente de correlação, essa métrica possui apenas um limite para seus resultados. Este limite é o valor 0, o qual indica a situação onde os valores esperados são exatamente iguais aos valores verificados por meio dessa métrica. Dessa forma, valores NMSE elevados indicam resultados mais distantes do esperado.

5.1.1.3 Desvio fracional padrão (FSD)

Por último, o desvio fracional padrão, do inglês *Fractional Standard Deviation* (FSD) [51], é uma métrica que basicamente indica se a dispersão da previsão gerada (DSNSF) em torno da concentração média dos dados observados é sobreestimada ou superestimada. Em outras palavras, essa medida é capaz de apontar se o DSNSF gerado é predominantemente superior ou inferior ao tráfego real observado, ou seja, se o erro entre as duas séries temporais é predominantemente positivo ou negativo. O FSD entre duas séries temporais pode ser calculado por meio da equação:

$$FSD = \frac{2(\sigma_D - \sigma_T)}{\sigma_D + \sigma_T} \tag{16}$$

Na equação (16), observa-se que a métrica FSD é baseada na utilização do desvio padrão σ das séries temporais *D* e *T*, que representam os vetores que contém dados do DSNSF gerado e do Tráfego observado, respectivamente.

Os resultados obtidos por meio dessa métrica variam no intervalo de -2 a 2, sendo que seu valor ótimo é 0. Entretanto, valores que se encontram entre o intervalo que vai de -0.67 até 0.67 são considerados bons resultados para essa métrica [51].

5.1.1.4 Erro percentual médio absoluto simétrico (sMAPE)

Como métrica complementar, foi utilizada a técnica denominada Erro percentual médio absoluto simétrico, ou do inglês *Symmetric Mean Absolute Percentage Error* (sMAPE) [52]. Como o próprio nome sugere, também é uma medida de erro entre duas séries temporais, tal como o NMSE. Métricas relativas a erros são amplamente utilizadas em análises de precisão de previsões de séries temporais. Dessa forma, o sMAPE é utilizado por abordar o conceito de erro de uma forma diferenciada. Essa métrica é uma modificação da tradicional técnica MAPE, com o diferencial de analisar os erros de forma simétrica, permitindo melhores análises dos resultados obtidos. Essa característica permite analisar através de percentuais e de forma simétrica os erros entre o DSNSF gerado e o movimento real de tráfego observado, analisando de forma homogênea erros positivos (DSNSF menor que o tráfego real) e negativos (DSNSF maior que o tráfego real). O cálculo do sMAPE é realizado por meio da seguinte equação:

$$\frac{2}{n}\sum_{i=1}^{n}\frac{|D_i - T_i|}{D_i - T_i} \tag{17}$$

O sMAPE, como qualquer medida de erro, possui resultado ótimo quando este valor for nulo (zero). Além disso, por se tratar de uma métrica que analisa de forma simultânea erros positivos e negativos, o sMAPE se limita a um erro máximo de 200%. Dessa forma, assim como ocorre no NMSE, quanto menores os resultados para a métrica sMAPE, melhor é o DSNSF gerado com relação ao tráfego analisado.

5.1.2 Detecção de Anomalias

A detecção de anomalias em redes de computadores é um processo essencial para que seja possível garantir a escalabilidade, disponibilidade e a qualidade dos serviços prestados. A identificação de comportamentos anômalos pode apontar falhas ou ataques de modo a facilitar que contra medidas possam ser tomadas por administradores de redes. Dessa forma, ferramentas e abordagens de detecção de anomalias devem possuir algumas características importantes para a garantia de sua efetividade, tais como:

- Alta taxa de alarmes Verdadeiros Positivos;
- Baixa taxa de alarmes Falsos Positivos;
- Alta taxa de precisão ou acurácia.

Dessa forma, se faz necessária a utilização de diferentes técnicas de validação de performance da ferramenta proposta, objetivando a mensuração de seu desempenho no processo de detecção de anomalias.

Segundo [53], a validação de resultados de problemas que envolvem precisão constantemente inicia-se pela classificação destes problemas usando apenas duas classes. O autor apresenta um exemplo genérico, o qual pode ser aplicado a qualquer problema de precisão na literatura. Neste trabalho o exemplo será focado no problema específico da detecção de anomalias. Dessa forma, cada intervalo de tempo verificado no problema da detecção de anomalias pode ser formalmente definido como uma instância do conjunto [*p*,*n*], onde *p* indica intervalos anômalos e *n* intervalos normais. Além disso, deve-se instanciar cada intervalo de tempo de acordo com as reações tomadas pelo sistema, as quais podem ser definidas como elementos do conjunto [*Y*,*N*], onde *Y* indica anomalia apontada pelo sistema, e *N* intervalo considerado normal pelo sistema. Dessa forma, uma matriz de confusão (ou tabela de contingência) pode ser definida, descrevendo todas as possíveis relações entre a saída do sistema e o que realmente ocorreu, conforme ilustrado na Figura 5.1.

Figura 5.1 - Matriz de Confusão [53].

Como pode ser observado na Figura 5.1, a classe real indica o comportamento real da rede, enquanto a classe hipotética indica o comportamento do sistema. Conforme a matriz de confusão apresentada, quatro diferentes resultados podem ser apresentados. Se uma instância é confirmada na classe real como anômala (*p*) e o sistema a classifica como anômala (*Y*) o intervalo avaliado é definido como Verdadeiro Positivo; caso contrário, se o sistema avaliar como normal (*N*), o intervalo é definido como Falso Negativo. Se uma instância é confirmada na classe real como normal (*n*) e o sistema a classifica como normal, o intervalo é classificado como Verdadeiro Negativo; caso contrário, se o sistema avaliar como anômalo (*Y*), o intervalo é definido como Falso Negativo.

Diferentes métricas de precisão podem ser derivadas das relações apresentadas pela matriz de confusão da Figura 5.1, algumas das quais serão utilizadas neste trabalho como métrica de precisão do sistema. Essas serão melhores descritas nos próximos capítulos.

5.1.2.1 Acurácia

A medida de acurácia ou precisão basicamente aponta o nível percentual de precisão do sistema com relação à classificação dos intervalos avaliados como anômalos ou normais. Essa medida é importante por ressaltar a eficiência do sistema de detecção de anomalias de forma geral.

A métrica de Acurácia ou precisão pode ser obtida por meio da Equação (18):

$$acurácia = \frac{VP + VN}{P + N} \tag{18}$$

Na Equação (18), *VP* indica a ocorrência de Verdadeiros Positivos, *VN* a ocorrência de verdadeiros negativos, e as variáveis *P* e *N* indicam o total das colunas *p* e *n*, conforme a Figura 5.1.

Como uma métrica percentual, o resultado em um cenário ideal seria a classificação de 100% de intervalos corretamente, assim como o pior caso seria que nenhum dos intervalos analisados fosse classificado corretamente (0% de acurácia).

5.1.2.2 *Receiver Operating Characteristic curve*

A métrica denominada *Receiver Operating Characteristic curve*, ou simplesmente curva ROC, é uma métrica gráfica que confronta duas diferentes métricas de precisão objetivando ilustrar o *trade-off* de eficiência do sistema testado. É importante ressaltar que tais métricas de precisão também são derivadas da matriz de confusão apresentada pela Figura 5.1. Em validações de performance de sistemas de detecção de anomalias, as métricas de precisão mais utilizadas em curvas ROC são as taxas de Verdadeiros Positivos (TVP) e de Falsos Positivos (TFP). Dessa forma, a curva ROC deve ser um gráfico onde o eixo das abscissas representa o valor percentual da métrica TFP, enquanto o eixo das ordenadas representa o valor percentual da métrica TVP. O resultado dessa métrica é uma curva originada no menor valor das duas métricas e que, ordenadamente, segue rumo ao maior valor delas. Dessa forma, quanto mais próxima de uma reta a curva se encontra, pior é o desempenho do sistema na detecção de anomalias, enquanto curvas mais acentuadas, as quais convergem para 100% de TVP rapidamente são considerados melhores resultados.

As métricas de taxa de Verdadeiros Positivos (TVP) e taxa de Falsos Positivos (FVP) pode ser obtida por meio das Equações (19) e (20):

$$TVP = \frac{VP}{P} \tag{19}$$

$$TFP = \frac{FP}{N} \tag{20}$$

Na Equação (19) e (20), *VP* indica a ocorrência de Verdadeiros Positivos, *FP* a ocorrência de falsos positivos, e as variáveis *P* e *N* indicam o total das colunas *p* e *n*, conforme a Figura 5.1, ou seja, o total de intervalos positivos e intervalos negativos, respectivamente.

5.2 VALIDAÇÃO DE EFETIVIDADE

Essa seção objetiva comprovar a efetividade de algumas técnicas e abordagens utilizadas pelo sistema apresentado de modo a justificar sua utilização de maneira qualitativa.

A primeira abordagem avaliada é a utilização da Suavização Exponencial na diminuição da granularidade dos dados avaliados, a qual é causada devido à diminuição do tamanho de janelas ou intervalos de análise temporal para 1 minuto.

A segunda abordagem avaliada é relativa à metodologia utilizada pelo sistema para a geração de Alertas. Conforme descrito na seção 4.2.1, o sistema apresentado utiliza dispara Alertas quando anomalias locais são detectadas em 5 ou mais dimensões, caso a assinatura dessas anomalias não seja previamente conhecida pelo sistema.

5.2.1 Utilização da Suavização Exponencial

Essa seção tem como objetivo a avaliação da técnica de Suavização Exponencial com relação à sua aplicabilidade no problema proposto: a diminuição da granularidade de movimentos de tráfego.

A suavização exponencial, termo que designa equações do tipo *Exponentially-Weighted Moving Average* (EWMA), descritas na seção 4.1.1, são caracterizadas basicamente por uma divisão em duas partes. Cada uma dessas partes é multiplicada por um fator de peso, dado por um "coeficiente de suavização". A soma dos pesos dados às duas partes deve necessariamente resultar em 1 (100%). Dessa forma, a distribuição dos pesos entre cada uma das partes deve ser realizada de acordo com a necessidade de cada aplicação.

Conforme descrito na seção 4.1.5, o sistema apresentado utiliza a Suavização Exponencial como forma de diminuir a granularidade dos dados relativos às sete diferentes dimensões de fluxos de redes de larga escala. Abordagens baseadas na análise de rede em intervalos de tempo de 5 minutos não precisam tratar essa granularidade, visto que quanto maior o intervalo de tempo utilizado mais suave será o movimento observado na série temporal como um todo. Entretanto, essas abordagens vêm se tornando cada vez mais impraticáveis na atualidade devido à crescente taxa de transmissão de dados em redes de larga escala. Assim, se um sistema de detecção de falhas levar 5 minutos para avisar o administrador de rede sobre um problema, é possível que uma quantidade massiva de informações seja comprometida. A redução da janela de análise utilizada pelo sistema apresentado de 5 para 1 minuto implica no aumento da granularidade dos dados, ou seja, no aumento da ocorrência de picos abruptos que, mesmo considerados normais, se diferenciam amplamente dos valores apresentados pelas janelas temporais vizinhas. Dessa forma, o processo de caracterização de tráfego é dificultado, prejudicando os resultados obtidos pelo

sistema com relação ao desempenho de suas funções. Por esse motivo, o tratamento dos dados neste tipo de situação como forma de diminuir essa granularidade sem descaracterizar o comportamento do tráfego analisado (tendências de crescimento e decrescimento) é uma solução vantajosa, principalmente se a técnica utilizada possuir um custo computacional baixo como a Suavização Exponencial.

É importante ressaltar que a utilização dessa técnica não se limita apenas à situação anteriormente mencionada da diminuição da janela de análise de 5 para 1 minuto em redes de larga escala. Em redes menores, tais como redes de pequenas empresas, ou mesmo Universidades de pequeno a médio porte, é comum que a utilização da rede por usuários individuais influencie no movimento de tráfego da rede como um todo. Essa influência também é um fator relacionado ao aumento da granularidade dos dados que, da mesma forma como ocorre nas redes de larga escala, prejudicam o processo da caracterização de tráfego. Dessa forma, a suavização exponencial também se aplica à este tipo de ambiente, reduzindo a ocorrência de picos abruptos na série temporal analisada de modo a otimizar o processo de caracterização de tráfego.

Para a realização dos testes, foram utilizados fluxos reais coletados na Universidade Estadual de Londrina (UEL). Os fluxos foram coletados por meio do protocolo de exportação sFlow e, devido ao alto volume de tráfego de dados, é utilizada uma amostragem de pacotes na escala 1:256.

Os dados coletados são relativos aos dias úteis do mês de Outubro de 2012, o qual foi utilizado nos testes de performance do método avaliado. Destes dados, foi extraída a dimensão "bits/s" dos fluxos de todos os dias analisados em janelas de tempo de 1 minuto, aplicando-se a suavização exponencial apresentada na Equação (13) e, posteriormente, avaliando as mudanças incorporadas pelos dados suavizados em comparação com os dados não tratados. Com relação ao coeficiente de suavização utilizado nessa equação, quanto menor este valor mais suave a série temporal se torna. Entretanto, este coeficiente não pode ser tão pequeno a ponto de descaracterizar o comportamento do tráfego. Dessa forma, define-se o coeficiente de suavização como $\omega = 0.3$, segundo análises exaustivas e baseado na literatura [20, 31].

As Figuras 5.1 e 5.2 ilustram o movimento de tráfego de bits/s com dados não tratados e suavizados exponencialmente, respectivamente, relativos ao dia 9 de Outubro de 2012. Como se pode observar, a aplicação da técnica de suavização exponencial reduz consideravelmente a ocorrência de picos abruptos no movimento de tráfego, ou seja, diminui com sucesso a granularidade dos dados analisados. Além disso, pode-se constatar que as

principais tendências de crescimento e decrescimento presentes na Figura 5.2 são preservadas mesmo após o processo de suavização presente na Figura 5.3, demonstrando que a utilização da técnica apresentada não descaracteriza o comportamento de tráfego observado neste dia.

Figura 5.2 - Tráfego de bits/s com dados não tratados.

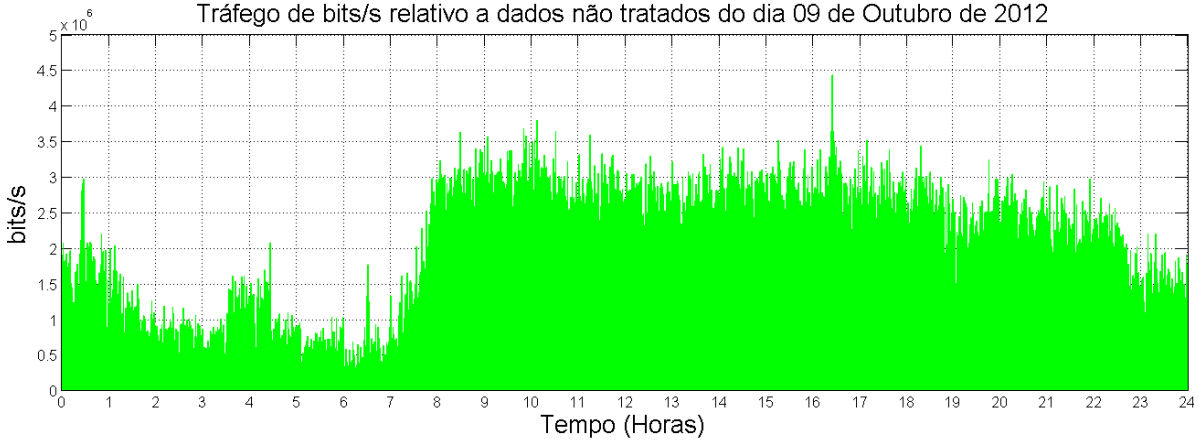
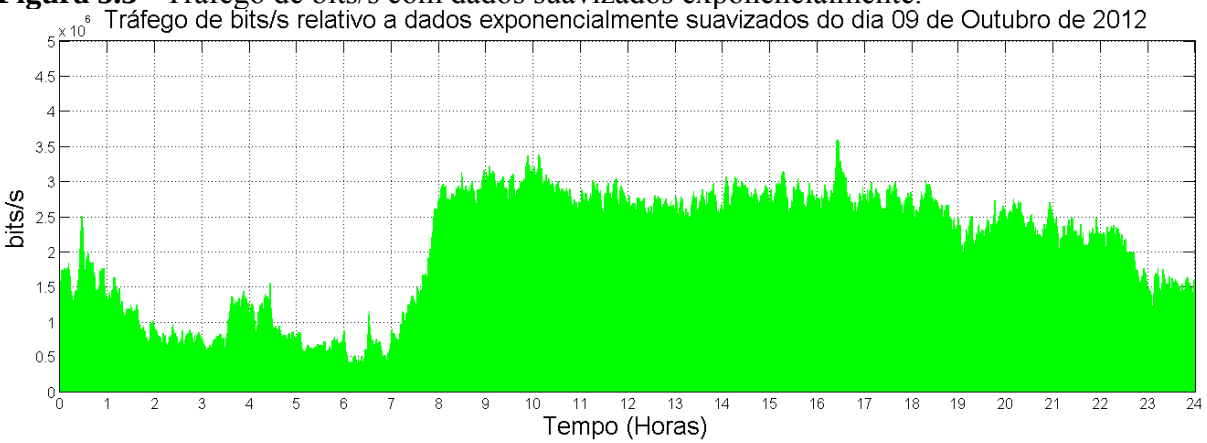


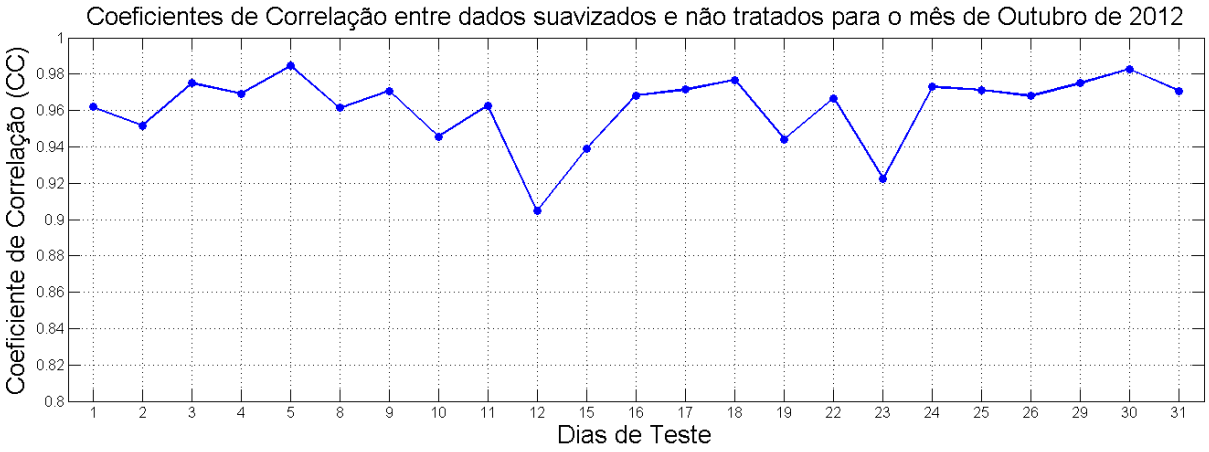
Figura 5.3 - Tráfego de bits/s com dados suavizados exponencialmente.



Embora os resultados obtidos por meio da utilização da técnica de Suavização Exponencial estejam visualmente bons, foram executados testes numéricos de performance para avaliar sua efetividade com dados relativos a um mês de coleta.

A primeira métrica analisada foi o Coeficiente de Correlação (CC), o qual mede o grau de similaridade entre os dados suavizados e não tratados, avaliando se as tendências de crescimento e decrescimento do movimento de tráfego de dados não tratados são preservados após o processo de suavização. A Figura 5.4 ilustra os resultados obtidos por meio da aplicação dessa técnica para os dias úteis de Outubro de 2012.

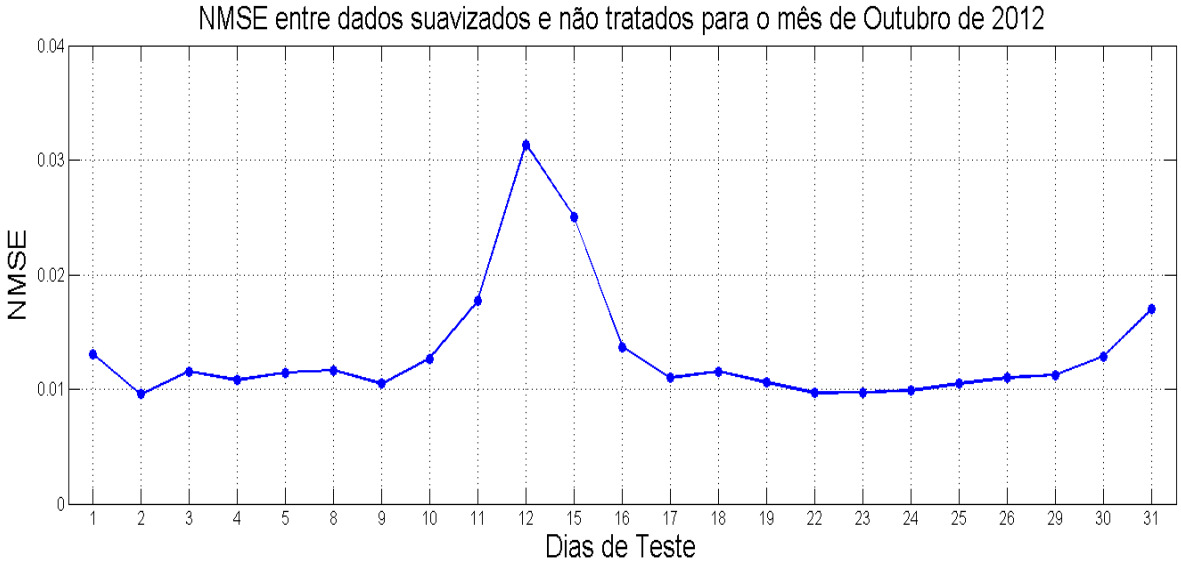
Figura 5.4 - Coeficientes de Correlação entre dados não tratados e exponencialmente suavizados.



Como observa-se na figura apresentada, os valores obtidos como resultado para essa métrica são todos acima de 0.9, sendo que a maior parte dos dias testados possui coeficiente de correlação maior que 0.96. Considerando-se que o valor ótimo para essa métrica é 1, pode-se concluir que, mesmo após o processo de suavização exponencial, os dados preservam as características comportamentais do dia analisado com relação às tendências de crescimento e decrescimento do movimento de tráfego.

A segunda métrica utilizada é o Erro Médio Quadrático Normalizado (NMSE), responsável por mensurar o quão distante duas séries temporais se encontram, ou seja, o erro entre o movimento de tráfego não tratado e o exponencialmente suavizado. A Figura 5.5 apresenta os resultados obtidos por meio da utilização dessa técnica:

Figura 5.5 - Teste NMSE entre dados não tratados e exponencialmente suavizados

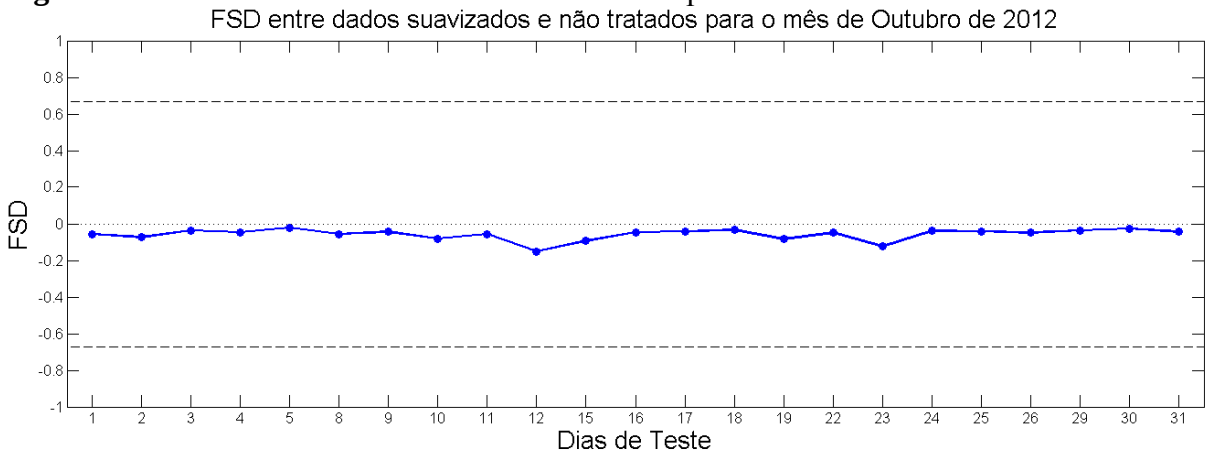


.

Segundo ilustrado, os resultados dos testes através da utilização da técnica NMSE não foram maiores que 0.04, e que a maior parte dos dias testados obtiveram resultados inferiores a 0.02. Como qualquer medida de erro, o valor ótimo para essa métrica é 0. Os resultados obtidos evidenciam que a utilização da suavização exponencial não implica na perda significativa de informações.

A terceira métrica denominada, Desvio Fracional Padrão (FSD), foi aplicada ao cenário de testes. Essa métrica visa avaliar se a dispersão dos dados suavizados em torno da média dos dados reais é super ou subestimada. A Figura 5.6 apresenta os resultados obtidos por meio da aplicação do FSD ao cenário de testes:

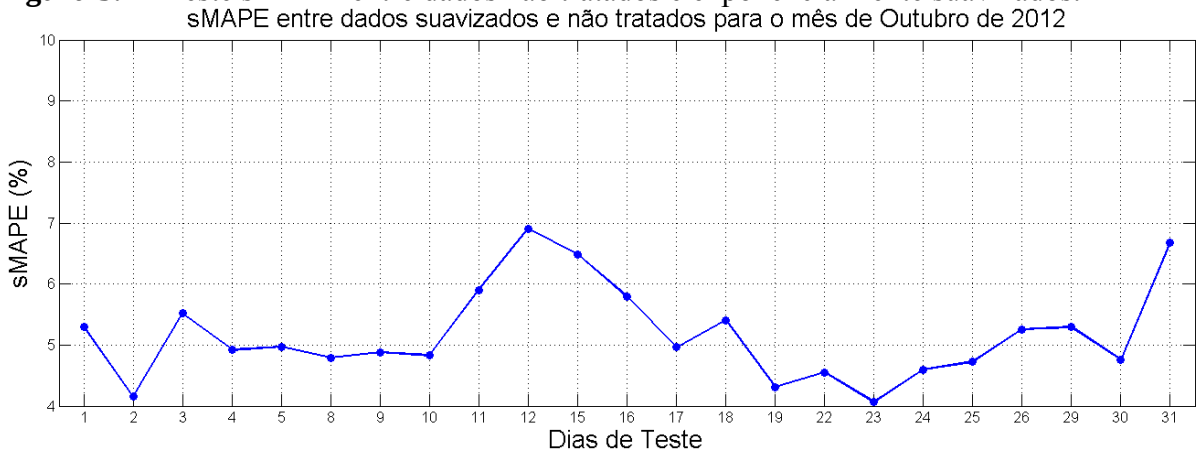
Figura 5.6 - Teste FSD entre dados não tratados e exponencialmente suavizados.



Como pode-se observar, os resultados do teste FSD demonstram que os dados suavizados se encontram muito próximos dos dados não tratados. Além disso, pode-se constatar que o erro entre as duas séries temporais é predominantemente negativo, ou seja, os dados suavizados são menores que os dados não tratados. Isso ocorre devido à perda de informação decorrente do processo de suavização. Entretanto, a proximidade dos resultados obtidos, os quais não foram inferiores a -0.1, ao resultado ótimo (zero) comprova, juntamente com as medidas de erro apresentadas, que a perda de informações é mínima, sendo ela insignificante para o processo de análise da rede.

Por fim, foi aplicada no processo de análise da suavização exponencial a métrica Erro percentual médio absoluto simétrico (sMAPE), técnica capaz de mensurar a distância ou o erro entre duas séries temporais de forma simétrica, ou seja, analisando em conjunto erros positivos e negativos entre os dados não tratados e suavizados. A Figura 5.7 ilustra os resultados obtidos por meio desse processo de análise:

Figura 5.7 - Teste sMAPE entre dados não tratados e exponencialmente suavizados.



Como pode-se observar, os resultados obtidos através do teste utilizando a métrica sMAPE não foram superiores a 7%, sendo que grande parte dos dias analisados apresentaram taxas de erros percentuais por volta de 5%. Conforme abordado na seção 5.1.1.4, os valores ótimo e de pior caso para essa métrica são 0% e 200%, respectivamente. Assim, a diferença entre as duas séries temporais analisadas é considerada baixa, comprovando que a perda de informações após o processo de suavização não é significativa.

Por meio dos testes apresentados, pode-se concluir que a utilização da técnica de Suavização Exponencial é capaz de eficientemente reduzir a granularidade dos dados referentes à movimentos de tráfego analisados em janelas de tempo de 1 minuto. Além disso, pode-se observar que o processo de suavização é capaz de preservar o comportamento observado do tráfego (tendências de crescimento e decrescimento), e que a perda de informações oriundas deste processo não são significativas.

5.2.2 Validação da Geração de Alertas

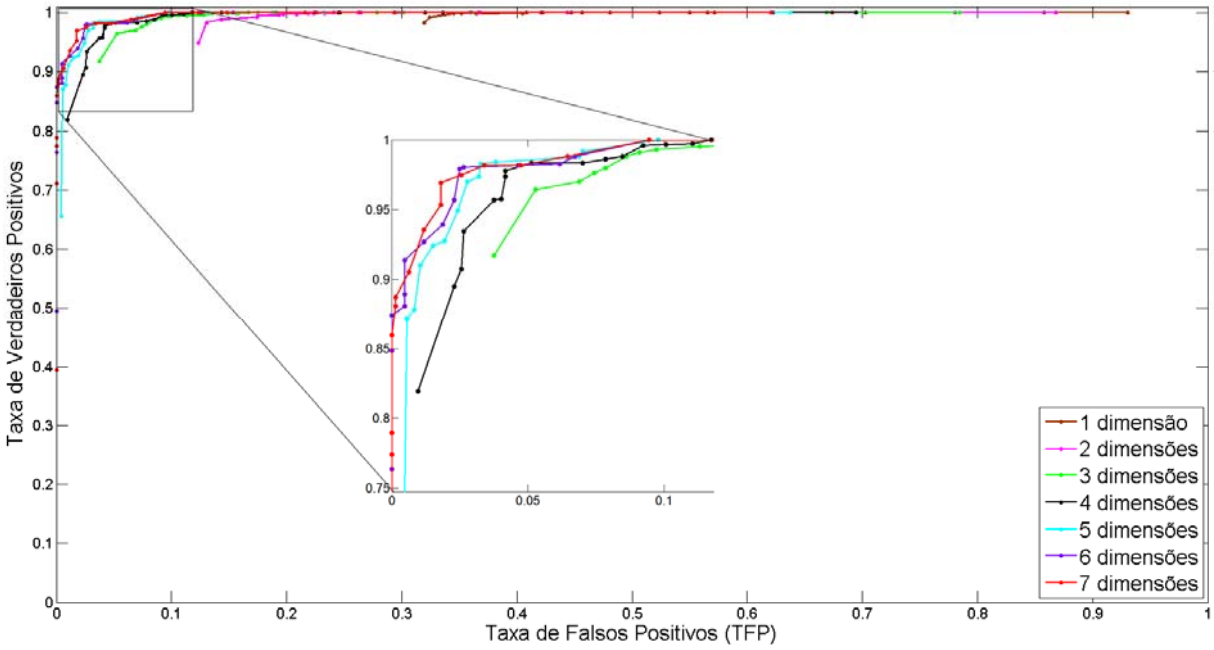
Esta seção tem como objetivo a validação de performance da abordagem de geração de alertas utilizada pelo sistema apresentado, a qual é descrita na seção 4.2.1. Conforme discutido, o sistema é capaz de detectar anomalias de comportamento previamente conhecido por meio de Alarmes, bem como detectar comportamentos anômalos ainda desconhecidos através de Alertas.

A abordagem de geração de Alertas utilizada pelo sistema apresentado, a qual pode ser observada na Figura 4.5, consiste na identificação de anomalias locais (anomalias isoladas detectadas nas diferentes dimensões analisadas). Quando 5 ou mais

anomalias locais são detectadas, uma anomalia global do tipo "Alerta" é caracterizada, alertando o administrador da ocorrência de um problema de comportamento ainda desconhecido pelo sistema.

O número de alarmes locais necessários para a geração de um Alerta foi exaustivamente testado, provando-se o número de dimensões mais eficiente dentre todas as possíveis. Para comprovar tal eficiência, testes foram realizados utilizando registros de fluxos relativos à Universidade Estadual de Londrina (UEL), por um período que compreende os meses de Setembro e Outubro de 2012. O mês de Setembro foi utilizado como período de treinamento para o sistema, enquanto Outubro foi utilizado como validação de performance. O sistema apresentado foi aplicado ao cenário proposto sem quaisquer registros comportamentais de anomalias, ou seja, sem a geração de Alarmes, para que todas as anomalias detectadas sejam classificadas como Alertas. Os testes realizados compreendem a utilização de 1 até 7 dimensões na geração de Alertas, objetivando comprovar qual abordagem possui maior ganho de eficiência.

Figura 5.8 - Curva ROC relativa ao número de dimensões utilizadas na geração de Alertas.



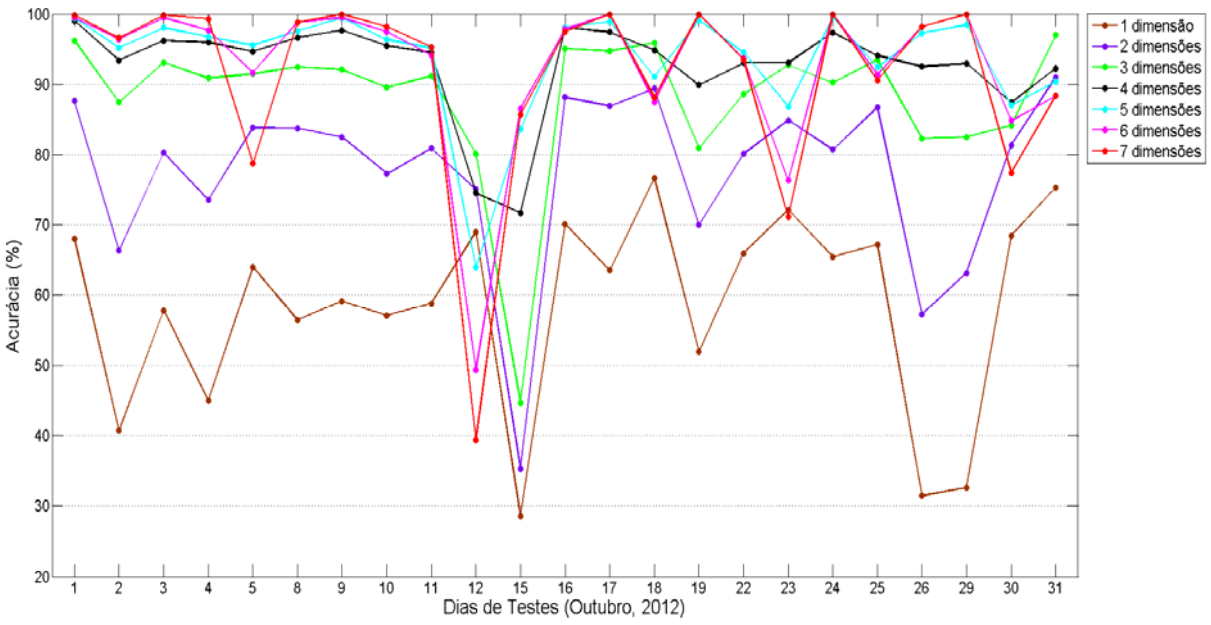
Para os testes de efetividade, foram utilizadas as métricas descritas na seção 5.1.2, as quais avaliam e eficiência do processo de detecção de anomalias para o cenário proposto. A primeira métrica utilizada foi o gráfico da curva ROC, o qual confrontam a taxa de Alertas Verdadeiros Positivos (TVP) com a taxa de Alertas Falsos Positivos (TFP). Os resultados obtidos podem ser verificados na Figura 5.8, onde as curvas relativas às dimensões

de 1 a 7 são representadas pelas cores marrom, rosa, verde, preto, azul claro, roxo e vermelho, respectivamente. Como pode ser observado, a utilização de apenas 1 ou 2 dimensões na geração de Alertas leva à ocorrência de uma taxa elevada de Falsos Positivos de no mínimo 33% e 13%, respectivamente. Os resultados obtidos pelas demais dimensões é mais próximo, o que justifica a aproximação representada pela Figura 5.8. Nela, pode-se observar que quanto maior o número de dimensões utilizadas, mais próximos do valor ótimo (taxas de 0 Falsos Positivos e 1 Verdadeiros Positivos) os resultados se encontram.

Entretanto, a curva ROC apresenta apenas medidas relacionadas às taxas de Verdadeiros Positivos (anomalias que ocorreram e foram detectadas pelo sistema) e Falsos Positivos (anomalias apontadas pelo sistema, mas que não ocorreram na realidade). A utilização de um número maior de dimensões como critério para a geração de Alertas acarreta na diminuição de anomalias detectadas e, consequentemente, as taxas de Alertas Falsos Positivos também são reduzidas. Assim, pode-se concluir por meio dessa métrica que quanto maior o número de dimensões utilizadas na geração de alertas, menos alertas são gerados.

Para se mensurar a eficiência do sistema como um todo, levando em consideração também situações onde anomalias ocorreram e não foram detectadas, foi utilizada a Acurácia. Nessa métrica, quanto mais próximos de 100% os resultados obtidos, mais preciso é o sistema avaliado na classificação de intervalos como anômalos ou normais. Os resultados obtidos podem ser observados na Figura 5.9.

Figura 5.9 - Acurácia relativa ao número de dimensões utilizadas na geração de Alertas.



Como se pode observar, a acurácia geral para 1, 2 e 3 dimensões é relativamente baixa em comparação com as demais testadas. A utilização de 4 a 7 dimensões apresenta resultados de precisão mais promissores no geral. Entretanto, avaliando de forma mais completa, em alguns dias a precisão apresentada pela utilização de 6 e 7 dimensões diminui bruscamente, como por exemplo nos dias 5, 23 e 30. Durante o desenvolvimento deste trabalho, pode-se observar que estes dias apresentaram alguns comportamentos anômalos para este cenário de testes. Com isso podemos concluir que a utilização de 6 ou 7 dimensões diminui o número de alertas a ponto de não permitir a detecção de anomalias reais.

Com isso, elimina-se a utilização de duas outras abordagens, restando apenas a utilização de 4 ou 5 dimensões na geração de Alertas. Como observado nas Figuras 5.8 e 5.9, os resultados dessas suas abordagens são bastante semelhantes. Como forma de avaliar qual a melhor abordagem para o sistema apresentado uma tabela comparativa foi desenvolvida, a qual pode ser observada na Tabela 5.2.

Tabela 5.2 - Comparativo de Acurácia entre a utilização de 4 e 5 dimensões na geração de alarmes.

	Média	*Mediana*	*Moda*
4 Dimensões	0.9275	0.9451	0.9306
5 Dimensões	0.9370	0.9639	0.9944

Como pode-se observar, mesmo com resultados extremamente eficientes e próximos para as três métricas estatísticas, pode-se concluir que a utilização de 5 dimensões na geração de Alertas é a abordagem mais eficiente dentre as avaliadas e, por isso, é a utilizada pelo sistema apresentado.

5.3 CENÁRIOS DE TESTE

Nessa seção serão apresentados os cenários de testes utilizados na validação de performance do sistema apresentado. Diferentes cenários de análise apresentam características únicas relativas tanto à ambientes de gerenciamento de redes quanto ao próprio sistema, possibilitando uma análise mais rica e precisa de sua efetividade.

No primeiro cenário, o sistema proposto será submetido a dados relativos à rede da Universidade Estadual de Londrina (UEL), uma rede de larga escala com grande agregação de tráfego. Este ambiente possui tráfego semelhante ao de grandes redes de

computadores, tais como servidores *Cloud Computing*, redes hospitalares, redes de grandes corporações ou órgãos governamentais e redes de provedores de serviço de Internet.

No segundo cenário, o sistema apresentado será submetido a dados relativos à rede da Universidade Tecnológica Federal do Paraná (UTFPR) - Campus Toledo, uma rede de pequeno a médio porte. Este ambiente possui tráfego semelhante ao de médias empresas e órgãos governamentais, onde a utilização de usuários individuais influi diretamente no comportamento da rede como um todo.

5.3.1 Cenário 1

Este cenário objetiva a avaliação de performance do sistema apresentado em um ambiente de alta agregação de tráfego para comprovar sua eficiência de aplicação em redes de larga escala.

Os métodos Holt-Winters e HWDS são avaliados na criação de *Digital Signatures of Network Segment using Flow analysis* (DSNSF) neste ambiente como forma de comprovar o aumento de eficiência do método HWDS em relação à sua versão tradicional. Além do processo de caracterização de tráfego, a detecção de anomalias provida pelo sistema é avaliada com base em dados reais coletados e em dados reais com anomalias específicas simuladas, visando mensurar a performance do sistema na detecção de anomalias diferentes das que foram detectadas Durante o período de testes.

5.3.1.1 Testes com dados reais

Foram coletados registros de fluxos reais da Universidade Estadual de Londrina - Paraná, uma rede de larga escala composta por mais de 7000 diferentes *hosts*. Os fluxos foram coletados por meio do protocolo de exportação sFlow e, devido ao alto volume de tráfego de dados, é utilizada uma amostragem de pacotes na escala 1:256.

Os dados coletados são relativos aos dias úteis de Setembro a Novembro de 2012. O primeiro mês coletado é utilizado como treinamento para o sistema na geração de DSNSFs das sete dimensões analisadas, enquanto os demais meses são utilizados em seus testes de validação de performance. É importante ressaltar que os dias 12 e 15 de Outubro, bem como os dias 02, 15 e 20 de Novembro são feriados nacionais, apresentando comportamentos que diferem do esperado (dias anômalos).

Conforme abordado no capítulo 4, os coeficientes de suavização utilizados nos métodos Holt-Winters, HWDS e na Suavização Exponencial devem ser pequenos para garantir que informações históricas possuam uma maior influência que novos dados no DSNSF gerado. Os coeficientes de suavização utilizados neste cenário possuem valores α = 0.28, β = 0.0035, γ = 0.1 e ω = 0.3 para os métodos HW e HWDS, os quais foram definidos como os melhores na caracterização de tráfego através de testes exaustivos e com base em trabalhos anteriores presentes na literatura [31, 33, 54].

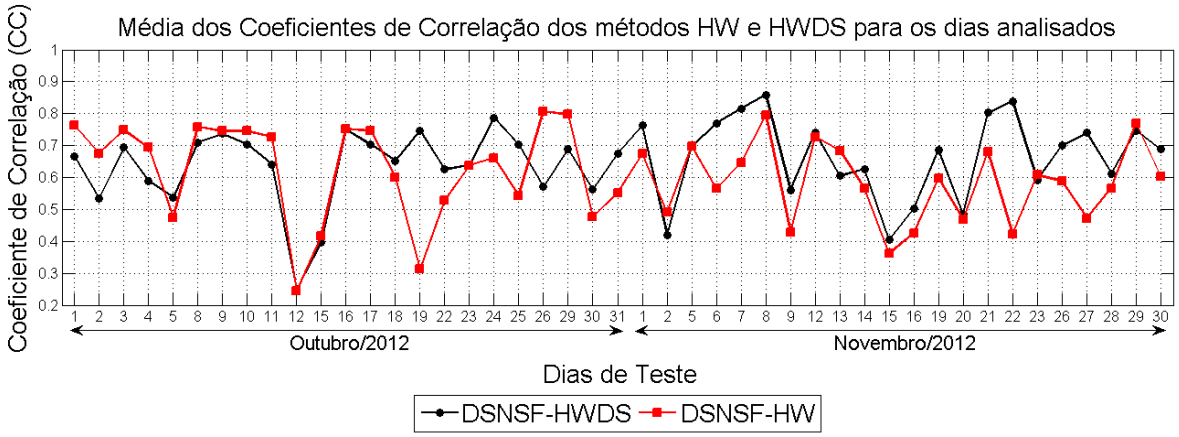
O ciclo sazonal, definido pela constante *s*, representa o número de janelas de tempo que a série temporal utilizada possui. Em outras palavras, representa o número de valores que descrevem cada um dos dias analisados. Os dados coletados são divididos em intervalos de 1 minuto, o que define o valor da constante *s* como 1440. Dessa forma, cada dia é representado em 1440 diferentes intervalos.

Como forma de se verificar a eficiência dos métodos Holt-Winters e HWDS no cenário proposto, as técnicas descritas na seção 5.1.1 são aplicadas ao processo de caracterização de tráfego. Como o sistema proposto se utiliza de uma análise hepta-dimensional de fluxos para o processo de caracterização do tráfego da rede verificada, 7 DSNSFs são gerados a cada dia objetivando a previsão de seu comportamento normal. Isso implica que cada um dos testes aplicados possuem 7 resultados diferentes para cada dia mensurado, o que inviabiliza sua visualização por meio de gráficos convencionais. Visando simplificar o processo de verificação dos resultados obtidos pelos métodos nas 7 dimensões, foi calculada a média destes resultados observados, gerando um valor único para cada dia analisado pelos testes mencionados, que representa todo o processo de caracterização de tráfego.

O primeiro teste utilizado é a medida de Coeficientes de Correlação (CC), as quais visam a mensuração do grau de similaridade entre os DSNSFs gerados e o tráfego observado. Essa métrica aponta se as tendências de crescimento e decrescimento seguidas pelas duas séries temporais analisadas seguem o mesmo padrão. É importante ressaltar que essa métrica utiliza uma análise ponto a ponto, sendo possível a degradação dos resultados em cenários com elevada granularização do movimento. No ambiente utilizado neste cenário de testes, os dados foram submetidos ao processo de Suavização Exponencial, técnica responsável pela redução dessa granularidade e, consequentemente, suavização do movimento de tráfego. Entretanto, como pode-se observar nas Figuras 5.2 e 5.3, essa técnica não elimina a ocorrência de picos abruptos, apenas diminuindo a intensidade dessas ocorrências a um

nível aceitável para a execução do processo de caracterização de tráfego. A Figura 5.10 ilustra os resultados obtidos por meio do teste CC para o cenário de testes proposto.

Figura 5.10 - Coeficientes de Correlação entre os DSNSFs gerados pelos métodos HW e HWDS e o tráfego observado para os meses de Outubro e Novembro de 2012.



Como pode-se observar, os resultados para o teste de CC são bem irregulares para ambos os métodos. Com exceção dos dias anteriormente apontados como feriados nacionais, os resultados obtidos variam entre 0.55 e 0.86. Esses resultados ilustram o impacto da granularidade na análise de CC, de modo que mesmo valores considerados baixos (próximos de 0.5) não implicam que o DSNSF gerado seja ruim. Por esse motivo, a aplicação de múltiplas técnicas de verificação de performance é essencial para a real mensuração dos resultados obtidos. Na média geral para os dias testados, os métodos HW e HWDS obtiveram resultados de CC de 0.60 e 0.65, respectivamente, o que ilustra a superioridade do método HWDS sobre sua versão tradicional mesmo em ambientes desfavoráveis.

Além disso, a Tabela 5.3 apresenta os resultados obtidos por meio do teste CC relativo à utilização dos métodos analisados em cada uma das sete dimensões separadamente. Essa abordagem é válida devido ao comportamento heterogêneo apresentado pelas diferentes dimensões analisadas.

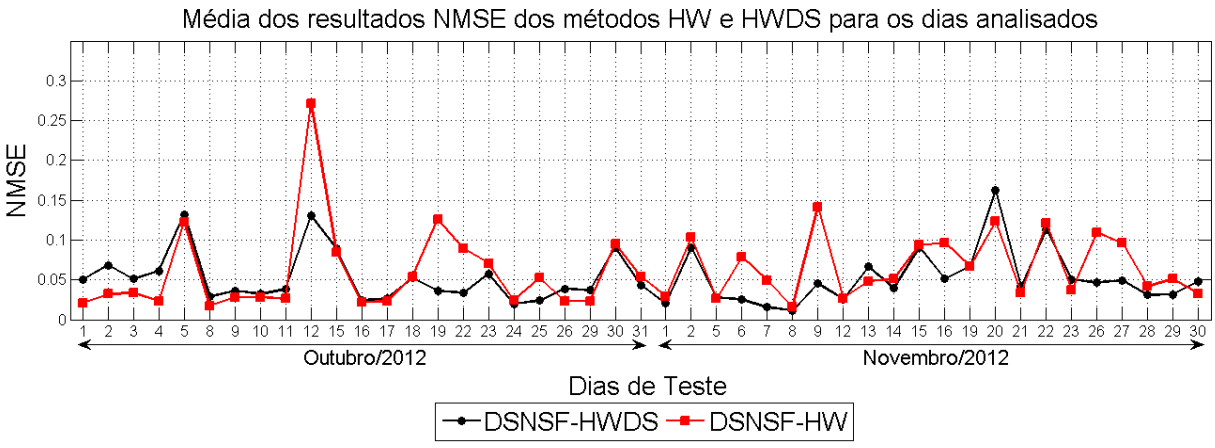
Tabela 5.3 - Resultados de CC dos métodos analisados em cada dimensão.

		bits	pacotes	fluxos	IP origem	IP destino	Porta Origem	Porta Destino
Média	HW	0.72	0.61	0.59	0.79	0.30	0.46	0.72
	HWDS	0.73	0.57	0.57	0.84	0.43	0.56	0.83
Mediana	HW	0.75	0.47	0.58	0.82	0.31	0.50	0.85
	HWDS	0.76	0.57	0.58	0.87	0.49	0.59	0.90
Moda	HW	0.75	0.47	0.37	0.87	0.42	0.52	0.89
	HWDS	0.77	0.61	0.62	0.91	0.58	0.68	0.92

Como pode-se observar, com exceção das dimensões de pacotes/s e fluxos/s, o método HWDS obteve melhores resultados de CC que o tradicional método HW. Além disso, pode-se observar um comportamento heterogêneo entre as dimensões analisadas: as dimensões bits/s, IP de origem e Porta de Destino possuem um comportamento mais estável, enquanto as demais dimensões (em especial a dimensão de IP de destino) possuem um comportamento mais instável, ou seja, com mudanças comportamentais abruptas.

A segunda técnica utilizada no processo de análise de performance dos métodos abordados é o Erro Quadrático Médio Normalizado (NMSE). Essa métrica visa mensurar a distância ou erro entre o DSNSF gerado pelos métodos analisados e o movimento real de tráfego observado, evidenciando a precisão dessas abordagens. A Figura 5.11 apresenta os resultados obtidos por meio da utilização dessa técnica no ambiente de testes apresentado.

Figura 5.11 - NMSE entre os DSNSFs gerados pelos métodos HW e HWDS e o tráfego observado para os meses de Outubro e Novembro de 2012**.**



Diferentemente dos resultados obtidos por meio dos testes de CC, os erros apresentados pela Figura 5.11 são mais regulares, onde se pode observar claramente o aumento de performance obtido por meio da utilização do método HWDS. É possível verificar também que os índices de erros não ultrapassam a faixa de 0.1, com exceção dos resultados referentes aos feriados nacionais anteriormente mencionados. Além disso, em alguns dos dias analisados, tais como os dias 5 e 30 de outubro, foi identificado um desvio comportamental, o que foi responsável pela ocorrência de índices de erros elevados. Entretanto, esses dias foram considerados como normais no processo de caracterização de tráfego pois, neste momento do trabalho, ainda não é possível afirmar-se a ocorrência ou não de anomalias. Na média, os métodos HW e HWDS obtiveram resultados para este teste com valores 0.06 e 0.05, respectivamente.

A Tabela 5.4 apresenta os resultados obtidos por meio do teste NMSE relativa à utilização dos métodos analisados em cada uma das sete dimensões separadamente.

Tabela 5.4 - Resultados de NMSE dos métodos analisados em cada dimensão.

		bits	pacotes	fluxos	IP origem	IP destino	Porta Origem	Porta Destino
Média	HW	0.16	0.06	0.06	0.01	0.03	0.06	0.04
	HWDS	0.14	0.06	0.06	0.01	0.02	0.04	0.02
Mediana	HW	0.10	0.04	0.05	0.01	0.03	0.05	0.02
	HWDS	0.09	0.05	0.05	0.01	0.02	0.03	0.01
Moda	HW	0.06	0.03	0.03	0.01	0.03	0.03	0.01
	HWDS	0.04	0.03	0.03	0.01	0.02	0.02	0.01

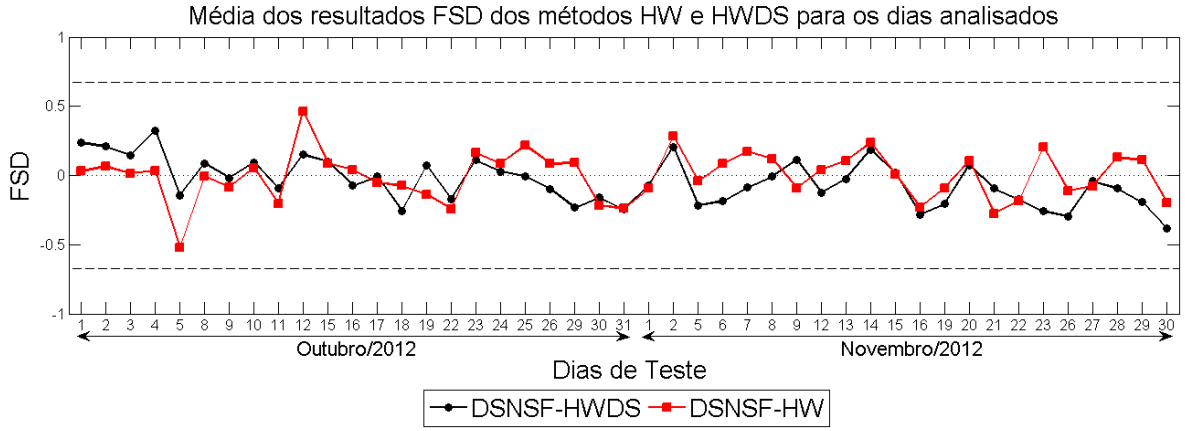
Como apresentado pela tabela, o método HWDS obteve resultados com erro inferior ou igual ao tradicional método HW em todas as dimensões analisadas, evidenciando o ganho de performance obtido por meio de sua utilização. Os erros NMSE relativos à dimensão bits/s são elevados em relação às demais dimensões devido à escala dos dados analisados (da ordem de 10^6). Como essa métrica não normaliza os dados para o cálculo do erro, ocorre essa pequena disparidade.

A terceira técnica utilizada é o Desvio Fracional Padrão (FSD), a qual foi aplicada aos métodos discutidos no ambiente de testes proposto com o objetivo de identificar a dispersão dos erros relativos aos DSNSFs gerados e o movimento real de tráfego observado. Em outras palavras, essa métrica descreve se os DSNSFs gerados são predominantemente

superiores ou inferiores ao tráfego observado, bem como o quão distante essa dispersão média se encontra do limite aceitável. A Figura 5.12 apresenta os resultados obtidos por meio da utilização da métrica FSD.

Conforme destacado na seção 5.1.1.3, embora os resultados da técnica FSD variem entre -2 e 2, valores entre o intervalo -0.67 e 0.67 (linhas tracejadas) são considerados bons do ponto de vista da dispersão média, onde valores representados por 0 (linha pontilhada ao centro) são considerados ótimos. Conforme apresentado na Figura 5.12, ambos os métodos se encontram dentro do intervalo considerado como bom pelo método FSD, se apresentando próximos do valor ótimo. A média geral dos resultados FSD obtidos pelos métodos HW e HWDS obtiveram valores de -0.0032 e -0.0467, respectivamente. Isso ocorre devido ao fato de que o método HW oscila bastante entre resultados positivos e negativos, o que acaba por aproximar o resultado médio de 0, enquanto o método HWDS se mantém predominantemente em resultados negativos.

Figura 5.12 - FSD entre os DSNSFs gerados pelos métodos HW e HWDS e o tráfego observado para os meses de Outubro e Novembro de 2012.



A Tabela 5.5 apresenta a média, mediana e moda dos resultados obtidos por meio do teste FSD relativo à utilização dos métodos analisados em cada uma das sete dimensões separadamente. Nessa tabela, os dados apresentados representam a média absoluta dos resultados FSD, objetivando uma análise comparativa mais precisa dos resultados obtidos.

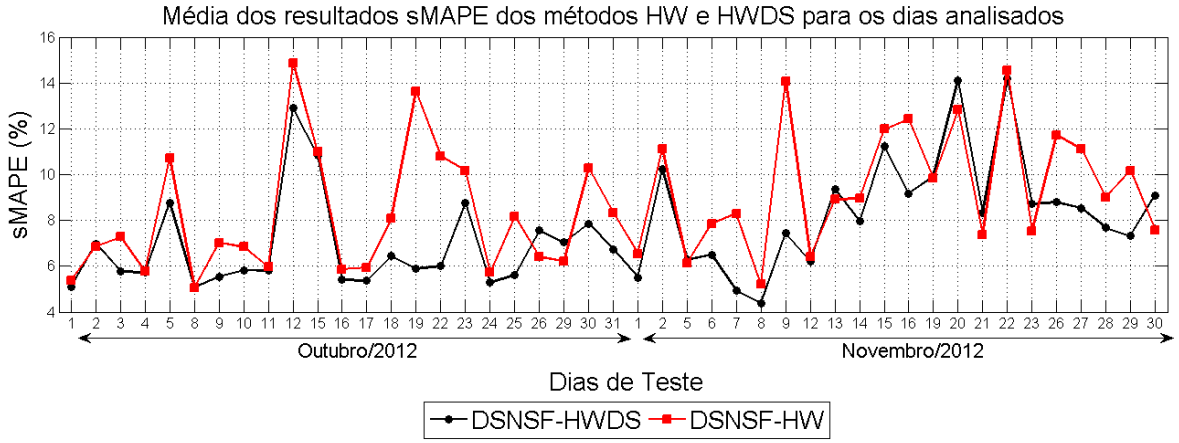
Tabela 5.5 - Resultados de FSD absolutos dos métodos analisados em cada dimensão.

		bits	pacotes	fluxos	IP origem	IP destino	Porta Origem	Porta Destino
Média	HW	0.25	0.32	0.30	0.21	0.22	0.17	0.26
	HWDS	0.22	0.27	0.27	0.21	0.27	0.24	0.21
Mediana	HW	0.21	0.22	0.19	0.16	0.22	0.14	0.21
	HWDS	0.19	0.24	0.24	0.17	0.29	0.20	0.18
Moda	HW	0.30	0.04	0.07	0.09	0.27	0.11	0.09
	HWDS	0.04	0.01	0.01	0.01	0.14	0.01	0.04

Conforme observado na tabela apresentada, o método HWDS se saiu melhor nas dimensões bits/s, pacotes/s e fluxos/s, ambos os métodos obtiveram resultados iguais para a dimensão de IP de origem, e o método HW se saiu melhor para as dimensões de IP de destino e portas de origem e destino. Os resultados obtidos pelos métodos são muito próximos, com ambos estando dentro do intervalo que designa bons valores para o teste FSD e estando próximos do valor ótimo. Embora os resultados gerais apontem o método HW como melhor, a média comum pode anular o real desempenho dos métodos, o que não ocorre com a análise da média absoluta ilustrada na Tabela 5.5, a qual aponta um empate de desempenho entre ambos os métodos.

Por fim, o Erro percentual médio absoluto simétrico (sMAPE) foi aplicado, métrica que, assim como o NMSE, é responsável por calcular a distância ou erro entre os DSNSFs gerados e o movimento real observado. Entretanto, essa métrica possui o diferencial de analisar de forma simétrica os erros positivos (DSNSF inferior ao movimento) e negativos (DSNSF superior ao movimento), resultando em um erro percentual que varia de 0 a 200%. Dessa forma, é possível uma análise de erro diferenciada e mais justa, a qual verifica os dois tipos de erro simetricamente. A Figura 5.13 apresenta os resultados obtidos para os métodos HW e HWDS por meio da utilização dessa métrica.

Figura 5.13 - sMAPE entre os DSNSFs gerados pelos métodos HW e HWDS e o tráfego observado para os meses de Outubro e Novembro de 2012.



Como pode ser observado na Figura 5.13 apresentada, novamente o método HWDS se saiu visivelmente melhor que o método tradicional HW. Com relação à média geral referente aos resultados da métrica sMAPE para os métodos HW e HWDS, foram obtidos os valores resultantes de 8.8% e 7.6%, respectivamente. Isso novamente ilustra o ganho de performance da utilização do método HWDS sobre o método tradicional.

Os resultados obtidos através da utilização dessa métrica com relação às sete dimensões separadamente são apresentados pela Tabela 5.6, onde pode-se verificar o comportamento dessas dimensões de forma mais precisa.

Tabela 5.6 - Resultados de sMAPE dos métodos analisados em cada dimensão.

		bits	pacotes	fluxos	IP origem	IP destino	Porta Origem	Porta Destino
Média	HW	15.1%	9.0%	9.4%	3.7%	7.5%	9.9%	7.0%
	HWDS	13.3%	8.5%	8.5%	3.4%	5.8%	7.9%	5.5%
Mediana	HW	13.7%	8.2%	8.7%	3.2%	7.2%	8.5%	5.1%
	HWDS	11.8%	7.6%	7.6%	3.2%	5.8%	6.9%	4.0%
Moda	HW	11.4%	7.9%	4.2%	3.1%	7.7%	8.3%	5.0%
	HWDS	6.6%	7.4%	3.9%	2.9%	5.8%	6.1%	4.1%

Como ilustrado pela Tabela 5.6, os erros percentuais relativos à ambos os métodos são considerados baixos, visto que o erro máximo da métrica é de 200%. Ainda sim, mesmo que as taxas de erro não cheguem ao máximo, quanto mais elevadas elas são, maiores as chances de o processo de caracterização de tráfego não conseguir descrever com êxito o

comportamento normal da rede, prejudicando no funcionamento geral do sistema. Como pode ser verificado, o método HWDS novamente se saiu melhor em todas as dimensões, em relação ao método tradicional HW.

Para ilustrar de forma gráfica os resultados obtidos pelos métodos HW e HWDS na caracterização de tráfego neste cenário, as Figuras 5.14 a 5.18 mostram o movimento de tráfego real e os DSNSFs gerados por estes métodos para cada uma das 7 dimensões analisadas, relativos aos dias 22 a 26 de Outubro de 2012.

Figura 5.14 - Tráfego e DSNSFs gerados relativos ao dia 22 de Outubro de 2012.

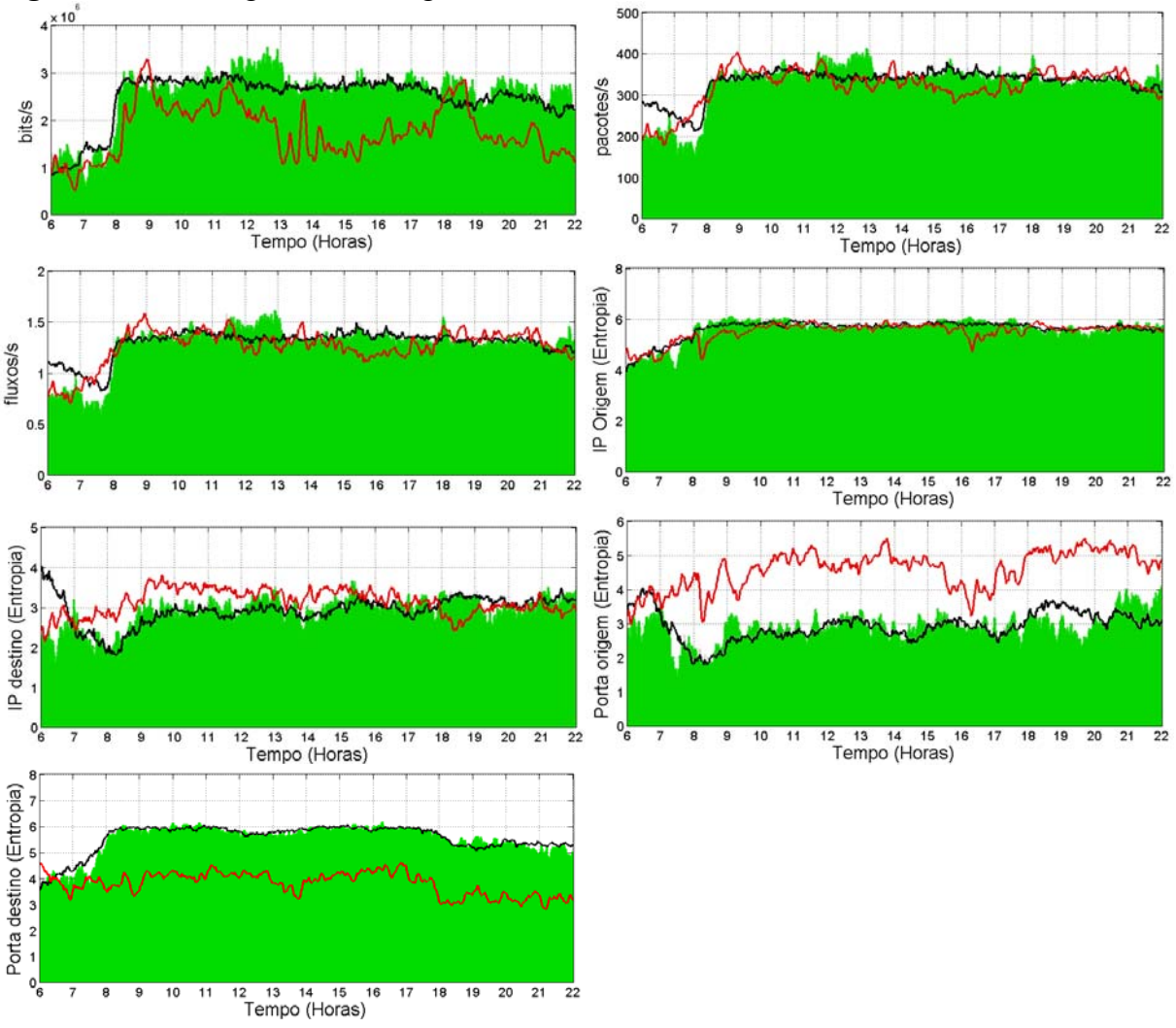


Figura 5.15 - Tráfego e DSNSFs gerados relativos ao dia 23 de Outubro de 2012.

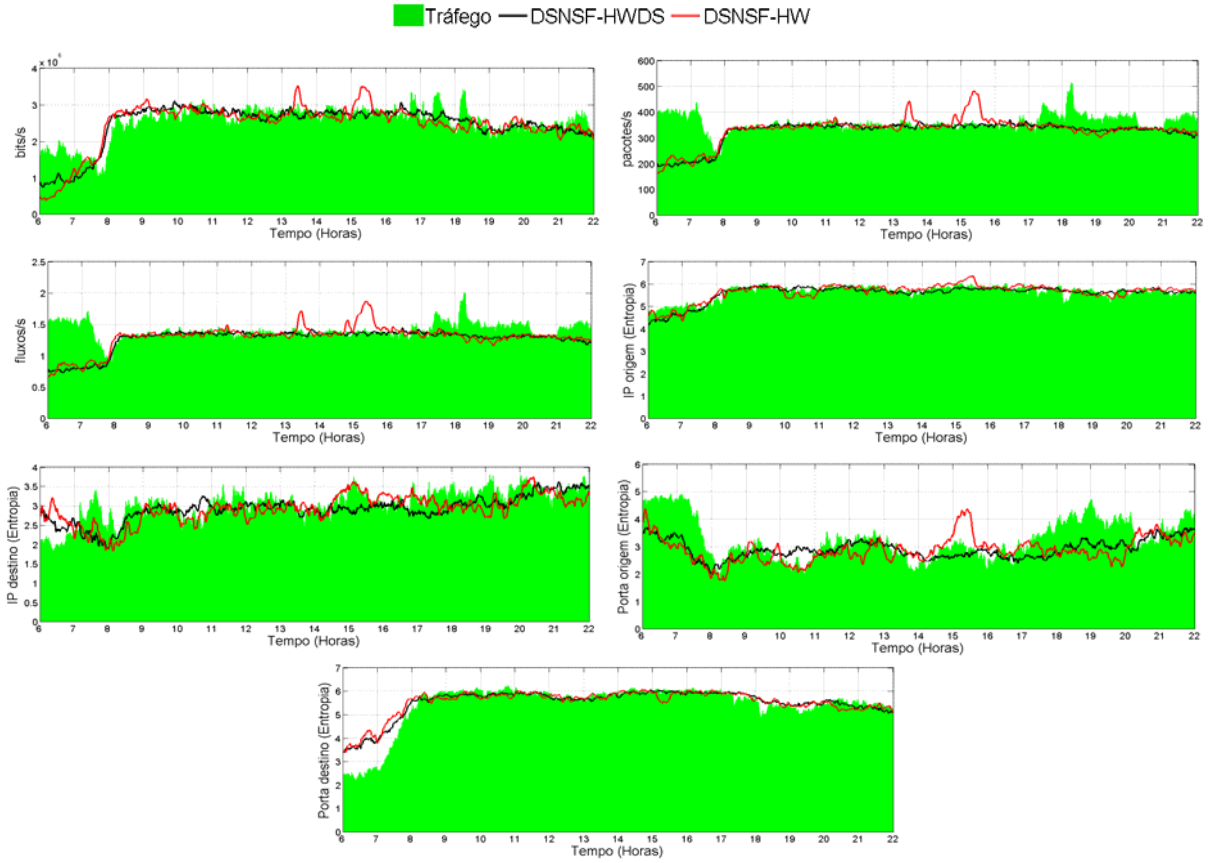


Figura 5.16 - Tráfego e DSNSFs gerados relativos ao dia 24 de Outubro de 2012.

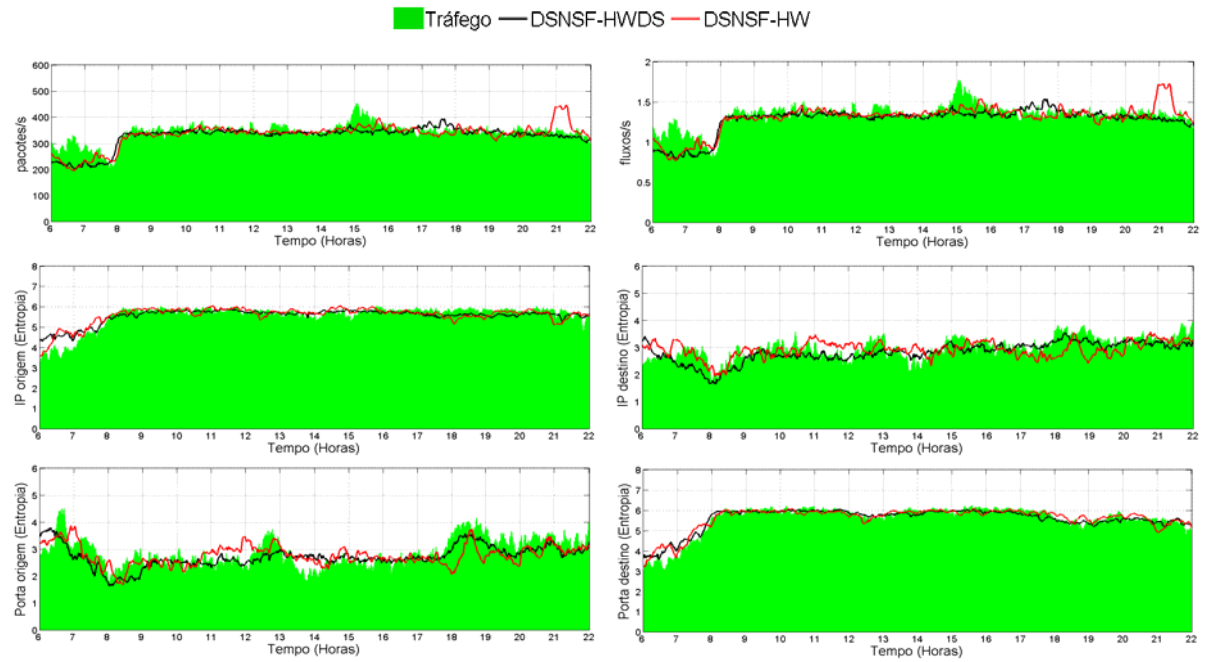


Figura 5.17 - Tráfego e DSNSFs gerados relativos ao dia 25 de Outubro de 2012.

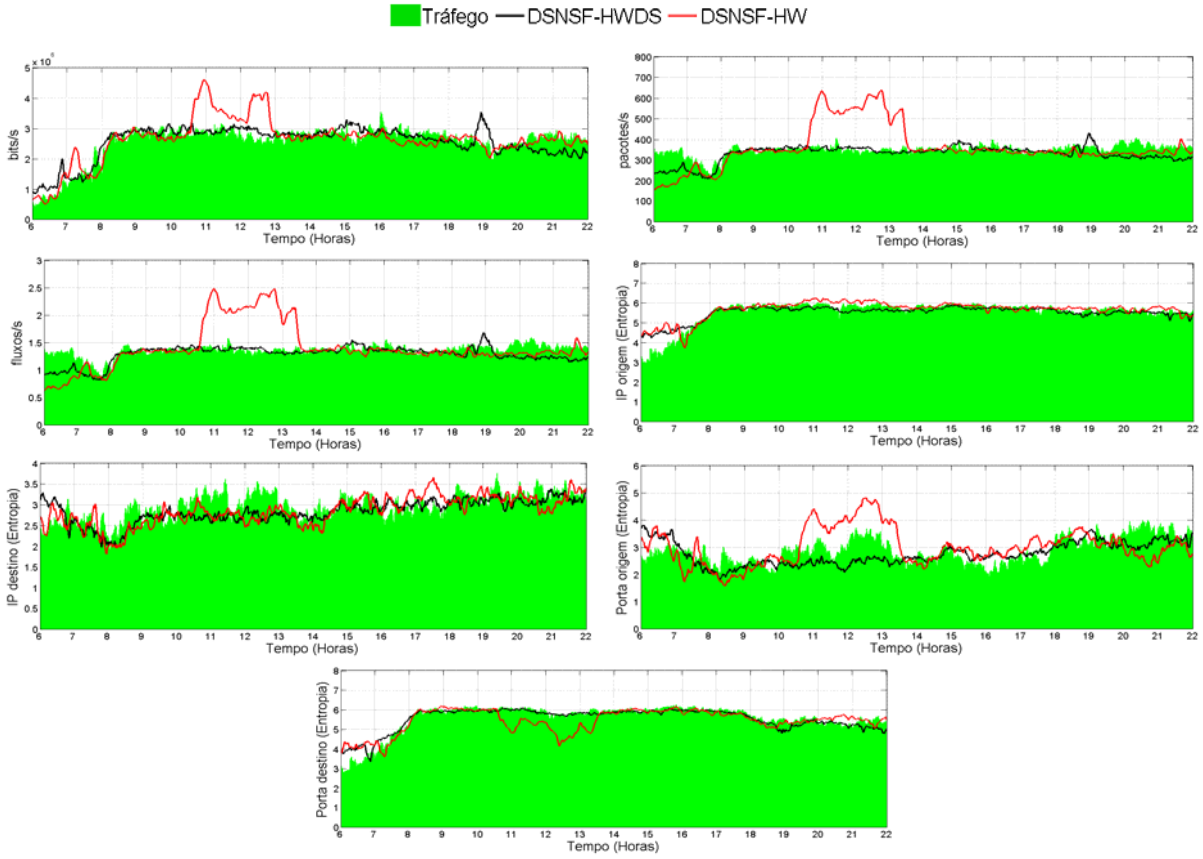
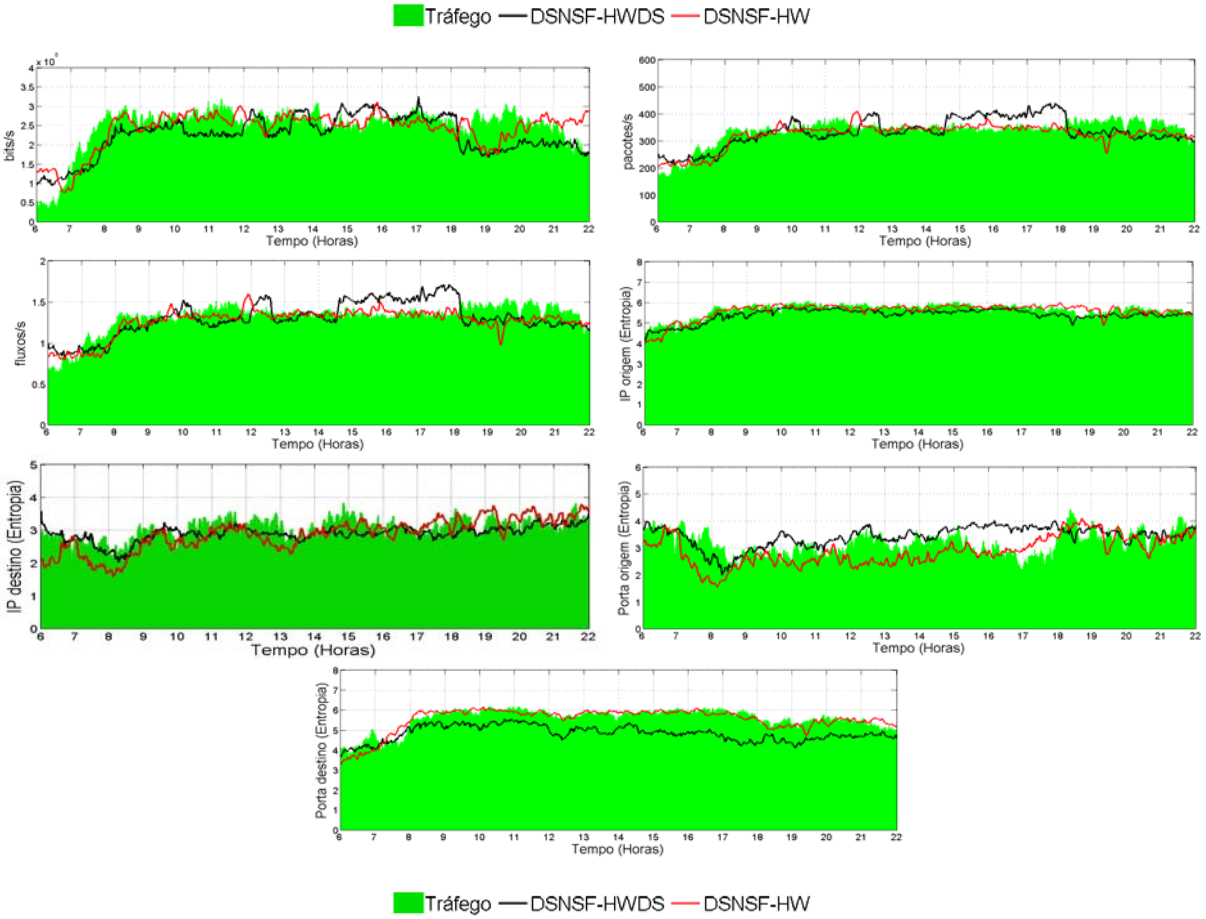


Figura 5.18 - Tráfego e DSNSFs gerados relativos ao dia 26 de Outubro de 2012.



Como se pode observar por meio dos gráficos expostos, os DSNSFs apresentados por ambos os métodos eficientemente descrevem o movimento de tráfego observado nas sete dimensões analisadas. Entretanto, o método HW mostra-se muito mais suscetível à incorporação de comportamentos que diferem do normal no DSNSF gerado, o que prejudica o processo da caracterização de tráfego e, consequentemente, pode ocasionar a diminuição de eficiência do processo de detecção de anomalias. Além disso, observa-se que o DSNSF gerado pelo método HWDS é capaz de eficientemente descrever o comportamento do tráfego de rede, apresentando boas previsões em todas as dimensões.

Outra conclusão que pode ser tomada, com base nas Figuras 5.14 a 5.18, é que as dimensões IP de origem e porta de destino são extremamente estáveis, enquanto as dimensões de volume (bits/s, pacotes/s e fluxos/s) demonstram uma estabilidade mediana e as demais dimensões (IP de destino e portas de origem) são mais instáveis. Isso implica que as dimensões de IP de destino e portas de origem apresentam um comportamento caracterizado pela presença de muitos picos no movimento, o que dificulta o processo de caracterização de

tráfego. Mesmo assim, os métodos obtiveram bons resultados neste processo, o que demonstra a efetividade dos mesmos para o problema proposto.

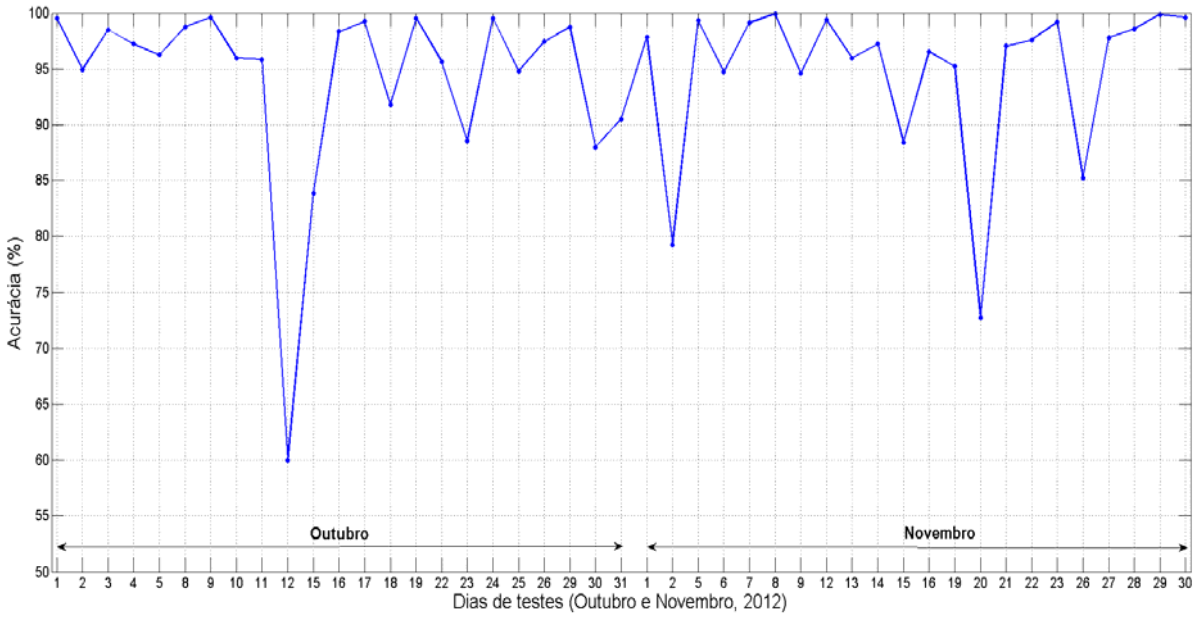
Com base nos testes de performance apresentados, bem como nos resultados gráficos ilustrados, pode-se concluir que o método HWDS possui um considerável ganho de performance sobre o tradicional método HW. Os resultados de performance apresentados por meio das técnicas CC, NMSE, sMAPE e FSD comprovam que o método HWDS se saiu melhor ou igual, no pior caso, ao método tradicional. Em um primeiro momento, ao se avaliar o ganho de performance obtido por meio dessa modificação do método tradicional, pode parecer que este ganho é muito baixo para justificar a modificação. Entretanto, ao se observar os DSNSFs gerados por ambos os métodos, é possível notar a clara vantagem de eficiência da utilização do método HWDS. Além disso, conforme discutido anteriormente, o processo de caracterização de tráfego é a base de funcionamento do sistema de detecção de anomalias apresentado neste trabalho. Sendo assim, quanto melhores os resultados providos por essa etapa, mais precisos e eficientes serão os resultados obtidos por meio do processo de detecção de anomalias.

Com isso, pode-se concluir que o método HWDS é mais eficiente que o tradicional método HW quando aplicado ao processo de caracterização de tráfego (criação de DSNSFs) de redes de larga escala.

Com relação à detecção de anomalias, o sistema apresentado foi aplicado ao ambiente de testes aqui descrito como uma ferramenta funcional, avaliando seu comportamento com relação aos dias úteis de Outubro e Novembro de 2012. A sinalização dos dados avaliados para a validação de eficiência deste sistema foi realizada por um grupo de administradores da rede analisada. Tal sinalização foi utilizada como gabarito para os testes de acurácia e eficiência realizados.

Para a avaliação de performance do sistema, foram utilizadas as métricas descritas na seção 5.1.2. A primeira métrica avaliada foi a Acurácia, técnica que avalia o quão preciso o sistema é na classificação de intervalos como anômalos ou normais, ou seja, evidencia a eficiência de classificação geral do sistema. A Figura 5.19 ilustra os resultados obtidos pelo sistema por meio da utilização dessa técnica.

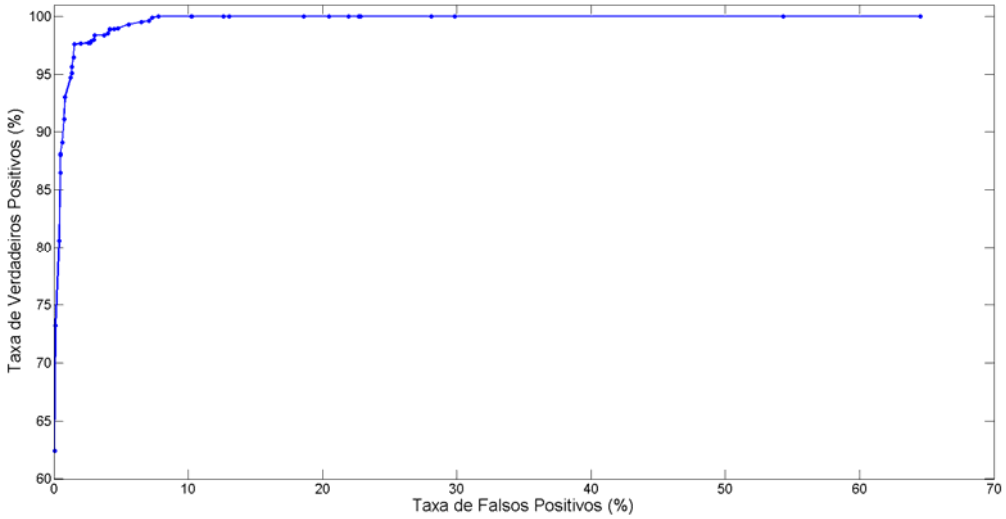
Figura 5.19 - Medidas de Acurácia do sistema para os dias úteis de Outubro e Novembro de 2012.



Como pode-se observar, com exceção dos dias 12 e 15 de Outubro e 02, 15 e 20 de Novembro, o sistema apresenta índices de Acurácia superiores a 90%, com medidas de média geral, mediana e moda de 94%, 97% e 99%, respectivamente. Os resultados apontam que o sistema é capaz de eficientemente classificar intervalos como anômalos ou normais, auxiliando administradores de rede na detecção de comportamentos anômalos com precisão.

Outra métrica utilizada é a Curva ROC, gráfico que confronta as métricas de taxas de Verdadeiros Positivos e Falsos Positivos, evidenciando o *trade-off* do sistema na classificação de anomalias. As taxas de Verdadeiros Positivos (TVP) apontam a porcentagem de anomalias reais detectadas, enquanto as taxas de Falsos Positivos (TFP) apontam a porcentagem de intervalos normais classificados como anômalos (erroneamente) pelo sistema. Os resultados obtidos por meio da utilização dessa técnica podem ser observados na Figura 5.20.

Figura 5.20 - Curva ROC do sistema apresentado relativa aos resultados de detecção de anomalias nos meses de Outubro e Novembro de 2012.



Como apontado na seção 5.1.2.2, quanto mais próxima a linha resultante deste teste se encontrar de taxas de 0% de TFP e 100% de TVP, melhores são os resultados de classificação. Em outras palavras, quanto maior a área abaixo da curva, melhor são os resultados do sistema com relação à geração de Alarmes e Alertas. Como se pode observar na Figura 5.20, os resultados obtidos foram próximos do ótimo, onde o sistema apresentado pode atingir um *trade-off* de 97% de TVP com 5% de TFP, o que ilustra a alta precisão e eficiência do sistema na detecção de comportamentos anômalos.

Além disso, é importante destacar que o sistema apresentado não somente detecta a ocorrência de anomalias, mas também disponibiliza ao administrador da rede informações importantes e relevantes acerca dessas anomalias. Para ilustrar essa funcionalidade, uma requisição de informações (Módulo de Informação) foi executada no intervalo de tempo relativo ao dia 30 de Outubro de 2012, às 20h. Neste intervalo, uma anomalia do tipo *Flash Crowd* foi detectada e identificada pelo sistema. A Figura 5.21 apresenta a análise global, visão hepta-dimensional do intervalo de tempo solicitado, o qual evidencia a assinatura relativa à *Flash Crowds*. Nota-se que todas as dimensões, exceto a entropia de Endereços IP de origem, estão fora do limite esperado. Além disso, as Tabelas 5.7 a 5.11 apresentam os dados relativos à classificação de usuários com maior frequência de ocorrência neste intervalo de tempo, o qual disponibiliza os 3 endereços IP de origem e destino, portas de origem e destino e protocolos com maior índice percentual de ocorrência.

Figura 5.21 - Visão hepta-dimensional de uma anomalia do tipo *Flash Crowd* detectada.

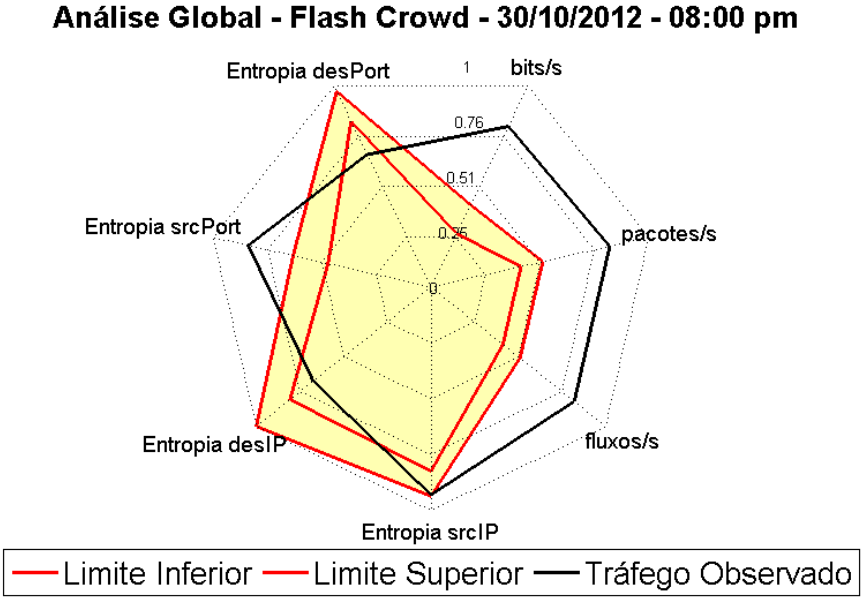


Tabela 5.7 - Módulo de Informação - *Flash Crowd* - 30/10/2012 - 08:00 pm - Endereços IP de Origem

	Classificação por Frequência
	SrcIP
TOP 1	**189.58.159.46** *(6%)*
TOP 2	**189.60.244.73** *(6%)*
TOP 3	**187.64.34.95** *(5%)*
Outros	*(83%)*

Tabela 5.8 - Módulo de Informação - *Flash Crowd* - 30/10/2012 - 08:00 pm - Endereços IP de Destino

	Classificação por Frequência
	DesIP
TOP 1	**189.90.77.148** *(52%)*
TOP 2	**189.90.65.11** *(23%)*
TOP 3	**189.90.67.66** *(4%)*
Outros	*(21%)*

Tabela 5.9 - Módulo de Informação - *Flash Crowd* - 30/10/2012 - 08:00 pm - Portas de Origem

	Classificação por Frequência
	SrcPort
TOP 1	**80** *(21%)*
TOP 2	**443** *(8%)*
TOP 3	**56379** *(6%)*
Outros	*(65%)*

Tabela 5.10 - Módulo de Informação - *Flash Crowd* - 30/10/2012 - 08:00 pm - Portas de Destino

	Classificação por Frequência
	DesPort
TOP 1	**14428** *(47%)*
TOP 2	**80** *(5%)*
TOP 3	**13473** *(3%)*

Tabela 5.11 - Módulo de Informação - Flash Crowd - 30/10/2012 - 08:00 pm - Protocolos

	Classificação por Frequência
	Protocolo
TOP 1	**TCP** *(60%)*
TOP 2	**UDP** *(40%)*
TOP 3	----------

Através dos dados disponibilizados pelo sistema, foi possível identificar que um dos endereços IP mais acessados (destacado em vermelho na Tabela 5.8) era referente ao *website* da Universidade responsável pela organização de processos seletivos. Por meio de uma pesquisa mais aprofundada pode-se concluir que o evento *Flash Crowd* provavelmente ocorreu devido à divulgação do resultado de um concurso público da Polícia Civil do Paraná [55].

Dessa forma pode-se concluir que, além da efetividade do processo de caracterização de tráfego, o sistema apresentado é eficiente e preciso na detecção de anomalias que ocorrem em redes de larga escala. Além disso, as informações providas pelo sistema se mostraram úteis na identificação da causa de um problema detectado, o que comprova sua efetividade também na identificação de problemas.

5.3.1.2 Testes com anomalias simuladas

Durante o período de testes abordado pela seção 5.3.1.1, apenas anomalias do tipo *Flash Crowd* foram detectadas. Visando validar a performance do sistema apresentado em outras situações anômalas, tais como ataques DoS, DDoS ou *Port Scans*, foram utilizados dados simulados. Dessa forma, a ferramenta Scorpius - sFlow *Anomaly Simulator* [56], descrita no Apêndice A, foi utilizada nessa simulação.

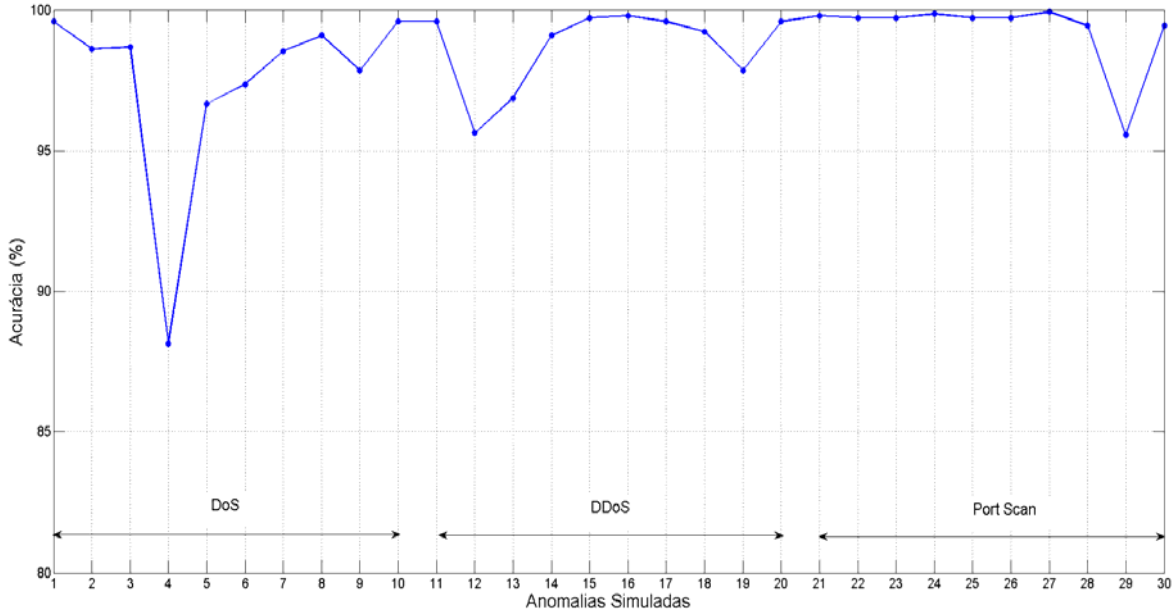
Foram coletados registros de fluxos reais da Universidade Estadual de Londrina - Paraná, tal como abordado na seção anterior. Os fluxos coletados são relativos ao mês de Setembro de 2012, o qual foi utilizado como período de treinamento para o sistema. Além disso, o dia 9 de Outubro de 2012 (um dia de comportamento normal, segundo os resultados da seção anterior) foi utilizado como entrada para a ferramenta Scorpius, a qual injetou comportamentos anômalos específicos descritos anteriormente.

Cada anomalia verificada foi testada 10 vezes diferentes. Os ataques DoS injetam fluxos relacionados a um único endereço IP de origem exaustivamente transmitindo pacotes UDP para um endereço IP de destino individual, de portas específicas de origem e destino. Os ataques DDoS injetam fluxos relacionados a diversos endereços IP de origem diferentes, exaustivamente transmitindo pacotes UDP para um único endereço IP de destino, de portas específicas de origem e destino. Finalmente, os *Port Scans* injetam fluxos relacionados a um único endereço IP de origem transmitindo mensagens de conexão TCP para um único endereço IP de destino, de uma porta específica de origem para um amplo intervalo (*range*) de portas de destino.

Para os ataques DoS, foi utilizado o endereço IP fictício de origem 11.11.11.11, através da porta número 80, atacando o endereço IP fictício de destino 22.22.22.22, através da porta 8081. Para os ataques DDoS, foram utilizados de 10 a 2560 diferentes endereços IP fictícios de origem, através da porta 80, atacando o endereço IP fictício de destino 22.22.22.22 por meio da porta 8081. Por último, para os ataques do tipo *Port Scan*, foi utilizado o endereço IP fictício de origem 11.11.11.11, através da porta 80, para verificar diferentes intervalos de portas (de 1~3000 até 1~65535) do endereço de IP fictício de destino 22.22.22.22.

Os resultados obtidos por meio dos testes de Acurácia são apresentados na Figura 5.22, onde os dados das diferentes anomalias testadas são divididos da seguinte forma: no eixo *x*, de 1 a 10 representa os resultados de ataques DoS, 11 a 20 são relacionados a ataques DDoS, e 21 a 30 representam ataques *Port Scan*. Conforme observado, o sistema apresentado atingiu bons valores de acurácia, com taxas maiores que 95% em cada um dos testes executados.

Figura 5.22 - Medidas de Acurácia do sistema para diferentes anomalias simuladas.



A curva ROC ilustrada na Figura 5.23 representa os resultados de taxas de Verdadeiros Positivos (TVP) e Falsos Positivos (TFP) para este cenário utilizando os dados com anomalias simuladas. Como observado, o sistema atingiu 95% de TVP com 1% de TFP, o que representa um bom *trade-off* do ponto de vista da eficiência da geração de alarmes.

Os dados relativos ao módulo de Informação da primeira simulação de anomalia para cada tipo de ataque avaliado pode ser observado na Figura 5.24, onde os sub-gráficos (a), (b) e (c) representam os gráficos de radar que descrevem a visão hepta-dimensional dos ataques DoS, DDoS e *Port Scan*, respectivamente.

Figura 5.23 - Curva ROC do sistema apresentado para diferentes anomalias simuladas.

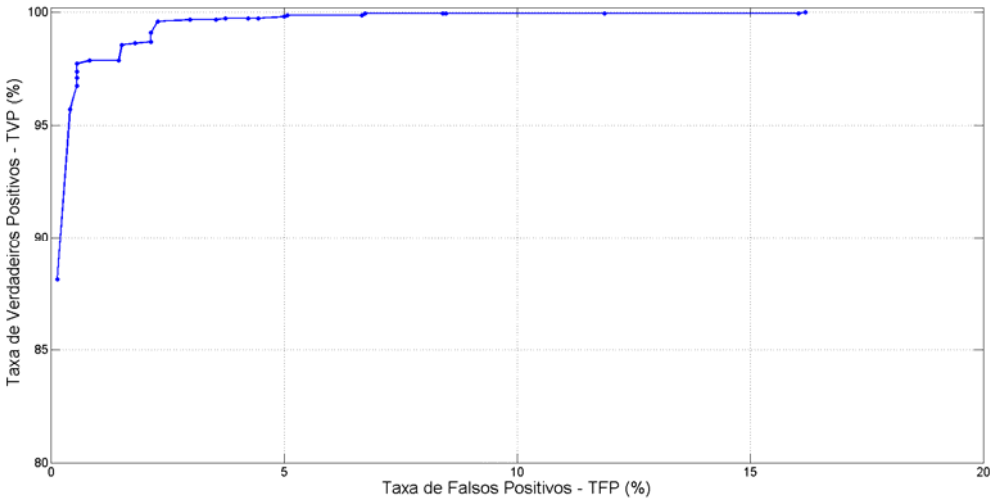


Figura 5.24 - Visão hepta-dimensional que ilustra o comportamento das diferentes anomalias simuladas.

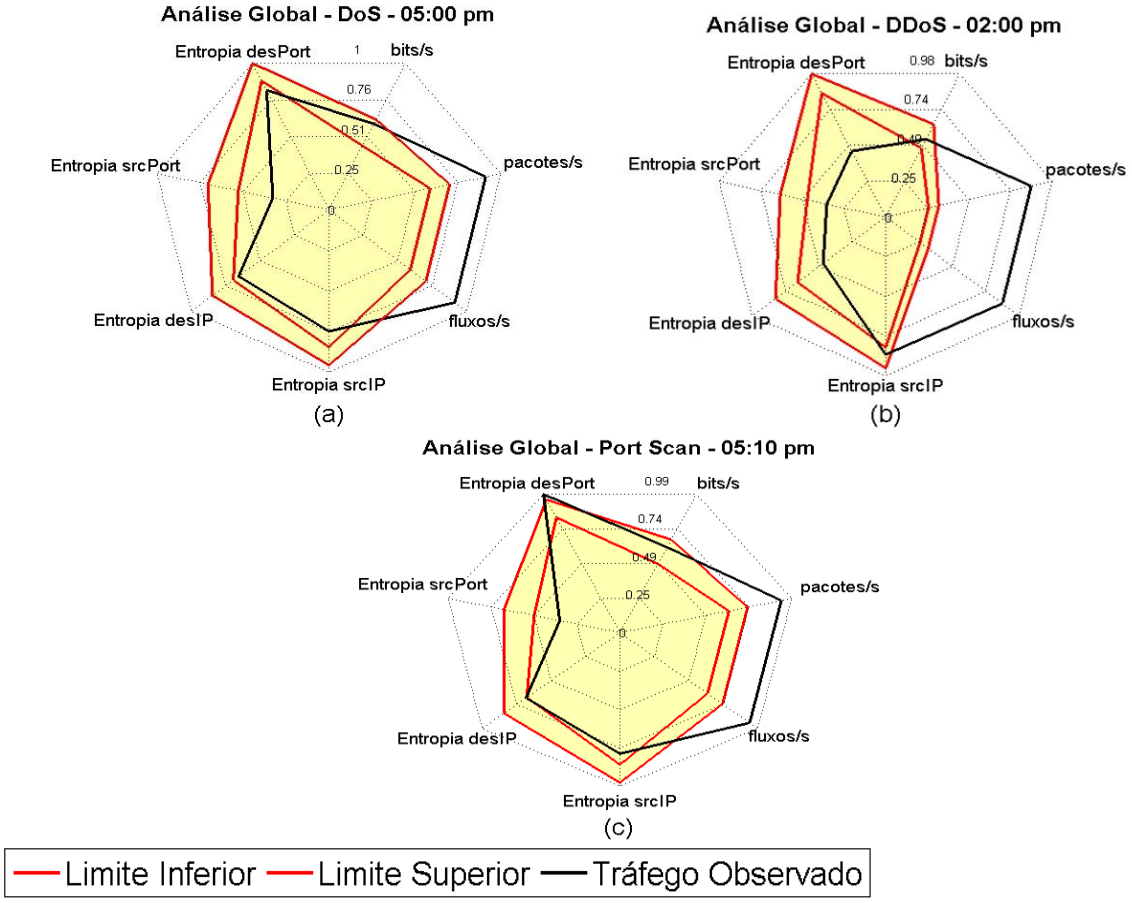
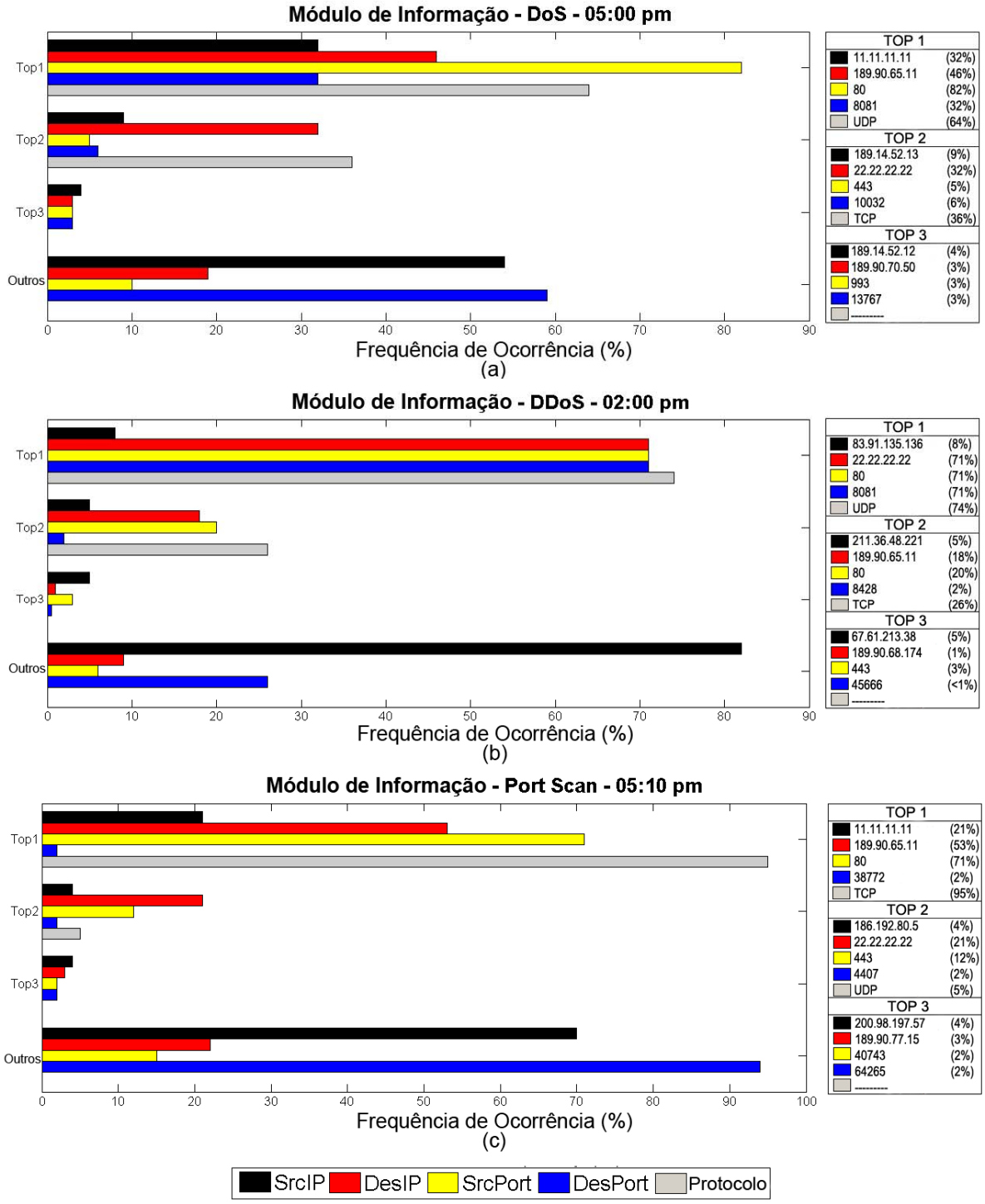


Figura 5.25 - Módulo de Informação que ilustra uma classificação de frequência de ocorrência de diferentes atributos para as anomalias simuladas.



Além disso, as informações relativas à classificação de principais frequências relacionadas a estes ataques são mostradas na Figura 5.25, onde os sub-gráficos (a), (b) e (c) representam os ataques DoS, DDoS e *Port Scan*, respectivamente. Como pode ser observado, no ataque DoS o sistema foi capaz de identificar o dispositivo de origem do ataque e o dispositivo alvo, bem como suas respectivas portas. No ataque DDoS, alguns dos

endereços IP fictícios aleatórios de origem foram detectados mas, como o sistema gerou um Alarme do tipo DDoS, o administrador de redes deve focar seus esforços em fechar a porta que está sendo especificamente atacada, a qual também foi identificada pelo sistema. Finalmente, no ataque do tipo *Port Scan*, o sistema apresentado foi capaz de identificar com sucesso os dispositivos de origem e destino do ataque.

Com isso, pode-se concluir que, assim como apontado na seção anterior, o sistema é capaz de eficientemente detectar anomalias que ocorrem, com alta taxa de acurácia e alarmes Verdadeiros Positivos, e com baixas taxas de alarmes Falsos Positivos. Além disso, o módulo de informação permite a identificação de diferentes anomalias por suas assinaturas, conforme a Análise Global, apresentando uma visão hepta-dimensional da anomalia detectada, bem como a identificação de suas possíveis causas por meio da eficiente classificação de diferentes atributos por frequência de ocorrência.

5.3.2 Cenário 2

Este cenário objetiva a avaliação de performance do sistema apresentado em um ambiente de baixa a média agregação de tráfego para comprovar sua eficiência de aplicação em redes menores, onde a utilização de usuários individuais influi diretamente no comportamento geral da rede.

O sistema apresentado será avaliado tanto no processo de caracterização de tráfego, onde a eficiência da criação de *Digital Signatures of Network Segment using Flow analysis* (DSNSF) por meio do método HWDS será analisada, quanto na detecção de anomalias. Ambas as abordagens de análise são baseadas em dados reais coletados.

Foram coletados registros de fluxos reais da Universidade Federal Tecnológica do Paraná (UTFPR) - Campus Toledo, uma rede de baixa a média escala composta por cerca de 400 diferentes *hosts*. Os fluxos foram coletados através da nona versão do protocolo de exportação Netflow sem a utilização de qualquer mecanismo de amostragem, ou seja, com escala de coleta de pacotes de 1:1.

Os dados coletados são referentes aos dias úteis de Abril e Maio de 2013. Assim como no cenário de testes anterior, o primeiro mês é utilizado como treinamento para o sistema na geração de DSNSFs das sete dimensões avaliadas, enquanto o segundo mês é utilizado nos testes de validação de performance do sistema. É importante destacar que os dias 01 e 30 do mês de Maio são feriados nacionais e o dia 31 deste mesmo mês representa um recesso, apresentando comportamentos que diferem do esperado (dias anômalos). Além disso,

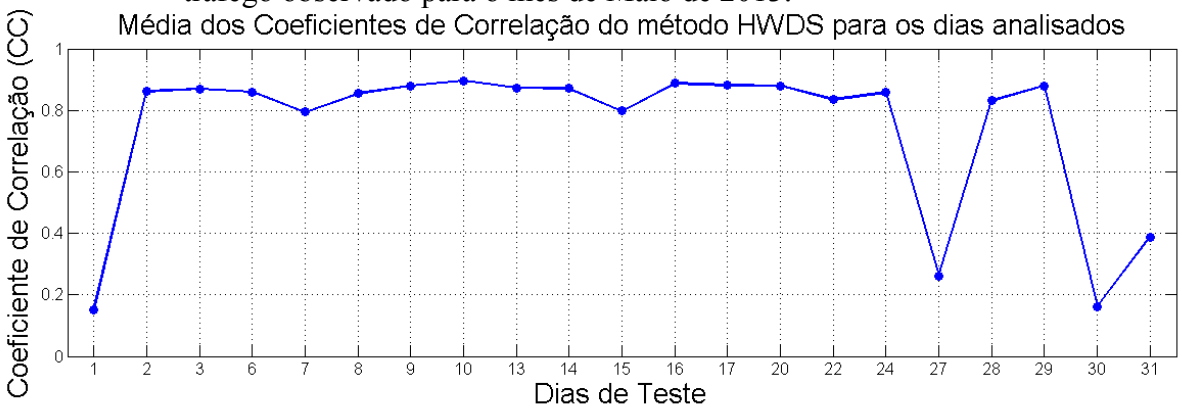
os registros de fluxos IP relativos aos dias 21 e 22 de Maio foram comprometidos devido à alguma falha no processo de exportação, uma vez que os arquivos de fluxos referentes à estes dias se encontram incompletos. Dessa forma, estes dois últimos dias mencionados não serão incluídos no processo de análise de performance do sistema, embora os feriados mencionados sejam analisados normalmente.

Os valores definidos para os coeficientes de suavização utilizados no método HWDS e no processo de Suavização Exponencial são os mesmos definidos no cenário de testes anterior, possuindo valores de $\alpha = 0.28$, $\beta = 0.0035$, $\gamma = 0.1$ e $\omega = 0.3$. Estes valores foram definidos como os melhores para o processo de caracterização de tráfego através de testes exaustivos e baseado em trabalhos anteriores da literatura [31, 33, 54]. Além disso, o ciclo sazonal, o qual é definido pela constante *s* no método HWDS, representa o número de janelas de tempo que a série temporal possui. Os dados coletados são divididos em intervalos de análise de 1 minuto, de modo que essa constante é definida com o valor 1440. Em outras palavras, cada dia analisado é representado por 1440 diferentes intervalos de tempo ou janelas temporais de análise.

Como forma de se verificar a efetividade do sistema apresentado na caracterização de tráfego, as técnicas descritas na sessão 5.1.1 serão aplicadas ao método HWDS. Como este sistema utiliza uma análise hepta-dimensional de fluxos IP no processo de caracterização de tráfego, 7 diferentes DSNSFs são criados para representar o comportamento normal de cada dia, o que implica em 7 diferentes resultados para todos esses dias e, consequentemente, inviabiliza a representação dos resultados por meio de gráficos convencionais. Para simplificar o processo de verificação dos resultados obtidos nas 7 dimensões, foi calculada a média dos resultados observados, gerando um valor único para cada dia avaliado que representa todo o processo de caracterização de tráfego.

A primeira métrica a ser utilizada é o Coeficiente de Correlação, objetivando mensurar o grau de similaridade entre as tendências de crescimento e decrescimento entre os movimentos reais observados e os DSNSFs gerados pelo sistema. Os resultados obtidos por meio da utilização dessa métrica podem ser observados na Figura 5.26.

Figura 5.26 - Coeficientes de Correlação entre os DSNSFs gerados pelo método HWDS e o tráfego observado para o mês de Maio de 2013.



Como se pode observar, os resultados para o teste de CC são bem regulares, ao contrário do observado no cenário anterior. Isso se deve à diferença entre as tendências de crescimento observadas nos dois cenários: no primeiro cenário as alterações de crescimento e decrescimento ocorriam com grande frequência e baixa variação, enquanto no segundo cenário essas alterações ocorrem com mesma frequência e alta variação. No caso deste cenário, as tendências de crescimento e decrescimento são mais significativas, ocasionando em melhores resultados para a métrica CC. Com exceção dos dias anteriormente apontados como feriados nacionais e recesso, o sistema apresentado atingiu um índice de CC médio de 0.85.

Além disso, a Tabela 5.12 apresenta a média, mediana e moda dos resultados obtidos por meio do teste CC relativo à utilização do método de previsão HWDS em cada uma das 7 dimensões separadamente. Essa tabela tem como objetivo evidenciar o comportamento heterogêneo apresentado pelas diferentes dimensões avaliadas.

Tabela 5.12 - Resultados de CC do método HWDS em cada dimensão.

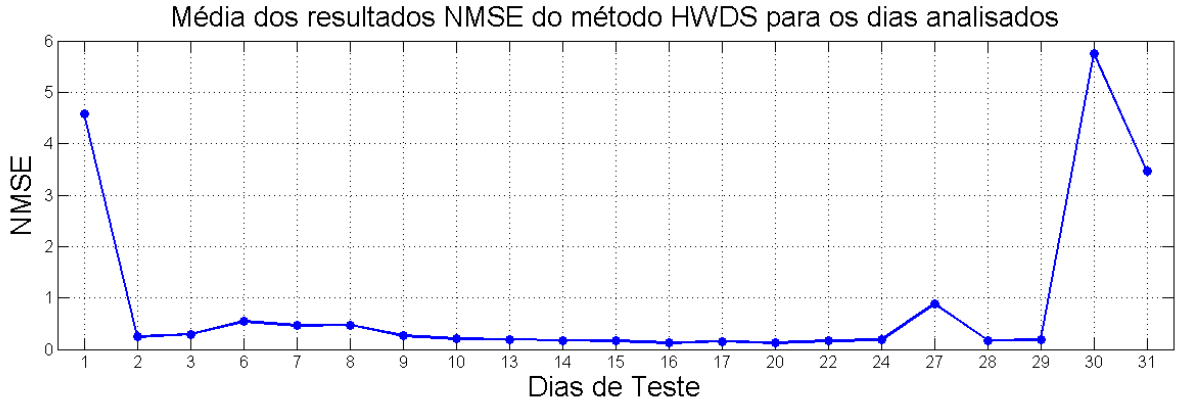
	bits/s	pacotes/s	fluxos/s	IP origem	IP destino	Porta Origem	Porta Destino
Média	0.64	0.67	0.73	0.80	0.74	0.78	0.81
Mediana	0.74	0.78	0.86	0.89	0.81	0.92	0.93
Moda	0.78	0.82	0.81	0.87	0.77	0.78	0.97

Como se pode observar, as dimensões de volume (bits, pacotes e fluxos por segundo) obtiveram resultados da métrica CC inferiores às demais dimensões. Isso implica que essas dimensões possuem um comportamento mais instável, com mudanças comportamentais (tendências de crescimento e decrescimento) mais abruptas mesmo após o

processo de suavização exponencial utilizado pelo sistema apresentado. As dimensões relativas à entropia de endereços IP e portas de origem e destino se mostraram mais estáveis, de modo que seu comportamento pode ser caracterizado com maior facilidade.

A segunda técnica utilizada na análise de performance do método HWDS neste cenário é o Erro Quadrático Médio Normalizado (NMSE). Essa métrica mede a distância ou erro entre o DSNSF gerado e o movimento real de tráfego observado, de modo a comprovar a precisão do sistema. A Figura 5.27 apresenta os resultados obtidos por meio dessa métrica para este cenário de testes.

Figura 5.27 – NMSE entre os DSNSFs gerados pelo método HWDS e o tráfego observado para o mês de Maio de 2013.



Como se pode observar, com exceção dos feriados e recessos anteriormente mencionados, o sistema obteve resultados bastante estáveis e satisfatórios para a métrica NMSE, com erros médios de 0.28. Embora este resultado seja considerado bom, estes erros são mais elevados que os obtidos no cenário 1. Redes de larga escala, como é o caso do primeiro cenário de análise, possuem um comportamento estável, enquanto redes de menor porte possuem traços comportamentais de tráfego instáveis, o que dificulta o processo de caracterização de tráfego. Isso ocorre pois, em redes menores, a utilização dos recursos e serviços de rede por usuários individuais influi diretamente no traço comportamental observado.

A Tabela 5.13 apresenta a média, mediana e moda dos resultados obtidos por meio da métrica NMSE relativo à utilização do método de previsão HWDS em cada uma das 7 dimensões separadamente.

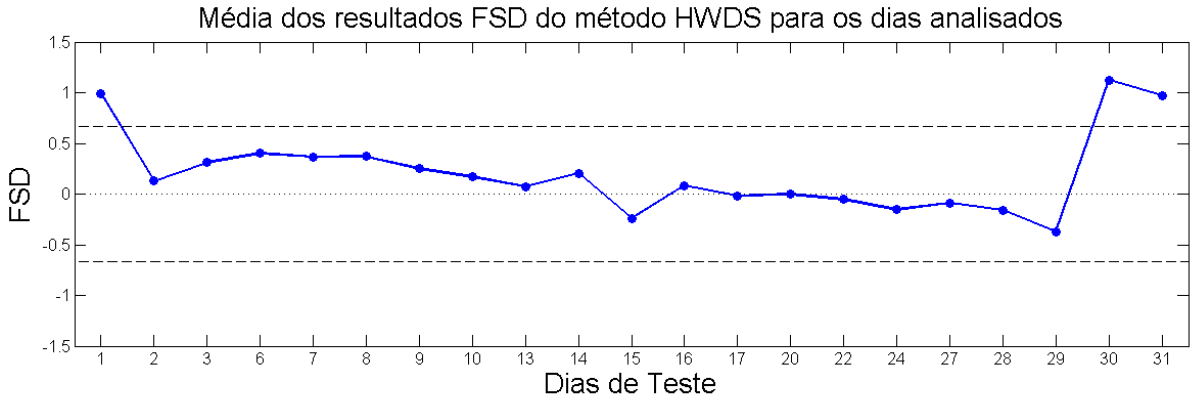
Tabela 5.13 - Resultados de NMSE do método HWDS em cada dimensão.

	bits/s	pacotes/s	fluxos/s	IP origem	IP destino	Porta Origem	Porta Destino
Média	2.15	1.99	1.92	0.07	0.08	0.03	0.03
Mediana	0.60	0.44	0.30	0.03	0.04	0.01	0.01
Moda	0.33	0.27	0.13	0.01	0.02	0.002	0.006

Conforme ilustrado na tabela, novamente as dimensões relativas à volume (bits, pacotes e fluxos por segundo) obtiveram resultados de performance inferiores às demais dimensões. Dessa forma, este teste novamente indica que essas dimensões possuem padrões comportamentais instáveis, enquanto as demais dimensões são caracterizadas por uma maior estabilidade, facilitando o processo de caracterização de tráfego.

A terceira métrica, o Desvio Fracional Padrão (FSD), foi aplicada ao sistema apresentado objetivando identificar a dispersão de erros relativos aos DSNSFs gerados e o movimento real de tráfego observado, avaliando se as assinaturas gerais são predominantemente superiores ou inferiores ao tráfego observado. A Figura 5.28 apresenta os resultados obtidos por meio dessa métrica.

Figura 5.28 - FSD entre os DSNSFs gerados pelo método HWDS e o tráfego observado para o mês de Maio de 2013.



Como evidenciado pelo gráfico, embora os erros apresentados nos testes anteriores sejam superiores aos erros obtidos nos testes do cenário anterior, isso não significa que os DSNSFs gerados são ineficientes: com exceção dos feriados e recesso previamente mencionados, os resultados FSD de todos os dias analisados se encontram dentro do intervalo de -0.67 a 0.67, o que classifica os DSNSFs gerados como bons no ponto de vista da dispersão média de erros. Novamente, nota-se a partir do dia 6 ao dia 13 de Maio um período onde os DSNSFs gerados se encontram superiores ao movimento real observado. A partir do

dia 13, nota-se uma tendência de maior aproximação do valor ótimo (zero) e estabilização dos resultados obtidos.

A Tabela 5.14 apresenta a média, mediana e moda dos resultados obtidos com a utilização métrica FSD relativo à utilização do método de previsão HWDS em cada uma das 7 dimensões separadamente. Nessa tabela, os dados apresentados representam os resultados absolutos da métrica FSD, objetivando uma análise comparativa mais precisa dos resultados obtidos.

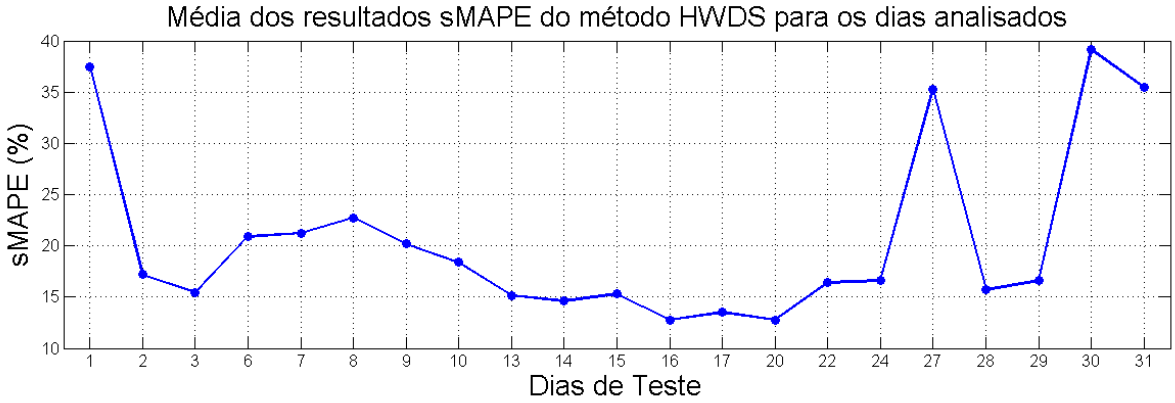
Tabela 5.14 - Resultados de FSD do método HWDS em cada dimensão.

	bits/s	pacotes/s	fluxos/s	IP origem	IP destino	Porta Origem	Porta Destino
Média	0.46	0.44	0.53	0.19	0.22	0.31	0.36
Mediana	0.32	0.27	0.46	0.10	0.21	0.25	0.32
Moda	0.003	0.02	0.01	0.001	0.01	0.05	0.06

Como pode-se observar, novamente as dimensões relativas às medidas de entropia se mostraram mais estáveis, embora todas as dimensões se encontrem dentro do intervalo da métrica FSD que descreve bons resultados. Além disso, a Moda dos resultados de FSD para todas as dimensões é bem próxima de zero, ou seja, os resultados obtidos inferem que os DSNSFs gerados descrevem com eficácia o comportamento de todas as dimensões avaliadas.

Por fim foi aplicado o Erro percentual médio absoluto simétrico (sMAPE), técnica percentual responsável por calcular a distância ou erro entre os DSNSFs gerados e o movimento real observado de forma simétrica. Em outras palavras, mensurando da mesma forma erros positivos e negativos. A Figura 5.29 apresenta os resultados obtidos por meio dessa métrica neste cenário de testes.

Figura 5.29 - sMAPE entre os DSNSFs gerados pelo método HWDS e o tráfego observado para o mês de Maio de 2013.



Como ilustrado, a média dos resultados sMAPE para feriados e recessos é em torno de 35 a 40%. Os demais dias apresentaram erros sMAPE que variam de 15 a 24%. Em comparação com os resultados obtidos no cenário anterior, os erros aqui apresentados são consideravelmente superiores. Novamente, isso ocorre devido ao fato de que redes de pequeno e médio porte sofrem influência direta de usuários individuais em seu padrão comportamental, o que dificulta o processo de caracterização de tráfego. Entretanto, isso não implica que este processo seja falho neste cenário: muito embora os erros tenham sido elevados, os DSNSFs gerados são capazes de eficientemente descrever o padrão comportamental da rede analisada. Além disso, é possível identificar uma tendência de decrescimento do erro do dia 6 (primeira segunda-feira do mês) até o dia 13 (segunda segunda-feira do mês), seguida por um período de estabilidade. Isso pode ser interpretado como um período de aprendizado, de modo que estes erros tendem a estabilizar.

A Tabela 5.15 apresenta a média, mediana e moda dos resultados obtidos com a utilização métrica sMAPE relativo à utilização do método de previsão HWDS em cada uma das 7 dimensões separadamente.

Tabela 5.15 - Resultados de sMAPE do método HWDS em cada dimensão.

	bits/s	pacotes/s	fluxos/s	IP origem	IP destino	Porta Origem	Porta Destino
Média	42.2	35.9	32.7	10.7	11.8	5.4	5.5
Mediana	37.3	29.6	27.6	8.4	9.9	3.7	4.1
Moda	28.2	22.9	13.9	5.5	3.8	1.7	1.7

Conforme apresentado pela tabela, novamente as dimensões bits/s, pacotes/s e fluxos/s apresentaram resultados inferiores às demais, consolidando o fato de que essas dimensões possuem por característica uma maior instabilidade com relação a seus padrões comportamentais. Além disso, dentre as dimensões de entropias de endereços IP e portas de origem e destino, as dimensões relativas às portas se mostraram mais estáveis, o que torna o processo de geração de DSNSFs mais simples e eficiente.

Para ilustrar de forma gráfica os resultados obtidos pelo método HWDS na caracterização de tráfego neste cenário, as Figuras 5.30 a 5.34 mostram o movimento de tráfego real e os DSNSFs gerados por estes métodos para cada uma das 7 dimensões analisadas, relativos aos dias 13 a 17 de Maio de 2013.

Figura 5.30 - Tráfego e DSNSFs gerados relativos ao dia 13 de Maio de 2013.

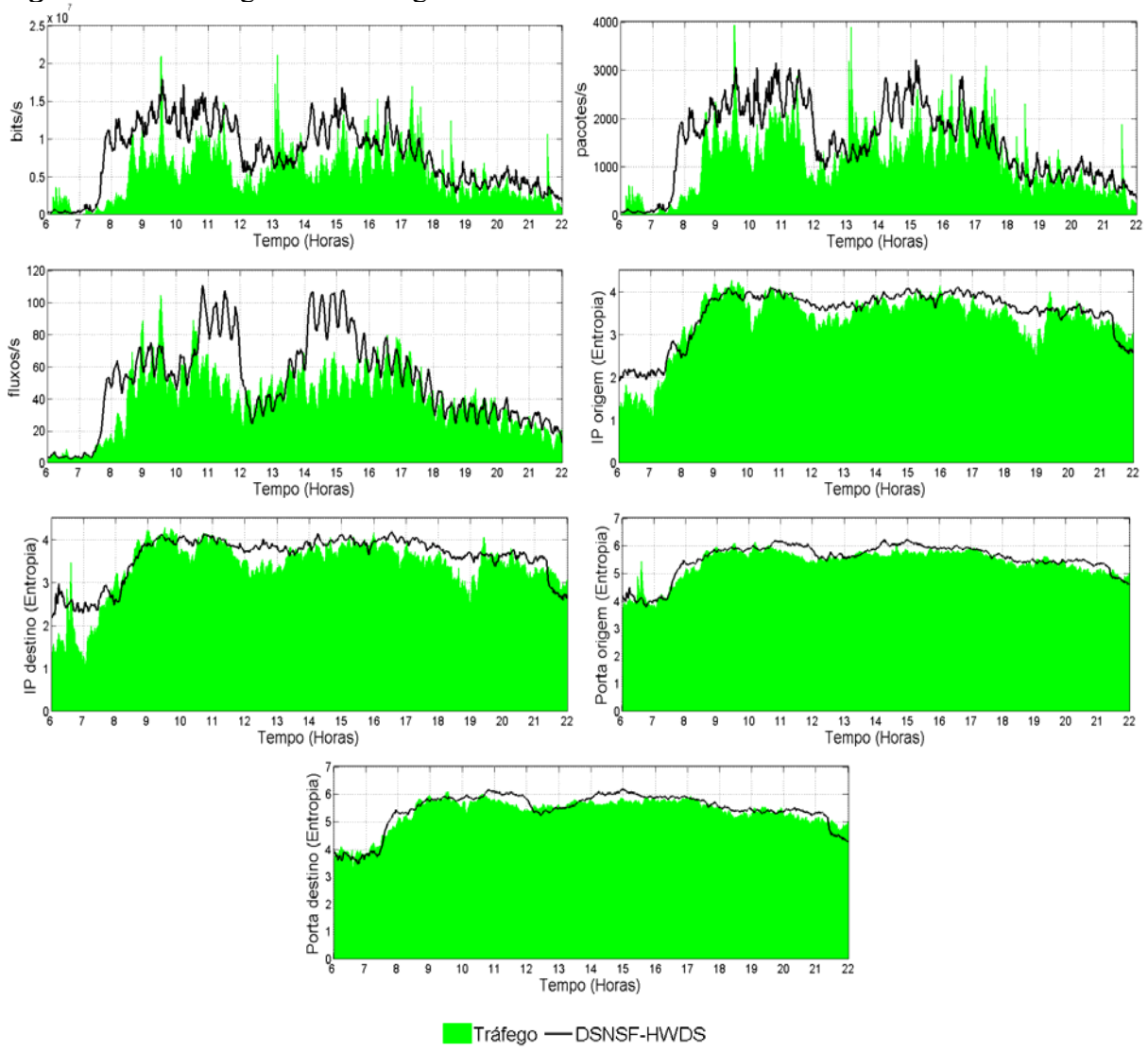


Figura 5.31 - Tráfego e DSNSFs gerados relativos ao dia 14 de Maio de 2013.

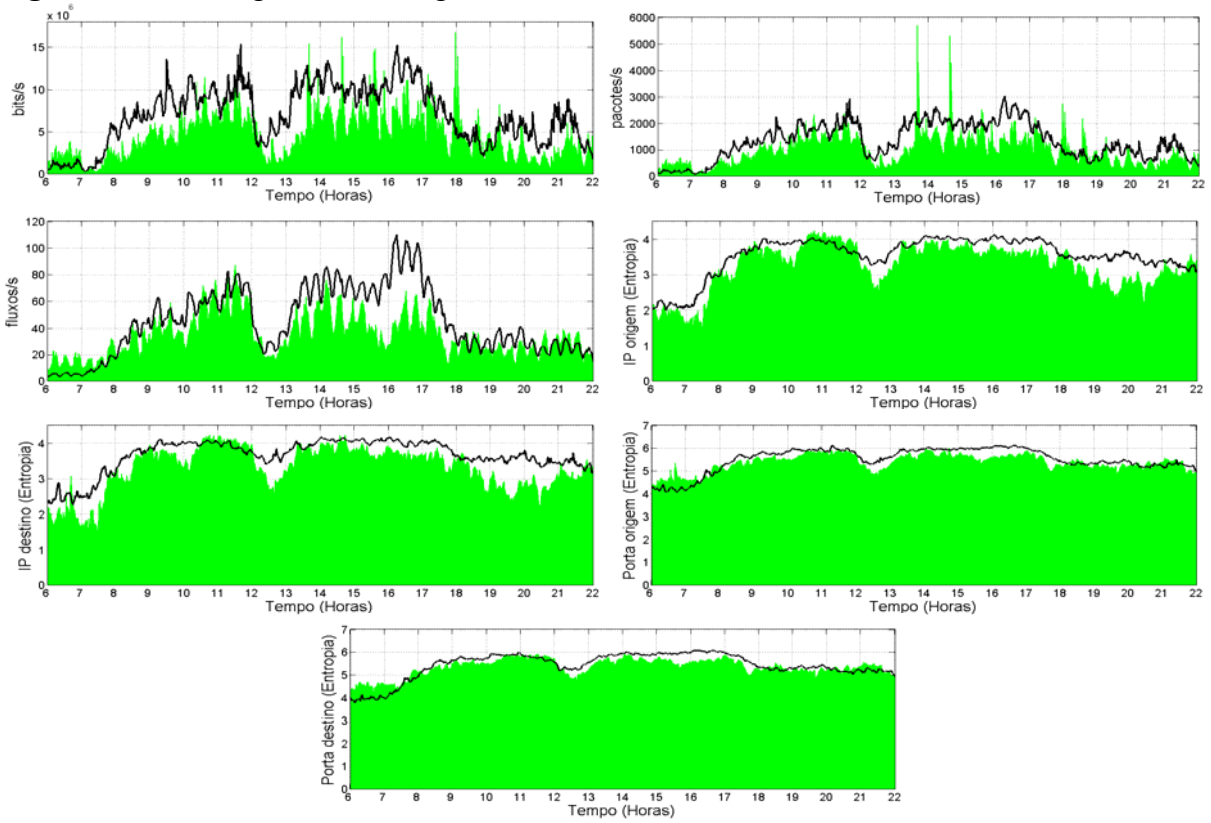


Figura 5.32 - Tráfego e DSNSFs gerados relativos ao dia 15 de Maio de 2013.

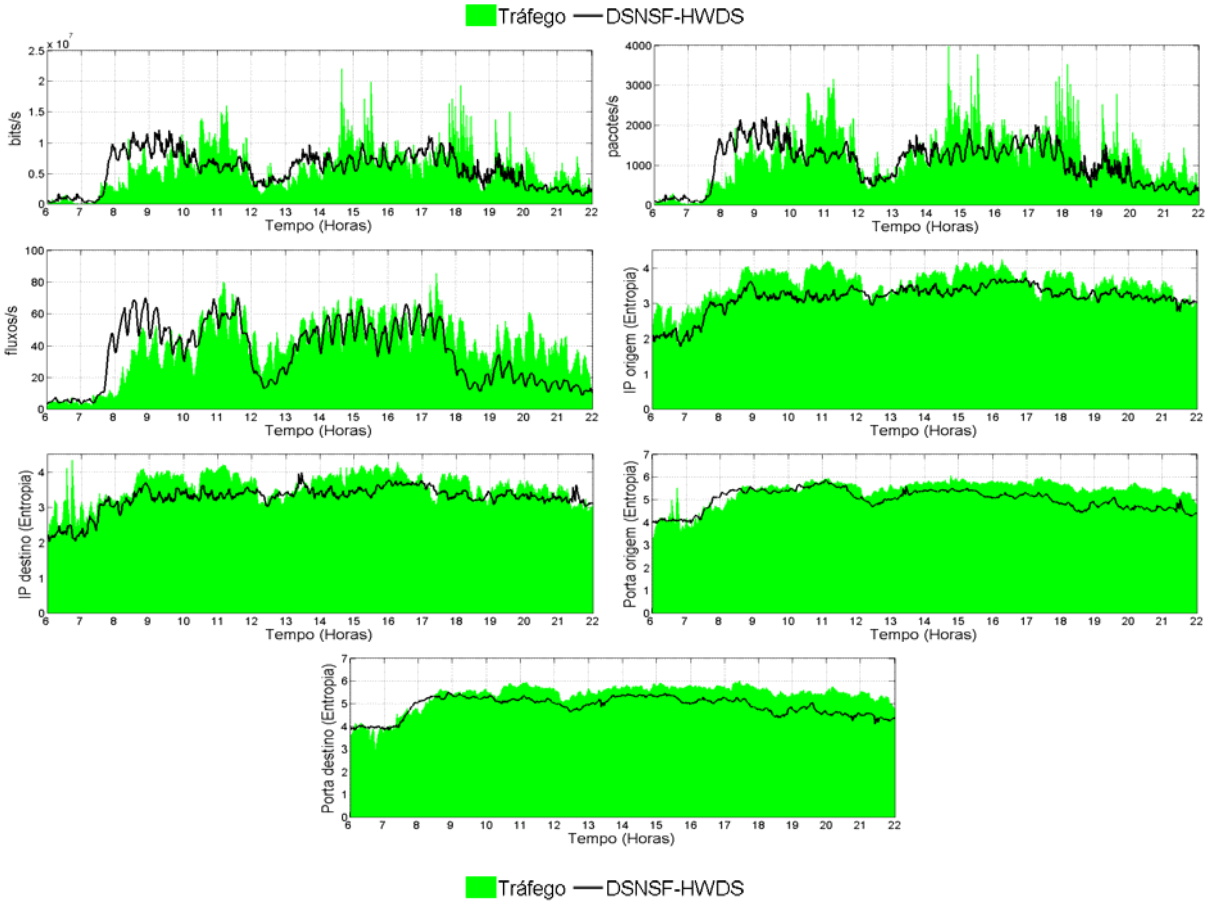


Figura 5.33 - Tráfego e DSNSFs gerados relativos ao dia 16 de Maio de 2013.

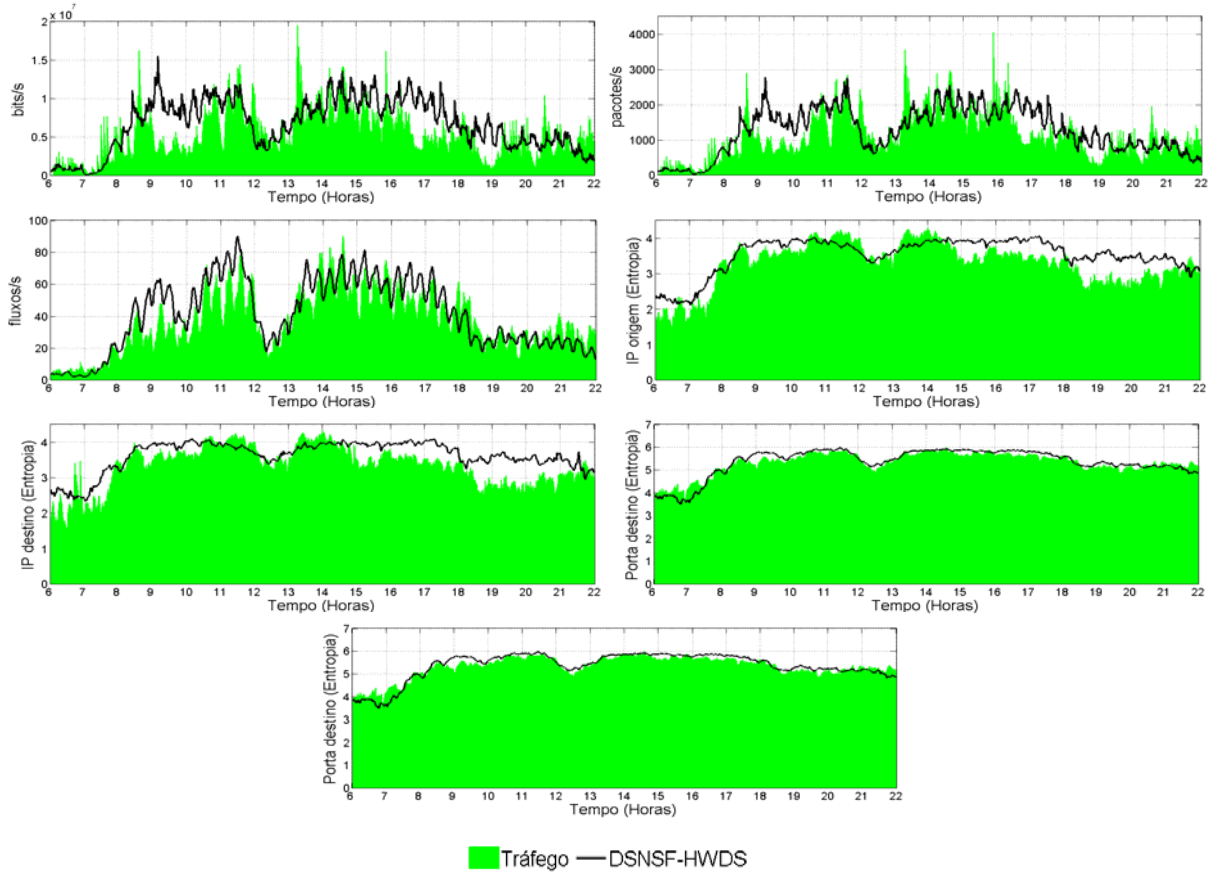
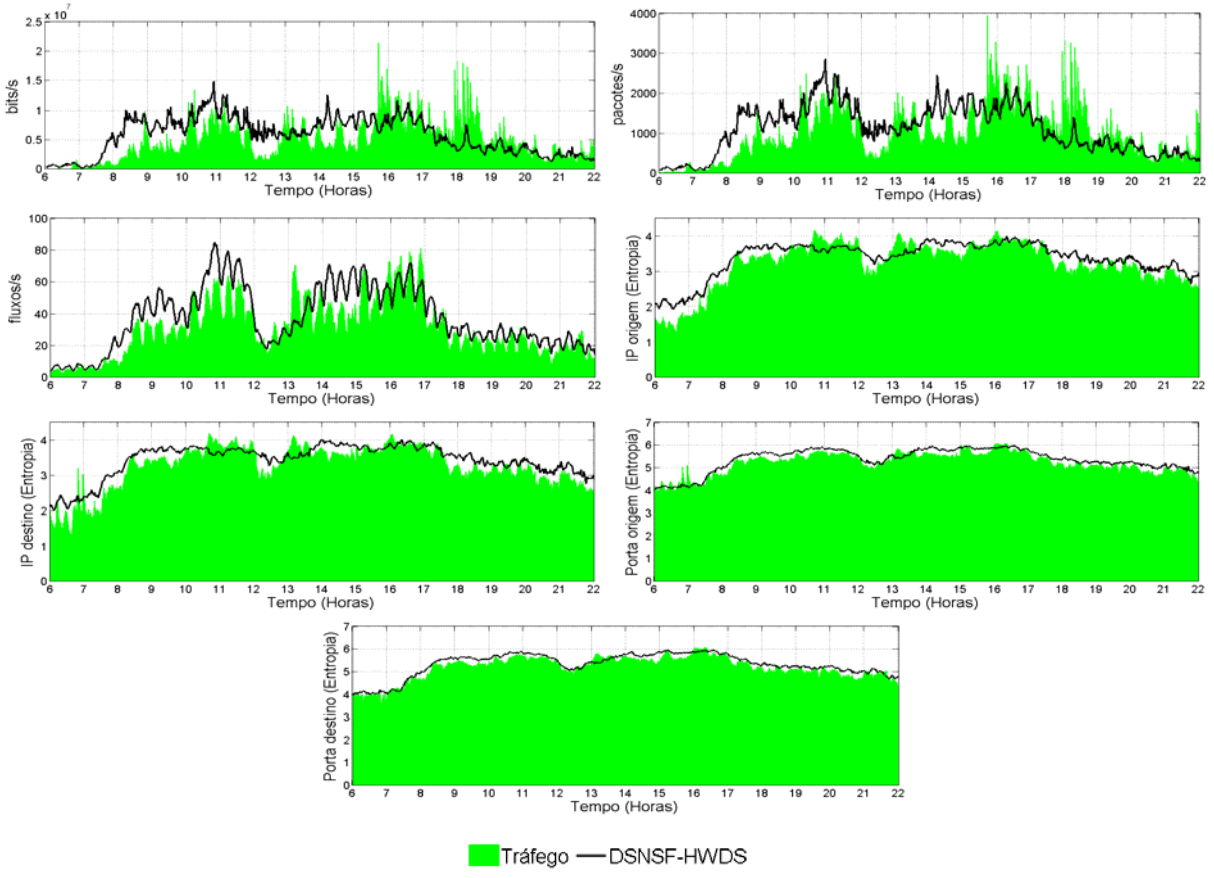


Figura 5.34 - Tráfego e DSNSFs gerados relativos ao dia 17 de Maio de 2013.



Como é possível observar através dos gráficos apresentados, os DSNSFs gerados pelo sistema eficientemente descrevem o movimento de tráfego observado em cada uma das sete dimensões avaliadas. Além disso, pode-se observar que os DSNSFs gerados são capazes de descrever as tendências de crescimento e decrescimento do tráfego avaliado com sucesso, onde há um aumento na utilização dos recursos de rede às 8 da manhã, bem como a diminuição de tal utilização nos períodos de intervalo entre as aulas (10h, 12h e 15h) e finalização do expediente (17h).

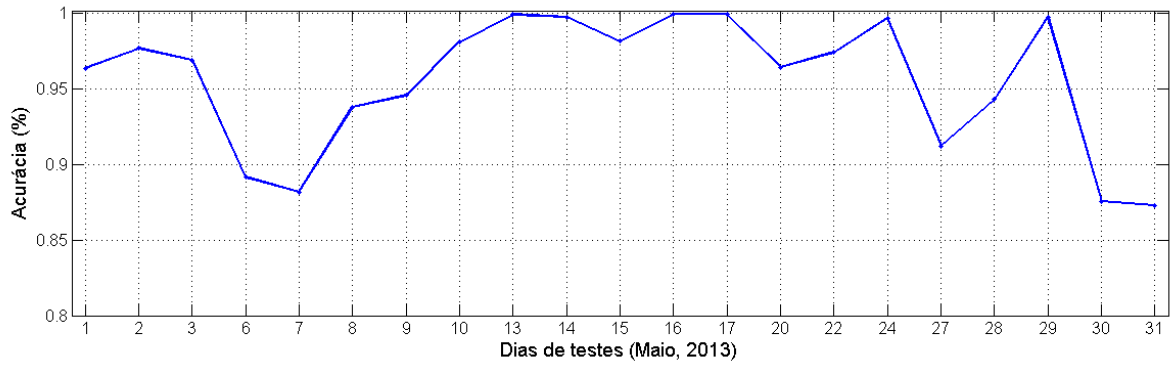
Além disso, conforme os testes de performance realizados já haviam apontado, pode-se notar por meio da análise das Figuras 5.30 a 5.34 que as dimensões de porta de origem e destino são extremamente estáveis, enquanto as dimensões de endereços IP de origem e destino demonstram uma estabilidade mediana e as dimensões de volume (bits/s, pacotes/s e fluxos/s) são mais instáveis. Dessa forma, as dimensões de volume apresentam muitos picos de movimento, o que implica no aumento da dificuldade de realização do processo de caracterização de tráfego. Entretanto, os resultados obtidos pelo sistema ainda são bons, o que demonstra a efetividade da utilização do método HWDS mesmo em ambientes de baixa agregação de tráfego.

Comparando os resultados dos testes de performance dos cenários 1 e 2, nota-se que os resultados obtidos no cenário 2 possuem erros mais elevados. Com isso, pode-se concluir que quanto maior a rede, mais facilmente é executado o processo de caracterização de tráfego. Tendo como base os testes de performance anteriormente apresentados em conjunto com os resultados gráficos ilustrados, pode-se concluir que o sistema apresentado é capaz de descrever os movimentos de tráfego da rede analisada com precisão, apresentando suas tendências de crescimento e decrescimento de forma satisfatória. Com isso, conclui-se que o método HWDS, utilizado pelo sistema apresentado na caracterização de tráfego, é capaz de eficientemente gerar assinaturas digitais (DSNSFs) que descrevam o comportamento normal tanto de redes de pequena/média escala até redes de alta agregação de tráfego (larga escala).

Além da caracterização de tráfego, o sistema apresentado foi aplicado e avaliado no ambiente de testes aqui descrito como uma ferramenta funcional na detecção de anomalias. Este processo utilizou, assim como os testes direcionados à caracterização de tráfego, os dias úteis de Abril e Maio de 2013, sendo que o primeiro mês foi direcionado ao treinamento do sistema e o segundo para os testes de performance. A sinalização dos dados utilizados foi realizada por um grupo de administradores da rede analisada. Tal sinalização foi utilizada como gabarito para os testes de acurácia e eficiência realizados.

Para a realização destes testes, foram utilizadas as técnicas e métricas descritas na seção 5.1.2. A primeira delas é a Acurácia, métrica que mensura o nível de precisão do sistema na classificação de intervalos como normais ou anômalos, evidenciando o nível de efetividade do sistema na classificação de intervalos. A Figura 5.35 evidencia os resultados obtidos pelo sistema por meio dessa métrica.

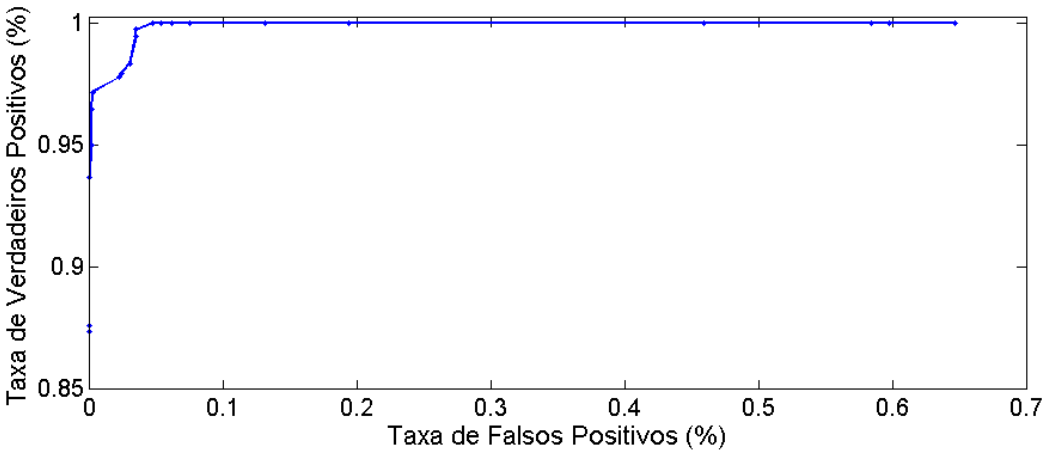
Figura 5.35 - Medidas de Acurácia do sistema para os dias úteis de Maio de 2013.



Como pode-se observar, o sistema obteve altos níveis de acurácia para os dias de teste analisados, no geral acima de 90%. Além disso, até mesmo os feriados mencionados tiveram uma taxa de acurácia relativamente alta em relação aos feriados obtidos no cenário anteriormente analisado. Isso ocorre devido à característica de cada rede, visto que redes de menor porte possuem um comportamento mais definido em feriados que redes de larga escala, onde servidores e serviços continuam funcionando mesmo sem a presença de grande parte de usuários. Os resultados gerais para média, mediana e moda neste cenário de testes foram de 95%, 97% e 99%, respectivamente. Os resultados apontam que, mesmo com as disparidades entre o comportamento dos feriados entre os dois cenários analisados, ambos obtiveram resultados de performance similares com relação à taxa de acurácia.

A segunda técnica utilizada é a Curva ROC, métrica gráfica que confronta as medidas de taxas de Verdadeiros Positivos e Falsos Positivos de modo a ilustrar o *trade-off* atingido pelo sistema na classificação de anomalias. Assim como descrito na seção 5.1.2.2, as Taxas de Verdadeiros Positivos (TVP) apontam a porcentagem de anomalias reais detectadas, enquanto as Taxas de Falsos Positivos (TFP) apontam a porcentagem de intervalos erroneamente classificados como anômalos pelo sistema. Os resultados obtidos pela Curva ROC podem ser observados na Figura 5.36.

Figura 5.36 - Curva ROC do sistema apresentado relativa aos resultados de detecção de anomalias no mês de Maio de 2013.



Conforme descrito anteriormente, quanto mais próxima a linha resultante deste teste se encontra do valor ótimo (taxas de 0% de TFP e 100% de TVP), melhores são os resultados de classificação de anomalias. Como pode-se observar por meio da Figura 5.36, os resultados foram bem próximos do ótimo, onde o sistema atingiu um *trade-off* de 98% de TVP com 5% de TFP, resultado semelhante ao obtido no cenário de testes anterior, que ilustra a acurácia e eficiência do sistema apresentado na detecção de anomalias, inclusive para redes de pequeno e médio porte.

É importante destacar que o sistema não somente detecta anomalias, mas também identifica as possíveis causas de sua ocorrência. Entretanto, para o cenário de testes apresentado nesta seção, apenas Alertas foram identificados, os quais não se enquadram em nenhum comportamento previamente conhecido pelo sistema (Tabela 5.16), representando apenas leves desvios comportamentais gerados por usuários individuais na rede (característica de redes de baixa e média escala).

Tabela 5.16 - Assinaturas de Anomalias/Ataques conhecidos pelo sistema.

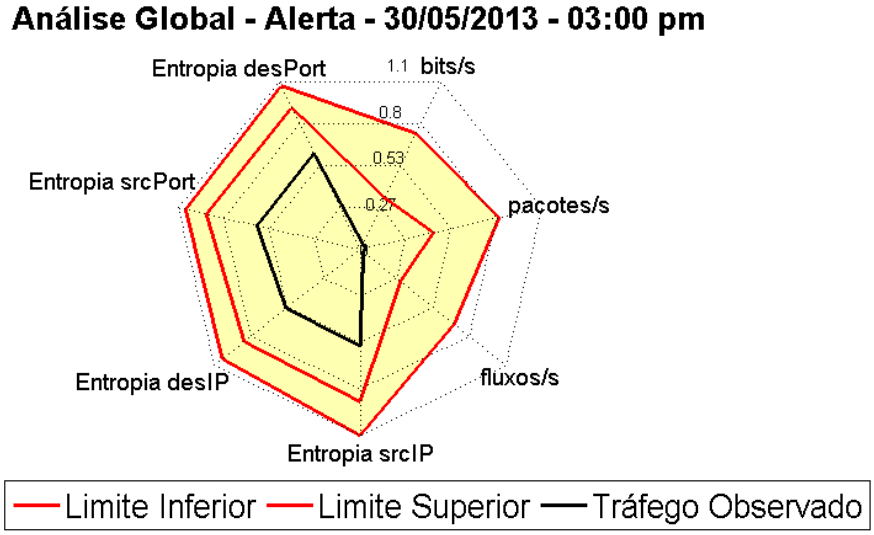
Anomalia	Dimensões de Fluxos IP						
	bits	pacotes	fluxos	IP origem	IP destino	Porta origem	Porta destino
Flash Crowd	++	++	++	N/A	--	+-	--
DoS	N/A	++	++	--	--	--	--
DDoS	N/A	++	++	N/A	--	--	--
Port Scan	N/A	++	++	--	--	--	++

Na Tabela 5.16, o símbolo "++" indica um crescimento no movimento comportamental, "--" representa seu decrescimento, "+-" indica que o comportamento pode ser afetado por um crescimento ou decrescimento comportamental e o símbolo "N/A" aponta que a dimensão não é afetada pela anomalia. Como observado, diferentes anomalias se comportam de maneiras diferentes para as diferentes anomalias conhecidas pelo sistema, o que ilustra a importância de análises multidimensionais utilizada pelo sistema apresentado.

Dessa forma, ao contrário de se ilustrar o comportamento do sistema na detecção e identificação de anomalias já conhecidas (cenário 1), neste cenário será ilustrada a capacidade do sistema de incorporar novas assinaturas comportamentais de anomalias desconhecidas a princípio. Como exemplo serão utilizados registros de fluxos IP relativos ao dia 30 de Maio de 2013, feriado de Corpus Christi. Neste dia, assim como nos demais feriados analisados, o movimento de tráfego difere dos DSNSFs gerados no período das 8h às 18h, horário onde se concentra a maior parte das atividades da Universidade de coleta de dados. Durante todo o período deste intervalo, o sistema gerou Alertas, os quais representam comportamentos anômalos detectados que não se enquadram em nenhuma assinatura de anomalia previamente conhecida.

Entretanto, é de conhecimento do administrador de redes que este dia é um feriado nacional, ou seja, o motivo da anomalia detectada já está identificado sem a necessidade da utilização da classificação dos principais usuários. Entretanto o sistema ainda não conhece essa assinatura, de modo que irão gerar alertas sempre que houver um feriado. Para cadastrar a nova assinatura comportamental no sistema, primeiro o administrador de redes precisa saber qual o comportamento do tráfego analisado em cada uma das sete dimensões do sistema. Para isso utiliza-se a visão global, gráfico de radar do Módulo de Informação que apresenta o comportamento simultâneo dessas dimensões num determinado intervalo de tempo. Para este exemplo, foi utilizado o intervalo de tempo relativo às 15h do dia avaliado, e seu resultado pode ser observado na Figura 5.37.

Figura 5.37 - Visão hepta-dimensional de um Alerta detectado relativo a um feriado.



Como é possível observar, o tráfego de um feriado é caracterizado pelo decréscimo do movimento comportamental de tráfego em todas as dimensões. As dimensões de volume diminuem devido ao fato de que há uma diminuição na utilização dos recursos de rede por usuários. Já no caso das dimensões de entropia, uma diminuição dos resultados aponta uma maior concentração de mesmos endereços IP e portas ativos. Dessa forma, com menos *hosts* ou máquinas ligados na Universidade, menos endereços IP e portas diferentes são utilizados, ocasionando em resultados de entropia menores que os limites ou intervalos de confiança calculados pelo sistema. Dessa forma, pode-se concluir que essa é a assinatura comportamental da anomalia do tipo "Feriado", de modo que o administrador de redes pode atualizar o sistema com essas informações. A Tabela 5.17 apresenta as assinaturas de anomalias e ataques conhecidos pelo sistema, já atualizada após essa análise.

Tabela 5.17 - Assinaturas atualizadas de Anomalias/Ataques conhecidos pelo sistema.

Anomalia	Dimensões de Fluxos IP						
	bits	pacotes	fluxos	IP origem	IP destino	Porta origem	Porta destino
Flash Crowd	++	++	++	N/A	--	+-	--
DoS	N/A	++	++	--	--	--	--
DDoS	N/A	++	++	N/A	--	--	--
Port Scan	N/A	++	++	--	--	--	++
Feriado	--	--	--	--	--	--	--

Dessa forma pode-se concluir que, para o cenário de testes avaliado correspondente a uma rede de baixa a média escala, o sistema apresentado se mostrou eficiente não somente no processo de caracterização de tráfego, mas também na detecção de anomalias. Além disso, a sua flexibilidade quanto à inserção de novas assinaturas de anomalias/ataques demonstrada neste cenário de testes comprova a capacidade do sistema apresentado de constantemente melhorar seus resultados de acordo com as características específicas de cada ambiente de redes no qual é aplicado.

6 CONCLUSÃO

Neste trabalho, foi feita a apresentação de um sistema de detecção de anomalias baseado na análise hepta-dimensional de fluxos IP, onde foram utilizados os atributos de fluxo: bits/s, pacotes/s, fluxos/s, IP de origem e destino e portas de origem e destino. A base deste sistema é composta por um mecanismo de caracterização de tráfego responsável pela criação de perfis ou assinaturas que descrevam o comportamento normal da rede analisada em cada uma dessas dimensões, perfil aqui denominado *Digital Signature of Network Segment using Flow analysis* (DSNSF). Para executar essa tarefa, foram analisados dois métodos estatísticos de previsão de séries temporais: o Holt-Winters e o Holt-Winters *for Digital Signature* (HWDS), versão aperfeiçoada do método tradicional voltada à geração de DSNSFs.

Um diferencial da abordagem apresentada, além da utilização de sete dimensões de fluxos, é a utilização de janelas temporais de análise de 1 minuto, ao contrário da abordagem de janelas de 5 minutos comumente utilizada por diferentes ferramentas e modelos presentes na literatura. Essa abordagem, além de tornar os processos de análise mais ágeis e eficientes em redes de larga escala, aumenta a granularidade dos dados de tráfego, os quais passam a apresentar uma grande quantidade de picos abruptos nos movimentos que descrevem seu tráfego. Por esse motivo é utilizada a técnica de Suavização Exponencial na redução da granularidade dos dados analisados, o que possibilita que o processo de caracterização de tráfego seja executado com mais eficiência e precisão. Foram realizados testes sobre o impacto causado pela aplicação dessa técnica, e os resultados obtidos comprovam que seu emprego eficientemente reduz a granularidade dos dados analisados, o que torna os movimentos que descrevem o tráfego mais suaves e, consequentemente, torna o processo de caracterização de tráfego mais preciso. Além disso, foi constatado que a utilização dessa técnica não descaracteriza o comportamento da rede analisada, mantendo as tendências de crescimento e decrescimento do tráfego.

Foram propostos dois diferentes cenários de testes para a verificação de performance do sistema proposto. O primeiro deles utiliza registros de fluxos IP coletados em uma rede de larga escala da Universidade Estadual de Londrina por meio do protocolo de exportação sFlow, e com taxa de amostragem de 1:256 devido ao volume de dados. Neste cenário foram avaliados os resultados obtidos na utilização dos métodos Holt-Winters e HWDS no processo de caracterização de tráfego. Os resultados obtidos comprovam que o método HWDS possui um considerável ganho de performance com relação ao método

tradicional Holt-Winters, tendo seus resultados sempre superiores ou, no pior caso, iguais ao método tradicional. Além disso, foram realizados testes de acurácia e eficiência quanto ao processo de detecção de anomalias por meio da utilização de dados reais coletados e simulados por meio da ferramenta Scorpius. Em ambos os tipos de testes, o sistema atingiu bons resultados, com taxas de acurácia acima de 90% e taxas de alarmes Verdadeiros Positivos e Falsos Positivos de 95% e 5%, respectivamente, comprovando sua eficiência. O sistema também foi capaz de identificar os *hosts* e aplicações de origem e destino de todos os ataques simulados, além de identificar a possível causa de uma anomalia real que ocorreu durante o período utilizado para testes de performance.

O segundo cenário de testes analisa registros de fluxos IP coletados em uma rede de pequena a média escala por meio do protocolo de exportação Netflow *version* 9, sem quaisquer recursos de amostragem. Neste cenário o processo de caracterização de tráfego por meio do método HWDS foi avaliado. Os resultados obtidos foram inferiores aos do primeiro cenário de testes devido à diferença de magnitude entre as redes, visto que redes menores tendem a sofrer influência direta de usuários individuais em seus padrões comportamentais. Embora estes resultados tenham sido inferiores, as assinaturas digitais geradas foram capazes de descrever com sucesso o comportamento normal da rede, comprovando a eficiência do sistema na caracterização de tráfego. Neste cenário também foi testado o processo de detecção de anomalias, no qual o sistema apresentado obteve resultados gerais similares aos obtidos no cenário anterior, com taxas de acurácia superiores a 90% e taxas de alarmes Verdadeiros Positivos e Falsos Positivos de 95% e 5%, respectivamente. Por fim, a flexibilidade do sistema apresentado foi ilustrada neste cenário, onde uma nova assinatura comportamental de anomalia foi detectada e adicionada ao sistema, demonstrando sua capacidade de constante melhora de resultados conforme as características específicas de cada rede.

Além disso, a complexidade computacional do sistema proposto foi avaliada, sendo possível constatar que a maior parte dos métodos utilizados no sistema apresentado possui complexidade linear, com exceção do cálculo da Entropia de Shannon utilizado na transformação das dimensões qualitativas de fluxos, endereços IP e portas de origem e destino, em dimensões quantitativas (a qual é quadrática), possibilitando a geração de assinaturas digitais para esses atributos. Dessa forma, a complexidade assintótica do sistema é considerada como quadrática. Entretanto, essa é uma complexidade considerada baixa com relação à quantidade de dados analisados e informações providas pelo sistema. Com relação ao desempenho de execução do sistema, no cenário 1, Universidade Estadual de Londrina, foi constatado que ele é capaz de calcular e convergir resultados relativos a 2 meses

em menos de cinco minutos, a análise hepta-dimensional de dias individuais é executada em cerca de 30 segundos. No cenário 2, Universidade Tecnológica Federal do Paraná – Campus Toledo, o tempo de cálculo e convergência para dados relativos a dois meses é executado em menos de dez minutos, com análise hepta-dimensional de dias individuais executada em cerca de 1 minuto, o que comprova a agilidade de execução do sistema apresentado.

Dessa forma, conclui-se que, devido a sua eficiência e acurácia nos processos de detecção e identificação de anomalias, bem como flexibilidade e adaptação a diferentes ambientes, o sistema apresentado representa uma inovadora e poderosa abordagem capaz de auxiliar nos processos de gerenciamento de redes tanto de baixa/média escala quanto de larga escala, garantindo a disponibilidade e a qualidade dos serviços por elas prestados.

Dentre os trabalhos futuros pode-se destacar a avaliação de performance do sistema a diferentes cenários de testes de modo a melhorar e eficiência do sistema apresentado para diferentes serviços e aplicações, bem como a análise da viabilidade da utilização de dimensões de fluxo adicionais no sistema. Além disso, pretende-se comparar o modelo de detecção apresentado com diferentes abordagens determinísticas e não determinísticas presentes na literatura, tais como *Ant Colony Optimization* (ACO), *Autoregressive Integrated Moving Average* (ARIMA) e *Principal Component Analysis* (PCA).

REFERÊNCIAS

[1] JENNINGS, B. *et al.* Towards autonomic management of communications networks. **Communications Magazine, IEEE,** v. 45, n. 10, p. 112-121, 2007. ISSN 0163-6804.

[2] MINSOO, L. *et al.* **Autonomous Network Management Using Cooperative Learning for Network-Wide Load Balancing in Heterogeneous Networks**. Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. Nov. 30 2008-Dec. 4 2008, 2008. 1-5 p.

[3] PRIETO, A. G.; STADLER, R. **Adaptive real-time monitoring for large-scale networked systems**. Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on. 1-5 June 2009, 2009. 790-795 p.

[4] TSAGKARIS, K. *et al.* **Identifying standardization opportunities of an operator-driven, framework for unifying autonomic network and service management**. Communications (ICC), 2012 IEEE International Conference on. 10-15 June 2012, 2012. 6921-6925 p.

[5] WANG, Z.; WANG, X. **NetFlow Based Intrusion Detection System**. MultiMedia and Information Technology, 2008. MMIT '08. International Conference on. 30-31 Dec. 2008, 2008. 825-828 p.

[6] XIN, H.; GANAPATHY, S.; WOLF, T. **A Framework for Network State Management in the Next-Generation Internet Architecture**. Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. Nov. 30 2008-Dec. 4 2008, 2008. 1-5 p.

[7] XIONG, N. *et al.* A novel self-tuning feedback controller for active queue management supporting TCP flows. **Information Sciences,** v. 180, n. 11, p. 2249-2263, 6/1/ 2010. ISSN 0020-0255. Disponível em: < http://www.sciencedirect.com/science/article/pii/S0020025509005258 >.

[8] MILLER, M. **Managing internetworks with SNMP: the definitive guide to the simple network management protocol, SNMP2v2, RMON, and RMON2**. M&T Books, 1997. ISBN 9781558515611. Disponível em: < http://books.google.com.br/books?id=c2yBkQEACAAJ >.

[9] NFDUMP. Netflow processing tools. http://nfdump.sourceforge.net/, 2013. Acesso em: 03/11/2013.

[10] IETF. IP Flow Information Export (IPFIX) - RFCs. IETF Data Tracker, Disponível em: < http://datatracker.ietf.org/wg/ipfix/ >. Acesso em: 09/09/2013.

[11] PHAAL, P.; LAVINE, M. SFlow version 5. 2004. Disponível em: < http://www.sflow.org/sflow_version_5.txt >. Acesso em: 09/09/2013.

[12] TRAMMELL, B.; BOSCHI, E. An introduction to IP flow information export (IPFIX). **Communications Magazine, IEEE,** v. 49, n. 4, p. 89-95, 2011. ISSN 0163-6804.

[13] ANG, L.; LIN, G.; KUAI, X. **Fast Anomaly Detection for Large Data Centers**. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. 6-10 Dec. 2010, 2010. 1-6 p.

[14] KANDA, Y.; FUKUDA, K.; SUGAWARA, T. **A Flow Analysis for Mining Traffic Anomalies**. Communications (ICC), 2010 IEEE International Conference on. 23-27 May 2010, 2010. 1-5 p.

[15] MOLNAR, S.; MOCZAR, Z. **Three-Dimensional Characterization of Internet Flows**. Communications (ICC), 2011 IEEE International Conference on. 5-9 June 2011, 2011. 1-6 p.

[16] CORTEZ, P.; RIO, M.; ROCHA, M.; SOUSA, P. **Internet Traffic Forecasting using Neural Networks**. Neural Networks, 2006. IJCNN '06. International Joint Conference on. 0-0 0, 2006. 2635-2642 p.

[17] LAKHINA, A. *et al.* Structural analysis of network traffic flows. **SIGMETRICS Perform. Eval. Rev.,** v. 32, n. 1, p. 61-72, 2004. ISSN 0163-5999.

[18] YOOHEE, C.; YIHAN, K. **Case study of an anomalous traffic detection on the aggregation points of enterprise network**. Advanced Communication Technology (ICACT), 2011 13th International Conference on. 13-16 Feb. 2011, 2011. 1245-1248 p.

[19] SHANNON, C. E. A mathematical theory of communication. **SIGMOBILE Mob. Comput. Commun. Rev.,** v. 5, n. 1, p. 3-55, 2001. ISSN 1559-1662.

[20] BROWN, R. G. **Exponential Smoothing for Predicting Demand**. Little, 1956. Disponível em: < http://books.google.com.br/books?id=Eo_rMgEACAAJ >.

[21] PARK, N. H.; OH, S. H.; LEE, W. S. Anomaly intrusion detection by clustering transactional audit streams in a host computer. **Information Sciences,** v. 180, n. 12, p. 2375-2389, 6/15/ 2010. ISSN 0020-0255. Disponível em: < http://www.sciencedirect.com/science/article/pii/S0020025510001131 >.

[22] WINTERS, P. R. Forecasting Sales by Exponentially Weighted Moving Averages. **Management Science,** v. 6, n. 3, p. 324-342, 1960. Disponível em: < http://EconPapers.repec.org/RePEc:inm:ormnsc:v:6:y:1960:i:3:p:324-342 >.

[23] KASHIHARA, S.; TSURUSAWA, M. **Dynamic Bandwidth Management System Using IP Flow Analysis for the QoS-Assured Network**. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. 6-10 Dec. 2010, 2010. 1-5 p.

[24] CHEN, T. Y.; HU, P.; LI, H.; TSE, T. H. An enhanced flow analysis technique for detecting unreachability faults in concurrent systems. **Information Sciences,** v. 194, n. 0, p. 254-269, 7/1/ 2012. ISSN 0020-0255. Disponível em: < http://www.sciencedirect.com/science/article/pii/S0020025511006190 >.

[25] TAO, Q.; XIAOHONG, G.; WEI, L.; PINGHUI, W. **Monitoring Abnormal Traffic Flows Based on Independent Component Analysis**. Communications, 2009. ICC '09. IEEE International Conference on. 14-18 June 2009, 2009. 1-5 p.

[26] DEWAELE, G. *et al.* **Extracting hidden anomalies using sketch and non Gaussian multiresolution statistical detection procedures**. Proceedings of the 2007 workshop on Large scale attack defense. Kyoto, Japan: ACM**:** 145-152 p. 2007.

[27] SHON, T.; MOON, J. A hybrid machine learning approach to network anomaly detection. **Information Sciences,** v. 177, n. 18, p. 3799-3821, 9/15/ 2007. ISSN 0020-0255. Disponível em: < http://www.sciencedirect.com/science/article/pii/S0020025507001648 >.

[28] SIRIS, V. A.; PAPAGALOU, F. **Application of anomaly detection algorithms for detecting SYN flooding attacks**. Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE. 29 Nov.-3 Dec. 2004, 2004. 2050-2054 Vol.4 p.

[29] TCHOLTCHEV, N.; CAVALCANTE, A. B.; CHAPARADZA, R. **Scalable Markov Chain Based Algorithm for Fault-Isolation in Autonomic Networks**. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. 6-10 Dec. 2010, 2010. 1-6 p.

[30] SONG, J.; TAKAKURA, H.; OKABE, Y.; NAKAO, K. Toward a more practical unsupervised anomaly detection system. **Information Sciences,** v. 231, n. 0, p. 4-14, 5/10/ 2013. ISSN 0020-0255. Disponível em: < http://www.sciencedirect.com/science/article/pii/S0020025511004245 >.

[31] BRUTLAG, J. D. **Aberrant Behavior Detection in Time Series for Network Monitoring**. Proceedings of the 14th USENIX conference on System administration. New Orleans, Louisiana: USENIX Association**:** 139-146 p. 2000.

[32] LES COTTRELL, R. *et al.* **Evaluation of Techniques to Detect Significant Network Performance Problems using End-to-End Active Network Measurements**. Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP. 3-7 April 2006, 2006. 85-94 p.

[33] SHUYING, C. *et al.* **A flow-based anomaly detection method using entropy and multiple traffic features**. Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on. 26-28 Oct. 2010, 2010. 223-227 p.

[34] TIKUNOV, D.; NISHIMURA, T. **Traffic prediction for mobile network using Holt-Winter's exponential smoothing**. Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007. 15th International Conference on. 27-29 Sept. 2007, 2007. 1-5 p.

[35] PROENCA, M. L.; ZARPELAO, B. B.; MENDES, L. S. **Anomaly detection for network servers using digital signature of network segment**. Telecommunications, 2005. advanced industrial conference on telecommunications/service assurance with partial and intermittent resources conference/e-learning on telecommunications workshop. aict/sapir/elete 2005. proceedings. 17-20 July 2005, 2005. 290-295 p.

[36] ADANIYA, M. H. A. C. *et al.* **Anomaly detection using DSNS and Firefly Harmonic Clustering Algorithm**. Communications (ICC), 2012 IEEE International Conference on. 10-15 June 2012, 2012. 1183-1187 p.

[37] ZACARON, A. M. *et al.* **Digital Signature of Network Segment using Flow Analysis**. DCNET/ICE-B/OPTICS. OBAIDAT, M. S.;SEVILLANO, J. L.*, et al*: SciTePress**:** 35-40 p. 2012.

[38] GROUP, T. C. Cacti: the complete rrdtool-based graphing solution. http://www.cacti.net, 2004. Acesso em: 16/08/2013.

[39] NTOP. NTop: Network Monitoring Solutions. http://www.ntop.org, 1998. Acesso em: 16/08/2013.

[40] NFSEN. NetFlow visualisation and investigation tool. http://nfsen.sourceforge.net, 2005. Acesso em: 16/08/2013.

[41] CASE, J.; FEDOR, M.; SCHOFFSTALL, M.; DAVIN, J. **Simple Network Management Protocol (SNMP)**. RFC 1157: Working Group, Internet Engineering Task Force, 1990. Disponível em: < http://www.ietf.org/rfc/rfc1157.txt >.

[42] LTDA, N. D. B. Ataques de pishing crescem 60% e causam prejuízo de US$ 1,5 bilhão em 2012. IDGNOW! , 2013. Disponível em: < http://idgnow.uol.com.br/internet/2013/01/30/ataques-de-phishing-crescem-60-e-causam-prejuizo-de-us-1-5-bilhao-em-2012/ >. Acesso em: 09/09/2013.

[43] DERI, L. NTop - Flow Based Monitoring. Disponível em: < http://www.ntop.org/solutions/flow-based-monitoring/ >. Acesso em: 09/09/2013.

[44] BRUINS, B. L.; KERR, D. R. **Network flow switching and flow data export**. US Patent Number US 6243667 2001.

[45] LI, B.; SPRINGER, J.; BEBIS, G.; HADI GUNES, M. A survey of network flow applications. **Journal of Network and Computer Applications,** v. 36, n. 2, p. 567-581, 3// 2013. ISSN 1084-8045. Disponível em: < http://www.sciencedirect.com/science/article/pii/S1084804512002676 >.

[46] PHAAL, P.; PANCHEN, S.; MCKEE, N. InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. RFC 3176, 2001. Disponível em: < http://www.ietf.org/rfc/rfc3176.txt >. Acesso em: 09/09/2013.

[47] QUITTEK, J.; ZSEBY, T.; CLAISE, B.; ZANDER, S. Requirements for IP Flow Information Export (IPFIX). RFC 3917, 2004. Disponível em: < http://www.ietf.org/rfc/rfc3917.txt >. Acesso em: 09/09/2013.

[48] PAESSLER. Comparison of SNMP, Packet Sniffing, and NetFlow. Disponível em: < http://www.paessler.com/manuals/prtg_traffic_grapher/comparisonofsnmppacketsniffingandnetflow1 >. Acesso em: 09/09/2013.

[49] GOODWIN, P. The Holt-Winters Approach to Exponential Smoothing: 50 Years Old and Going Strong. **Foresight: The International Journal of Applied Forecasting**, n. 19, p. 30-33, 2010.

[50] POLI, A. A.; CIRILLO, M. C. On the use of the normalized mean square error in evaluating dispersion model performance. **Atmospheric Environment. Part A. General Topics,** v. 27, n. 15, p. 2427-2434, 10// 1993. ISSN 0960-1686. Disponível em: < http://www.sciencedirect.com/science/article/pii/096016869390410Z >.

[51] EPA. **Protocol for Determining the Best Performing Model**. U.S. Environmental Protection Agency, 1992. Disponível em: < http://books.google.com.br/books?id=xxXxygAACAAJ >.

[52] FLORES, B. E. A pragmatic view of accuracy measurement in forecasting. **Omega,** v. 14, n. 2, p. 93-98, // 1986. ISSN 0305-0483. Disponível em: < http://www.sciencedirect.com/science/article/pii/0305048386900137 >.

[53] FAWCETT, T. An introduction to ROC analysis. **Pattern Recogn. Lett.,** v. 27, n. 8, p. 861-874, 2006. ISSN 0167-8655.

[54] BARFORD, P.; KLINE, J.; PLONKA, D.; RON, A. **A signal analysis of network traffic anomalies**. Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment. Marseille, France: ACM**:** 71-82 p. 2002.

[55] (COPS), C. D. P. S. Concurso Público Polícia Civil do Paraná. Coordenadoria de Processos Seletivos, Disponível em: < http://www.cops.uel.br/concursos/92_policia_civil/ >. Acesso em: 27/01/2014.

[56] ASSIS, M. V. O. Scorpius - sFlow Anomaly Simulator. http://redes.dc.uel.br/scorpius/, 2013. Acesso em: 31/03/2014.

APÊNDICES

APÊNDICE A

Scorpius - sFlow *Anomaly Simulator*

Uma das principais dificuldades no desenvolvimento de novas técnicas, modelos e sistemas de detecção de anomalias em redes de computadores é o teste. Essas ferramentas devem ser testadas nos mais variados tipos de ambientes, de modo a validar sua eficiência de forma mais completa possível. Dentre as possibilidades de testes existentes, se encontram:

• Redes Simuladas: Ambiente de testes completamente controlado, onde se pode configurar todas as variáveis da rede de modo a reproduzir o comportamento desejado. Embora este método seja extremamente completo, a complexidade de montagem de uma rede simulada é relativamente alta;

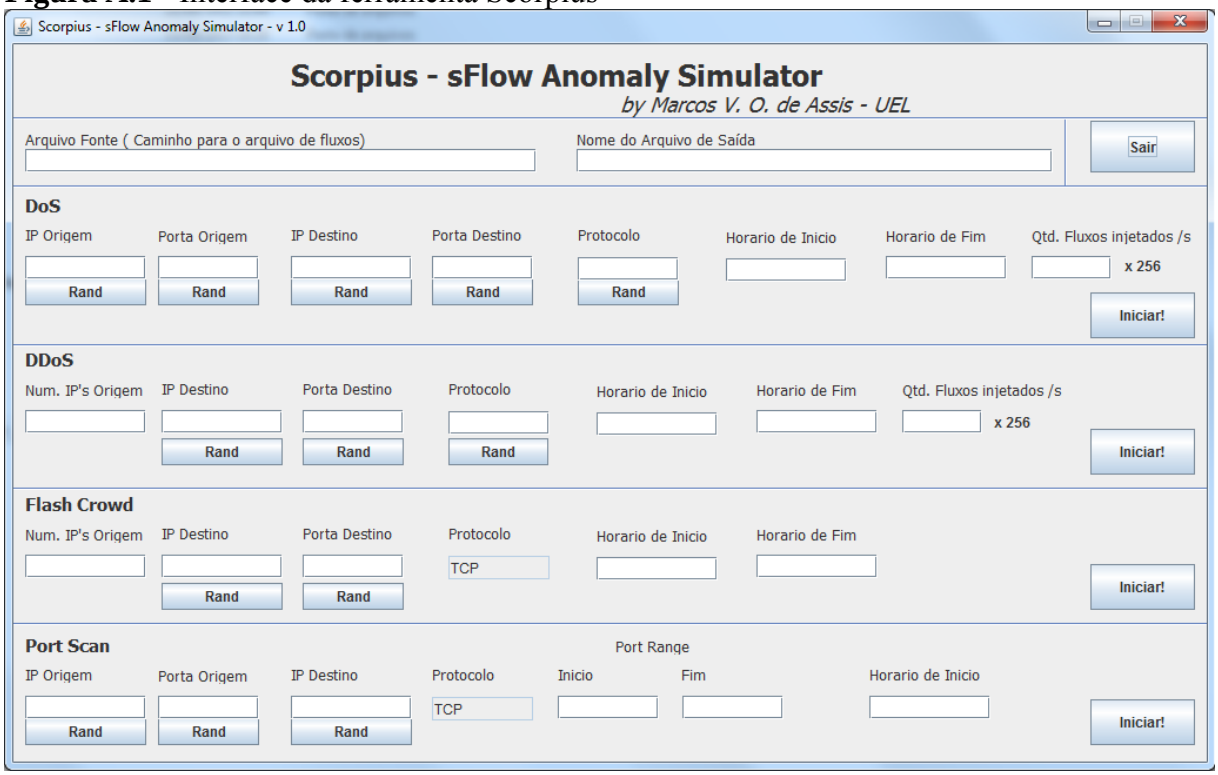
• Redes Reais: Ambiente de testes onde são utilizados dados reais coletados de redes em funcionamento (ambiente de produção), onde pode-se avaliar a efetividade da ferramenta testada num ambiente onde a mesma destina-se a ser aplicada. Os testes em redes reais são extremamente importantes para a validação de sistemas de detecção de anomalias, visto que ilustram exatamente cenários sob os quais esses sistemas atuam. Sua maior vantagem também acaba sendo uma desvantagem, pois o nível de completude dos testes está diretamente relacionado com a diversidade de anomalias que ocorrem na rede. Dessa forma, se a rede utilizada apresenta apenas anomalias do tipo *Flash Crowd*, o sistema não será testado quanto à outros tipos de anomalias, tais como DoS, DDoS ou *Port Scan*;

• Ambientes Controlados: Ambiente de testes onde diferentes anomalias são direcionadas à uma rede de computadores específica de forma intencional. Nestes tipos de ambientes, normalmente são selecionados horários específicos de modo a não prejudicar o funcionamento normal da rede. Embora seja menos complexo que a criação de redes simuladas, estes ataques, mesmo que controlados, podem prejudicar o funcionamento normal da rede, principalmente em redes de grande porte (larga escala) as quais são utilizadas 24 horas por dia.

Visando facilitar o processo de validação de performance do sistema de detecção de anomalias apresentado, foi desenvolvida uma ferramenta de simulação de ataques em fluxos IP que une as principais vantagens das diferentes abordagens citadas. Essa ferramenta é denominada Scorpius - sFlow Anomaly Simulator [56], e simplifica significativamente o processo de análise e validação de performance de sistemas de detecção

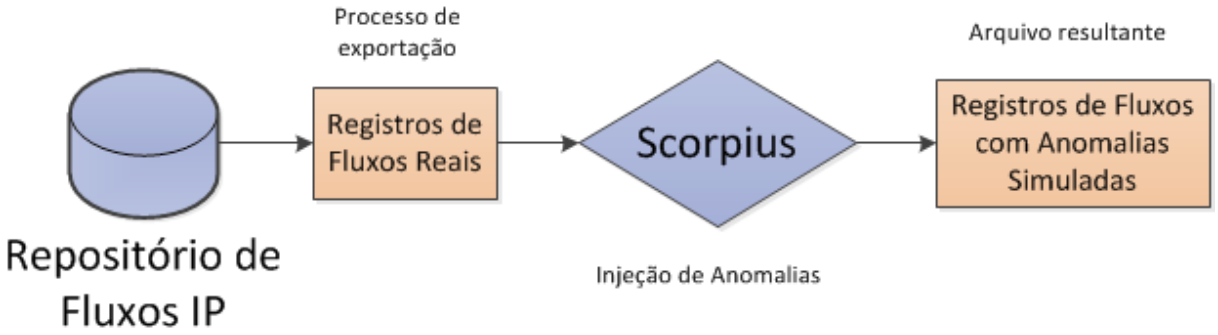
de anomalias baseados na análise de fluxos IP. A Figura A.1 apresenta a ferramenta Scorpius em sua versão de número 1.

Figura A.1 - Interface da ferramenta Scorpius



Trata-se de um aplicativo desenvolvido utilizando a linguagem de programação JAVA, desenvolvido utilizando-se o ambiente de produção Eclipse versão Helios. A ferramenta Scorpius une o controle do ambiente de Redes Simuladas, a riqueza de informação de Redes reais e a diversidade de ataques de Ambientes Controlados com a segurança de uma simulação rápida e simplificada. Seu funcionamento pode ser avaliado com base na análise do diagrama apresentado pela Figura A.2:

Figura A.2 - Diagrama da aplicação da ferramenta Scorpius



Como se pode verificar, a Scorpius utiliza um arquivo de fluxos reais como entrada, injeta fluxos anômalos com a característica requerida (anomalias suportadas são *DoS*, *DDoS*, *Flash Crowd* e *Port Scan*) no intervalo de tempo solicitado, gerando um novo arquivo de fluxos IP como saída já com tais anomalias incorporadas. Este arquivo pode ser utilizado para testes de forma idêntica ao ambiente de Redes Reais, uma vez que seus dados são de fato reais com exceção das anomalias simuladas em horários específicos. Essas anomalias são injetadas como comportamentos adicionais ao comportamento normal da rede no período de tempo solicitado, não excluindo quaisquer registros de fluxos reais. Dessa forma, diferentes tipos de anomalias podem ser testadas em ambientes reais, mesmo que tais anomalias não ocorram durante o período de tempo utilizado para testes na rede real. Além disso, o funcionamento da rede utilizada no processo de validação de performance do sistema de detecção de anomalias não sofre quaisquer influências em sua operação. A Figura A.3 apresenta um trecho de um arquivo de fluxos IP antes e depois da injeção de uma anomalia do tipo DoS iniciada às 10h do dia 01 de Outubro de 2012.

Figura A.3 - Trecho de arquivo de fluxos: Antes e Depois de um ataque DoS simulado.

Antes:

```
2012-10-01 09:59:58.500     0.000 UDP      108.35.22.143:50039 ->     189.90.71.56:55893      256    17920     1
2012-10-01 10:00:01.608     0.000 TCP      74.125.234.162:80   ->     189.90.69.164:61529     256   367104     1
2012-10-01 10:00:01.608     0.000 TCP      209.207.230.25:80   ->     189.90.65.11:4479       256    71680     1
2012-10-01 10:00:01.608     0.000 TCP      201.54.66.11:80     ->     189.90.65.11:32247      256    17408     1
2012-10-01 10:00:01.608     0.000 TCP      177.177.181.110:27566 ->   189.90.74.46:64576      256    17408     1
2012-10-01 10:00:01.608     0.000 TCP      74.125.134.108:465  ->     189.90.72.124:49614     256    18944     1
2012-10-01 10:00:05.607     0.000 TCP      201.54.66.10:80     ->     189.90.65.11:30355      256   389632     1
2012-10-01 10:00:05.607     0.000 TCP      189.14.52.15:80     ->     189.90.65.11:26071      256   389632     1
2012-10-01 10:00:05.607     0.000 UDP      71.45.153.156:6881  ->     189.90.74.46:22271      256    17920     1
```

Depois:

```
2012-10-01 09:59:58.500     0.000 UDP      108.35.22.143:50039 ->     189.90.71.56:55893      256    17920     1
2012-10-01 10:00:01.608     0.000 TCP      74.125.234.162:80   ->     189.90.69.164:61529     256   367104     1
2012-10-01 10:00:01.608     0.000 UDP      11.11.11.11:80      ->     22.22.22.22:80          256     2048     1
2012-10-01 10:00:01.608     0.000 TCP      209.207.230.25:80   ->     189.90.65.11:4479       256    71680     1
2012-10-01 10:00:01.608     0.000 TCP      201.54.66.11:80     ->     189.90.65.11:32247      256    17408     1
2012-10-01 10:00:01.608     0.000 TCP      177.177.181.110:27566 ->   189.90.74.46:64576      256    17408     1
2012-10-01 10:00:01.608     0.000 TCP      74.125.134.108:465  ->     189.90.72.124:49614     256    18944     1
2012-10-01 10:00:05.607     0.000 TCP      201.54.66.10:80     ->     189.90.65.11:30355      256   389632     1
2012-10-01 10:00:05.607     0.000 UDP      11.11.11.11:80      ->     22.22.22.22:80          256     2048     1
```

É importante ressaltar que essa é a primeira versão da ferramenta, a qual possui suporte apenas para fluxos no formato padrão exportados pelo protocolo sFlow.

Seu funcionamento, do ponto de vista do usuário, é simplificado: primeiramente o usuário digita no campo "Arquivo Fonte" o endereço completo do arquivo de fluxos IP utilizado como base para a injeção de anomalias. Em seguida, o campo "Nome do Arquivo de Saída" é também preenchido com o endereço e nome do arquivo resultante (caso o caminho não seja especificado, a Scorpius irá gerar o arquivo no mesmo diretório que ela se

encontra). Em seguida, uma anomalia é escolhida pelo usuário, que preenche os campos relativos a ela. Alguns dos campos possuem um botão de geração de dados aleatórios, o que facilita o processo de análise em situações onde apenas a detecção da anomalia é importante, não sendo necessária a identificação de sua origem. No caso de endereços IP, é possível que sejam gerados endereços IP não válidos em um ambiente real, o que não influencia no processo de validação de performance de sistemas de detecção de anomalias. Os campos de Horários devem ser preenchidos na forma HH:MM:SS (horas:minutos:segundos), sendo que o horário de inicio deve necessariamente ser mais cedo que o horário de término. Por último, o campo "Qtd. de Fluxos Injetados" deve ser preenchido com a quantidade de fluxos injetados a cada segundo no arquivo. É importante ressaltar que o protocolo sFlow possui suporte nativo à amostragem e, por isso, cada fluxo injetado por segundo representa outros 256 fluxos coletados pelo switch. Por isso este valor muitas vezes é definido como 1 na maioria dos casos.

Do ponto de vista de baixo nível, cada anomalia suportada possui diferentes comportamentos, os quais foram implementados pelo programa conforme descrito a seguir:

- DoS: O ataque de negação de serviço (*Denial of Service*) é, basicamente, um ataque de um único host à um determinado host destino que visa o congestionamento de um serviço ou servidor. Dessa forma, após todos os dados preenchidos e a seleção do botão "Iniciar!" pelo usuário, a ferramenta injeta o número de fluxos presentes no campo "Qtd. Fluxos Injetados" a cada segundo desde o horário de início até o horário de fim estipulado. Estes fluxos contêm as informações de Endereços IP de origem e destino, portas de origem e destino e protocolo estipulados. Embora o protocolo utilizado seja de livre escolha (TCP, UDP ou ICMP), recomenda-se a utilização do protocolo UDP, visto que é o mais comumente utilizado nestes tipos de ataques, seguido do ICMP. O atributo de fluxo Bytes é calculado de acordo com o tamanho mínimo de envio de pacotes para cada um dos diferentes protocolos;
- DDoS: De forma semelhante ao DoS, ataques de negação de serviço distribuídos (*Distributed Denial of Service*) são tentativas de congestionamento de um serviço ou servidor. Entretanto, ao contrário do DoS, este ataque se utiliza de vários hosts que, intencionalmente ou não (como é o caso de BotNets, ou redes zumbis, compostas de

computadores infectados que são controlados remotamente por hackers) atacam um único host destino. Seu funcionamento na Scorpius é semelhante ao DoS, com o diferencial de que não se especifica quais os endereços IP de ataque, apenas quantos diferentes hosts participam do mesmo. Os endereços IP destes hosts são gerados de forma aleatória pela ferramenta, que cria um arquivo de fluxo para cada host de origem, potencializando o impacto causado na rede com relação ao DoS;

- *Flash Crowd*: No caso, eventos *Flash Crowd* não são considerados ataques, sendo classificados como anomalias. São eventos em que uma grande quantidade de usuários utiliza um serviço ao mesmo tempo, causando um congestionamento involuntário no serviço ou servidor. Esses eventos ocorrem com maior frequência em sites ou sistemas WEB, tais como endereço eletrônico de universidades que divulgam resultados de processos seletivos. Dessa forma, o protocolo utilizado para acesso é na maior parte dos casos o TCP e, por isso, este protocolo é fixo neste tipo de injeção de anomalia. Como os Endereços IP de origem são muito variados, a cada novo segundo novos endereços IP são gerados aleatoriamente pela ferramenta, sendo que cada um destes endereços de origem geram um fluxo por segundo;
- *Port Scan*: Esta anomalia se trata de um procedimento utilizado para se verificar vulnerabilidades em um determinado host. Dessa forma, um host de origem realiza um escaneamento em todas ou em uma faixa de portas de um host destino, verificando quais delas se encontram abertas. Diversas metodologias podem ser utilizadas neste processo, a maior parte delas se utilizando do protocolo TCP (o qual foi definido como padrão neste tipo de injeção de anomalia). Para a ferramenta Scorpius, foi escolhido o método denominado *Half-Open*, amplamente utilizado por não permitir que a conexão TCP se estabeleça, impedindo que o atacante seja identificado. Este método basicamente envia uma mensagem SYN para uma porta específica no host destino e, se receber uma resposta SYN+ACK, a qual indica que a porta se encontra aberta, responde com uma mensagem RST para

finalizar a conexão antes que a mesma se estabeleça. Sendo assim, apenas 3 pacotes são trocados por porta. Na Scorpius, o usuário deve preencher os campos Endereço IP de origem e destino, porta de origem e horário de início do ataque. Este ataque não possui horário de fim pois é finalizado assim que todas as portas solicitadas são escaneadas. Além disso, o usuário deve preencher os campos "Inicio" e "Fim" relativos ao *Port range*, ou amplitude de portas analisadas, que podem variar de 1 a 65535. A cada segundo um novo fluxo referente a uma porta do host destino é gerado no arquivo, sendo que o próximo fluxo será relativo à porta de numero 256 posterior devido à taxa de amostragem anteriormente mencionada. Dessa forma, se 1024 portas são analisadas, apenas 4 fluxos são gerados, uma vez que a cada porta analisada foi selecionada no processo de amostragem do protocolo sFlow com taxa de 1:256.

Trabalhos Publicados

Conferências:

1. ASSIS, M. V. O. ; ZACARON, A. M. ; PROENÇA JR., M. L. *Time Series Forecasting Methods for Creating Digital Signature of Network Segments Using Flow Analysis*. Em: XXXI International Conference of the Chilean Computer Science Society (SCCC'2012), 2012, Valparaiso-CL. ***(Qualis CC 2013, B3)***
2. ASSIS, M. V. O. ; CARVALHO, L. F. ; RODRIGUES, J. J. P. C. ; PROENÇA JR., M. L. *Holt-Winters Statistical Forecasting and ACO Metaheuristic for Traffic Characterization*. Em: IEEE International Conference on Communications (ICC 2013), 9-13 June, 2013, Budapest-HU. IEEE International Conference on Communications (ICC 2013), 2013. ***(Qualis CC 2013, A2)***
3. ASSIS, M.V. O. ; RODRIGUES, J. J. P. C. ; PROENÇA JR., M. L. *A Novel Anomaly Detection System based on Seven-dimensional Flow Analysis*. Em: IEEE Gobal Communications Conference (GLOBECOM'13), 9-13 December, 2013, Atlanta-USA. IEEE Gobal Communications Conference (GLOBECOM'13), 2013.***(Qualis CC 2013 A1)***
4. ASSIS, M.V.O. ; RODRIGUES, J. J. P. C. ; PROENÇA JR., M. L. *A Hybrid Approach for Anomaly Detection on Large-scale Networks using HWDS and Entropy*. Em: International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2013), 2013, Primosten-HR. ***(Qualis CC 2013 - B4)***
5. CARVALHO, L.F.; ASSIS, M.V.O.; FERNANDES JR., G. ; RODRIGUES, J.J.P.C.; PROENÇA JR., M. L. *Digital Signature of Network Segment using PCA, ACO and Holt-Winters for Network Management*. Em: 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom), 2013, Lisboa-PT. ***(Qualis CC 2013 - B4)***
6. PENA, E.H.M.; ASSIS, M.V.O.; PROENÇA JR., M.L. *Anomaly detection using forecasting methods ARIMA and HWDS*. In: XXXII International Conference of the Chilean Computer Science Society (SCCC'2013), 2013, Temuco-CL. Proceedings of XXXII International Conference of the Chilean Computer Science Society (SCCC'2013), 2013. ***(Qualis CC 2013 - B3)***

Periódicos:

1. ASSIS, M.V.O.; RODRIGUES, J.J.P.C.; PROENÇA Jr., M.L. *A Seven-Dimensional Flow Analysis to Help Autonomous Network Management*. Information Sciences International Journal, ISSN: 0020-0255, 2014. ***(Qualis CC 2013 - A1)***
2. *(Em Avaliação)* PROENÇA Jr, M.L.; FERNANDES Jr., G.; CARVALHO, L.F.; ASSIS, M.V.O.; RODRIGUES, J. J. P. C. *Digital Signature to Help Network Management Using Flow Analysis*. International Journal of Network Management (IJNM), ISSN: 1099-1190, 2013. ***(Qualis CC 2013 - B3)***
3. *(Em Avaliação)* CARVALHO, L.F.; ASSIS, M.V.O.; FERNANDES Jr., G.; RODRIGUES, J.J.P.C.; PROENÇA Jr., M.L. *Digital Signature of Network Segment for Healthcare Environments Support*. Innovation and Research in BioMedical engineering (IRBM), ISSN: 1959-0318, 2013.