Universidade Estadual de Londrina

LUIZ FERNANDO CARVALHO

METAHEURÍSTICA ANT COLONY OPTIMIZATION E ANÁLISE DE FLUXOS IP APLICADOS À DETECÇÃO DE ANOMALIAS E À GERÊNCIA DE REDES

Londrina - Pr
2014

LUIZ FERNANDO CARVALHO

METAHEURÍSTICA ANT COLONY OPTIMIZATION E ANÁLISE DE FLUXOS IP APLICADOS À DETECÇÃO DE ANOMALIAS E À GERÊNCIA DE REDES

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação do 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 - Pr
2014

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

Dados Internacionais de Catalogação-na-Publicação (CIP)

C331m Carvalho, Luiz Fernando.
Metaheurística Ant Colony Optimization e análise de fluxos IP aplicados à detecção de anomalias e à gerência de redes / Luiz Fernando Carvalho. – Londrina, 2014.
118 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 – Medidas de segurança – Teses. 3. TCP/IP (Protocolo de rede de computação) – Teses. 4. Sistemas auto-organizadores – Teses. 5. Redes de computadores – Anomalias – Teses. 6. Aprendizado do computador – 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

LUIZ FERNANDO CARVALHO

METAHEURÍSTICA ANT COLONY OPTIMIZATION E ANÁLISE DE FLUXOS IP APLICADOS À DETECÇÃO DE ANOMALIAS E À GERÊNCIA DE REDES

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação do 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.
Universidade Estadual de Londrina

_____

Prof. Dr. Rodolfo Miranda de Barros
Universidade Estadual de Londrina

_____

Prof. Dr. Bruno Bogaz Zarpelão
Universidade Estadual de Londrina

_____

Prof. Dr. Rodrigo Sanches Miani
Universidade Federal de Uberlândia

Londrina, 26 de fevereiro de 2014.

A minha mãe Maria, minha avó Antônia e ao meu avô João, os quais tiveram uma importância incontestável no caminho trilhado até aqui.

AGRADECIMENTOS

A Deus, primeiramente, por tudo que me proporciona.

A minha família pelo apoio incondicional, especialmente à minha mãe, Maria, que durante o mestrado não poupou esforços para que este fosse concluído.

Ao professor Dr. Mario Lemes Proença Jr., grande responsável pela minha escolha em seguir a carreira acadêmica. Agradeço pela confiança, orientação e incentivo.

Agradeço a todos os professores que, direta ou indiretamente, contribuíram para a construção desse trabalho. Sou grato ao professor Sylvio Barbon por compartilhar uma pequena fração do seu vasto conhecimento e ao professor Bruno Zarpelão, pelas dicas e aconselhamentos. Também agradeço o apoio oferecido pelo professor Joel do Instituto de Telecomunicações da Universidade Beira Interior, Portugal. Não posso deixar de mencionar o esforço incondicional dos professores Rodolfo e Mario para que as melhores condições para a elaboração dos trabalhos fossem oferecidas aos seus alunos. Muito Obrigado.

Aos amigos do grupo de redes: Gilberto, Marcos e Eduardo. Aos integrantes da GAIA Anderson e Bruno, com os quais dividi alegrias, conhecimento e, sobretudo muito trabalho. Aos amigos veteranos, Alexandro Zacaron, Mário "Pajé" Adaniya e Alexandre Amaral. Obrigado pelas diversas oportunidades de troca de conhecimento!

A minha amiga e namorada Jeniffer pela paciência, apoio e cumplicidade ao longo desse processo.

A CAPES pela bolsa concedida.

Aos que não foram nominados, a importância que tiveram em algum momento não é menor ou maior, e peço sinceras desculpas.

A todos que, com boa intenção, colaboraram para a realização deste trabalho.

CARVALHO, Luiz Fernando. **Metaheurística Ant Colony Optimization e Análise de Fluxos IP Aplicados à Detecção de Anomalias e à Gerência de Redes**. 2014. 118 f. Dissertação (Mestrado) – Universidade Estadual de Londrina, Londrina, 2014.

RESUMO

O monitoramento do tráfego é uma atividade indispensável para o gerenciamento de redes, uma vez que promove informações importantes para a manutenção e controle dos mecanismos de comunicação. Para que essa tarefa seja cumprida com rigor, é necessário o uso de uma abordagem que reconheça de forma proativa comportamentos do tráfego que possam prejudicar o funcionamento correto da rede. Neste trabalho, é apresentado um sistema capaz de identificar tais comportamentos, emitindo alarmes quando um evento não esperado, algum mau funcionamento de dispositivos ou ameaças à segurança são detectados. A fim de alcançar este objetivo, uma metodologia de aprendizado não-supervisionado é utilizada para extrair características do tráfego através de atributos dos fluxos IP. Para assegurar que essa abordagem seja eficiente, uma modificação da metaheurística *Ant Colony Optimization* é utilizada, a qual por meio da auto-organização de seus agentes otimiza a análise multidimensional desses atributos e dessa maneira faz com que esta tarefa seja realizada em tempo hábil para seu uso em redes de larga escala. É apresentada também uma abordagem denominada *Adaptive Dynamic Time Warping*, responsável pelo reconhecimento de variações do tráfego que diferem do comportamento normal esperado. Essa análise ainda considera a relação entre os atributos do fluxo, permitindo maior acurácia na classificação do problema detectado, garantindo que o administrador de rede não seja sobrecarregado com notificações de falsas anomalias.

Palavras-chave: Ant colony optimization. Caracterização de tráfego. Gerenciamento de redes. Aprendizagem não-supervisionada. Agentes auto-organizáveis.

CARVALHO, Luiz Fernando. **Metaheurística Ant Colony Optimization e Análise de Fluxos IP Aplicados à Detecção de Anomalias e à Gerência de Redes**. 2014. 118 p. Dissertação (Mestrado) – Universidade Estadual de Londrina, Londrina, 2014.

ABSTRACT

Traffic monitoring is an indispensable network management activity, since it promotes important information for the maintenance and control of the communication. For this task is enforced, the use of an approach that recognizes proactively traffic behaviors that may impair the proper functioning of the network is required. In this work, a system which is able to identify such behaviors by emitting alarms when an unexpected event, a malfunctions of devices or security threats are detected is proposed. To achieve this goal, an unsupervised learning method is used to extract features of traffic from IP flows attributes. To ensure the effectiveness of this approach, a modification of the Ant Colony Optimization metaheuristic is proposed, which through self-organization agents optimizes the multidimensional analysis of these attributes and makes this task done in time for large-scale networks. One approach called Adaptive Dynamic Time Warping, responsible for recognizing traffic fluctuations that diverge from the expected normal behavior is presented as well. This analysis also considers the relationship between the IP flow attributes, allowing greater accuracy in the classification of a detected problem and ensuring that the network administrator is not overloaded with reports of false anomalies.

Keywords: Ant colony optimization. Traffic characterization. Network management. Unsupervised learning. Self-organized agents.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACO	Ant Colony Optimization
ACODS	Ant Colony Optimization for Digital Signature
ADTW	Adaptive Dynamic Time Warping
CLN	Competitive Learning Network
CRANE	Common Reliable Accounting for Network Element Protocol
DDoS	Distributed Denial of Service
DLA	Device Level Alarm
DSNSF	Digital Signature of Network Segment using Flow analysis
DTW	Dynamic Time Warping
FA	Firefly Algorithm
FHCA	Firefly Harmonic Clustering Algorithm
GBA	Gerenciamento de Backbone Automático
ICLN	Improved Competitive Learning Network
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IPTV	Internet Protocol Television
ISO	International Organization for Standardization
KHM	K-Harmonic means
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
M2M	Manager-to-Manager
NMSE	Normalized Mean Square Error
PCA	Principal Component Analysis
PoP	Point of Presence
PSAMP	Packet Sampling
PSO	Particle Swarm Optimization
QoS	Quality of Service
RFC	Request for Comments
SICLN	Supervised Improved Competitive Learning Network
SIP	Session Initiation Protocol

SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
SCTP	Stream Control Transmission Protocol
TES	Traffic Entropy Epectrum
UDP	User Datagram Protocol
UEL	Universidade Estatual de Londrina
UTFPR	Universidade Tecnológica Federal do Paraná
VLAN	Virtual Local Area Network
VoIP	Voice over IP

LISTA DE SÍMBOLOS

Símbolo	Descrição
H	Entropia de Shannon
S	Total de todas as ocorrências presentes no histograma usado no cálculo da entropia
X	Matriz contendo o DSNSF dos 7 atributos do tráfego
E	Total de elementos a serem clusterizados
K	Número total de clusters
C	Conjunto de agrupamento
J	Função Objetivo
$min[.]$	Operador que retorna o menor valor
$max[.]$	Operador que retorna o maior valor
A	Dimensionalidade dos dados
R	Índices de associação dos elementos aos clusters
τ	Trilha de feromônio
q	Probabilidade que define qual abordagem de atribuição de um elemento a um cluster será usada
L	Número de soluções mais promissoras criadas a cada iteração
ρ	Taxa de evaporação do feromônio
I	Número de total de iterações
γ	Valor atribuído à busca local
p_j	Quantidade de elementos agrupados ao cluster j
δ	Valor da medida Índice Dunn
$S(i)$	Valor do teste Silhouette para o elemento i
Y	Matriz contendo o tráfego real
D	Distância calculada dentre duas séries após a distorção causada pela DTW
w	Melhor caminho entre o alinhamento temporal de duas séries
Δ_t	Distância entre duas séries temporais no intervalo t
s_t	Medida de similaridade entre duas séries temporais no intervalo t
r	Resultado final da divergência entre o DSNSF e o tráfego real
Φ	Coeficiente de significância usado na abordagem de detecção de anomalias
F	Erro relativo entre o DSNSF e o tráfego real
$\bar{d}$	Diferença entre as médias das séries DSNSF e tráfego real
σ	Desvio padrão

SUMÁRIO

1 INTRODUÇÃO

A praticidade de se trabalhar em redes tornou essa ferramenta indispensável para os diversos meios de comunicação, promovendo importantes recursos e mecanismos como pesquisas, compartilhamento de arquivos, acesso remoto e interação entre pessoas. Grande influência desse processo é decorrente da difusão de tecnologias como voz sobre IP (VoIP - Voice over IP), televisão sobre IP (IPTV – IP television), *e-health* e o *e-commerce,* as quais contribuem para o crescente número de usuários que são atraídos pelos serviços cada vez mais sofisticados e de menores custos [1]. Outro fator considerável desse processo é o crescente número de dispositivos móveis e portáteis conectados às redes. Estima-se que esses dispositivos ultrapassem 10 bilhões de unidades em 2017 e sejam capazes de gerarem um tráfego mensal de 10 hexabytes [2]. Com isso, há uma necessidade iminente de que as redes permitam que todos esses aparelhos sejam conectados de forma transparente, e que possam ser provisionados de transmissões de alto desempenho.

As exigências da crescente demanda por novos serviços fizeram com que as redes se tornassem sistemas complexos, constituídos por diversos elementos heterogêneos que operam em alta velocidade, mantendo uma interação constante entre si [3]. Utilizando redes de larga escala, o monitoramento e controle são ainda mais dificultados, em que tarefas como a configuração correta dos equipamentos ou a própria verificação do funcionamento adequado são atividades que exigem pessoal altamente especializado, bem como grande quantidade de tempo e esforço. Dessa forma, a própria evolução das tecnologias de comunicação condiciona a necessidade da automatização das funções de gestão de rede [4].

Os operadores de rede são geralmente confrontados com inúmeros eventos incomuns, alguns dos quais podem apresentar um comportamento malicioso. Como pôde ser notado durante a última década, além dos tradicionais métodos de ataques como DDoS (*Distributed Denial of Service*) e *port scan*, a espionagem e guerras cibernéticas têm se apresentado como coadjuvantes na evolução das técnicas de quebra de segurança. Há uma crescente preocupação sobre a possibilidade do uso de *malwares* para ataques diretos às infraestruturas críticas de redes, assim como as informações que podem ser comprometidas [5]. A fim de manter as características de confiabilidade, resiliência e disponibilidade, o administrador de rede deve assegurar que o monitoramento do tráfego seja realizado de forma precisa para promover o diagnóstico que auxilie na tomada de decisões, mediante algum problema encontrado.

Novas vulnerabilidades e ameaças são descobertas constantemente e mecanismos de defesa rotineiros como *firewall* e sistema de detecção de intrusão (SDI) mostram-se insuficientes na prevenção desses ataques, cada vez mais numerosos e indesejáveis. Neste cenário, a detecção e classificação de anomalias ainda constituem um campo de pesquisa desafiador, uma vez que o monitoramento do tráfego se torna mais complexo a cada dia, devido à profusão das redes de larga escala, requerendo, portanto, métodos proativos que detectem essas atividades de forma antecipada, amenizando seus efeitos e assegurando o bom funcionamento da rede [6] [7]. Na literatura, os métodos de detecção de anomalias são divididos em dois grupos. Tradicionalmente, na detecção baseada em assinaturas, os sistemas possuem uma base de dados disponibilizada por especialistas contendo as características das anomalias que podem ser detectadas [8]. A segunda categoria compreende a detecção baseada em perfis. Essa abordagem estabelece um perfil de comportamento normal da rede levando-se em consideração o histórico do tráfego analisado. A detecção é realizada a partir do reconhecimento de alterações significativas nos indicadores de funcionamento da rede, as quais não são coerentes com as estimativas definidas no perfil de comportamento normal do tráfego [9] [10].

No presente trabalho é apresentado um sistema capaz de detectar automaticamente anomalias com o objetivo de auxiliar os administradores na gerência de redes. Mais especificamente, tal aplicação tem o propósito de reconhecer desvios comportamentais do tráfego que condizem com eventos que possam afetar a segurança e integridade da rede, e fazendo isso com alta taxa de acertos e os mínimos falsos alarmes possíveis. De acordo com Molnar *et al.*[11], muitos trabalhos anteriores são focados no monitoramento de um único atributo do tráfego - geralmente *bits* transmitidos por segundo - para detecção de anomalias, tornando esse processo inviável para o reconhecimento de ataques complexos. A abordagem apresentada contorna essa limitação com o desenvolvimento de uma análise de sete dimensões do tráfego. Para tanto, acredita-se que maior precisão é conseguida utilizando tanto informações referentes ao volume de tráfego, isto é, *bits*, pacotes e fluxos transmitidos por segundo, bem como os atributos contidos no cabeçalho dos pacotes IP (endereços IP de origem e destino, portas de origem e destino).

O nível de detalhes do monitoramento do sistema apresentado está ligado à análise de fluxos IP utilizando os protocolos de gerenciamento de redes NetFlow, IPFIX e sFlow. As características do tráfego, endereços de origem e destino, portas de origem e destino, tipos de protocolos usados e demais propriedades das camadas de rede e transporte, tornam possível a identificação de padrões de comportamentos entre *hosts*, visando a

identificação de problemas, anomalias e ataques. Essa abordagem de gerenciamento é uma alternativa ao modelo tradicional disponibilizado pelos contadores SNMP (*Simple Network Management Protocol*).

O sistema apresentado neste trabalho segue a metodologia de criação de perfis de comportamento, sendo dividido em duas etapas. A primeira consiste na caracterização do tráfego da rede baseado no volume e também na distribuição dos atributos endereços IP e portas. Para isso, é apresentado o conceito de *Digital Signature of Network Segment using Flow Analysis* (DSNSF), o qual é responsável por descrever o perfil de comportamento normal da rede para os atributos analisados. Uma modificação da metaheurística *Ant Colony Optimization* (ACO) é utilizada para a criação do DSNSF e tal adaptação é denominada *Ant Colony Optimization for Digital Signature* (ACODS). Esta abordagem visa otimizar a extração de padrões de comportamentos do tráfego através de um mecanismo de aprendizado não-supervisionado. Essa etapa do sistema também inclui o tratamento das informações usadas para construção da assinatura digital, tais como a redução da granularidade dos atributos - extraídos diretamente dos protocolos de exportação de fluxos, e a transformação dos valores dos atributos descritivos (IP e portas) para quantitativos, a fim de que possam ser processados juntamente com os atributos de volume para construção do DSNSF.

A segunda etapa corresponde à detecção de comportamentos anômalos. Esta fase é responsável por confrontar o perfil de comportamento normal, descrito pela assinatura digital, com as amostras coletadas a partir do tráfego real observado, a fim de determinar se ocorrem diferenças. Para essa finalidade é utilizada a abordagem *Adaptive Dynamic Time Warping* (ADTW), uma modificação da técnica do tipo *pattern matching*, desenvolvida inicialmente para o reconhecimento de padrões de voz. Através do alinhamento temporal, a ADTW fornece uma detecção de anomalias precisa, reconhecendo eventos discrepantes entre as séries temporais que descrevem o DSNSF e o tráfego real, possibilitando a melhoria da análise de eventos pontuais tanto quanto daqueles que se deslocam ao longo do tempo.

O ACODS foi submetido à avaliação utilizando dados provenientes de ambientes reais. Os fluxos foram coletados na rede da Universidade Estadual de Londrina (UEL) e da Universidade Federal Tecnológica do Paraná (UTFPR) – Campus Toledo. Além dessas fontes de dados, anomalias foram injetadas ao tráfego real para complementar o estudo e verificar a eficácia do ACODS na detecção dos diversos tipos de ataques.

A abordagem de detecção de anomalias que utiliza a caracterização do tráfego normal da rede baseado na análise de fluxo e que gera relatórios referentes aos eventos anômalos, apresenta as seguintes contribuições:

- **Adaptação da metaheurística *Ant Colony Optimization:*** tal modelo heurístico é modificado para criação do sistema *Ant Colony Optimization for Digital Signature,* o qual é capaz de reconhecer o comportamento normal do tráfego, gerando uma assinatura digital do segmento de rede.
- **Adaptação da técnica *Dynamic Time Warping* (DTW):** propiciou a elaboração da abordagem ADTW, eficaz no reconhecimento de comportamentos anômalos do tráfego.
- **Detecção proativa de anomalias:** o sistema possibilita a detecção automática de eventos anômalos. Uma das vantagens da automação do monitoramento é o auxílio nas atividades manuais de gerência, garantindo maior precisão e a diminuição de erros provenientes dessa prática.
- **Análise do tráfego em janelas de um minuto:** Contrário aos tradicionais modelos que apresentam detecção de anomalias em períodos de cinco minutos, ACODS é desenvolvido para realizar essa tarefa em intervalos de um minuto, permitindo ao administrador ser alertado mais rapidamente e evitando que o comprometimento dos serviços de rede seja prolongado.
- **Fornecimento de informações referentes aos eventos anômalos detectados:** O administrador é suprido com informações sobre o uso de recursos no exato momento da ocorrência da anomalia para que sirvam de base na construção de uma solução para o problema.

O restante deste trabalho está organizado da seguinte maneira: O capítulo 2 apresenta trabalhos relacionados à caracterização de tráfego e detecção de anomalias encontradas em diversas publicações recentes. O capítulo 3 aborda alguns padrões e recursos da gerência de redes com a utilização de fluxos. O capítulo 4 detalha a caracterização de tráfego e criação de assinaturas digitais utilizando a abordagem *Ant Colony Optimization for Digital Signature,* juntamente com a metodologia de detecção de anomalias *Adaptive Dynamic Time Warping*. O capítulo 5 demonstra e avalia a aplicação das assinaturas geradas

sobre diversos cenários formados por ambientes reais de rede e simulado. Por fim, o capítulo 6 apresenta as considerações acerca do trabalho e as futuras direções da pesquisa.

2 TRABALHOS RELACIONADOS

Este capítulo apresenta uma breve descrição de diversos trabalhos que são destinados à criação de soluções viáveis para a detecção de anomalias em redes de computadores. Essas publicações foram escolhidas por sua relevância na literatura ou por externarem o estado da arte nesse campo de pesquisa.

De acordo com Patcha e Park [9], detecção de anomalias é o ato de reconhecer ações que venham a comprometer a confidencialidade, integridade ou disponibilidade de uma rede. Sob essa perspectiva, as técnicas de detecção de anomalias podem ser divididas em duas categorias: baseadas em assinatura e técnicas de caracterização do comportamento normal do tráfego. Um sistema de detecção de anomalias, que utiliza assinaturas, identifica padrões de tráfego maliciosos previamente conhecidos. A detecção baseada na observação do comportamento normal constrói um perfil de tráfego e os eventos anômalos são identificados a partir de desvios em relação a esse padrão. Uma terceira categoria, não muito comum, denominada híbrida, agrega conceitos das duas técnicas anteriores.

Ambas as metodologias, baseadas em assinatura e caracterização do tráfego, apresentam suas vantagens e desvantagens. O principal benefício adquirido com o uso da detecção baseada em assinatura é que os ataques conhecidos podem ser detectados de forma eficiente com uma baixa taxa de falsos positivos. Sua principal desvantagem é a necessidade de que uma assinatura deve ser definida para todos os possíveis ataques que o atacante pode empregar contra a rede. Sistemas que caracterizam o comportamento normal do tráfego apresentam duas grandes vantagens sobre os sistemas de detecção baseados em assinatura. A primeira diz respeito à capacidade de detectar ataques desconhecidos. Esta vantagem é devido à propriedade desses sistemas modelarem o funcionamento normal de uma rede e detectar desvios a partir dele. A segunda vantagem é que os perfis de atividade normal são personalizados para cada rede, tornando difícil para um atacante saber quais as atividades que podem ser realizadas sem que ele seja detectado. No entanto, essa abordagem também apresenta sua parcela de desvantagens. A complexidade do sistema, assim como a alta porcentagem de falsos alarmes associada à dificuldade de determinar qual evento específico desencadeou os indicativos de anomalias, são alguns dos muitos desafios técnicos que precisam ser tratados antes de sua implantação.

Os métodos de detecção de anomalias pertencentes às duas categorias mencionadas podem também ser classificados de acordo com a classe de algoritmo utilizado para realização dessa tarefa. Essas abordagens incluem a detecção de anomalia através de ferramentas estatísticas, métodos baseados em mineração de dados e técnicas que utilizam aprendizagem de máquina.

Segundo Grossman [12], a mineração de dados inclui métodos preocupados com o descobrimento de padrões, associações, mudanças, anomalias, estruturas significativas e eventos que não podem ser vistos facilmente em um conjunto de informações. Enquanto isso, os modelos estatísticos usados para detecção de anomalias criam perfis de comportamentos normais a partir de análises de uma base histórica. Esses perfis são modelados matematicamente para descreverem limiares, os quais indicam a taxa de variação máxima que o tráfego pode apresentar em relação ao modelo normal, evitando o acionamento de alarmes de anomalias [9]. Contrário à abordagem estatística, que tende a se concentrar em entender o processo que gerou os dados, as técnicas de aprendizagem de máquina se destinam à construção de um sistema que aprimore o seu próprio desempenho com base nos resultados anteriores. Em outras palavras, os sistemas baseados nesse paradigma possuem a capacidade de alterar a sua estratégia de execução com base nas informações recentemente adquiridas.

No campo de pesquisa sobre mineração de dados, é encontrada a característica de aprendizado não-supervisionado, apreciada para sistemas de segurança de redes de computadores, sendo empregada na maioria das pesquisas através da técnica de clusterização. Tendo em vista os benefícios dessa técnica, Corral *et al.* [13] apresentam uma análise de segurança a qual agrupa dispositivos de redes em conjuntos, ou *clusters*, levando-se em conta seus comportamentos e fragilidades. Quando uma vulnerabilidade é detectada e resolvida em algum equipamento, a solução pode ser aplicada aos demais dispositivos desse *cluster*. Essa abordagem proporciona a priorização de grupos de equipamentos que demandam maior atenção para que a rede continue a funcionar corretamente.

Grande parte das pesquisas em detecção de anomalias recorre às estratégias baseadas em assinaturas ou aprendizagem supervisionada. Estas abordagens têm várias desvantagens tais como a ineficiência em tratar dados não rotulados e a necessidade de um agente supervisor externo, responsável por auxiliar o aprendizado da técnica utilizada. Outro fator de grande importância que atenta quanto ao uso dessas técnicas é a diminuição da eficiência quando há ocorrência de anomalias desconhecidas. Assim, Mazel *et al.* [14] introduziram uma abordagem não-supervisionada para detectar e caracterizar as anomalias de rede. A abordagem inicialmente funciona usando uma técnica de agrupamento, combinando o

sub-espaço de clusterização com o acúmulo de resultados a cada iteração para a construção de conjuntos de características que permitam a identificação de anomalias nos fluxos do tráfego.

A criação de uma ferramenta que descreve o perfil de comportamento da rede é essencial para um sistema de segurança. Dessa maneira, Rocha *et al.* [15] propõem um sistema de caracterização capaz de identificar *hosts* que geram tráfego malicioso. Tal ferramenta analisa diversos atributos de conexões TCP/IP de aplicações da Internet e as classifica, comparando com o perfil previamente criado. A abordagem proposta pelos autores trata de questões de segurança que incluem o encapsulamento de tráfego ilícito em comunicações legítimas e a replicação dos perfis normais de comunicações, as quais tentam burlar os vários mecanismos de defesa da rede.

Vários trabalhos anteriores são restritos ao reconhecimento de determinados tipos de anomalias como ataques DDoS [16], *port scan* [17] e *worms* [18] [19]. Os autores de [20] propõem um sistema de detecção de *flash crowds* baseado na análise de objetos SMNP (*Simple Network Management Protocol*) coletados diretamente da MIB (*Management Information Base*) de um *switch*. Este sistema é baseado em perfis e utiliza uma assinatura que caracteriza o comportamento normal do tráfego, a qual é gerada pela ferramenta GBA (Gerenciamento de *Backbone* Automático) [21]. Para a detecção de comportamentos anômalos, o algoritmo de clusterização K-means agrupa o tráfego real com assinatura de tráfego normal para extrair diferenças comportamentais de ambos os conjuntos. Uma técnica evolucionária denominada *Particle Swarm Optimization* (PSO) é usada para melhorar a qualidade e desempenho da clusterização. Embora mostre resultados promissores, essa última abordagem somente trata atributos de volume de tráfego, o que é justificável pelo uso dos objetos SNMP.

Um trabalho semelhante ao anterior é apresentado por Adaniya *et al*. [22]. Os autores utilizam a mesma fonte de dados, contudo, propõem um algoritmo híbrido de clusterização, *Firefly Harmonic Clustering Algorithm* (FHCA). O objetivo é a detecção de anomalias no volume de tráfego combinando o uso dos modelos *K-Harmonic means* (KHM) e *Firefly Algorithm* (FA).

Ainda, sob a mesma linha de pesquisa, é encontrado o trabalho de Zacaron *et al.* [23]. Diferentemente das abordagens anteriores, o tráfego a ser analisado é coletado utilizando o protocolo de exportação de fluxos Netflow e, através de um modelo de aprendizado não-supervisionado, o tráfego pôde ser caracterizado. O uso da rede é verificado no nível de protocolos, em que é possível observar o volume de dados transmitido utilizando os protocolos de transporte UDP e TCP. Esta tarefa é realizada por meio da adaptação do

algoritmo de clusterização K-means para a geração de assinaturas digitais, capazes de descreverem o comportamento normal do tráfego de um segmento de rede.

O sistema proposto por Casas *et al.* [24] trata a detecção de anomalias de volume em toda a rede utilizando uma análise de tráfego no nível de fluxo, seguindo a abordagem Origem-Destino (OD). Para tanto, o tráfego agregado total dos fluxos transmitidos entre uma entrada e uma saída de um *link* ou PoP (*Point of Presence*) é coletado a partir do protocolo SNMP por contadores de *bytes* transmitidos. Os autores propõem algoritmos para o reconhecimento sequencial de anomalias com capacidade de isolar tais comportamentos, a fim de encontrar a variação do fluxo de OD que causou o tráfego anormal. A principal contribuição deste trabalho é a criação de um modelo de tráfego baseado em *splines* lineares para descrever o comportamento anômalo de uma rede IP de grande escala. Entretanto, o sistema considera um único atributo do tráfego, o que torna sua análise restrita. Além disso, o uso de SNMP pode provocar limitações, uma vez que, devido ao uso do protocolo de transporte UDP para leituras dos contadores, a comunicação se torna não confiável, logo as falhas de sincronização durante a obtenção dos dados devem ser consideradas.

Amaral *et al*. [25] propõem um sistema de correlação de alarmes dividido em três camadas. A camada de pré-processamento analisa os atributos espaciais e temporais dos alarmes para reduzi-los em um único, chamado *Device Level Alarm* (DLA). A camada de correlação infere o caminho de propagação da anomalia, sua origem e destino pela combinação de DLAs e informações da topologia da rede, que é representada por um gráfico de dependência. A camada de apresentação oferece uma visão ampla dos cenários de rede afetados pela anomalia, proporcionando a visualização dos enlaces e elementos de rede afetados durante a propagação da anomalia. É apresentada também uma medida baseada no conceito de entropia não extensiva. Esta medida é aplicada para reduzir as incertezas geradas por alarmes ruidosos na identificação do caminho de propagação das anomalias.

A Tabela 2.1 apresenta as principais características dos métodos de detecção de anomalias discutidos neste capítulo.

Tabela 2.1 - Comparativo entre as abordagens propostas nos trabalhos relacionados.

	Metodologia de detecção	Classificação da técnica empregada	Fonte de dados	Destaque
Corral et al. [13]	Assinatura	Mineração de dados	Fluxos	Classifica em grupos os dispositivos de redes afetados pelas anomalias, facilitando a implantação da solução
Mazel et al. [14]	Assinatura	Mineração de dados	Fluxos	Cria um sistema baseado em aprendizado não-supervisionado, capaz de reconhecer comportamentos incomuns sem intervenção humana
Rocha et al. [15]	Perfil	Estatística	SNMP	Reconhecimento de padrões de comportamentos ilícitos injetados no tráfego de aplicações legítimas
Lu et al. [16]	Perfil	Aprendizagem de máquina	Fluxos	Explora a correlação espacial e temporal do tráfego de ataques DDoS
Kim et al. [17]	Assinatura	Estatística	Fluxos	Uso de limiares adaptativos e demais parâmetros que torna essa abordagem flexível na detecção de *port scans*
Kim e Karp [18]	Perfil	Mineração de dados	Fluxos	Criação de assinaturas de forma automática que acompanha a evolução da maioria dos *worms* que se propagam através do protocolo TCP
Byungseung et al. [19]	Perfil	Estatística	Fluxos	Utiliza janelas temporais para a detecção de *worms* apresentados em diferentes frequências no tráfego da rede
Lima et al. [20]	Perfil	Mineração de dados	SNMP	Reconhecimento de padrões de comportamentos do tráfego é realizado com a combinação de duas técnicas de clusterização
Adaniya et al. [22]	Perfil	Mineração de dados	SNMP	Combina algoritmos de clusterização para reconhecer desvios comportamentais do tráfego que definem anomalias
Zacaron et al. [23]	Perfil	Mineração de dados	Fluxos	Utiliza de agrupamento de dados para a caracterização de um segmento de rede usando análise de fluxos IP
Casas et al. [24]	Perfil	Estatística	SNMP	Cria um modelo estatístico parcimonioso capaz de trabalhar em redes com altas taxas de transferências de dados
Amaral et al.[25]	Perfil	Estatística	SNMP	Possibilita a identificação do trajeto de propagação de anomalias de rede

Embora os trabalhos apresentados na Tabela 2.1 demonstrem peculiaridades e características distintas, compartilham a existência de um conceito subjacente de normalidade. A noção de comportamento normal da rede é geralmente fornecida por um modelo formal que expressa as relações entre as variáveis envolvidas na dinâmica do monitoramento do tráfego. Por conseguinte, um evento é classificado como anômalo quando o grau de desvio em relação ao perfil de comportamento característico do tráfego, especificada pelo modelo de normalidade, é bastante elevado e ultrapassa um limiar previamente estabelecido.

A abordagem apresentada nesta pesquisa vai além dos trabalhos citados anteriormente. Examinando a distribuição dos atributos endereços IP e portas, é possível apresentar diagnósticos mais detalhados sobre as anomalias que os fornecidos pelo protocolo SNMP. Por meio dessas informações, é possível localizar as fontes geradoras das anomalias e qual tipo de aplicação está associado a esses eventos. Além disso, as limitações impostas pelo diagnóstico de anomalias específicas são contornadas através da realização de uma análise multidimensional do fluxo IP, o que garante observar comportamentos irregulares correlacionados entre os atributos em uma variedade de ataques, ampliando a escala de reconhecimento de eventos anômalos.

O aprendizado não-supervisionado proveniente da mineração de dados é um fator importante para construção deste trabalho. Juntamente com a capacidade de auto-organização da metaheurística *Ant Colony Optimization for Digital Signature* (ACODS), garante a mínima intervenção humana na caracterização do tráfego, além de tornar desnecessário o uso de dados rotulados (classificados como normais ou anômalos) para o treinamento e aprimoramento do sistema. Essas características são asseguradas através da capacidade do sistema de se avaliar e utilizar reforços de experiências anteriores para construção de perfis de comportamentos que contribuem para a detecção de anomalias.

3 GERÊNCIA DE REDES E MONITORAMENTO DO TRÁFEGO

Devido à agilidade e eficiência que proporcionam à troca de informações, as redes se destacaram nos meios de comunicações atuais, melhorando a interação entre as pessoas e proporcionando a criação de serviços indispensáveis. No entanto, o progresso no desenvolvimento de tecnologias de redes implica na crescente complexidade do seu gerenciamento. Isso aumenta a responsabilidade do administrador em detectar anomalias e problemas para que não causem nenhum impacto significativo sobre a qualidade ou a interrupção dos serviços fornecidos aos usuários. Com essa finalidade, a gerência de redes aborda várias questões para assegurar a confiabilidade, integridade e disponibilidade da comunicação. Reconhecendo essa situação, a organização internacional de normalização ISO (*International Organization for Standardization*) desenvolveu uma arquitetura para o gerenciamento de redes. Segundo Hunt [26], este modelo contém as seguintes características:

- Gestão de falhas: Necessária para detectar a deterioração das condições operacionais do sistema, erros em aplicações ou ainda falha de um componente de *hardware*. Essa área também pode incluir as atividades de isolamento e correções de falhas.
- Gestão de contabilidade: Desejável para registro do uso da rede por parte de seus usuários. Pode ser utilizado para organizar o uso de recursos para aplicações e operadores apropriados.
- Gestão de configuração: Tarefas ligadas a essa área devem manter registros de *softwares* e *hardwares*. Além disso, devem proporcionar informações sobre manutenção, inclusão e atualização de relacionamentos entre os dispositivos durante a operação da rede.
- Gestão de desempenho: Indispensável para testes, monitoramentos, bem como para fornecimento de estatísticas como vazão da rede, tempo de resposta e disponibilidade de equipamentos. Estas informações também tem a finalidade de assegurar que a rede atue de acordo com a qualidade de serviço firmada pelos usuários.
- Gestão de segurança: Trata da integridade dos dados trafegados e também do funcionamento correto da rede. Para esse fim, comporta

> atividades como monitoramento constante dos recursos disponíveis e restrição de acesso para evitar o uso incorreto dos recursos pelos usuários legítimos e agentes sem autorização.

Além das áreas destacadas anteriormente, a gerência de redes divide suas atividades em duas categorias distintas [10]. A primeira é o monitoramento, responsável pela observação constante de todo os eventos da rede e tem como objetivo contabilizá-los. A segunda categoria é relacionada ao controle, o qual pode ser definido como atividades que visam ajustar os parâmetros de rede para garantir seu desempenho.

Abrangendo as cinco áreas de gestão propostas pela ISO, o gerente possui grande controle sobre a rede. Dessa forma, ele é provido com informações relevantes que o auxiliam no monitoramento constante do comportamento do tráfego, facilitando a análise e o reconhecimento dos mais variados eventos que prejudicam o funcionamento correto da rede. Entretanto, devido ao montante de informações conferidas a partir desse processo, é inviável que se realize manualmente diagnósticos e se crie relatórios sobre o estado da rede, pois esta tarefa requer cada dia mais recurso humano especializado e maior esforço para ser completada.

O monitoramento da rede pode ser realizado de duas formas [10]. A abordagem passiva averigua o conteúdo trafegado na rede sem interferir no fluxo de dados, e consequentemente não prejudica o desempenho da mesma. Tal proposição analisa uma grande quantidade de informações, tornando-se um desafio restringir o volume de dados que são necessários para o gerenciamento. No monitoramento ativo ocorre a inserção e análise de pacotes de teste na rede. A dificuldade desse procedimento é adequar o volume de pacotes inseridos para realização dos testes e métricas desejadas sem que ocorra o acometimento dos recursos de rede.

Escolhido como o monitoramento deverá ocorrer, a origem dos dados se torna um fator importante a ser considerado. As fontes de informações utilizadas para o monitoramento do tráfego são essenciais para o sucesso da gerência de redes, visto que a eficiência das ferramentas de detecção de anomalias é dependente dos dados contidos nessas fontes. Desta forma, quanto maior a precisão das informações utilizadas para a modelagem do comportamento da rede, melhor será a detecção realizada pelo modelo escolhido para tal

propósito. Thottan e Chuanyi [10] estabelecem as diferentes fontes de onde podem ser obtidos os dados da rede. São elas:

- Sondas de rede: são ferramentas especializadas assim como *ping* e *traceroute* capazes de obter parâmetros de desempenho específicos da rede, por exemplo, atrasos de conexões e perda de pacotes.
- Estatísticas baseadas em fluxos usando filtragem de pacotes: essa abordagem realiza uma amostragem dos pacotes IP de fluxos, capturando as informações do cabeçalho. Os dados derivados dessa coleta são usados para o gerenciamento, pois proporcionam um conjunto extenso de atributos do tráfego, incluindo endereços IP de origem e destino, como também portas de origem e destino, *flags* de sinalização, entre outros.
- Dados oriundos de protocolos de roteamento: abordagens que seguem esse padrão podem obter informações sobre os eventos de rede através dos protocolos que atuam diretamente nas tabelas de roteamento. Tais informações podem ser utilizadas para análises baseadas na topologia da rede, uma vez que proporciona o monitoramento constante dos seus enlaces.
- Dados provenientes de protocolos de gerenciamento de redes: Esses protocolos têm a função de oferecer estatísticas sobre o tráfego de rede. Utilizam-se de variáveis que correspondem aos contadores do tráfego e são coletadas diretamente dos dispositivos. As informações são extraídas passivamente dos elementos de rede monitorados. Embora as informações originadas dessa fonte possam não representar diretamente uma métrica de desempenho da rede, é amplamente utilizada para caracterização do tráfego e, em consequência, para detecção de anomalias.

Para uma detecção de anomalias eficaz, a fonte de dados deve fornecer informações importantes para o monitoramento das atividades da rede e que auxiliem no reconhecimento dos comportamentos incomuns do tráfego. Dessa forma, observa-se o uso predominante de dados provenientes de protocolos de gerenciamento de redes e da abordagem usada para o desenvolvimento deste trabalho, estatísticas baseadas em fluxos de pacotes.

3.1 GERENCIAMENTO DE REDES UTILIZANDO SNMP

Segundo Thottan e Chuanyi [10], o SNMP (*Simple Network Management Protocol*) é classificado como um protocolo de aplicação capaz de fornecer informações destinadas à gerência de redes. Este protocolo obteve sucesso devido à sua rápida implantação e o fato de que, na maioria das vezes, ele funciona perfeitamente e é simples o suficiente para ser implementado na maioria dos dispositivos como *switch*, roteador, *hub*, interface WAN (*Wide Area Network*), entre outros. Foi idealizado para operar em grandes redes e está principalmente preocupado com monitoramento e isolamento de falhas [27].

O SNMP é baseado em uma interação gerente-agente, a qual atua seguindo o modelo cliente/servidor sobre o protocolo de transporte sem conexão UDP, embora o transporte sobre TCP e outros protocolos também seja possível. Normalmente, o agente coleta, em tempo real, dados do dispositivo no qual ele reside. O gerente controla os agentes para acompanhar o estado dos recursos monitorados. Dessa forma, pode-se definir o gerente como uma entidade que assume o papel operacional de gerar requisições para recuperar e modificar informações, cabendo a ele manipular as repostas às requisições transmitidas pelos agentes. Já o agente é considerado o elemento responsável por receber as requisições, providenciar o conteúdo exigido e encaminhá-lo ao gerente.

As informações de gerenciamento trocadas entre o agente e o gerente são armazenadas na MIB (*Management Information Base*), a qual armazena informações necessárias para o monitoramento da rede. Este repositório possui uma lista de variáveis, denominados de objetos gerenciados, e os seus respectivos valores. Os objetos gerenciados são definidos de acordo com a necessidade requerida para o monitoramento da rede, entretanto, alguns deles são obrigatórios de acordo com as especificações do próprio equipamento que abriga o agente.

De forma concisa, Perkins [28] estabelece que o modelo de gerência que utiliza o protocolo SNMP deve consistir dos seguintes elementos:

- Um ou mais elementos de rede gerenciados. Cada um desses deve estar empregando sua própria entidade agente;
- Um ou mais gerentes residentes em estações de gerência;

- Um protocolo de transporte utilizado pelos agentes e gerente para a troca de mensagens;
- Uma base de informações de gerenciamento denominada MIB, a qual descreve a configuração, estado, estatísticas e controle das ações do equipamento gerenciado.

O SNMP agiu como pioneiro no campo da gerência de redes, e rapidamente se tornou um padrão através da *Request for Comments* (RFC) 1157 [29]. Apesar da sua popularidade, alguns inconvenientes ainda eram encontrados, por isso, novas versões tiveram que ser implementadas para que o SNMP acompanhasse o crescimento das redes. Por exemplo, ao mesmo tempo em que é referenciada como uma vantagem, a simplicidade do SNMP muitas vezes é encarada como uma desvantagem. O modelo gerente-agente proporciona um simples entendimento e uma fácil interação entre os dispositivos gerenciados. Porém, à medida que as redes se tornaram robustas, esse modelo se tornou obsoleto para sua gestão, as quais já eram formadas por diversas sub-redes ou até mesmo outras redes distribuídas geograficamente.

A versão sucessora do SNMP, nomeada de SNMPv2 é documentada através da RFC 1905 [30]. Esse novo modelo estende seu antecessor com duas mudanças significativas. A primeira é o estabelecimento da comunicação M2M (*manager-to-manager*), propiciando que as entidades gerentes possam interagir entre si. A grande vantagem oferecida por essa modificação é a característica de criação de uma hierarquia de estações de gerenciamento. Dessa forma, cada sub-rede pode conter uma entidade gerente que se comunica com uma entidade de gerenciamento central, responsável por coordenar todos os equipamentos envolvidos na gerência baseada em SNMP. A segunda mudança está relacionada à segurança. Um esforço foi atribuído no emprego de técnicas criptográficas ao transmitir senhas de autenticação do gerente, dificultando a ação de intrusos. Além disso, o acesso aoss objetos gerenciados tornou-se mais difícil, prevenindo o acesso não autorizado.

Embora a segunda versão do protocolo SNMP tenha apresentado melhorias na segurança, estas foram consideradas discretas e muito progresso nessa área precisava ser feito. Por isso, a terceira versão do protocolo foi desenvolvida e sua documentação pode ser observada principalmente na RFC 3410 [31]. Grande enfoque foi dado à segurança de forma que o SNMPv3 passou a agregar privacidade, autenticação e controle mais rígido de acesso.

3.2 GERÊNCIA BASEADA EM ANÁLISE DE FLUXOS DE PACOTES

Atualmente, as ferramentas tecnológicas são as grandes responsáveis por propiciarem o aumento de produtividade nos diversos setores da sociedade. Com tal influência, elas devem ser otimizadas para que possam alcançar os objetivos para os quais foram desenvolvidas. Nesse contexto, podem ser citados os novos serviços de telecomunicações, multimídia e VoIP (Voz sobre IP, do inglês *Voice over* IP) que se tornam cada vez mais presentes nos mais variados meios de produção. Enquanto atuante deste processo, a qualidade dos serviços deve necessariamente estar relacionada ao gerenciamento de redes.

Com o surgimento dessas novas tecnologias, a demanda por técnicas inovadoras de monitoramento tornaram-se eminentes. A complexidade de tais serviços refletia diretamente na necessidade da análise de novos elementos e atributos gerenciados que apresentassem de forma mais detalhada os eventos de rede. Dessa forma, era necessário extrapolar as informações contidas nos contadores dos objetos SNMP, agregando uma vasta gama de dados que propiciariam ao administrador obter maior precisão em seus relatórios de monitoramento e diagnósticos de anomalias.

Dessa maneira, em resposta ao monitoramento das tecnologias emergentes, foi criada a gerência baseada em análise de fluxos de pacotes. Essa abordagem foi introduzida pela empresa Cisco Systems através do protocolo proprietário NetFlow, o qual se tornou um padrão pela adoção em diversos dispositivos de vários fornecedores. Outro protocolo utilizado para o mesmo propósito é o sFlow, criado pela empresa InMon. Pode ser definido como um acrônimo de *Sampling Flow*, isto é, amostragem de fluxos. Seu nome distingue a maior diferença em relação ao protocolo NetFlow: a amostragem de pacotes. A ideia básica do sFlow é fornecer um protocolo simples de exportação, capaz de operar em redes que atuam a taxas de transferências de 10 a 100 Gbp/s. Finalmente, o IPFIX (*Internet Protocol Flow Information Export*), definido na RFC 3917 [32], e tem como objetivo monitorar as aplicações consideradas de significativa importância hoje e para o futuro das redes IP. Este foi desenvolvido pela IETF, baseando-se na versão 9 do protocolo NetFlow.

Essas abordagens utilizam o agrupamento de pacotes com sessões de transmissões unidirecionais e que compartilham características como protocolo de transporte, endereços IP de origem e destino e portas [33]. A cada um desses agrupamentos é dado o

nome de fluxo. Desde que possam ser identificados pelas características em comum, os fluxos podem ser facilmente relacionados à uma aplicação, equipamento de rede ou usuário.

Tomando como base os protocolos de exportação NetFlow, IPFIX e sFlow é possível verificar elementos comuns utilizados no processo de monitoramento e coleta de fluxos. O primeiro deles são os sensores que têm a finalidade de capturar os pacotes, verificar a qual fluxo pertencem através do rastreamento de conexão com propriedades comuns e então submetê-los ao coletor. Os sensores são equipamentos de redes, geralmente *switches* ou roteadores, porém, *softwares* podem desempenhar esse papel desde que simulem as funções de tais dispositivos.

O gerenciamento baseado na análise de fluxos monitora o tráfego de forma passiva, portanto, um grande volume de informação é gerado. Sob esse aspecto, é primordial selecionar o tráfego que deverá ser verificado, implicando na localização em que se encontra o sensor. A abordagem mais simples consiste na implementação do sensor no *gateway* da rede, acarretando a análise de todo tráfego gerado por ela.

De acordo com Claise e Wolter [34], os seguintes benefícios podem ser atingidos utilizando a gerência baseada na análise de fluxos:

- Monitoramento da rede: O tráfego de rede pode ser analisado tanto individualmente para cada dispositivo como de forma agregada, reunindo todo o tráfego disponível. Esta característica contribui para o reconhecimento de problemas na arquitetura da rede ou na detecção de algum equipamento que apresente falhas.
- Monitoramento de aplicativos e perfis: Com as informações disponíveis através da análise de fluxos, é possível averiguar a quantidade de recursos utilizados por cada aplicação. Dessa forma, essas informações contribuem para a eficiência de alocação dos recursos para os usuários finais.
- Monitoramento de usuários e perfis: é possível observar a quantidade de recursos de rede que cada usuário utiliza e distribuí-los de acordo com a necessidade exigida por cada um. Além disso, relatórios detalhados podem ser realizados com a finalidade de apurar problemas de violação de políticas de segurança.

- Planejamento da rede: através de uma análise histórica do tráfego, auxilia na expansão da rede. Essa característica assegura que observando o tráfego é possível fazer projeções de escalabilidade, garantindo a qualidade de serviço (QoS) e a disponibilidade da rede.
- Análise de segurança: Visualizando alterações no tráfego de rede é possível identificar anomalias como ataques distribuídos de negação de serviços DDoS (*Distrituted Denial of Service*), *worms* e vírus em um intervalo próximo ao tempo real. Ainda, usando o histórico do tráfego, podem-se assimilar os comportamentos dos eventos maliciosos através da sucessão de modificações que estes causam aos atributos monitorados.
- Armazenamento: Os fluxos armazenados podem posteriormente ser utilizados para extração de comportamentos e criação de perfis de uso da rede. Além de fornecer informações quanto o uso de recursos, os registros de fluxos têm um papel fundamental na segurança através da detecção de anomalias e eventos incomuns.

Ao se comparar as informações fornecidas pelo protocolo SNMP e as disponibilizadas pelos protocolos de exportação de fluxos, pode-se concluir que a gama de informações fornecida pelos protocolos IPFIX, NetFlow e sFlow é mais extensa. Esse conjunto de informações permite ao administrador verificar a origem, destino, duração e a aplicação utilizada na comunicação de *hosts*. Além disso, utilizando o SNMP, todos os dispositivos que se deseje monitorar devem possuir um agente em funcionamento. Com a análise de fluxos, apenas um coletor em um ponto de observação específico é necessário para realização dessa tarefa. As próximas seções descrevem o funcionamento dos principais protocolos de exportação de fluxos usados para o gerenciamento de redes.

3.2.1 NetFlow

Desenvolvido por Darren Kerr e Barry Bruins na empresa Cisco Systems em 1996, o NetFlow figura como a primeira tecnologia de medição e exportação de fluxos utilizada na gerência de redes [1]. Seu desenvolvimento se deu em resposta às novas exigências colocadas diante aos operadores de rede, principalmente a compreensão do comportamento do tráfego da rede de forma mais detalhada do que já era possível com o uso do protocolo SNMP. A solução foi a criação do NetFlow, que possibilitaria o monitoramento dos seguintes aspectos:

- Uso da rede e de aplicações;
- Utilização de recursos de rede;
- O impacto das mudanças na rede;
- Anomalias e vulnerabilidades de segurança;
- Questões de configurações e seus efeitos.

O NetFlow atende a essas necessidades, criando um ambiente onde os administradores têm as ferramentas para descobrir quem, o quê, quando, onde e como o tráfego da rede está sendo transmitido. Segundo a empresa Cisco [35], quando o comportamento da rede é conhecido, sua gestão melhora e uma trilha de auditoria pode ser estabelecida. Este aumento de compreensão sobre o uso da rede reduz o risco em relação à interrupção e permite o seu funcionamento pleno. Além disso, melhorias na operação das redes geram menores custos, pois garantem melhor utilização da sua infraestrutura.

Cada pacote encaminhado a partir de um roteador ou *switch* tem seu conjunto de atributos do cabeçalho IP verificado, como demonstrado na Figura 3.1. Esses atributos identificam se o pacote é único ou similar a outros. O NetFlow verifica as seguintes características dos pacotes:

- Endereço IP de origem;
- Endereço IP de destino;
- Porta de origem;
- Porta de destino;
- Protocolo da camada de transporte;

- Classe de serviço;
- Interface do roteador ou *switch*;

Todos os pacotes com os mesmos endereços IP de origem e destino, portas de origem e destino, protocolo, interface e classe de serviço são agrupados em um fluxo e então o tráfego é processado. Essa metodologia tem o propósito de ser escalável, pois o grande volume de informações derivados do monitoramento passivo da rede pode ser resumido dentro de uma base de dados do NetFlow, denominada *cache*. Caso algum pacote contenha um valor diferente para algum desses atributos em relação aos fluxos ativos na *cache*, este pacote se torna o primeiro de um novo fluxo.

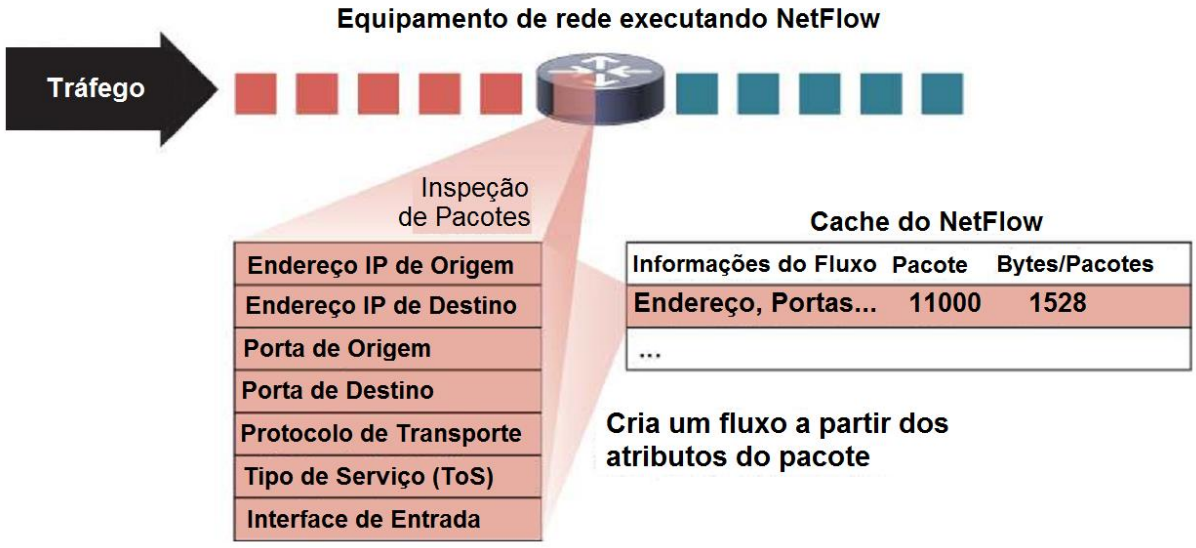

Figura 3.1 - Verificação dos atributos de fluxos usando o protocolo NetFlow. Adaptada de [1].

As informações atribuídas aos endereços IP identificam os usuários envolvidos na transmissão, ao passo que, as portas especificam as aplicações utilizadas para essa finalidade. A prioridade do tráfego é verificada a partir da análise da classe de serviço, enquanto que a interface de entrada mostra como os dados estão sendo utilizados pelo dispositivo de rede. Finalmente, as informações processadas como quantidade de pacotes e bytes, especificam o volume de tráfego transmitido.

Algumas informações extras são acrescentadas aos fluxos após sua criação. São elas:

- *Timestamp*: compreende o tempo de vida de um fluxo. Esse atributo é útil para calcular o total de pacotes e bytes transmitidos em certa unidade de tempo;
- *Flags* do protocolo TCP: usadas para sinalizar o processo *handshake;*
- Máscaras de sub-rede: usadas para cálculo de prefixos.

3.2.1.1 Arquitetura do NetFlow

A arquitetura dos serviços providos pelo protocolo NetFlow pode ser classificada em três grupos distintos: pré-processamento, funções e pós-processamento [33], como mostrado na Figura 3.2.

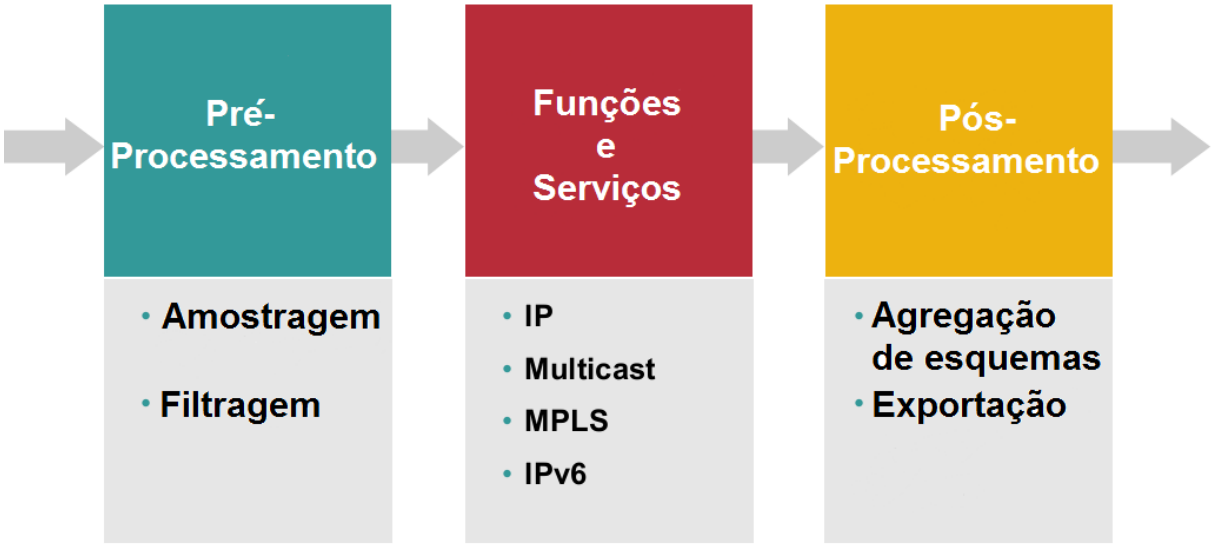

Figura 3.2 - Arquitetura de funcionamento do protocolo NetFlow da Cisco.

O pré-processamento engloba funções de filtragem e seleção de elementos amostrais do tráfego. A última versão do NetFlow (versão 9) disponibiliza funções e serviços que propiciam a medição de diversos tipos de tráfegos, como elementos *multicast*, originários de VLANs (*Virtual Local Area Networks*) ou encapsulados por meio do MPLS (*Multiprotocol Label Switching*). Por fim, o pós-processamento permite, basicamente, a manipulação da

maneira pela qual os fluxos são exportados, ou seja, como as informações do fluxo de pacotes são capturadas e enviadas ao coletor.

De maneira simples, o controle do monitoramento executado pelo NetFlow segue algumas etapas. A primeira consiste na criação de fluxos na cache. Uma política de tempo de vida útil de cada fluxo pode ser implementada, consolidando a segunda etapa. No passo seguinte é verificado se questões especiais de junção de fluxos devem ser levadas em consideração. Em caso afirmativo, a agregação entre os registros de fluxos será executada na cache de agregação. Finalmente, quando os fluxos estiverem aptos a serem exportados, o protocolo NetFlow verifica a versão da exportação (5, 7, 8 ou 9) e a definição do protocolo de transporte para comunicação com o coletor.

O tamanho da cache do NetFlow pode ser definido por meio de *software* e varia de 1024 a 524 mil entradas de registros de fluxos. Cada fluxo consome uma quantidade mínima de memória de aproximadamente 64 bytes. O número máximo de registros suportado pela cache está diretamente ligado à quantidade de memória física contida pelo sensor de gerenciamento.

Um ponto importante para o NetFlow conseguir escalabilidade e um desempenho considerável corresponde ao uso de algoritmos que gerenciam de forma eficiente a utilização da cache, especialmente para uso em roteadores de borda, no qual grande número de pacotes são trafegados e há fluxos de curta duração. As regras para determinar quando um fluxo NetFlow expira são as seguintes:

- Fluxos inativos durante certo intervalo de tempo são removidos da cache. O tempo definido como padrão é de 15 segundos podendo ser configurável para o período de 10 a 600 segundos;
- Fluxos ativos são expirados e removidos da cache quando atingem 30 minutos. Se a conexão que gerou o fluxo ainda estiver em atividade, será criado um novo fluxo para contabilizar essa transmissão.
- Após o preenchimento completo da cache NetFlow, políticas de exclusão de fluxos são postas em prática para o armazenamento de novos registros.
- Conexões TCP com as *flags* FIN ou RST são expiradas. Tais *flags* marcam o fim do fluxo associado à sessão TCP ativa na cache NetFlow.

À medida que os fluxos são expirados, são agrupados em um datagrama NetFlow Export para serem exportados para o coletor. No NetFlow v9, até trinta registros de fluxos podem compor o datagrama de exportação.

A Figura 3.3 demonstra um datagrama de exportação usado pelo NetFlow versão 9. Esta versão se difere das anteriores por apresentar um modelo (*template*) que apresenta o conjunto de informações contido nos registros, sendo os fluxos associados ao seu modelo.

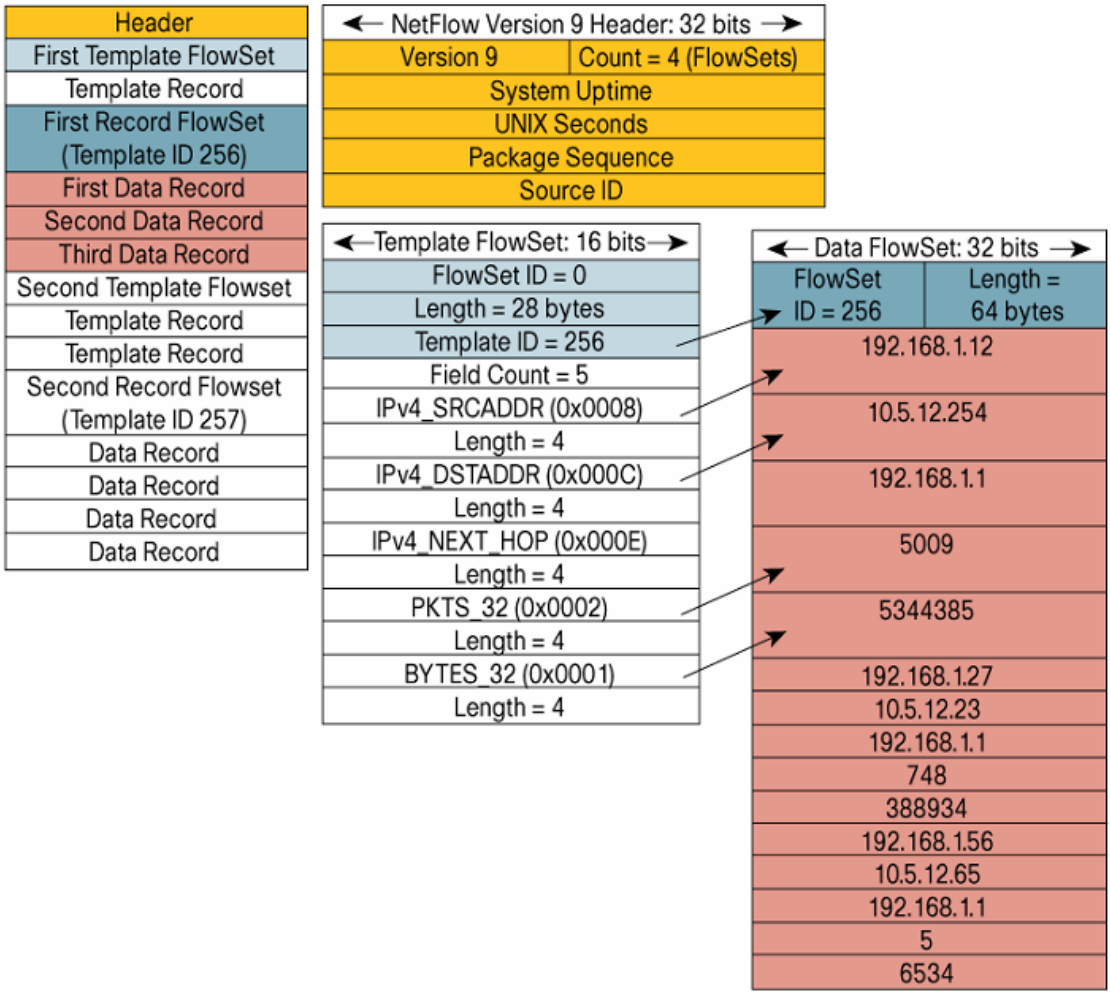

Figura 3.3 - Datagrama usado pelo NetFlow v9 para exportação de registros de fluxos. Retirado de [36].

Os dados de um conjunto de fluxos (*Data FlowSet*) representam um conjunto de registros de fluxos com base nas definições de um modelo e suas opções que descrevem a estrutura desses registros. A Figura 3.4 apresenta o exemplo de três registros de fluxos a serem exportados, os mesmo que estão contidos no pacote apresentado na Figura 3.3. São eles:

End. IP Origem	End. IP Destino	Endereço próx. salto	Pacotes	Bytes
198.168.1.12	10.5.12.254	192.168.1.1	5009	5344385
192.168.1.27	10.5.12.23	192.168.1.1	748	388934
192.168.1.56	10.5.12.65	192.168.1.1	5	6534

Figura 3.4 - Registros de fluxos que compõe o *Data FlowSet* do exemplo.

Os modelos usados para exportação apresentam as informações estruturais sobre os campos dos registros de fluxos e são usados pelos coletores para determinar onde e qual informação será gravada do registro de fluxo recebido. A utilização do conceito de registros de dados, baseados em modelos é que trouxe a flexibilidade ao protocolo para definição dos formatos de registros de forma arbitrária, com base nas necessidades dos clientes. Esta solução garante versatilidade na exportação, uma vez que, pode-se criar um modelo exclusivo para enviar mensagens do protocolo SIP (*Session Initiation Protocol*), ou informações de endereços IPv6. Dessa forma, o administrador não fica restrito aos atributos padrões fornecidos pelo NetFlow, podendo criar um modelo que possua informações que ele considere necessárias.

Após definidos pelos modelos, os registros de fluxos podem ser inseridos nos pacotes de exportação em qualquer ordem. Os datagramas de exportação podem apresentar: modelos de fluxos, conjunto de registros ou ainda a combinação de ambos. Todos os modelos devem ser armazenados pelo coletor e utilizados pelos registros de fluxos por meio da associação garantida pelo atributo do pacote *template ID.* Na Figura 3.3 é mostrado o esquema de exportação pela associação entre os registros de fluxos e os modelos definidos pelos campos*: template ID* = 256 e *FlowSet ID* = 256.

3.2.2 Internet Protocol Flow Information Export (IPFIX)

O IPFIX foi desenvolvido com o intuito de substituir os protocolos proprietários destinados ao monitoramento de redes através da exportação de fluxos. Dessa forma, atua por meio de sensores e coletores que processam e armazenam dados relevantes para o gerenciamento das redes. A IETF tem concentrado seus esforços para a padronização do IPFIX desde 2002 e, através da RFC 3917 [32], os requisitos que nortearam o grupo de trabalho para criação do novo protocolo foram definidos.

Dentre as especificações iniciais, a RFC 3917 destaca os requisitos para geração de fluxos. Estes devem ser criados a partir de pacotes que não possuam criptografia, em que as informações dos campos do cabeçalho possam ser facilmente analisadas. Isto implica na identificação do sentido dos fluxos a partir dos sensores que monitoram as interfaces de entrada e saída dos dispositivos de rede. Outro fator é a capacidade de criação de fluxos com base em atributos como endereços IP de origem e destino, tipo de protocolo, portas e até mesmo a versão do endereço IP em uso (IPv4 ou IPv6). Os requisitos ainda estipulam que os sensores devem oferecer suporte ao protocolo MPLS (*Multiprotocol Label Switching*) e a codificação Diffserv durante a criação e análise dos fluxos.

Ainda sobre as especificações, o item 5 da RFC 3917 trata do processo de medição do IPFIX. Tal processo tem a capacidade de reconhecer divergências entre o que foi recomendado para sua execução e a sua real eficiência. Durante o processo de medição as ferramentas de amostragens incluem abordagem sistemática ou seleção aleatória de uma amostra derivada de uma população previamente estipulada. Neste tópico ainda é assumida a responsabilidade do processo de medição de reconhecer comportamento de sobrecarga das suas atividades, a fim de mitigar tal problema por meio da diminuição das tarefas realizadas.

A respeito dos requisitos de exportação dos fluxos, ficou estabelecido que os *templates* utilizados para esse propósito devessem ser extensíveis, ou seja, apresentar os atributos gerenciados da rede de acordo com a necessidade do gerente. Além disso, a comunicação necessária para que os datagramas IPFIX fossem enviados ao coletor necessitaria apresentar confiabilidade, segurança e controle de congestionamento.

A partir dos requisitos mencionados, a IETF decidiu verificar alguns protocolos candidatos, buscando a conformidade com as características requeridas. Participaram da avaliação também os sistemas *Common Reliable Accounting for Network Element Protocol* (CRANE), Diameter, LFAP e Streaming IPDR, porém, através da RFC 3955, foi decidido que o NetFlow v9 se tornaria a base para as definições do protocolo IPFIX.

Assim como no NetFlow v9, os fluxos podem ser exportados de forma não segura, parcialmente segura ou totalmente segura através dos protocolos UDP (User Datagram Protocol), PR-SCTP (*Partial Reliability* SCTP) e SCTP (*Stream Control Transmission Protocol*), respectivamente. Uma peculiaridade inserida ao IPFIX é a capacidade de utilizar o protocolo TCP para transmissões seguras. Dessa forma, os sensores devem ser capazes de exportar dados a múltiplos coletores usando os diferentes protocolos de transportes mencionados.

A análise dos pacotes que chegam aos sensores é realizada observando-se sequencialmente, um-a-um. Entretanto, essa análise pode passar a ser feita através de conjuntos amostrais. Isso decorre do fato da sobrecarga que pode ocorrer nos sensores, os quais são responsáveis por criar, manter e exportar os fluxos. Dessa forma, considerando que o tratamento da sobrecarga é um requisito primordial para o IPFIX, a análise amostral se tornou um aspecto fundamental, permitindo que o monitoramento prossiga mesmo com a sobrecarga do sensor. Para isso, o IPFIX faz o uso do protocolo PSAMP (*Packet Sampling*) para extensão do seu modelo de informação relacionado aos processos de amostragem.

Os sistemas de amostragem definidos pelo protocolo PSAMP [37] são os seguintes: amostragem sistemática baseada em contagem, amostragem sistemática baseada em temporização, amostragem aleatória n-para-N, amostragem probabilística uniforme, amostragem baseada em regras de filtros e amostragem baseada em filtros de hash.

A amostragem sistemática baseada em contagem extrai os pacotes dos fluxos sequencialmente, em uma forma pré-definida. Dessa forma, um número de pacotes é estabelecido e a cada vez que a contagem de pacotes passantes em um sensor atinge esse valor, o pacote correspondente é amostrado. A amostragem sistemática baseada em temporização tem funcionamento similar, porém, diferencia-se da baseada em contagem por apresentar o parâmetro relacionado ao tempo. A cada intervalo pré-definido um pacote é amostrado. Essa última abordagem age independente da coleta independente da quantidade de pacotes, categoria ou tamanho.

No modelo de amostragem aleatória n-para-N um campo amostral sequencial de pacotes é criado, e sobre esse é realizada a coleta de amostras. Dessa forma, para valores $n = 1$ e $N = 10$, um pacote aleatório do conjunto sequencial de 10 pacotes é coletado.

A amostragem probabilística uniforme realiza o cálculo de probabilidade para cada pacote observado pelo sensor. Um determinado pacote é selecionado caso sua probabilidade atinja um valor superior a um parâmetro anteriormente definido. A amostragem baseada em regras de filtros coleta os pacotes que possuem o valor de um campo do pacote igual ao parâmetro previamente estabelecido. Já a amostragem baseada em filtros de hash calcula o hash do cabeçalho IP de todos os pacotes, e aqueles que apresentarem valores dentro de limites definidos são coletados.

Durante o desenvolvimento do IPFIX, tendo como base o NetFlow v9, a nomenclatura dos componentes da sua arquitetura foram definidas da seguinte maneira:

- Ponto de observação: representa um local da rede em que os pacotes podem ser visualizados. Pode ser único ou agregar vários outros pontos de observação;
- Processo de medição: atividades pertencentes a esse processo têm a finalidade de gerar os registros de fluxos. Atua analisando os cabeçalhos dos pacotes no ponto de observação. Suas funções ainda se estendem a: capturar pacotes, calcular *timestamps*, realizar amostragem, classificar e manter os registros de fluxos.
- Registro de fluxos: Responsável por armazenar as propriedades de medidas dos fluxos analisados no ponto de observação. Tais propriedades estão definidas na RFC 5102 [38] e incluem total de bytes, pacotes, endereços IP de origem e destino, portas de origem e destino, entre outras características.
- Processo de exportação: transmite os registros de fluxos para um ou mais coletores.
- Processo de coleta: constitui as atividades realizadas pelo coletor. Tarefas como recebimento dos registros dos processos de exportações e armazenamento dos fluxos estão inclusas nessa categoria.

3.2.3 sFlow

O nome sFlow é um acrônimo para *Sampling Flow*, isto é, amostragem de fluxos. Esse protocolo pode ser definido como uma tecnologia inserida nos roteadores e switches, a qual propicia a eles a capacidade de monitoramento constante do tráfego transmitido simultaneamente por todas as interfaces.

A arquitetura usada para o monitoramento passivo através da amostragem é detalhada na RFC 3176 [39]. Neste documento, são abordadas as principais características que devem ser asseguradas quando o recurso de amostragem está em uso: a precisão no monitoramento das redes de alto desempenho usando a estipulação de parâmetros dinâmicos que configuram a amostragem; escalabilidade, a qual indica a competência em se gerenciar

diversos sensores através um único ponto central. Por fim, é desejável que possua baixo custo computacional para sua operação.

O sistema de monitoramento do tráfego previsto pelo sFlow consiste em um sensor, denominado agente sFlow, o qual é intrínseco ao equipamento de rede, e um coletor central de dados. O agente possui a função de monitorar o tráfego e gerar os dados sFlow utilizando técnicas de amostragem e enviá-las ao coletor. O coletor é representado como uma aplicação que analisa o conteúdo recebido e gera as métricas necessárias para o gerenciamento da rede, como demonstrado na Figura 3.5.

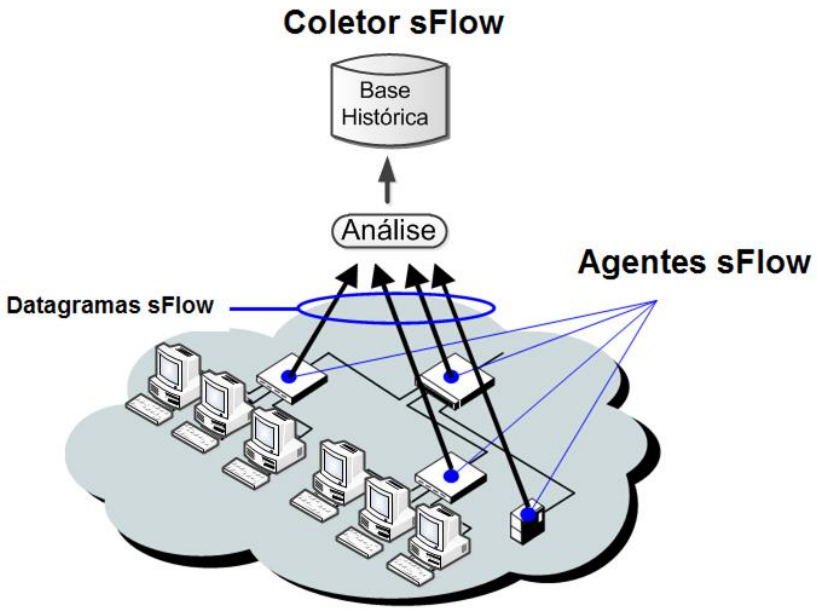

Figura 3.5 – Componentes e funcionamento do protocolo sFlow. Adaptada de [40].

O sFlow disponibiliza duas técnicas de amostragem para o tráfego de redes. A primeira é a amostragem estatística baseada em pacotes. Quando um pacote chega a uma interface do agente sFlow, o processo de filtragem é realizado, no qual é decidido se tal pacote deverá ser encaminhado à uma interface ou será descartado. Neste momento também é determinado se o pacote é amostrado. Os pacotes de um fluxo devem apresentar as mesmas chances de serem amostrados. O processo ainda conta com um contador que é decrementado a cada pacote analisado e, caso nenhum destes tenha sido amostrado, quando o contador chegar à zero, uma amostra deve necessariamente ser retirada do tráfego.

Esse processo envolve dois contadores. O *Total_Packets* é incrementado a toda verificação de um pacote, enquanto o contador *Total_Sample* define o número de pacotes

que foram amostrados. A taxa de amostragem é calculada através da divisão do total de pacotes analisados pelo número de amostras capturadas do tráfego.

A segunda técnica de amostragem utiliza contadores baseados no tempo. Essa abordagem faz com que cada contador possua informações específicas sobre os atributos monitorados da rede (*bytes*, pacotes e erros), e que periodicamente esses dados sejam atualizados. Para garantir a escalabilidade da amostragem, são criados contadores de sondagem (*polling)* nos agentes sFlow. Embora um valor máximo para o intervalo de sondagem seja estipulado, cada agente pode ajustar esse parâmetro para garantir a eficiência do protocolo.

Embora a amostragem por contadores seja diferente da amostragem baseada em pacotes, o gerente de rede não precisa optar entre a exportação de uma dessas abordagens. Isso decorre do fato de que o sFlow emprega simultaneamente ambas técnicas.

A amostragem, embora amplamente utilizada no monitoramento atualmente, só obteve ampla aceitação com o crescimento das taxas de transmissão das redes, as quais passaram de comutadas por circuito para comutadas por pacotes. A primeira empresa a utilizar amostragem baseada em pacotes foi a Hewlett Packard (HP), na Universidade de Genebra e no CERN.

Segundo [40], usando sFlow para monitorar continuamente os fluxos de tráfego em todas as portas, é possível conseguir visibilidade de todo uso da rede. Esta visibilidade substitui a adivinhação, mudando fundamentalmente a maneira como os serviços de rede são gerenciados. Além disso, o monitoramento sFlow de redes tem as seguintes propriedades:

- Acurácia: Por ser simples o suficiente para ser executada em *hardware*, a amostragem, não interfere no desempenho da rede. Além disso, sua simplicidade não prejudica a sua precisão no monitoramento do tráfego, ao contrário de abordagens que necessitam de maior custo computacional para serem executadas;
- Detalhamento: Através da análise completa do cabeçalho do pacote, incluindo informações de roteamento e encaminhamento, o sFlow proporciona um monitoramento eficiente desde a camada de enlace até a de aplicação;
- Escalabilidade: O sFlow se mostra eficaz no monitoramento de redes com 10Gbps, 100Gbps e de velocidades superiores. Outra

característica de destaque é a capacidade de que um único coletor pode monitorar milhares de equipamentos simultaneamente;

- Baixo custo: o agente sFlow é muito simples de ser implementado e induz um custo computacional ínfimo a um switch ou roteador;
- Conveniência: sFlow proporciona o monitoramento constante. Dessa forma, informação oportuna é importante para o fornecimento do controle da rede em tempo real, por exemplo, para gerenciar a qualidade dos serviços ou para defesa contra um evento malicioso.

3.3 CONSIDERAÇÕES SOBRE O CAPÍTULO

A operação de uma rede requer respostas às situações tais como falhas, congestionamento, e a qualidade inaceitável do serviço. Estas questões incluem a solução de problemas, ajustes na configuração dos equipamentos e o monitoramento de fluxos de tráfego. Para compreender a complexidade desta tarefa, é importante notar que o comportamento da rede é definido pela interação de diferentes dispositivos, vários segmentos, diferentes configurações e recursos. Desse modo, objetivando auxiliar o processo de gerência de redes, tornando menos difícil o seu controle, diversas ferramentas e protocolos foram criados.

O desenvolvimento de técnicas e modelos que contribuíssem com a gerência das redes, durante muito tempo, foi quase exclusivamente focado sobre o protocolo SNMP. Desde a sua introdução, este protocolo de monitoramento procurou apresentar maior visibilidade possível do comportamento da rede para os seus gerentes. Como consequência, diversas melhorias foram incluídas, fazendo com que esse protocolo se tornasse uma referência no campo de gerência de redes. Porém, concomitantes ao aprimoramento do SNMP, houve muito mais mudanças de comportamento e uso da rede nas últimas décadas. O surgimento de aplicações em tempo real, VoIP, vídeo conferência, VPNs, computação em nuvem, por exemplo, tornou evidente que uma nova ferramenta para entender o fluxo de dados e gerenciar as redes seria necessária.

Os protocolos que utilizam a análise fluxos são uma alternativa recente ao SNMP. Entre as principais que representam esse abordagem, podem ser citadas o NetFlow, sFlow e IPFIX. Com essas ferramentas, os gerentes de rede obtêm informações necessárias

para compreender a composição do tráfego, não somente a utilização de um enlace ou o volume de dados transmitidos como quando usado o SNMP. Grande parte do detalhamento do tráfego é derivada da variedade de atributos fornecido pela observação de fluxos de pacotes.

No capítulo seguinte será apresentada a abordagem de detecção de anomalias desenvolvida neste trabalho. A análise realizada pelo sistema ocorre simultaneamente em sete dimensões, ou atributos, do tráfego de rede. Para que isso seja possível, dados provenientes de protocolos de exportação de fluxos são utilizados. No capítulo 5 são demonstrados resultados de detecção e classificação de eventos anômalos a partir do tráfego coletado pelos protocolos sFlow e NetFlow.

4 SISTEMA DE DETECÇÃO DE ANOMALIAS ACODS

A detecção de comportamentos anômalos no tráfego de rede é uma atividade importante para seu gerenciamento e controle. Proença *et al.* [21] observaram que o tráfego é formado por comportamentos cíclicos, os quais são diretamente afetados pelo período de uso da rede. Um dos principais objetivos deste trabalho é o reconhecimento desses comportamentos e suas características para a criação de uma assinatura digital de segmentos de rede. Tal assinatura é responsável por abrigar informações sobre o comportamento do tráfego normal, sendo adotado para detecção de anomalias através do reconhecimento de desvios comportamentais que destoam do habitual.

Este capítulo descreve as principais etapas realizadas para a construção do sistema ACODS. A primeira delas é a definição de um perfil de comportamento, denominado *Digital Signature of Network Segment using Flow analysis* (DSNSF), o qual compreende as características da rede que podem ser adotadas como um padrão normal de tráfego. Para que isso seja possível, é apresentada uma modificação da metaheurística *Ant Colony Optimization* (ACO), chamada *Ant Colony Optimization for Digital Signature* (ACODS). Na abordagem apresentada, o ACODS atua otimizando o processo de clusterização, o qual é responsável por extrair os comportamentos e características do tráfego da rede.

Após a caracterização do tráfego, a abordagem de detecção de comportamentos anômalos é discutida. Esta fase é responsável por analisar o perfil de comportamento normal descrito pela assinatura digital para determinar se ocorrem diferenças em relação às amostras coletadas a partir do tráfego monitorado. Tanto a caracterização do tráfego, isto é, a criação da assinatura digital quanto o reconhecimento de comportamentos anômalos são duas etapas de execução distintas do sistema. Cada uma delas pode ser observada na Figura 4.1, em que é possível compreender as atividades que limitam seus escopos.

4.1 ARQUITETURA DO SISTEMA

O primeiro módulo do sistema realiza a extração de características dos atributos de fluxo analisados para geração do DSNSF. Estes dados são obtidos através do

tráfego histórico da rede, armazenados em um coletor de fluxo IP. Devido à diferença semântica da informação armazenada em cada atributo, é necessário realizar um pré-processamento. Os atributos descritivos armazenam informações qualitativas (endereço IP e porta), diferente dos atributos de volume. Assim, é necessário utilizar a entropia para medir o grau de dispersão desses atributos e assegurar que os seus comportamentos sejam representados por um valor quantitativo.

No segundo módulo, o DSNSF gerado pelo ACODS é comparado com o tráfego real a ser analisado. Com o intuito de promover uma detecção ao mesmo tempo eficiente e flexível, a abordagem *Adaptive Dynamic Time Warping* (ADTW) é utilizada. Usando esta técnica, o comportamento esperado para cada um dos sete atributos é examinado de modo a identificar padrões de tráfegos que diferem do especificado pelo DSNSF. Além disso, um classificador de anomalias para melhorar o reconhecimento de comportamentos incomuns é proposto. Esta rotina analisa o desvio comportamental dos atributos de fluxo durante a ocorrência de eventos anômalos e classifica-os de acordo as assinaturas previamente conhecidas pelo sistema. Assim, a combinação da ADTW com o classificador minimiza as taxas de falsos alarmes, não sobrecarregando o administrador de rede com notificações desnecessárias.

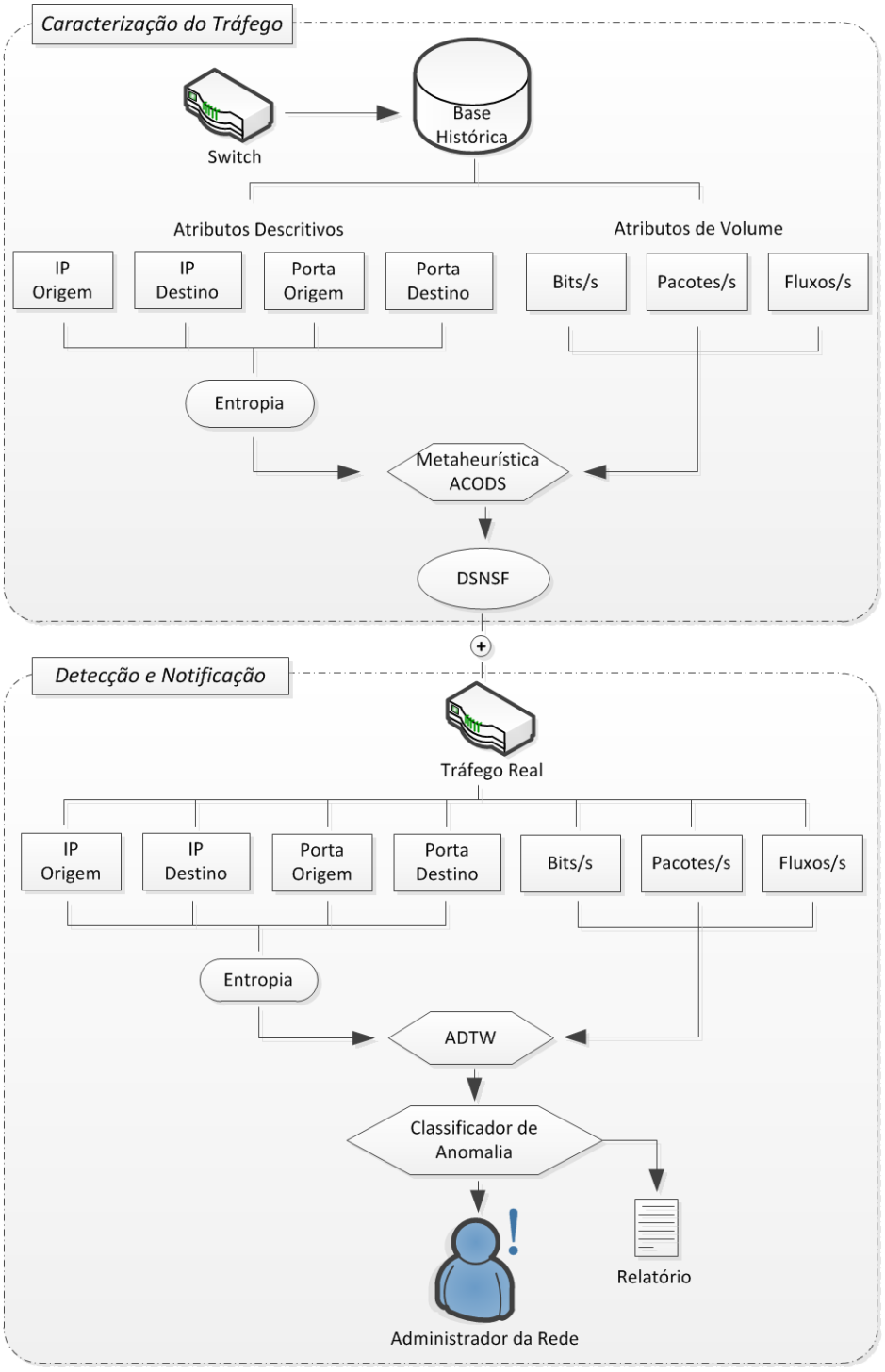

Figura 4.1 - Visão geral do sistema. A delimitação dos módulos ocorre de acordo com a finalidade das atividades realizadas no processo de detecção de anomalias.

O segundo módulo ainda engloba a geração de relatórios que fornecem informações sobre a utilização da rede. Os dados são apresentados em forma de estatísticas demonstrando qual a situação dos recursos do tráfego durante a detecção de um evento anômalo, facilitando a elaboração de uma contramedida capaz de combater tal atividade ou mitigar suas consequências.

Os módulos de caracterização do tráfego e detecção de anomalias são detalhados nas seções seguintes.

4.2 MÓDULO DE CARACTERIZAÇÃO DO TRÁFEGO

Nesta subseção são apresentados os conceitos envolvidos na caracterização do tráfego e como eles são empregados para a criação da assinatura digital. Inicialmente, o pré-processamento dos fluxos coletados é detalhado, bem como o uso da medida de entropia para quantificar a utilização de portas e endereços IP. Em seguida, é apresentada a essência do processo de clusterização, utilizada para a o reconhecimento de padrões normais do tráfego. Logo após, a modificação da metaheurística *Ant Colony Optimization* utilizada para otimizar a extração de padrões é detalhada, assim como a atribuição de parâmetros para que essa tarefa seja realizada eficientemente.

4.2.1 Pré-Processamento dos Dados

Levando-se em conta a caracterização do tráfego, logo após os dados serem coletados, é necessário realizar a extração dos atributos de fluxos utilizados para criação do DSNSF. Essa etapa é necessária para garantir que sejam utilizadas somente as características do tráfego que auxiliam a abordagem de detecção de anomalias, evitando o aumento da complexidade e ineficiência do sistema em redes de larga escala.

O primeiro conjunto de atributos apresenta informações relativas ao volume do tráfego, em que são coletados dados referentes à quantidade de *bits*, pacotes e fluxos transmitidos por segundo. Atributos de volume já eram utilizados para detecção baseada na gerência de objetos SNMP, porém, com a introdução do segundo conjunto de atributos, composto por endereços IP e portas, uma maior riqueza de detalhes do tráfego foi conseguida. A análise desses últimos atributos garante maior acurácia na detecção e classificação de anomalias, uma vez que, muitos desses eventos causam mudanças significativas na distribuição desses atributos. A Figura 4.2 ilustra os registros de fluxos contidos na base de dados que foram previamente coletados por um protocolo de exportação de fluxos.

	Date flow start	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes
2	2012-11-05 00:00:03.727	TCP	190.80.8.6:49380	->	189.90.64.141:443	256	17408
3	2012-11-05 00:00:03.727	TCP	189.76.43.249:49353	->	189.90.65.144:80	256	17408
4	2012-11-05 00:00:03.727	TCP	199.101.132.41:80	->	189.90.65.11:11100	256	389632
5	2012-11-05 00:00:03.727	TCP	72.246.216.55:1935	->	10.90.31.58:63741	256	389632
6	2012-11-05 00:00:03.727	TCP	72.246.216.55:1935	->	10.90.31.58:63741	256	389632
7	2012-11-05 00:00:06.896	TCP	62.115.247.72:80	->	189.90.74.216:62585	256	367104
8	2012-11-05 00:00:06.896	TCP	200.221.7.95:80	->	189.90.65.11:8407	256	17408
9	2012-11-05 00:00:06.896	TCP	187.37.25.39:51545	->	189.90.67.66:80	256	18944
10	2012-11-05 00:00:06.896	TCP	66.196.118.36:25	->	189.90.65.151:58416	256	18944
11	2012-11-05 00:00:06.896	TCP	157.55.56.142:443	->	10.90.63.246:49269	256	18432
12	2012-11-05 00:00:11.722	TCP	72.246.216.55:1935	->	10.90.31.58:63741	256	389632

Figura 4.2 - Exemplo de registros de fluxos utilizado pelo pré-processamento.

De acordo com Lakhina *et al.* [41], cada tipo de anomalia afeta de forma diferente a distribuição de determinados atributos do tráfego. Por exemplo, a distribuição dos endereços de origem se torna mais dispersa durante um ataque DDoS ou a distribuição de portas pode ser alterada quando elas são verificadas para encontrar vulnerabilidades. Ainda, quando uma grande quantidade de informações é recebida de um determinado endereço, a distribuição se torna mais concentrada para o atributo endereço de origem. Seguindo essa ideia, é apresentada a Tabela 4.1, a qual lista um conjunto de anomalias frequentemente encontradas em um tráfego de *backbone* e os efeitos causados aos atributos de fluxos.

Tabela 4.1 - Exemplos de anomalias e atributos de tráfego afetadas por elas. Adaptado de [41] [42].

Anomalia	Breve Descrição	Atributos do Tráfego Afetados
Flash Crowd	Grande quantidade de tráfego para um único destino	Endereço de destino, porta de destino e atributos de volume.
DoS	Tem o objetivo de tornar um recurso indisponível para seus usuários, inundando-o com inúmeras requisições.	Endereço de origem, endereço de destino e atributos de volume.
DDoS	Um ataque DoS realizado por várias origens	Endereço de origem, endereço de destino, portas de origem e destino e alguns atributos de volumes.
Port Scan	Muitas requisições enviadas para diferentes portas a partir de um número limitado de endereços de origem	Endereço de origem, endereço de destino, porta de destino e alguns atributos de volumes.
Eventos de interrupção	Tráfego é comprometido pela falha ou manutenção de equipamentos	Principalmente endereços IP e atributos de volume.

Os atributos utilizados para verificar a dispersão do tráfego são diretamente retirados do cabeçalho dos pacotes IP e correspondem a: endereço IP de origem, endereço IP de destino, porta de origem e porta de destino. Porém, devido à grande diversidade do tráfego, é necessário abordar um método que sumarize o comportamento desses atributos para facilitar a detecção de anomalias. Dessa forma, é utilizada a métrica de entropia proposta por Shannon, a qual determina o grau de concentração ou dispersão da distribuição dos atributos abordados. Para o seu cálculo, é necessário criar um histograma a partir de amostras de cada atributo. Dado o atributo $X = \{n_1, \dots, n_i, \dots, n_N\}$, em que n_i representa a quantidade de ocorrências da amostra i, a entropia para X é definida como mostra a Equação 4.1.

$$H(X) = -\sum_{i=1}^{N} \left(\frac{n_i}{S}\right) log_2 \left(\frac{n_i}{S}\right) \tag{4.1}$$

em que $S = \sum_{i=1}^{N} n_i$ é o total de todas as ocorrências presentes no histograma. Quando as distribuições das amostras estão concentradas, o valor da entropia é ínfimo, sendo zero quando todas as amostras são idênticas. De forma contrária, quanto mais próximo de $log_2 N$, maior é o grau de dispersão, atingindo esse valor quando $n_1 = n_2 = \cdots = n_N$.

4.2.2 Clusterização

Para a caracterização do tráfego, os atributos são dispostos em uma 7-upla composta pelos atributos de volume seguidos das entropias calculadas para endereços de origem e destino, e portas de origem e destino, respectivamente. Cada uma dessas 7-uplas é denominada de objeto ou elemento no processo de clusterização, pois representa um único ponto no espaço de pesquisa.

A clusterização é uma ferramenta de mineração de dados (do inglês, *data mining*) utilizada para encontrar e quantificar semelhanças entre objetos de um determinado conjunto de dados. Este processo procura minimizar a variância entre os elementos de um conjunto, denominado cluster, e maximizá-la em relação aos demais grupos [43]. Assim, o resultado desta abordagem é a configuração de grupos, em que um elemento do conjunto de dados é mais semelhante aos dados do seu grupo, do que qualquer outro.

Um ambiente de clusterização é tipicamente definido como: Dado um conjunto de E elementos, $X = \{X_1, X_2, \dots, X_E\}$, é desejável criar K clusters $C = \{c_1, c_2, \dots, c_K\}$, em que os dados pertencentes a um cluster c_j, qualquer, sejam mais similares entre eles do que a outro cluster c_l pertencente a C. Enfim, pode-se considerar que C é um agrupamento de X com K clusters, caso as seguintes condições forem satisfeitas:

$$\bigcup_{j=1}^{K} c_j = X \tag{4.2}$$

$$c_j \neq \emptyset, \text{em que } 1 \leq j \leq K \tag{4.3}$$

$$c_j \cap c_h = \emptyset, 1 \leq j, h \leq K \; e \; j \neq h \tag{4.4}$$

A Equação (4.2) indica que todos os elementos do conjunto de dados devem participar do processo de agrupamento. A Equação (4.3) determina que nenhum cluster deve ser nulo, ou seja, cada conjunto necessita abrigar pelo menos um elemento a ser clusterizado. Finalmente, a última condição aponta a necessidade de que cada objeto pertença exclusivamente a um grupo, como mostrado na Equação (4.4). Desse modo, a clusterização ajuda a promover o conhecimento sobre o conjunto de dados, uma vez que a abordagem de agrupamento agindo como um processo de aprendizado não supervisionado em elementos não rotulados permite a extração de padrões, comportamentos e características quantitativas e qualitativas.

Devido à importância estratégica de agrupamento em muitos campos, vários algoritmos foram propostos na literatura para resolver problemas de clusterização [44] [45] [46]. Tal processo pode apresentar complexidade exponencial quando o número de clusters é alto e tornar-se um problema NP-difícil. Para solucionar essa inconveniência, modelos heurísticos têm se tornado cada vez mais populares nas técnicas de clusterização. Sistemas baseados em métodos heurísticos utilizam de mecanismos que exploram amplamente o espaço de soluções, fazendo com que as chances do encontro de uma solução ótima sejam maiores. Outro aspecto importante dos modelos heurísticos é a capacidade de convergência dos resultados mais rápida do que por métodos convencionais, por exemplo, algoritmos determinísticos. Essa propriedade é mais evidente ao passo que o problema analisado se torna mais complexo computacionalmente.

4.2.3 Metaheurística Ant Colony Optimization

O estudo sobre a auto-organização de colônias de formigas teve início a partir dos trabalhos desenvolvidos pelo pesquisador Jean-Louis Deneubourg. Pesquisas sobre esse tópico propiciaram a criação dos *Ant Algorithms,* uma coleção de métodos computacionais baseados em observações de comportamentos de colônia de formigas. Em Deneubourg *et al.* [47], é destacado um experimento de bastante importância na criação de tais algoritmos denominado *double bridge experiment* ou experimento da ponte dupla, realizado sobre uma colônia de formigas argentinas.

O teste foi realizado separando a colônia do local que abrigava os alimentos por duas pontes de mesmo tamanho, como mostra a Figura 4.3(a). Nesse cenário, as formigas começam a explorar os arredores da colônia depositando feromônio até atingirem a fonte de alimento. Inicialmente cada formiga escolhe aleatoriamente uma das pontes para seguir, depositando feromônio ao longo do trajeto. Entretanto, depois de algum tempo, um dos caminhos se torna mais atraente para as formigas que estarão por vir, uma vez que o acúmulo dessa substância nessa ponte será maior. Essa situação implica na convergência de toda a colônia sobre esse trajeto, preferencialmente o mais curto.

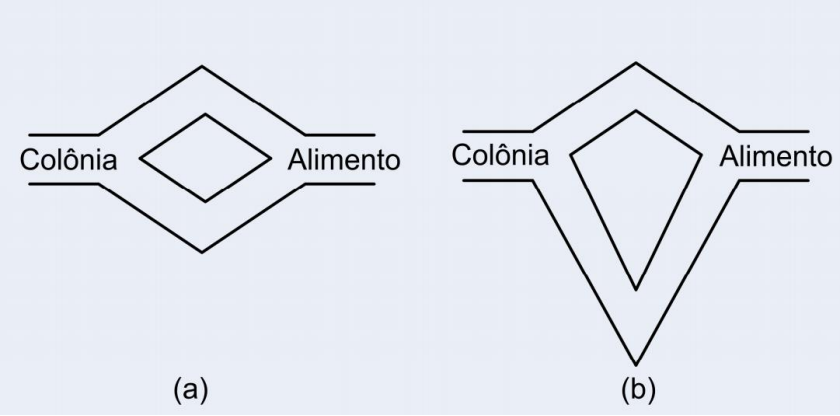

Figura 4.3 - Experimento da ponte dupla. Adaptado de [47].

Outro teste relatado por Deneubourg é uma variante do experimento ponte dupla. Neste caso, as pontes apresentam tamanhos diferentes, como representado na Figura 4.3(b). As formigas que escolheram aleatoriamente o caminho mais curto tendem a chegarem mais rapidamente ao alimento e voltar à colônia. Com isso, pode-se inferir que o menor

trajeto receberá maior concentração de feromônio em um tempo menor, tornando-se cada vez mais provável de ser tomado pelas demais formigas.

Seguindo esse princípio, no início da década de 90, Marco Dorigo desenvolveu a metaheurística *Ant Colony Optimization* (ACO). Projetada para solucionar problemas complexos de otimização [48], já recebeu várias modificações e versões para atender as exigências e peculiaridades dos problemas aos quais foi submetida. No entanto, a ideia e os propósitos iniciais sempre se mantiveram [49].

Além de ser classificada como *Ant Algorithm*, a metaheurística ACO pertence ao grupo denominado inteligência de grupo (do inglês, *Swarm intelligence*), o qual consiste em um conjunto de metodologias e técnicas relativamente novas que vêm ganhando importância na solução de problemas computacionais. Trabalhos desenvolvidos nessa área são inspirados no comportamento de grupos de animais ou agentes que vivem em sociedade e apresentam as seguintes características:

- Uma comunicação indireta não simbólica mediada pelo ambiente, ou seja, os agentes modificam as informações ao passo que modificam o ambiente ao seu redor;
- Essa comunicação é local, podendo ser observada somente por agentes próximos ou que passarem pelo ponto modificado.

Os algoritmos compreendidos pela técnica *Swarm Intelligence* são amplamente utilizados em clusterização e mineração de dados. Este campo de estudo lida com sistemas artificiais compostos por muitos indivíduos que são coordenados de forma descentralizada e que possuem a propriedade de auto-organização. Em particular, a pesquisa ocorre sobre os comportamentos coletivos que resultam das interações locais dos indivíduos com o outro e com o seu ambiente. Outros exemplos de sistemas estudados pela *Swarm Intelligence* são colônias de cupins, cardumes de peixes, bandos de pássaros, rebanhos de animais terrestres, entre outros.

Assim como as demais metaheurísticas, ACO é um conjunto de estratégias e algoritmos que têm a busca da solução direcionada por conjuntos de informações exclusivas do problema. Faz uso de escolhas baseadas em processos estocásticos, verificando as informações adquiridas de resultados anteriores para se orientarem ao longo do espaço de pesquisa [49]. O experimento da ponte dupla demonstra perfeitamente que as colônias de formigas possuem a capacidade de se organizarem e de construírem soluções ótimas. É

possível, portanto, a implementação de formigas artificiais capazes de se movimentar por um grafo construído como no experimento, a fim de que estas possam encontrar um menor caminho até o objetivo, ou seja, construir uma solução otimizada para um dado problema.

4.2.3.1 Similaridades e Diferenças entre as Formigas Reais e os Agentes Artificiais

O funcionamento do ACO é pautado no comportamento de agentes reais. A modelagem computacional dos membros de uma colônia de formigas tornou possível a criação dessa metaheurística, que é atualmente um robusto método de resolução de problemas que exigem soluções otimizadas.

A metaheurística *Ant Colony Optimization* é composta de uma população de agentes concorrentes e assíncronos globalmente, cooperando para criar uma solução para o problema tratado. Embora cada formiga possua capacidade de construir uma boa solução, tal qual uma formiga no mundo real pode encontrar de alguma forma um caminho entre o ninho e a comida, soluções mais promissoras são obtidas a partir da cooperação entre todos agentes da colônia.

Assim com as formigas reais, os agentes artificias alteram certas propriedades do ambiente em que estão inseridos. Segundo Dorigo *et al*. [50], enquanto formigas depositam feromônio pelo trajeto que caminham, os agentes alteram informações numéricas armazenadas localmente, as quais têm a função de descrever o estado das soluções para o problema tratado. Estas informações são adquiridas através do histórico e desempenho do agente na construção da solução.

No ACO, as informações que descrevem o progresso da construção de soluções são armazenadas na trilha de feromônio. Essa estrutura atua como canal de comunicação entre os agentes e somente eles têm acesso à trilha, isto é, somente as formigas possuem privilégios de leitura e modificação dos dados numéricos contidos nas trilhas locais. Com a mudança de valores da trilha de feromônio, os agentes modificam a forma como o ambiente (a situação do problema) é localmente percebido pelas formigas em função de todo o histórico da colônia.

Um importante componente do ACO é o mecanismo de evaporação de feromônio, semelhante ao que ocorre com a substância real. Esta característica permite que agentes esqueçam lentamente o seu histórico de soluções, a fim de que possam orientar sua

busca para novas direções sem ser limitadas por decisões passadas, evitando o problema de convergências precipitadas que podem gerar soluções não tão ótimas.

Diferentemente da movimentação contínua desenvolvida pelas formigas reais, os agentes do ACO caminham de forma discreta entre os vértices do grafo do campo de soluções. A simplicidade do movimento é explicada pela necessidade das formigas artificiais armazenarem as decisões tomadas a cada iteração. Em toda mudança de estado ocorre o processamento das novas informações recebidas e a modificação das já existentes até dado momento.

Os agentes são capazes de realizar tarefas difíceis, como encontrar o caminho mais curto para uma fonte de comida, organizar sua colônia, sincronizar seus movimentos como uma entidade coerente única com alta velocidade. Essas tarefas são mais representativas já que são realizadas sem a presença de uma entidade centralizada para controlar o movimento, por exemplo, a rainha da colmeia [51]. Assim, o ACO torna-se um processo de aprendizagem distribuída no qual um agente não se adapta ao problema, mas altera o modo como os demais agentes vão agir para construir suas soluções.

Uma diferença entre a formiga real e a artificial é que a última utiliza uma função determinante da quantidade de feromônio a ser depositada no trajeto. Esta função é calculada utilizando o valor de quão boa é a solução encontrada até o momento [48]. Isto é, quanto mais atraente for o trajeto para os agentes, maior será o estímulo exercido sobre eles, forçando-os a depositar elevadas quantidades de feromônio.

4.2.4 Criação da Assinatura com o *Ant Colony Optimization for Digital Signature*

Segundo Jiang *et al.* [52], o hábito da colônia de formigas de viver em conjuntos é essencialmente semelhante ao agrupamento de dados. Algoritmos baseados no comportamento das formigas têm vantagens naturais na aplicação da análise de clusters. Com isso, espera-se encontrar um ambiente de agrupamento ideal que otimize a distância entre os objetos e o centro do cluster (centróide) ao qual estão associados.

Assim sendo, os benefícios oferecidos pela metaheurística ACO são utilizados para a criação do ACODS (*Ant Colony Optimization for Digital Signature*), uma modificação da metaheurística original para a geração do DSNSF usando a abordagem de clusterização. O modelo apresentado é capaz de caracterizar o tráfego da rede, classificando-o

em grupos a partir dos dados de entrada. Para este propósito, assume-se que os caminhos do grafo, por onde as formigas caminham, são formados entre o centro de um grupo e cada elemento que irá ser agrupado.

O ACODS é executado de forma iterativa, ou seja, devem haver critérios explícitos de parada durante a execução do programa. O sistema pode ser encerrado de duas formas. A primeira diz respeito à qualidade das soluções geradas. Quando não há diferença entre as melhores soluções criadas em três iterações consecutivas, o sistema interrompe o processo iterativo, pois a colônia convergiu para criação de um único agrupamento de dados. A segunda maneira ocorre quando o limite de 100 iterações é atingido, impedindo que a execução do ACODS ocorra indefinidamente. Esse valor se mostrou suficiente para a convergência das soluções durante a geração dos DSNSFs avaliados no capítulo 5. As atividades realizadas em cada iteração podem ser divididas em três grupos:

- **Construção de soluções:** Esta etapa consiste no movimento simultâneo das formigas e de forma assíncrona por parte dos estados do problema. É determinado por agentes que se deslocam de um vértice para outro vizinho na estrutura do grafo;
- **Busca Local:** Destina-se a testar e avaliar soluções criadas pelas formigas através de uma busca local. Se a informação heurística sobre um domínio de problema particular não é facilmente alcançada, a busca local pode ajudar a construir boas soluções [53]. No modelo apresentado, esta atividade é usada para remover porções não promissoras das soluções;
- **Atualização do feromônio:** Este é o processo em que a trilha de feromônio é modificada. Os valores da trilha podem ser incrementados (quando formigas depositam feromônio nas arestas entre os vértices usados) ou pode ser diminuído. O aumento da concentração de feromônio é um fator essencial para a implementação do algoritmo, uma vez que direciona as formigas a buscar novos locais mais propensos a adquirir uma solução ideal.

O ACODS apresentado neste trabalho tem como objetivo otimizar a eficiência da clusterização, minimizando o valor da função objetivo J, definida pela Equação (4.5). Em outras palavras, pretende-se criar soluções para o agrupamento de dados de uma maneira que permita a extração de padrões, comportamentos e características do tráfego.

Assim, essa abordagem garante que cada elemento i será agrupado ao melhor cluster j. Além disso, permite a construção de soluções que não são dadas por ótimos locais, que é um problema recorrente em muitos algoritmos de clusterização.

$$J = \sum_{i=1}^{E} \sum_{j=1}^{K} \sqrt{\sum_{a=1}^{A} (x_{ia} - c_{ja})^2} \tag{4.5}$$

A Equação 4.5 é utilizada para mensurar quão boa é a solução criada por um agente. O valor correspondente ao seu resultado é a distância entre cada elemento i em relação ao centro do cluster ao qual pertence. Quanto menor o valor de J, melhor é a solução. Nessa equação, a variável E corresponde ao total de elementos a serem clusterizados e A indica a dimensionalidade dos dados, ou seja, a quantidade de atributos de fluxos que um elemento contém. Para a confecção do DSNSF os elementos adquiridos após o pré-processamento do tráfego são avaliados a cada intervalo de dez segundos, totalizando 8640 conjuntos de resultados ao longo do dia. A variável x_{ia} denota o valor do atributo a do elemento i, enquanto c_{ja} armazena o valor do centro do cluster j na dimensão a.

A operação do algoritmo ACODS utilizado para a clusterização é dividida em seis passos:

Passo 1: A trilha de feromônio τ é iniciada com pequenos valores aleatórios;

Passo 2: Cada formiga seleciona um objeto i;

Para determinar a associação de um cluster j a um objeto i e construir o vetor solução R, duas abordagens podem ser seguidas. A primeira permite que as formigas se movam de forma gananciosa para um vértice cujo produto do nível de feromônio e o valor heurístico sejam mais elevados. A situação é descrita pela Equação (4.6)

$$j = \left\{ max_{j \in N_i} \left\{ [\tau(i,j)]^{\alpha} [\eta^k(i,j)]^{\beta} \right\} \; se \; q \leq q_0, \right. \tag{4.6}$$

em que q_0 é um valor de probabilidade pré-definido, enquanto q é uma probabilidade gerada aleatoriamente. N_i representa o conjunto de vértices vizinhos a i e que correspondem a um cluster. A outra maneira é a verificação de todas as possibilidades de movimentos. A formiga

poderá escolher qual o melhor caminho, averiguando o vértice que apresentar maior probabilidade de ser selecionado. O cálculo da probabilidade é demonstrado pela Equação (4.7).

$$P^k(i,j) = \frac{[\tau(i,j)]^\alpha [\eta^k(i,j)]^\beta}{\sum_{j=1}^{K} [\tau(i,j)]^\alpha [\eta^k(i,j)]^\beta} \tag{4.7}$$

O resultado da equação acima é a probabilidade da formiga k atribuir o objeto i ao cluster j. O termo $[\tau(i,j)]^\alpha$ representa a trilha de feromônio entre o elemento i e o centro do cluster j, mensurando quão boa é essa ligação para a solução do problema. Já à $[\eta^k(i,j)]^\beta$ cabe quantificar a função heurística da formiga k, calculando o inverso da distância Euclidiana entre o elemento i e o centro do cluster j.

Passo 3: Verificar a solução R de cada formiga. Caso R(k) não esteja completo, o agente deverá selecionar um novo elemento i e recomeçar o processo do ponto 2;

Passo 4: Calcular a função objetivo $J(k)$ para cada agente usando a Equação (4.5). Logo após, deve-se ordenar de forma crescente os resultados computados. A solução que apresentar menor valor para a função objetivo é considerada a melhor solução da iteração. Esta é comparada com a melhor solução encontrada durante toda a execução e, caso possua o valor da função objetivo menor, é adotada como melhor solução da execução até o momento;

Passo 5: Atualizar as trilhas de feromônio. Esta etapa tem um papel importante na construção da solução final, porque direciona os agentes na busca de novas soluções usando caminhos promissores encontrados anteriormente. Os L caminhos mais utilizados são reforçados, ou seja, as ligações entre elemento-cluster que mostraram melhores resultados são intensificadas e devem ser usadas na construção de soluções cada vez melhores. Em contraste, as piores ligações elemento-cluster estão condenadas a serem esquecidas pelo algoritmo através do processo de evaporação do feromônio. A Equação (4.8) descreve a atualização do feromônio.

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(t) + \sum_{l=1}^{L} \Delta\tau_{ij}^{l} \tag{4.8}$$

Para a equação de atualização de feromônio (4.8) é definida uma constante ρ, a qual descreve a taxa de evaporação de feromônio e tem valor $\rho \in (0,1]$. A variável t identifica a iteração corrente. A quantidade de feromônio $\Delta\tau_{ij}^{l}$ depositado na ligação entre *i* e *j* é calculada tomando-se o inverso de J, dividido pelo número de elementos a ser agrupado, E.

> **Passo 6:** A última etapa consiste em verificar se o limite de iterações foi excedido. Em caso negativo, o algoritmo volta à execução a partir do passo 2. Quando o critério de parada é satisfeito ou o limite máximo de iterações é atingido, a execução é concluída e a melhor solução encontrada pelo algoritmo é retornada.

Essas etapas podem ser resumidas através do pseudo-código apresentado no Algoritmo 1. O resultado desse algoritmo descreve a combinação dos grupos mais representativos do ambiente clusterizado. Para obter o valor de X_{ta}, a média ponderada é calculada entre os grupos no instante t, tal como mostrado na Equação (4.9). Assim, o resultado estará mais próximo do cluster com o maior número de elementos, ou seja, daquele que melhor representar o comportamento dos dados coletados em intervalos de dez segundos.

$$X_{ta} = \frac{\sum_{j=1}^{K} c_{ja} p_j}{E} \tag{4.9}$$

De acordo com a Equação (4.9), c_{ja} é o valor central do cluster j na dimensão a e p_j é a quantidade de elementos associados ao conjunto de mesmo índice. Ao final da execução do algoritmo, uma matriz X de dimensões 8640×7 é retornada, ou seja, o DSNSF.

Algoritmo 1 - ACODS usado para criação do DSNSF

Entrada: Conjunto de atributos de volume e dos campos do cabeçalho do pacote coletados a partir de uma base de dados histórica, número de clusters, número máximo de iterações *I*.
Saída: Matriz compreendendo o DSNSF, na qual as linhas representam os intervalos de tempo (10 segundos) enquanto as colunas contêm os valores calculados para cada atributo no período de tempo correspondente.

1: **PARA** $t = 1$ **ATÉ** 8640 **FAÇA**
2: **PARA** *i* = 1 **ATÉ** ***I*** **OU** condição de parada não for satisfeita **FAÇA**
3: Criar solução
4: Avaliar solução utilizando a função objetivo
5: Atualizar a trilha de feromônio
6: **FIM-PARA**
7: Calcular o centro de cada cluster da melhor solução encontrada
8: **PARA** $j = 1$ **até** *K*
9: **SE** total de elementos no cluster $c_j < \gamma$ **ENTÃO**
10: descartar o cluster c_j
11: **FIM-SE**
12: **FIM-PARA**
13: **PARA** $\boldsymbol{a = 1}$ **até** $\boldsymbol{A}$
13: $X_{ta} \leftarrow$ média ponderada entre os clusters na dimensão a (Equação (4.9))
14: **FIM-PARA**
15: **Retornar** *X*

Após a clusterização, os grupos de dados são formados. Devido aos padrões de comportamento do tráfego de rede, muitas informações apresentam características semelhantes. Assim, os clusters formados por pequenas quantidades de dados que divergem muito do padrão devem ser rejeitados da construção da assinatura. Para tanto, é definido um limite γ, o qual determina a proporção mínima permitida de elementos agrupados em um cluster. Se algum grupo apresentar menos elementos associados a si do que o estipulado por γ, este é retirado da solução final, bem como elementos pertencentes a ele. Esta etapa compõe a estratégia de busca local, o que garante o mínimo envolvimento possível de tráfego anômalo na composição da assinatura.

Usando a eliminação de grupos menos representativos, o DSNSF pode descrever o padrão observado no conjunto de dados sem seguir qualquer tendência em especial, ressaltada em algum dos dias utilizados para sua criação. Além disso, a busca local garante que as alterações no DSNSF sejam suaves e só constituam um padrão no caso de muitas ocorrências desses certos comportamentos.

Um DSNSF, responsável por caracterizar o tráfego durante o período de 24 horas para os 7 atributos analisados, é gerado para cada dia da semana a partir de informações provenientes da base histórica de semanas anteriores. Assim, a assinatura é automaticamente

ajustada ao comportamento do tráfego através da introdução de novos comportamentos a cada semana. A importância da base histórica está diretamente relacionada à abordagem de busca local. Assumindo que um comportamento está presente na maioria dos dias analisados e se apresenta periodicamente, certamente será adicionado ao DSNSF. Caso contrário, pode ser caracterizado como um evento pontual, e a sua inclusão no padrão normal implicaria em numerosos falsos alarmes durante a detecção de anomalias.

Uma fragilidade da detecção baseada em perfis é que as anomalias podem ser lentamente introduzidas no padrão normal até que se tornem um evento legítimo. No entanto, a abordagem apresentada neste trabalho resolve essa limitação, oferecendo ao administrador informações relevantes que contribuem com a solução de tal problema. Desta forma, se esses eventos anômalos são interrompidos durante sua ação, não são incluídos na base histórica e, consequentemente, eles não irão compor o perfil de comportamento normal da rede.

4.2.5 Parâmetros Usados para a Caracterização do Tráfego

Quando se utiliza uma metaheurística, os valores das variáveis envolvidas devem ser calibrados, pois grande parte do sucesso na busca de soluções depende deles. A fim de garantir uma caracterização de tráfego eficiente e manter o ACODS com um desempenho desejável para realização dessa tarefa, os valores de alguns atributos foram previamente definidos. Esses valores foram configurados através de testes exaustivos, variando-se os valores entre os limites aceitáveis para a obtenção de bons resultados. Os testes para as variáveis que serão demonstradas apresentam grande significância para o trabalho aqui desenvolvido. Aqueles simplesmente referenciados não possuem importância menor, porém já foram amplamente estudados e discutidos na literatura.

4.2.5.1 Parâmetros do ACODS

O valor γ é representado por 5% da quantidade de elementos a serem clusterizados em cada iteração. Esse valor é ideal para a abordagem de busca local, o que

pode ser comprovado através dos resultados numéricos dos cenários no capítulo de testes. A intenção do uso desse parâmetro é produzir um sistema com o mínimo de supervisão humana possível. Portanto, como a base histórica analisada durante a criação do DSNSF pode conter eventos que não correspondem ao comportamento usual da rede, cabe à abordagem de busca local julgar se eles comporão a assinatura digital.

O parâmetro ρ tem uma função importante durante a execução do ACODS. Ele é responsável por ajustar o tempo de convergência das soluções através da evaporação do feromônio. Seu valor não pode ser demasiadamente pequeno, uma vez que a convergência se tornaria imediata, não permitindo que outras soluções possam ser verificadas. Por outro lado, valores acentuados para esse parâmetro tornam a convergência lenta, exigindo um número maior de iterações, o que é inviável para uma aplicação utilizada em redes de alto desempenho. Neste trabalho, é assumido o valor $\rho = 0{,}1$ para a taxa de evaporação do feromônio. Esse valor foi atribuído analisando a influência desse parâmetro na construção de soluções. O mesmo valor pode ser conferido em outros trabalhos [43] [54].

Os últimos parâmetros são relacionados aos agentes criadores de soluções. O número de formigas é definido como 15% do total de elementos a serem clusterizados. Cada agente cria sua própria solução durante a iteração, porém somente as L melhores vão receber incremento de feromônio. O valor atribuído a esse último parâmetro corresponde a 20% das soluções criadas a cada iteração, assegurando que a busca das soluções seja direcionada às mais promissoras. Os mesmos valores são assumidos por Shelokar *et al*. [53], os quais enfatizam que a utilização de parâmetros em proporção aos dados de entrada é um passo fundamental para a criação de um sistema mais autônomo.

4.2.5.2 Parâmetros de validação de clusters

Uma vez finalizado o processo de clusterização, é interessante verificar a disposição dos clusters criados, bem como avaliar o número adequado de grupos utilizados para a manipulação do conjunto de dados. Dois métodos são aplicados para esse propósito. O primeiro é o Índice Dunn [55], cujo objetivo é identificar o conjunto de clusters que estão compactos e melhor separados. Dessa forma, as soluções para o agrupamento apresentam melhores resultados quando a distância entre os clusters é grande, enquanto as distâncias dos elementos em relação ao centro do grupo ao qual pertencem são pequenas. Essa medida é

calculada através da razão entre a distância mínima intracluster e a distância máxima intercluster como demonstrado pela Equação (4.10).

$$\delta = \frac{d_{min}}{d_{max}}, \tag{4.10}$$

em que d_{min} corresponde a menor distância entre dois elementos de diferentes clusters, enquanto d_{max} define a maior distância entre dois objetos pertencentes ao mesmo cluster. O índice Dunn pode assumir valores no intervalo $0 \leq \delta < \infty$, e quanto maior esse valor, melhor clusterizado está o conjunto de dados.

O segundo método utilizado para a validação e interpretação dos clusters neste trabalho é o Silhouette [56]. Esta métrica proporciona uma representação gráfica do agrupamento de dados, permitindo a análise dos elementos dentro dos grupos. Os principais requisitos para a sua construção são: i) a obtenção de um particionamento dos dados, utilizando uma técnica de clusterização e ii) uma medida de proximidade entre os objetos do conjunto de dados. Assim, o gráfico Silhouette é útil quando a métrica de aproximação é apresentada em uma escala (como no caso da distância Euclidiana) e quando grupos compactos e claramente separados são procurados. Os gráficos da Figura 4.4 apresentam testes com diferentes valores de *K* utilizando o método Silhouette.

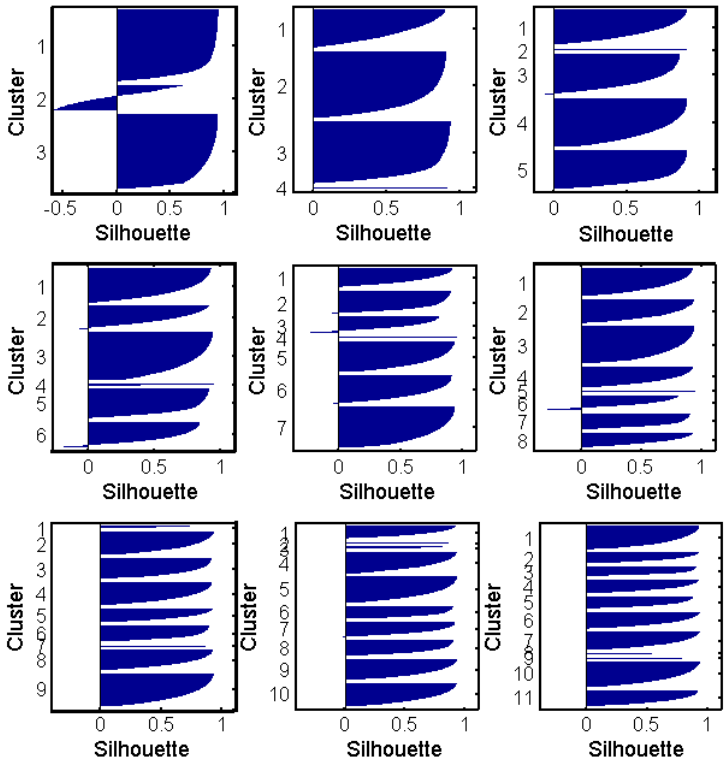

Figura 4.4 - Validação do número de clusters usando o método gráfico Silhouette.

Nos gráficos da Figura 4.4 o eixo y apresenta o número de centros K, utilizados para a clusterização, e o eixo x, o valor da função de Silhouette. Cada elemento i a ser clusterizado recebe o valor $-1 \leq s(i) \leq 1$ correspondente à função Silhouette, calculada em relação ao cluster ao qual pertence. De acordo com o valor dessa função, três situações distintas podem ser observadas. Quando $s(i)$ está próximo a 1, a semelhança entre o elemento i e outros objetos pertencentes ao mesmo cluster é grande. Assim, o elemento está bem agrupado e foi associado corretamente a um conjunto. Quando este valor tende a zero, há um caso intermediário no qual o elemento poderia ser atribuído a mais de um grupo. A pior situação ocorre quando $s(i)$ se aproxima do valor -1. Neste caso, o objeto i foi mal classificado e deve ser associado a outro grupo. A função Silhouette $s(i)$ é calculada como demonstrado pela Equação (4.11).

$$S(i) = \frac{b(i) - a(i)}{\max[a(i), b(i)]} \tag{4.11}$$

Dada a Equação (4.11), $a(i)$ representa a dissimilaridade média entre i e todos os demais elementos do mesmo cluster, como mostrado pela Equação (4.12). Enquanto isso, $b(i)$ corresponde à dissimilaridade média entre o elemento i e os demais elementos dos outros grupos.

$$a(i) = \frac{1}{E-1}\sum_{e=1}^{E} d(i,e) \quad \forall\, i \neq e \tag{4.12}$$

De acordo com a equação, E representa a quantidade de elementos pertencentes ao cluster em que o objeto i está associado. A distância Euclidiana entre os elementos i e e é descrita por $d(i,e)$.

Como pode ser observado pelo gráfico Silhouette da Figura 4.4, muitos elementos são agrupados aos clusters erroneamente utilizando $K < 9$. Para esses valores de K, é possível observar elementos com uma associação com $S(i)$ próximo a 1, mas o volume de dados associado a cada cluster é mínimo, de maneira que não torna interessante a classificação dos elementos, criando centros com poucos dados agrupados no seu entorno.

O gráfico mostrado na Figura 4.5 apresenta o resultado da validação do número de clusters necessários para caracterizar corretamente o comportamento da rede. Para essa finalidade, são expostos os valores dos testes de Índice Dunn e Silhouette para cada

configuração de K. Ambos os métodos de avaliação foram aplicados aos conjuntos de dados utilizados para treinamento e avaliação do sistema ACODS.

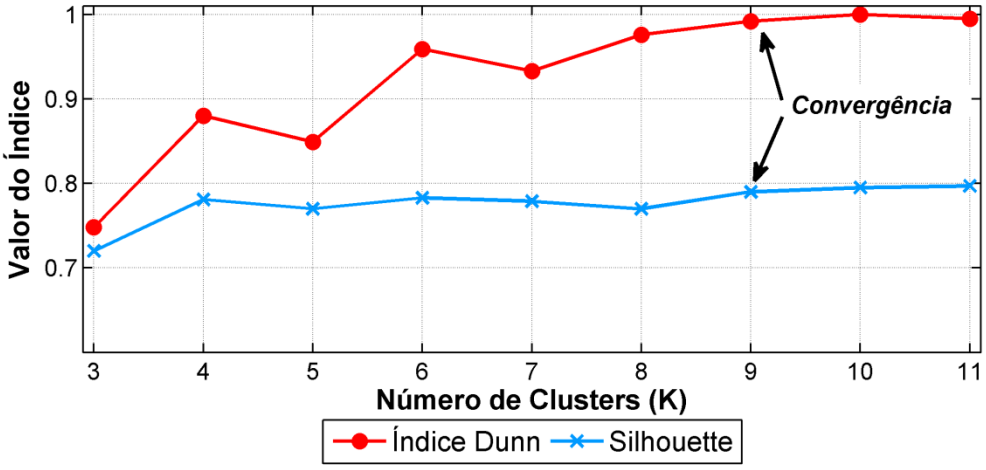

Figura 4.5 - Avaliação do número de clusters utilizado para extração de padrões do comportamento do tráfego. É possível observar a convergência dos valores a partir de $K \geq 9$.

Os valores obtidos pelo teste Silhouette apresentam pouca variação entre os diferentes valores assumidos pelo parâmetro K, pois neste gráfico é apresentada a média dos valores de $s(i)$ dos elementos clusterizados. Entretanto, em ambos os testes, resultados semelhantes são encontrados, indicando que, aproximadamente 9 a 11 grupos são necessários para reconhecer e classificar os diferentes comportamentos de tráfego. São mínimas as variações entre as medidas em relação à quantidade de clusters mencionada, fazendo com que ocorra uma convergência de resultados para essa faixa de valores. Dessa maneira, levando-se em consideração que o valor de K tem influência direta no desempenho do sistema, o número de clusters foi atribuído como o mínimo necessário para se obter boas soluções, mantendo a complexidade computacional do sistema menor possível, isto é, $K = 9$.

4.2.5.3 Parâmetros referentes ao DSNSF

Nesta seção também é abordada a escolha do número de semanas utilizadas pelo ACODS para a extração de padrões de comportamentos do tráfego que compõem as assinaturas digitais. Primeiramente foi estabelecido que essa quantidade derivasse da análise de um período de uma a oito semanas consecutivas e anteriores aos dias tomados como o movimento que os DSNSF deveriam descrever.

Os critérios de avaliação adotados para esse teste baseiam-se em dois princípios. O primeiro corresponde ao erro da previsão gerado a partir de um número arbitrário de semanas em relação ao movimento do tráfego real. Para essa tarefa foi utilizada a métrica *Normalized Mean Square Error* (NMSE) que calculou a diferença absoluta entre as séries temporais correspondentes. O segundo princípio diz respeito à capacidade do DSNSF de capturar as tendências do tráfego e prever o padrão de comportamento, incluindo períodos de maior uso ou decréscimo da utilização dos recursos de rede. A métrica indicada para essa finalidade é o coeficiente de correlação, a qual mensura a relação entre as tendências expressas pela assinatura e pelo movimento do tráfego do dia comparado. Quanto mais o coeficiente de correlação se aproxima do valor 1, maior a correlação entre o DSNSF e o tráfego analisado. O resultado desse teste pode ser observado na Figura 4.6.

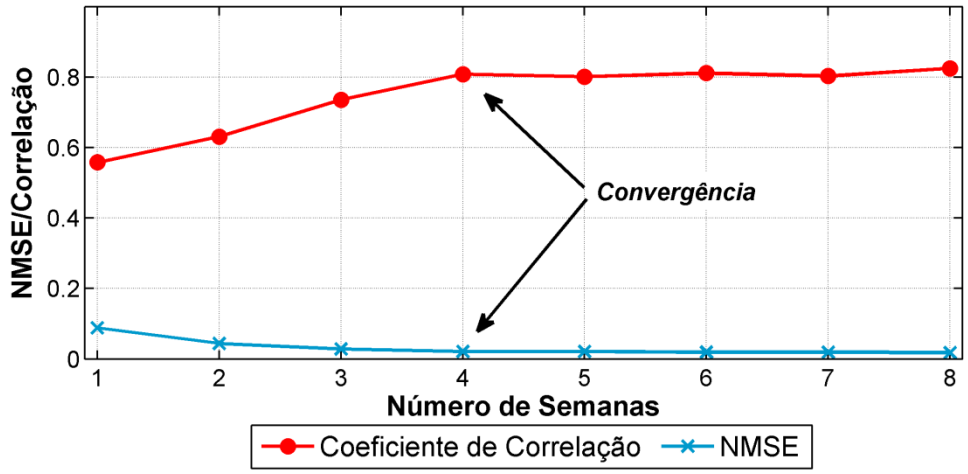

Figura 4.6 - Avaliação do número de semanas utilizadas para a criação do DSNSF. Valores superiores a 4 semanas não agregam melhora significativa na construção das assinaturas digitais.

Embora os melhores valores para os testes sejam encontrados quando 8 semanas são utilizadas, a convergência para esse resultado tem início a partir da quarta semana. Dessa forma, como pode ser visto, utilizando quatro semanas de base de dados, o DSNSF já está apto para assimilar de forma eficiente o comportamento normal do tráfego.

A diferença dos resultados de quatro semanas em relação aos melhores valores apresentados quando utilizadas 8 semanas é de apenas 2,1% e 5% para a correlação e o NMSE, respectivamente. Outro critério fundamental para a escolha de 4 semanas é o aspecto ocasionado pelo monitoramento autonômico, em que não havendo um agente externo classificador dos eventos incomuns, deve-se levar em consideração o impacto que uma mudança repentina do comportamento do tráfego causará ao DSNSF. Dessa maneira, o número de semanas utilizadas para a criação da assinatura digital não pode ser tão pequeno ao

ponto de que qualquer alteração em poucos dias analisados seja adicionada ao DSNSF, como por exemplo, falhas esporádicas, feriados ou recesso acadêmico. Por outro lado, esse valor não deve ser elevado, uma vez que eventos legítimos como *backups* poderiam demorar meses para serem incorporados ao perfil normal de comportamento.

Ainda sobre os parâmetros usados para a geração da assinatura digital, é importante destacar o tamanho da série temporal DSNSF. Após o pré-processamento dos fluxos, as informações do tráfego são organizadas a fim de que se represente o seu comportamento segundo a segundo, totalizando uma série temporal de 86400 elementos para cada atributo analisado. Utilizando essas informações, o sistema ACODS define uma assinatura digital composta por 8640 elementos para cada atributo utilizado neste trabalho. Porém, a detecção de anomalias ocorre em janelas de um minuto, sendo o DSNSF e o tráfego real avaliados através da ADTW utilizando séries temporais de 6 elementos cada (6 × 1400 minutos = 8640) a cada intervalo de análise. O uso de uma sequência de dados para a verificação dos comportamentos anômalos, ao invés de um único ponto para comparação é uma exigência do método ADTW. Embora pareça restritiva, essa característica torna a análise das séries temporais mais flexível e minuciosa [57], trazendo maior benefício para redes em que o comportamento do tráfego é mais volúvel em pequenos intervalos de tempo.

4.3 RECONHECIMENTO DE ANOMALIAS: ADAPTIVE DYNAMIC TIME WARPING

A fim de encontrar comportamentos de tráfego que são diferentes dos caracterizados pelo DSNSF, uma medida de similaridade deve ser adotada. A distância Euclidiana entre cada intervalo de tempo com o mesmo índice tem sido amplamente utilizada em séries temporais para esta finalidade [57]. No entanto, esta medida não é adequada para a identificação de alterações na sequência de dados, pois assume que o *i*-ésimo ponto deve ser alinhado com o outro *i*-ésimo termo da outra sequência, acarretando uma medida equivocada e nada flexível. Assim, dada duas séries temporais, uma delas deslocada em relação o eixo do tempo, é possível que, por meio do cálculo da distância Euclidiana, tais séries sejam classificadas como totalmente diferentes. Acreditando que o comportamento normal de tráfego pode sofrer deslocamentos temporais devido às mudanças no cronograma de atividades dos usuários, é desenvolvida uma medida de similaridade adaptável para atender essas situações.

Dynamic Time Warping (DTW) é uma técnica para comparação de padrões (*templates*) amplamente utilizada em reconhecimento de voz. Através dela é possível encontrar um alinhamento ótimo, *w*, entre duas séries, em que uma delas pode apresentar distorções, estando parcialmente alongada ou encurtada em relação à outra ao longo do eixo do tempo [58]. Assumindo que o DSNSF seja descrito por $X = \{x_1, x_2, \dots, x_M\}$, e o tráfego real, ou *template*, a ser comparado $Y = \{y_1, y_2, \dots, y_N\}$, esse caminho ótimo no plano (n, m) é conseguido minimizando-se a função que mensura a distância *D* dentre as séries, mostrada na Equação (4.13).

$$D = \sum_{n=1}^{N} d\left(X(n), Y\left(w(n)\right)\right) \tag{4.13}$$

Em que $d\left(X(n), Y\left(w(n)\right)\right)$ é a distância entre as séries temporais no intervalo n. É importante salientar que $w(n)$ deve começar no ponto $n = 1, m = 1$, atravessando o plano (n, m) e alcançando o ponto $n = N, m = M$ [59], como demonstrado pela Figura 4.7.

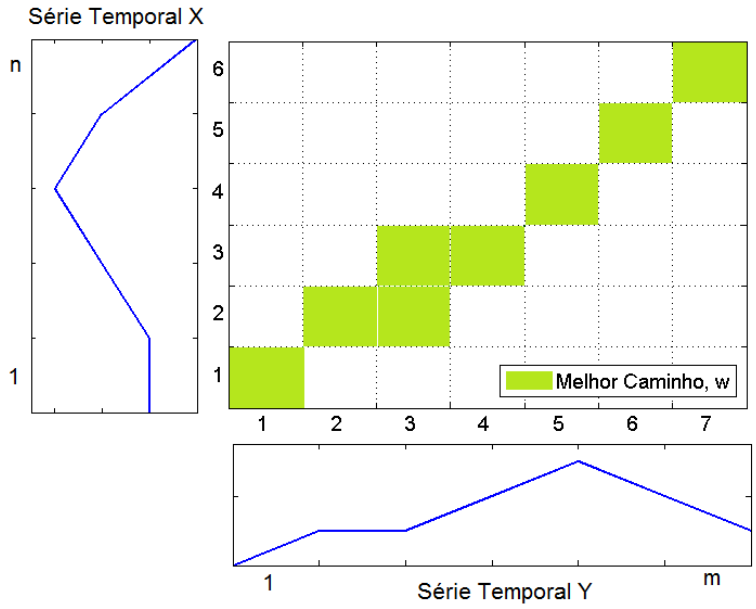

Figura 4.7 - Melhor caminho calculado por meio da distorção de duas séries temporais. Tal caminho é o que faz com que o valor da função *D* tenha o menor valor.

O cálculo do melhor caminho para comparação das séries temporais é dado por quatro etapas básicas. O algoritmo DTW se desenvolve seguindo os passos descritos em [60]:

Passo 1: Criar a matriz solução, *S*, que deve ser composta por *n* linhas e *m* colunas, em que cada elemento da linha *i* e coluna *j* representa o módulo da diferença entre cada intervalo das séries comparadas, uma vez que *n* representa o comprimento do DSNSF e *m* corresponde ao comprimento da série temporal que descreve o tráfego real.

Passo 2: Estabelecer a matriz distância acumulada (DA), formada por *n* linhas e *m* colunas. Essa matriz é dada pela soma dos seus próprios valores com o elemento superior da matriz solução, como mostrado na Equação (4.14).

$$DA_{i,j} = DA_{i-1,j} + S_{i,j} \qquad \text{para } i > 1, j > 1 \tag{4.14}$$

Passo 3: Criação da matriz de movimento de dimensões *n* linhas e *m* colunas. Essa matriz deve ser iniciada atribuindo o valor zero ao último elemento da primeira coluna. Então, uma iteração no sentido de baixo para cima deve ser realizada na matriz DA, para saber qual é o menor valor. Caso o menor valor esteja abaixo do elemento corrente da iteração, a matriz movimento deve ser preenchida com o valor 1; Se o menor valor em DA encontrar-se à esquerda, a matriz movimento deve receber o valor 3. Por fim, caso o menor valor esteja na diagonal inferior à esquerda ou os valores forem iguais, o valor atribuído ao elemento corrente da matriz movimento será 2.

Passo 4: Formação da matriz melhor caminho *w*. Para essa finalidade, deve-se analisar a matriz movimento, a partir do último elemento da primeira linha. Escolhe-se o elemento de menor distância, *d*, dos valores dos demais elementos, como sugerido pela Equação (4.15).

$$d = min\left(\left|w_{i,j} - w_{i-1,j}\right|, \left|w_{i,j} - w_{i,j-1}\right|, \left|w_{i,j} - w_{i-1,j-1}\right|\right) \qquad \text{para } i > 1, j > 1 \tag{4.15}$$

Assim, a cada elemento escolhido, uma marca na matriz *w* é criada. A iteração acaba quando o último elemento da primeira coluna é encontrado. Uma perfeita correspondência entre as séries temporais *X* e *Y* é descrita pela marcação de todos os elementos que compõe a diagonal da matriz *w* [58].

Utilizando as vantagens oferecidas pela técnica DTW, uma abordagem adaptada desse modelo é utilizada para a detecção de anomalias. A *Adaptive Dynamic Time Warping* (ADTW) é usada a cada intervalo de tempo predefinido para a análise do tráfego, *t*, como pode ser verificado na Figura 4.8. Como mencionado anteriormente, esse intervalo é fixado como um período de um minuto, totalizando t = 1440 análises durante o dia. É interessante realçar que o DSNSF, criado para cada dimensão, é composto por 8640 elementos e a cada período de análise, uma pequena subsérie x_t composta por 6 elementos é utilizada, isto é, $X = \{x_1, x_2, \dots, x_{1440}\}$.

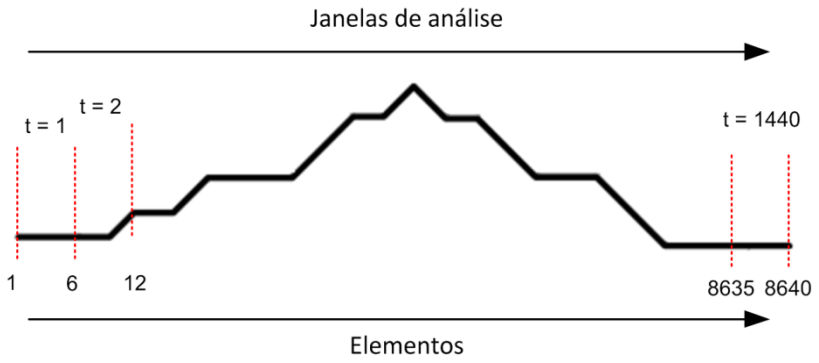

Figura 4.8 – Exemplo de como as janelas de análise são definidas. A cada 6 elementos, um minuto do tráfego é verificado.

A abordagem adaptativa da DTW é divida em duas etapas. A primeira compreende o cálculo da distância entre as duas séries, logo após o alinhamento temporal. Essa medida é dada pela similaridade, s_t, entre o tráfego real e o DSNSF no intervalo de tempo *t*, utilizando o algoritmo DTW convencional. Com isso, mesmo pequenas diferenças entre as séries são verificadas e o resultado pode indicar uma boa correspondência entre elas. Até então, só a equivalência entre as formas das séries temporais são conferidas.

Na segunda etapa, a distância Δ_t entre as séries é calculada, agora considerando suas amplitudes. Portanto, uma subtração entre a média dos valores de ambas as subséries é realizada no intervalo *t*, como mostrado pela Equação (4.16). O resultado usado na detecção de mudanças significativas do tráfego de rede em relação ao perfil normal é

calculado normalizando-se a multiplicação entre os vetores s e Δ, como apresentado pela Equação (4.17).

$$\Delta_t = média(Y_t) - média(X_t) \tag{4.16}$$

$$r = \frac{s \times \Delta}{max(s \times \Delta)} \tag{4.17}$$

A Figura 4.9(a) exemplifica a análise realizada pela ADTW para a comparação das séries temporais, em contraste com a abordagem da distância Euclidiana apresentada a Figura 4.9(b).

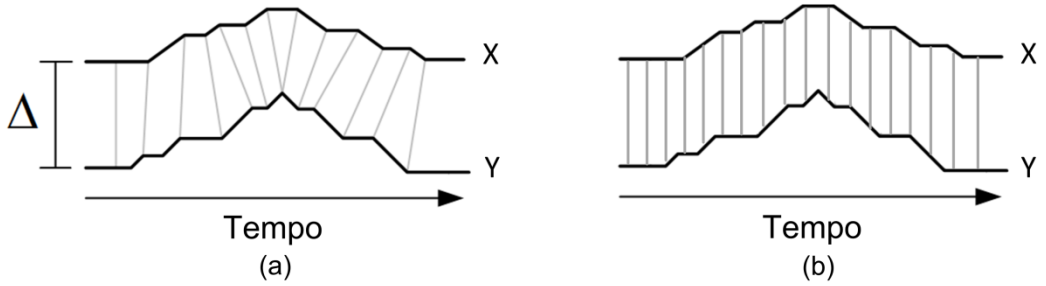

Figura 4.9 - Esquemas de comparação de duas séries temporais: (a) utilizando ADTW e (b) comparação das séries usando distância Euclidiana.

O propósito de elaborar uma abordagem baseada tanto na similaridade da forma das séries temporais quanto na distância entre elas é que ambas as medidas são complementares. Por exemplo, é possível que o resultado de s_t esteja próximo a zero, mas a distância entre as séries no intervalo *t* é acentuada. Esse fato pode ser consequência de uma falha ou erro de configuração de equipamentos, impossibilitando o uso eficiente dos recursos, uma vez que o tráfego apresenta comportamento normal, mas com uma intensidade diferente.

4.3.1 Classificador de Anomalias e Geração de relatórios

Para melhorar a eficiência do método de detecção do sistema ACODS, o movimento de tráfego real e o DSNSF são avaliados na mesma janela de tempo, *t*, a qual compreende um intervalo de um minuto. Esta abordagem permite que apenas um alarme seja gerado nesse intervalo, garantindo que o administrador não seja sobrecarregado com as notificações de anomalias.

Os atributos de fluxos são analisados separadamente, verificando a correspondência com o DSNSF gerado para cada um deles. Um coeficiente de significância $\Phi = 10\%$ é usado como limiar para o erro aceitável entre o tráfego e o DSNSF no intervalo *t*, ou seja, r_t. Esse coeficiente é usado para compensar possíveis imprecisões ocorridas durante o cálculo de *r*, assim como abordar as pequenas variações do uso legítimo da rede. As notificações somente ocorrem quando $r_t > \Phi$. Essa situação pode ser observada na Figura 4.10, em que as barras vermelhas correspondem aos intervalos onde anomalias foram reconhecidas. Os gráficos descrevem o comportamento do tráfego nas dimensões: *bits*, pacotes e fluxos transmitidos por segundo, entropia dos endereços IP de origem e destino, portas, entropia das portas de origem e destino. Embora alarmes sejam gerados durante a análise de cada um desses atributos, o administrador de rede somente é notificado, em tempo real, por um alarme geral, o qual pode ser disparado quando um comportamento anômalo que contenha a assinatura apresentada pela Tabela 4.1 ou um evento inesperado correlacionado os atributos descritivos e quantitativos no intervalo *t*. Caso não exista nenhuma correspondência entre comportamento gerado pela anomalia e as assinaturas reconhecidas pelo sistema, a anomalia é considera desconhecida e sua assinatura pode ser acrescentada ao ACODS para posteriores detecções.

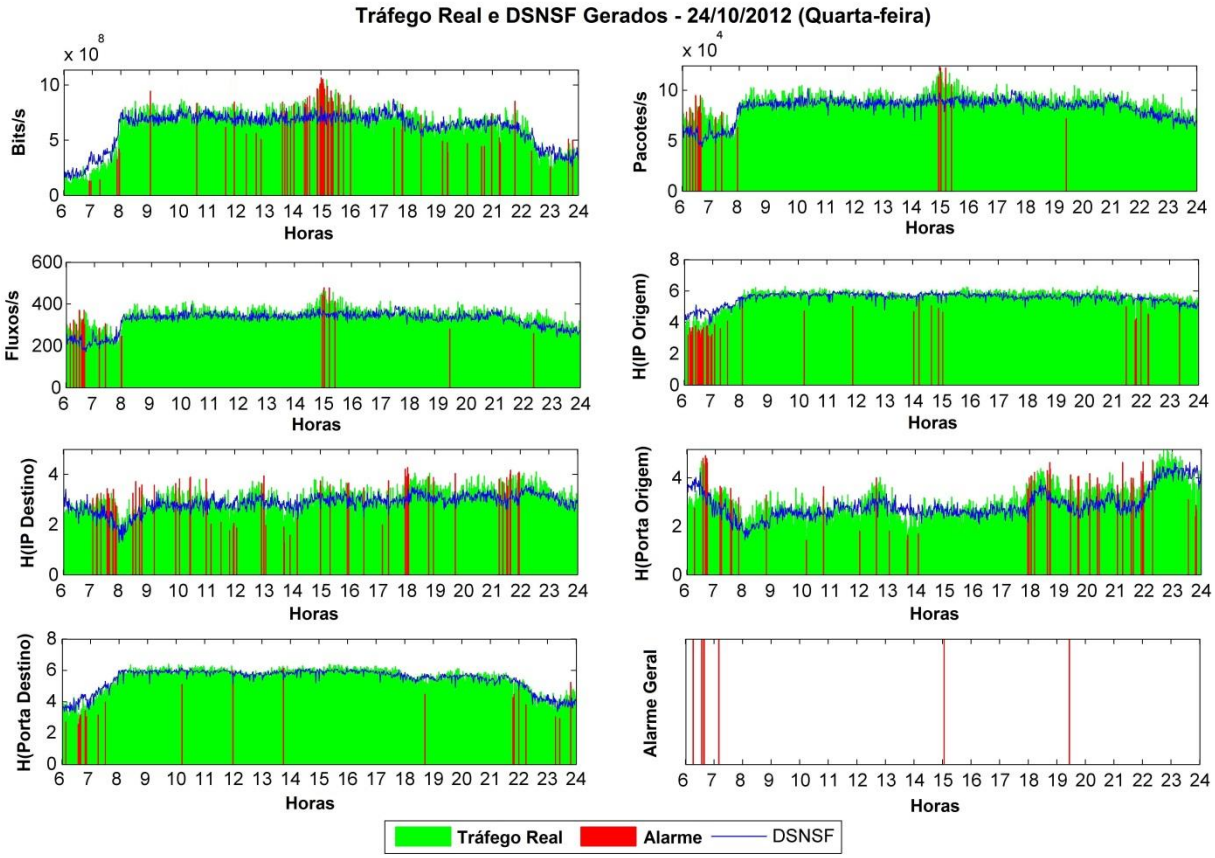

Figura 4.10 - Detecção de anomalias realizada em 24 de outubro de 2012. Administrador de rede é notificado quando um alarme geral é disparado.

Além disso, quando um comportamento diferente daqueles descritos pelo DSNSF é detectado e alarmes são disparados, um relatório com informações relevantes sobre as anomalias é gerado. Esse artifício tem a função de subsidiar o administrador com informações importantes para uma rápida tomada de decisão para solucionar o problema encontrado.

A geração de relatórios pode ocorrer de duas maneiras. Na primeira abordagem, informações que possibilitam inferir a origem do evento (portas e endereços IP de origem), como se desencadeou (protocolos de transporte) e o que foi afetado (portas e endereços IP de destino) são apresentados. Para tanto, esses atributos descritivos (IP e portas) são elencados em ordem decrescente de acordo com a frequência de ocorrência durante um determinado intervalo de análise. Tais dados contribuem para a descoberta dos usuários e serviços que mais utilizaram a rede durante a anomalia. Essas informações são adquiridas durante o pré-processamento e, uma vez que, compõe o histograma utilizado durante o cálculo da entropia, nenhum custo computacional é adicionado ao sistema. Um exemplo desse relatório é apresentado pela Figura 5.9.

A segunda abordagem analisa a relação dos sete atributos de tráfegos, bem como a consequente modificação em seu comportamento exercida pelos eventos anômalos. Esta será melhor detalhada no capítulo de resultados.

4.3.2 Parâmetros Utilizados na Detecção de Eventos Anômalos

Diversos trabalhos encontrados na literatura sobre detecção de anomalias utilizam análise de tráfego em intervalos fixos de cinco minutos [41] [61] [62]. Essa prática tem sido aplicada tanto em conjunto de dados do protocolo SNMP quanto em informações provenientes da análise de fluxos de pacotes, mostrando-se eficaz em ambas abordagens de gerenciamento. Entretanto, devido ao aumento contínuo das taxas de transmissão, o monitoramento do tráfego utilizando esse intervalo se torna impraticável. Uma rede que opera a 10 Gigabits/s, por exemplo, pode ter cerca de 3 Terabits de informações comprometidas durante o intervalo de cinco minutos. Dessa fortma, neste trabalho é empregada uma janela temporal de um minuto para análise do tráfego e do DSNSF, tornando o ACODS apto a atuar em redes de larga escala, uma vez que permite que o sistema reporte a existência de um evento anômalo mais rapidamente ao administrador.

Outro parâmetro importante é o coeficiente de significância Φ, o qual mostra o limiar de variação entre o DSNSF e o tráfego analisado durante o intervalo de um minuto. Neste trabalho esse parâmetro recebe o valor 10%, sendo medido após o cálculo da similaridade das séries temporais. Caso o erro entre elas seja mais significante que esse valor, um alarme é gerado. As análises de outros valores para esse parâmetro e a justificativas da escolha desse são detalhadas no capítulo de resultados.

5 RESULTADOS

O principal objetivo deste capítulo é demonstrar os resultados obtidos com o ACODS, tanto para a caracterização do tráfego quanto para a detecção de anomalias em redes de computadores. Para esse propósito, são utilizados dados provenientes de ambientes reais de rede. Juntamente com as anomalias inerentes ao tráfego analisado, foram induzidos ataques com diferentes intensidades. A intenção é averiguar se o sistema é capaz de estimar de forma eficiente um padrão normal de tráfego, o qual servirá como gabarito para o reconhecimento de eventos anômalos que possam vir a comprometer a operação da rede.

Fluxos IP coletados da Universidade Estadual de Londrina (UEL) foram usados para treinar o sistema e também avaliar o seu desempenho na criação da assinatura digital. Os dados, originados de cerca de sete mil *hosts* interligados, foram recolhidos a partir do *switch* BD8801 Extreme, localizado no núcleo da rede, agregando todo o tráfego da universidade. Devido ao grande volume de informação, os dados coletados são amostrados periodicamente, a uma taxa de 1 a cada 256 pacotes. Utilizou-se o aplicativo analisador de rede Softflowd para exportar os fluxos para o coletor no formato sFlow [39]. O coletor salva os fluxos exportados em arquivos binários a cada cinco minutos para ser processado pela ferramenta NFDUMP [63], de modo que possa ser usado posteriormente pelo sistema apresentado neste trabalho.

O período de coleta de dados é composto por sete semanas consecutivas, iniciado em 24 de setembro e finalizado em 09 de novembro de 2012. Para facilitar a avaliação do sistema, o conjunto de dados foi separado em dois grupos: as primeiras quatro semanas foram usadas pelo ACODS como informação histórica para criação do DSNSF e estipulação de parâmetros. Os dias úteis das últimas três semanas (de 22 de outubro a 09 de setembro) foram reservados para a avaliação do sistema no processo de caracterização do tráfego e detecção de anomalias. A escolha de analisar somente os dias de segunda a sexta-feira é devido à alta demanda de utilização da rede nos dias úteis. Desse modo, optou-se em realizar a análise dos demais dias da semana em trabalhos futuros.

A rede da Universidade Tecnológica Federal do Paraná (UTFPR) – Campus Toledo é a segunda avaliada neste trabalho. A coleta do tráfego agregado proveniente de aproximadamente quatrocentos dispositivos é realizada no *gateway* principal da rede, e os fluxos analisados são exportados pelo protocolo NetFlow v9, sem o uso de técnicas de amostragem. Os dados utilizados dessa rede são divididos em dois grupos. Quatro semanas no

período de 01 a 26 de abril são utilizadas para a criação do perfil de comportamento normal, enquanto as três semanas seguintes, 29 de abril a 17 de maio, são usadas para avaliação das assinaturas geradas.

Ambas as redes foram escolhidas por apresentarem ambientes e configurações distintas. A primeira delas é a quantidade de tráfego agregado que deverá ser analisado. Composta por maior número de usuários, a rede UEL dispõe de taxa de transmissão de 1Gb/s para acesso à Internet. Em contrapartida, a rede da UTFPR possuí dois *gateways* que somadas suas velocidades de transmissão, totalizam 20 Mb/s. A segunda característica que difere as redes é uma consequência da primeira. Uma vez que na análise da rede da UEL é necessário o uso de amostragem, o protocolo sFlow foi aplicado, diferentemente do protocolo NetFlow designado para rede UTFPR. Dessa forma, o intuito é verificar se o ACODS é capaz de contribuir para o gerenciamento de redes de diferentes escalas e que utilizam diferenciados protocolos de exportação de fluxos.

Complementando a avaliação, uma comparação com o tradicional algoritmo de clusterização K-means [64] foi realizada. Este método de aprendizado não supervisionado é um dos mais representativos nas pesquisas referentes à mineração de dados devido à sua habilidade de classificação e segmentação de dados. Na análise proposta, K-means realiza a extração de padrões de comportamento do tráfego para a criação de assinaturas digitais, as quais são comparadas aos DSNSF gerados pelo ACODS.

O sistema apresentado foi submetido a quatro cenários de testes, os quais se diferenciam pelas características avaliadas, bem como a metodologia abordada para desempenhar essa função. O primeiro cenário procura verificar a eficiência do ACODS na construção das assinaturas para cada dia útil da semana, analisando o tráfego da rede UEL. Ainda sob esse cenário é realizada a detecção de anomalia e a avaliação de seus resultados. O segundo cenário apresenta a mesma finalidade do anterior, porém são analisados e discutidos resultados provenientes da rede UTFPR. O cenário seguinte utiliza anomalias sintetizadas para comparação entre a abordagem heptadimensional descrita nesse trabalho e a detecção baseada em volume de tráfego. Finalmente, o quarto cenário confronta os resultados da caracterização do tradicional método K-means e ACODS, fornecendo também uma análise de tempo de convergência de soluções para ambas as abordagens. Os cenários estão descritos na Tabela 5.1.

Tabela 5.1 - Cenários de teste

Cenário	Experimento	Rede	Período
1	Aplicação do ACODS na caracterização de tráfego e detecção de anomalias.	• Rede UEL; • Fluxos coletados no formato sFlow; • Amostragem 1:256 pacotes.	Sete semanas: 24/09/2012 a 09/11/2012.
2	Aplicação do ACODS na caracterização de tráfego e detecção de anomalias	• Rede UTFPR; • Fluxos coletados no formato NetFlow v9; • Amostragem 1:1 pacotes.	Sete semanas: 01/04/2013 a 17/05/2013.
3	Teste de eficiência do ACODS e comparação com abordagem de detecção baseada em volume	• Rede UEL; • Anomalias sintéticas injetadas no tráfego; • Amostragem 1:256 pacotes.	Sete semanas: 24/09/2012 a 09/11/2012.
4	Comparativo entre ACODS e K-means.	• Rede UEL; • Fluxos coletados no formato sFlow; • Amostragem 1:256 pacotes.	Sete semanas: 24/09/2012 a 09/11/2012.

Adiante, poderá ser observado que primeiramente são abordados os conceitos das métricas utilizadas para mensurar a eficiência do sistema ACODS, e em seguida, a estipulação de valores de parâmetros das abordagens de caracterização e detecção. Por fim, são apresentados os resultados numéricos acompanhados das suas análises.

5.1 MÉTRICAS DE AVALIAÇÃO

Um sistema de detecção de anomalias baseado em perfis tem sua eficiência totalmente relacionada à caracterização de tráfego. A primeira técnica utilizada para medir a aplicabilidade do ACODS é o Erro Quadrático Médio Normalizado (*Normalized Mean Square Error* - NMSE) [65]. Essa medida avalia a diferença absoluta entre o que foi previsto pelo DSNSF e o que realmente é verificado através do tráfego real. Ao apresentar valores de zero a infinito, é possível verificar que resultados próximos a zero indicam excelente caracterização do tráfego enquanto valores elevados indicam divergências entre as séries temporais analisadas, DSNSF e movimento do tráfego. A Equação (5.1) demonstra como o NMSE é calculado para duas séries temporais X e Y, ambas de tamanho N.

$$NMSE = \frac{\sum_{t=1}^{N}(X_t - Y_t)^2}{\sum_{t=1}^{N}(Y_t)^2} \tag{5.1}$$

Outra abordagem utilizada para medir a adaptabilidade da caracterização também está relacionada ao erro entre as séries temporais que representam o DSNSF e o tráfego analisado. Além do NMSE, é usada a análise de desvios proposta por Bland e Altman [66]. Essa medida considera a diferença entre o movimento predito para o tráfego e o que realmente foi observado. Tais diferenças devem estar contidas no intervalo definido por $\bar{d} \pm 1{,}96 * \sigma$, em que $\bar{d}$ corresponde à diferença entre as médias das séries analisadas e σ é o desvio padrão entre as diferenças. Segundo os autores, para que um bom ajuste entre as séries seja considerado, um limiar mínimo de 95% dos desvios, ou erros, devem estar dentro dos limites determinados. A Figura 5.1 ilustra um exemplo do gráfico gerado a partir dos resultados do teste de Bland-Altman. Nesse gráfico é apresentada a correspondência entre o DSNSF do atributo *bits* por segundo e o tráfego a ser analisado na sexta-feira dia 02/11/2012.

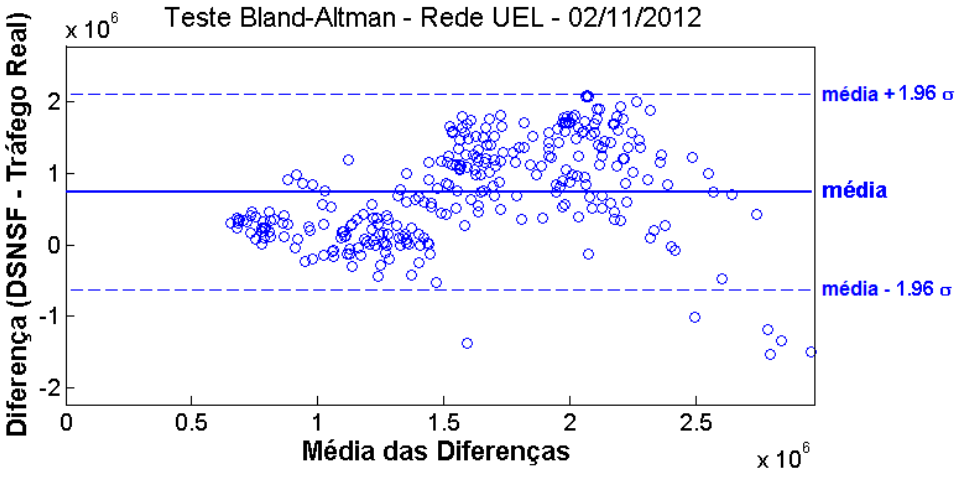

Figura 5.1 - Exemplo de gráfico gerado a partir do teste Bland-Altman.

Bland e Altman apresentam sua proposta como uma alternativa ao teste de coeficiente de correlação entre dois conjuntos de dados. A justificativa parte do princípio que uma forte correlação não implica necessariamente que duas medidas, ou séries, sejam concordantes entre si. Um exemplo é a mudança de escala, em que a correlação não sofre modificação, porém o ajuste entre as séries é afetado. Logo, uma medida que avalia a diferença sistemática entre o previsto e o observado e os desvios provenientes dessa análise, se mostra mais interessante e útil.

Quanto à avaliação do método de detecção, são utilizadas as métricas de desempenho adotadas em [67]. A primeira é a acurácia, cuja finalidade é calcular a probabilidade de o sistema fornecer resultados corretos, ou seja, disparar alarmes para intervalos com anomalias e apresentar resultado negativo nos demais intervalos. Em outras palavras, essa medida trata da relação entre as taxas de verdadeiro-positivos e verdadeiro-negativos. Estas taxas representam a segunda e a terceira métrica utilizada na avaliação. A Equação (5.2) demonstra o cálculo da taxa de acurácia.

$$Acurácia = \frac{Verdadeiro\ Positivo + Verdadeiro\ Negativo}{Amostras\ Normais + Amostras\ Anômalas} \tag{5.2}$$

A função dessas medidas é demonstrar o número de amostras que o sistema foi capaz de classificar corretamente. A taxa de verdadeiro-positivos corresponde aos comportamentos anômalos que foram reconhecidos como tal, ao passo que a taxa de verdadeiro-negativos mostra a parte do comportamento normal que foi classificada corretamente como legítima. No entanto, para que elas sejam contabilizadas é preciso um

conhecimento prévio sobre o comportamento do tráfego, ou seja, cada intervalo de um minuto analisado deve ser classificado como normal ou anômalo. Essa classificação foi realizada pelos próprios integrantes do grupo de pesquisa em rede do departamento de computação da UEL, tendo em vista os conhecimentos adquiridos através da observação de ocorrências de anomalias e de pesquisas realizadas para o desenvolvimento do sistema de detecção apresentado neste trabalho.

Outra medida utilizada é a taxa de falso-positivos, a qual determina a quantidade de intervalos que foram erroneamente classificados como anômalos. Esta medida é combinada com a taxa de verdadeiro-positivos para a construção do gráfico *Receiver Operating Characteristics* (ROC) [68], que possibilita uma análise visual da precisão do sistema no reconhecimento de comportamentos anômalos.

5.2 Cenário 1: Caracterização e Detecção Utilizando Tráfego da UEL

A metodologia usada para a criação da assinatura digital parte do princípio de que um único DSNSF é gerado para cada dia, com base no histórico de comportamento do tráfego de suas semanas anteriores. Dessa forma, foram reunidas quatro semanas do tráfego a partir de 24 de setembro até 19 de outubro para a criação do DSNSF. Em relação à avaliação do ACODS, três semanas de 22 de outubro a 09 de novembro são usadas para verificar se este é capaz de reconhecer os diversos comportamentos do tráfego e estabelecer o padrão de normalidade.

A Figura 5.2 apresenta a caracterização do tráfego para as 24 horas do dia 22 de outubro de 2012. Da mesma maneira, as Figura 5.3 e Figura 5.4 demonstram o movimento do tráfego e as assinaturas geradas para os dias 23, 24, 25 e 26 do mesmo mês. Os dados coletados da Universidade Estadual de Londrina são exibidos em verde e os DSNSF gerados para cada atributo de fluxo compreendem as linhas azuis. Durante o período entre as 8 e as 22 horas, a rede apresenta elevados níveis de tráfego devido ao horário de funcionamento dos diversos setores da instituição. Nessas figuras é possível observar o ajustamento entre o DSNSF e o tráfego real, demonstrando a eficiência do sistema para criação de perfis da rede.

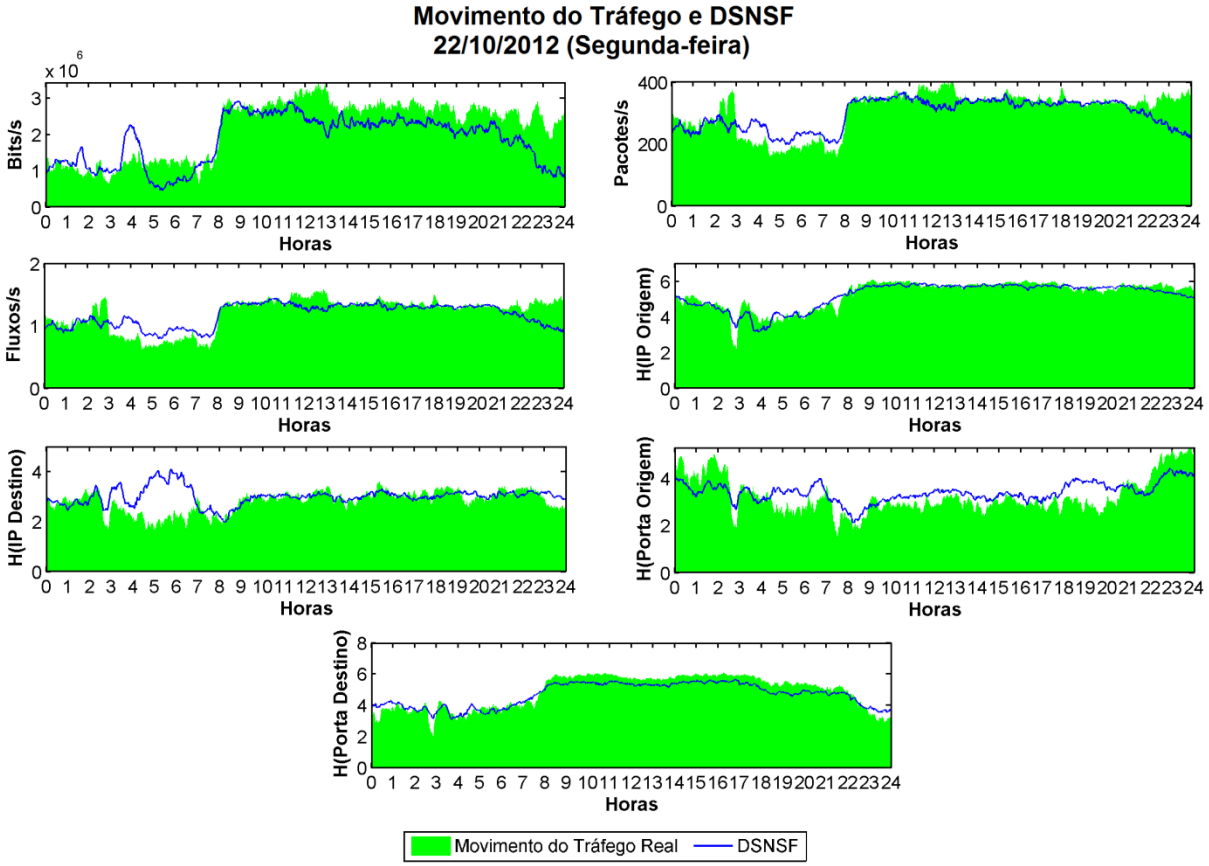

Figura 5.2 - Caracterização dos sete atributos do fluxos para o dia 22/10/2012.

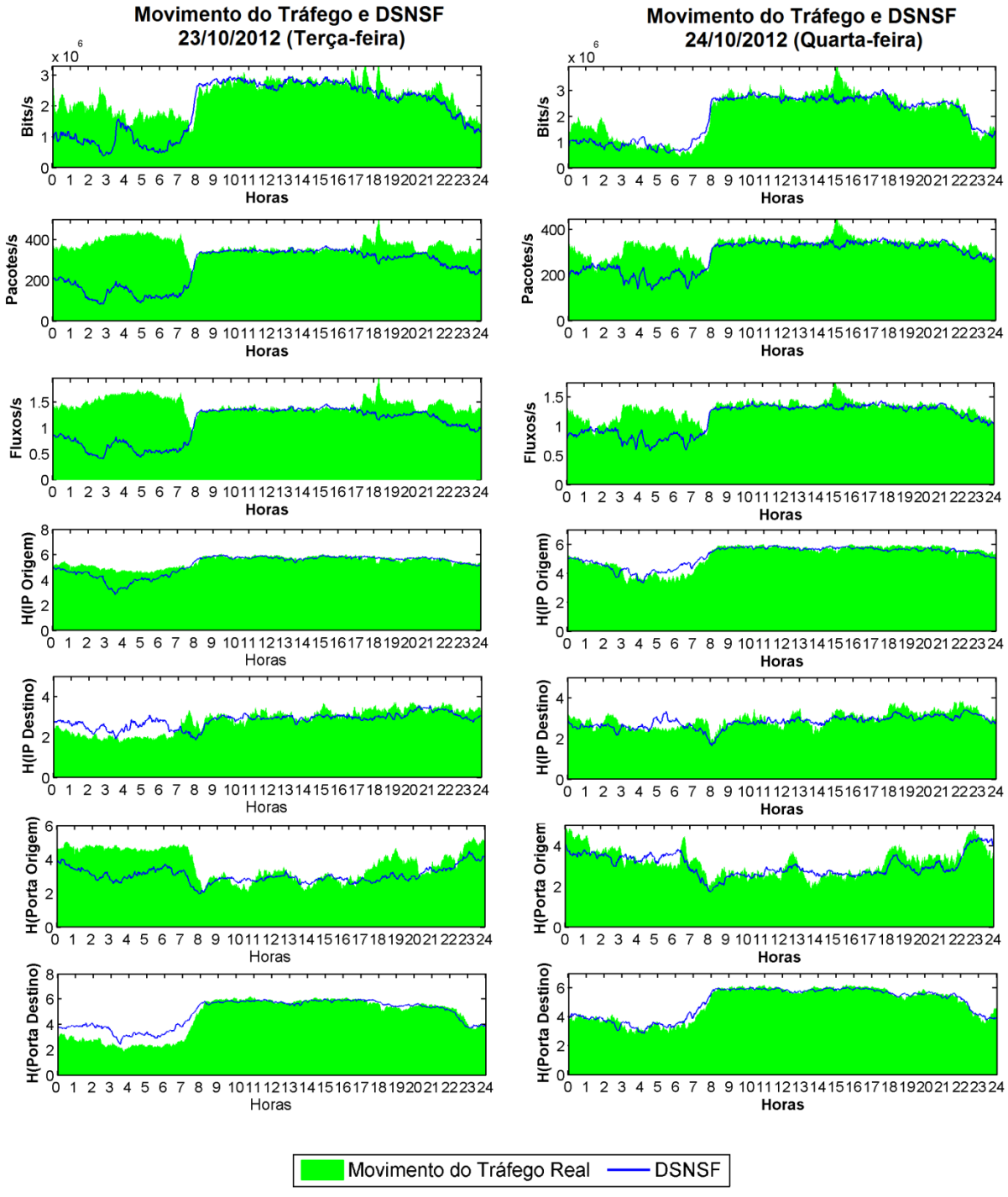

Figura 5.3 - DSNSF e movimento do tráfego dos dias 23 e 24 de outubro.

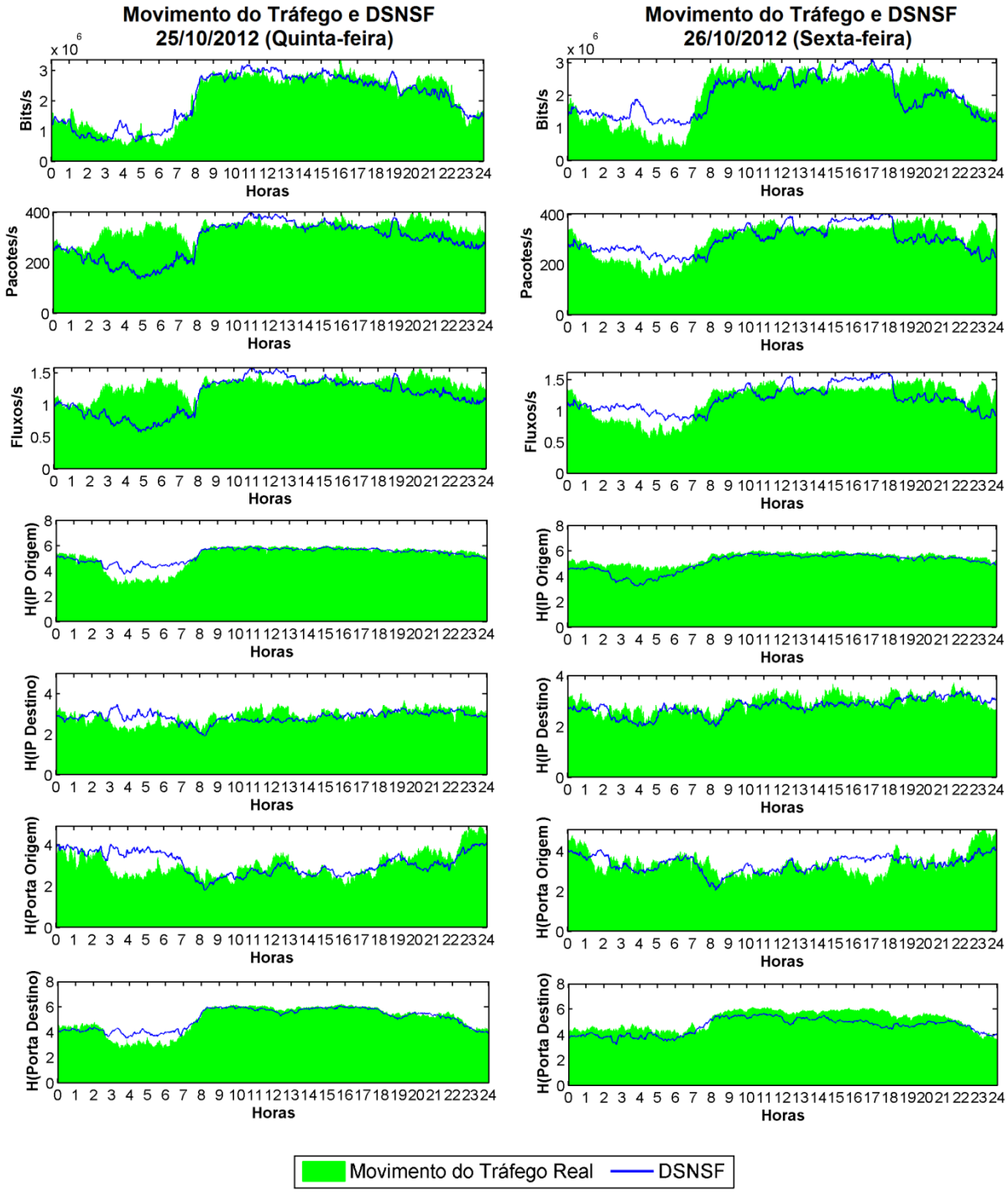

Figura 5.4 - DSNSF e movimento do tráfego dos dias 25 e 26 de outubro.

Os DSNSF gerados foram submetidos ao teste NMSE, e os valores obtidos estão ilustrados na Figura 5.5. Os resultados apresentados no gráfico indicam os valores do erro médio calculado entre os sete atributos do fluxo para cada dia avaliado. O dia 2 de novembro apresentou o pior valor para o teste. Por se tratar de um feriado nacional, o tráfego observado nesse dia se manteve abaixo do esperado, uma vez que a rede não foi usada como de costume. Além disso, em 30 de outubro foi observado um erro perceptível decorrente de

vários padrões de comportamento incomum que afetou principalmente os atributos de volume, com picos de até 66% em excesso ao tráfego previsto pelo DSNSF. O restante dos dias examinados apresentaram pequenas taxas de erros e até mesmo valores próximos ao ótimo.

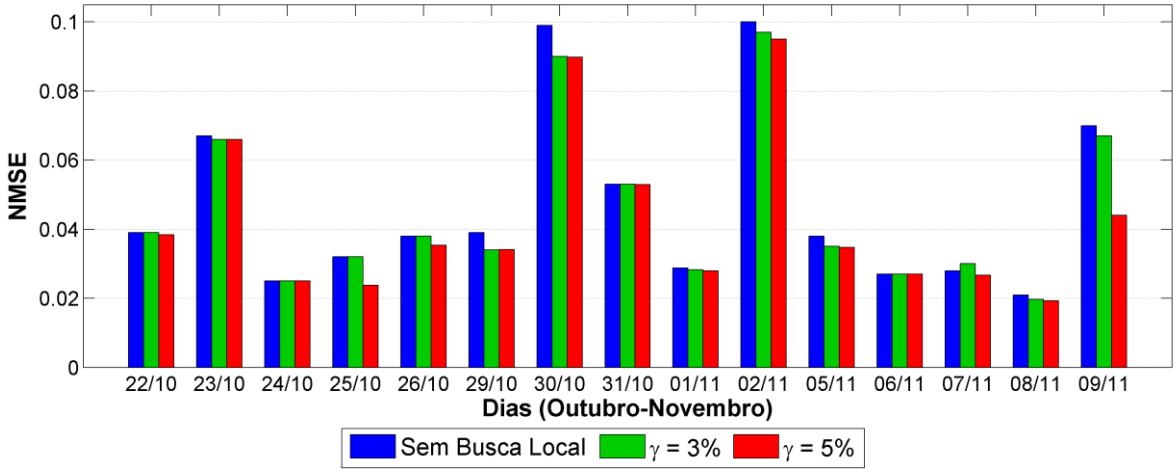

Figura 5.5 - Teste NMSE entre os DSNSF gerados e os movimentos reais de tráfego dos dias analisados.

É importante destacar a relevância do uso da abordagem de busca local. Atuando como otimizadora das soluções, essa etapa faz com que o DSNSF descarte tendências de tráfego inerentes aos dias particulares, os quais não compõem o comportamento usual da rede. Dessa forma, como pode ser verificado por meio da Figura 5.5, o resultado para três abordagens diferentes de busca local é apresentado. Quando ela não é usada, os resultados permanecem mais elevados do que os outros valores atribuídos ao parâmetro γ, ou seja, o DSNSF incorpora pequenos comportamentos de cada dia usado para sua criação, divergindo grandemente quando comparado a um dia que não apresenta tais eventos. Além de gerar uma caracterização tendenciosa, esse caso pode resultar no aumento de falsos alarmes na detecção de comportamentos suspeitos. Usando $\gamma = 3\%$, o resultado é ligeiramente melhorado, no entanto, permanece superior do que o valor escolhido para este trabalho, $\gamma = 5\%$. Outros valores foram analisados para esta abordagem e pôde-se notar que o uso de valores maiores do que o adotado ocasiona a exclusão de clusters necessários para se criar o perfil normal da rede, prejudicando, assim, o monitoramento do tráfego e a detecção de anomalias.

A Tabela 5.2 apresenta os resultados numéricos do teste NMSE para os diversos valores do parâmetro γ utilizado na busca local. Diferentemente do gráfico apresentado na Figura 5.5, a tabela traz as médias dos erros das 3 semanas de análises, agrupadas por atributos. Os valores destacados indicam os melhores resultados para o teste,

isto é, realçam qual abordagem de busca local obteve menores erros. A última coluna demonstra, em porcentagem, qual o ganho obtido ao se utilizar o valor $\gamma = 5\%$ em relação à geração de DSNSF sem busca local.

Tabela 5.2 - Resultados do teste NMSE agrupados por atributos. A abordagem de busca local utilizando γ=5% obteve melhores resultados.

Atributo	Sem Busca Local	$\gamma = 3\%$	$\gamma = 5\%$	$\gamma = 7\%$	Melhoria (%)
Bits	0,1109	0,1127	0,1058	0,1088	4,88
Pacotes	0,0467	0,0448	0,0441	0,0458	5,83
Fluxos	0,0455	0,0447	0,0424	0,0457	7,23
IP Origem	0,0108	0,0085	0,0073	0,0102	48,25
IP Destino	0,0388	0,0339	0,0321	0,0365	20,78
Porta Origem	0,0582	0,0541	0,0505	0,0587	15,27
Porta Destino	0,0195	0,0189	0,0167	0,0188	17

A Figura 5.6 expõe os resultados para o teste Bland-Altman realizado sobre os dias analisados. Assim como o NMSE, esta medida permite avaliar a similaridade das séries temporais DSNSF e tráfego real. Mais uma vez, a média dos erros dos sete atributos analisados é mostrada para cada dia avaliado. Como pode ser observado, os dias 30 de outubro e 2 de novembro apresentaram maior erro do que os demais, o que pode ser verificado pelos baixos índices de concordância entre o DSNSF e o movimento do tráfego analisado. Foi possível observar também que o resultado manteve-se superior a 95% para a maioria dos dias, confirmando que DSNSF é eficaz na previsão do comportamento do tráfego.

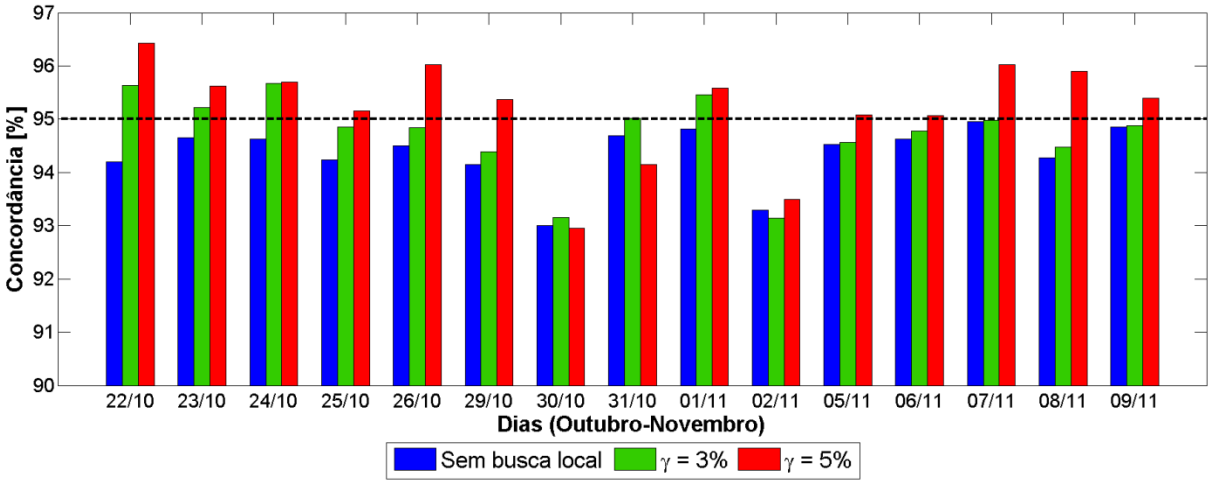

Figura 5.6 - Teste Bland-Altman entre os DSNSF gerados e os movimentos reais de tráfego dos dias analisados.

Além disso, os resultados para variados valores assumidos pelo parâmetro γ também foram analisados pelo teste Bland-Altman. A melhor caracterização do tráfego é observada quando $\gamma = 5\%$. Resultados sem o uso da busca local são piores do que outras abordagens analisadas, no entanto, é possível constatar que para alguns dias, os resultados foram semelhantes. Essas exceções demonstram que o tráfego utilizado para a construção do DSNSF apresentou uma distribuição igualitária entre os grupos durante o processo de clusterização, por isso não houve a necessidade da eliminação de clusters menos representativos.

Outra perspectiva sobre os resultados do teste Bland-Altman é apresentada na Tabela 5.3. Pode ser observado que a busca local é uma ferramenta desejável para a caracterização, uma vez que, sem ela os erros entre o DSNSF e o tráfego analisado atingiram as maiores taxas. As maiores taxas de concordâncias foram destacadas e, segundo os resultados, grande parte das assinaturas digitais foi criada de forma satisfatória quando $\gamma = 5\%$, porém, alguns DSNSF caracterizam melhor o tráfego com valores $\gamma = 3\%$. Ao analisar o motivo desses acontecimentos, foi verificado que o tráfego de pacotes apresentou diversos *outliers* durante esses dias, requerendo maior rigidez da abordagem de busca local durante a criação do perfil normal de comportamento. Logo, o erro gerado pelo DSNSF desse atributo pôde ser minimizado quando clusters com quantidades inferiores a 7% dos elementos clusterizados foram excluídos. O contrário é observado com o atributo IP Origem, o qual apresentou as menores taxas de erros. Este acontecimento indica que é mais simples de se extrair um comportamento normal desse atributo, e consequentemente uma política de busca local menos restritiva poderia ser utilizada.

Tabela 5.3 - Resultados do teste Bland-Altman agrupados por atributos.

Atributo	Sem Busca Local	$\gamma = 3\%$	$\gamma = 5\%$	$\gamma = 7\%$
Bits	93,95	94,66	94,84	94,18
Pacotes	94,68	94,87	94,85	95,07
Fluxos	94,61	94,91	95,19	94,88
IP Origem	94,25	95,30	94,40	94,11
IP Destino	94,67	94,97	95,60	94,66
Porta Origem	94,78	95,21	95,83	95,02
Porta Destino	93,54	93,90	94,73	93,7

Em relação à detecção de anomalias, cada dia analisado é fracionado em intervalos de tempo de um minuto, totalizando 1440 períodos verificados em 24 horas. Assim, a abordagem ADTW reporta o horário exato do intervalo em que ocorreu a anomalia e conta o número de intervalos anômalos detectados durante os testes. Esta fase de avaliação também foi usada para testar os valores assumidos pelo coeficiente de significância Φ. A Figura 5.7 mostra os resultados para o teste de acurácia durante as três semanas de teste.

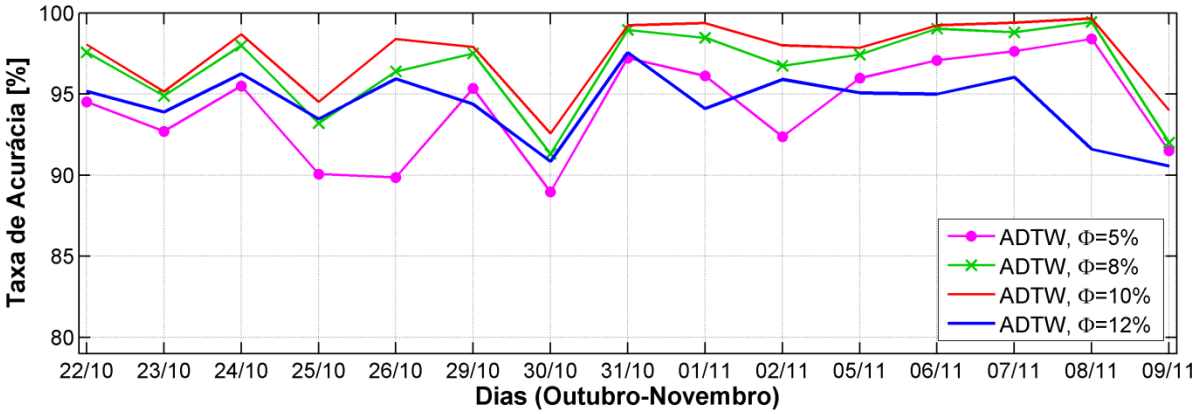

Figura 5.7 - Taxas de acurácia para variados os valores assumidos pelo parâmetro Φ.

De acordo com Lei e Ghorbani [69] nenhuma medida de desempenho tal qual a acurácia, os falso-positivos ou mesmo a taxa de verdadeiro-positivos pode sozinha representar completamente a aplicabilidade de um sistema. Desta maneira, é utilizada a curva ROC, para melhor averiguação da correlação existente entre as taxas de acertos e falsos alarmes disparados pelo processo de detecção. Confirmando a escolha do coeficiente de significância Φ durante o teste de acurácia, maior precisão da detecção com ocorrência mínima falso-positivos é atingida quando Φ = 10%, o que pode ser verificado na Figura 5.8.

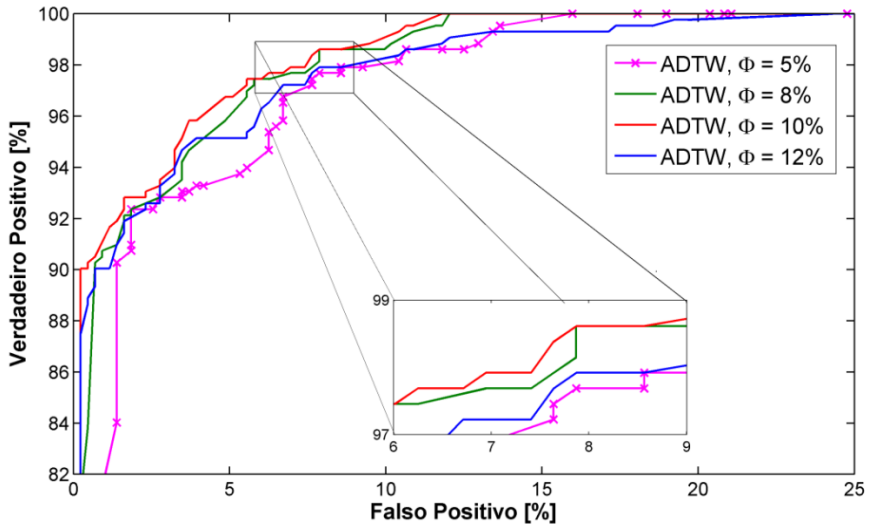

Figura 5.8 - Curvas ROC geradas a partir da detecção de anomalias utilizando os DSNSF e a ADTW. A melhor relação entre detecção e falsos alarmes é conseguida quando o parâmetro Φ recebe o valor 10%.

Vários outros valores para o coeficiente Φ foram examinados, entretanto, ficou atestado que valores inferiores a 5% apresentam os piores resultados, levando-se em consideração as taxas de acertos. É possível também confirmar que a redução desse limiar permite que variações mínimas do tráfego real em relação ao DSNSF, incluindo comportamentos legítimos, sejam classificadas como anomalias. Por outro lado, quando este valor é maior do que 10%, as anomalias são detectadas apenas quando o seu comportamento induz uma mudança considerável no tráfego em relação ao padrão estabelecido pelo DSNSF, o que pode mascarar a ocorrência de diversos ataques de pequenas e médias magnitudes. Por meio da análise da curva ROC apresentada na Figura 5.8 pode-se inferir que tal situação acarreta baixas taxas de verdadeiro-positivos e maiores taxas de falso-positivos, e esta característica aumenta ao passo que o valor de Φ é incrementado.

Analisando especificamente o comportamento do tráfego ocorrido durante o dia 30 de outubro foi possível verificar que os atributos de fluxos que mais divergiram do padrão definido pela assinatura digital foram os de volume, endereço IP de destino e porta de destino. Eventos incomuns correlacionando essas informações são classificados pelo sistema ACODS como anomalias do tipo *flash crowd*, o que pode ser conferido na Tabela 4.1. O evento se desencadeou ao longo do dia, se intensificando nos horários das 20 às 22 horas. A Figura 5.9 apresenta o tráfego analisado, juntamente com o DSNSF, e um relatório sobre a situação do uso da rede em uma janela de análise de um minuto, iniciada às 21 horas.

Ainda sobre a Figura 5.9, pode ser observado que durante o intervalo correspondente à anomalia, as entropias em relação aos atributos endereço IP de destino e porta de destino se apresentaram mais concentradas do que o previsto pelo DSNSF. Isso ocorreu devido às diversas requisições para a porta 14428 (cerca de 47,8% das ocorrências durante o período de análise) e para o endereço 189.90.77.148, sendo este o destino de 49% de todo o tráfego analisado. Também é possível verificar que o atributo endereço de origem exibiu um comportamento diferente do normal. A razão para esse evento é a grande quantidade e diversidade de endereços IP de origem acessando os servidores da rede UEL, o que destoa do comum e, é classificado como um comportamento anômalo.

Por meio da análise dos alarmes gerados nas sete dimensões, ou atributos, o classificador de anomalias do sistema pôde constatar que o evento ocorrido nessa terça-feira caracterizou uma anomalia do tipo *flash crowd*. Ciente do acontecimento, através da observação das notificações disparadas no alarme geral, o administrador pode solicitar o relatório sobre o uso da rede no intervalo em que o evento foi detectado. O intuito é fornecer

informações para que as partes envolvidas no evento possam ser identificadas e que contramedidas para conter o avanço da anomalia possam ser aplicadas.

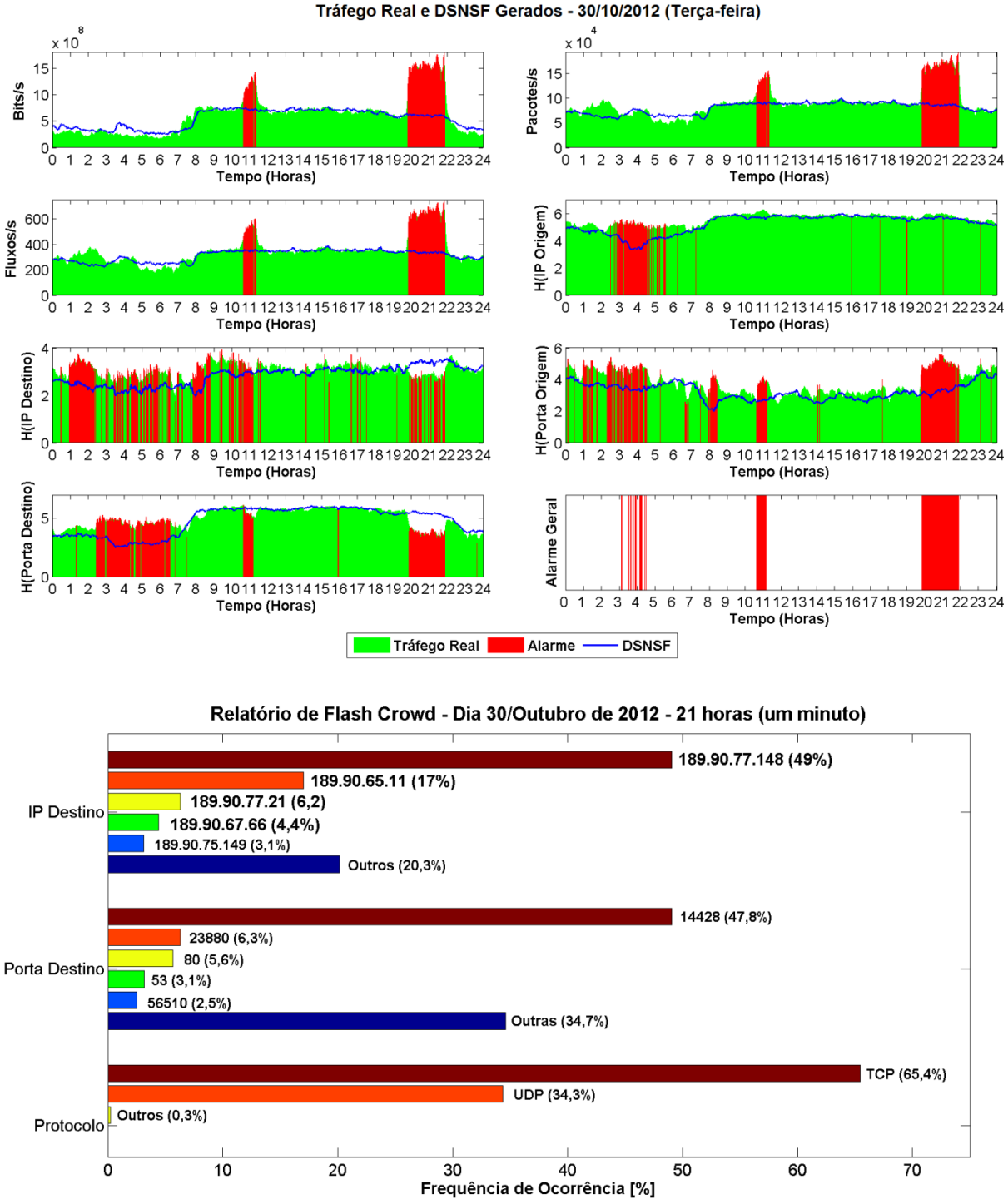

Figura 5.9 - Relatório de uso da rede gerado durante uma anomalia *flash crowd*.

Com base no relatório apresentado na Figura 5.9, foi possível verificar que os endereços e portas de destino mais acessados correspondiam aos servidores da entidade responsável por organizar processos seletivos na universidade. O grande volume de tráfego ocorreu devido à divulgação do resultado do concurso público da polícia civil estadual.

Embora essa anomalia não apresente comportamento malicioso, é interessante a realização do seu monitoramento para assegurar que esse evento não comprometa o funcionamento da rede e dos demais serviços prestados.

5.3 Cenário 2: Caracterização e Detecção Utilizando Tráfego UTFPR

Como abordado no cenário anterior, a caracterização de um perfil normal do tráfego de rede é o principal aspecto para o bom funcionamento do sistema apresentado. Dessa forma, novamente a eficiência na criação do DSNSF pelo ACODS foi avaliada. Para tanto, fluxos IP coletados da rede da UTFPR foram conferidos. A escolha dessa rede é motivada por apresentar aspectos diferentes aos da rede UEL, incluindo sua dimensão, protocolo de exportação de fluxos e a amostragem de pacotes 1:1.

Novamente, o conjunto de dados é divido em duas partes. A primeira é utilizada pelo ACODS para a extração de padrões de comportamentos normais, compreendendo o intervalo de 01 a 26 de abril. A segunda parte abrange as três semanas seguintes, de 29 de abril a 17 de maio, sendo utilizadas para avaliação das assinaturas digitais criadas a partir desses padrões e também para a detecção de anomalias.

A Figura 5.10, Figura 5.11 e Figura 5.12 apresentam o tráfego da semana de 06 a 10 de maio. O tráfego real observado é exibido em verde, enquanto o DSNSF gerado para cada atributo do fluxo é definido em azul. As atividades no campus da UTFPR iniciam-se às 7 horas e têm fim às 23 horas. Como pode ser observado, a maior parte do tráfego é concentrada nesse período, resultado das atividades acadêmicas e administrativas.

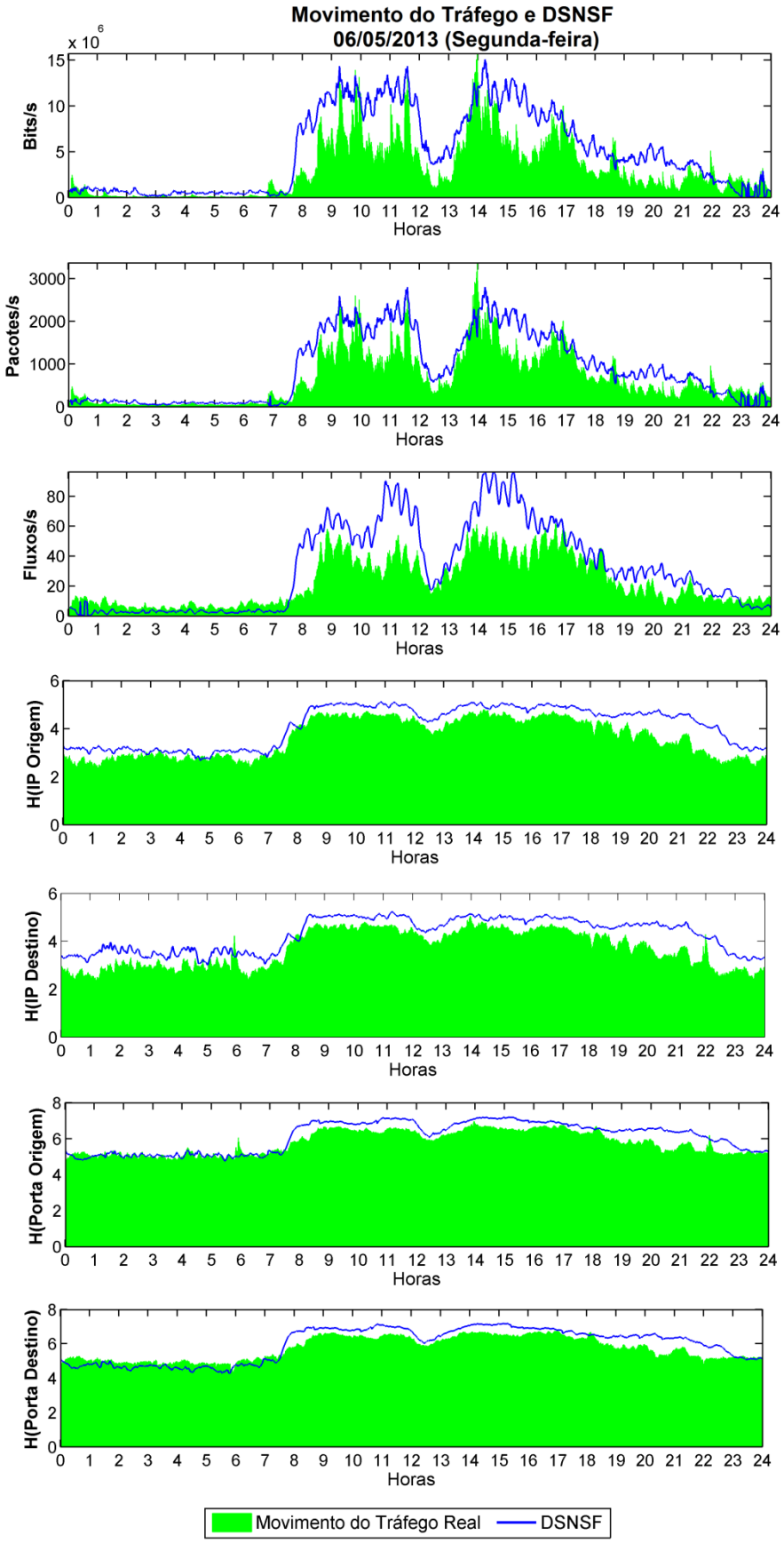

Figura 5.10 - DSNSF e movimento do tráfego do dia 06 de maio.

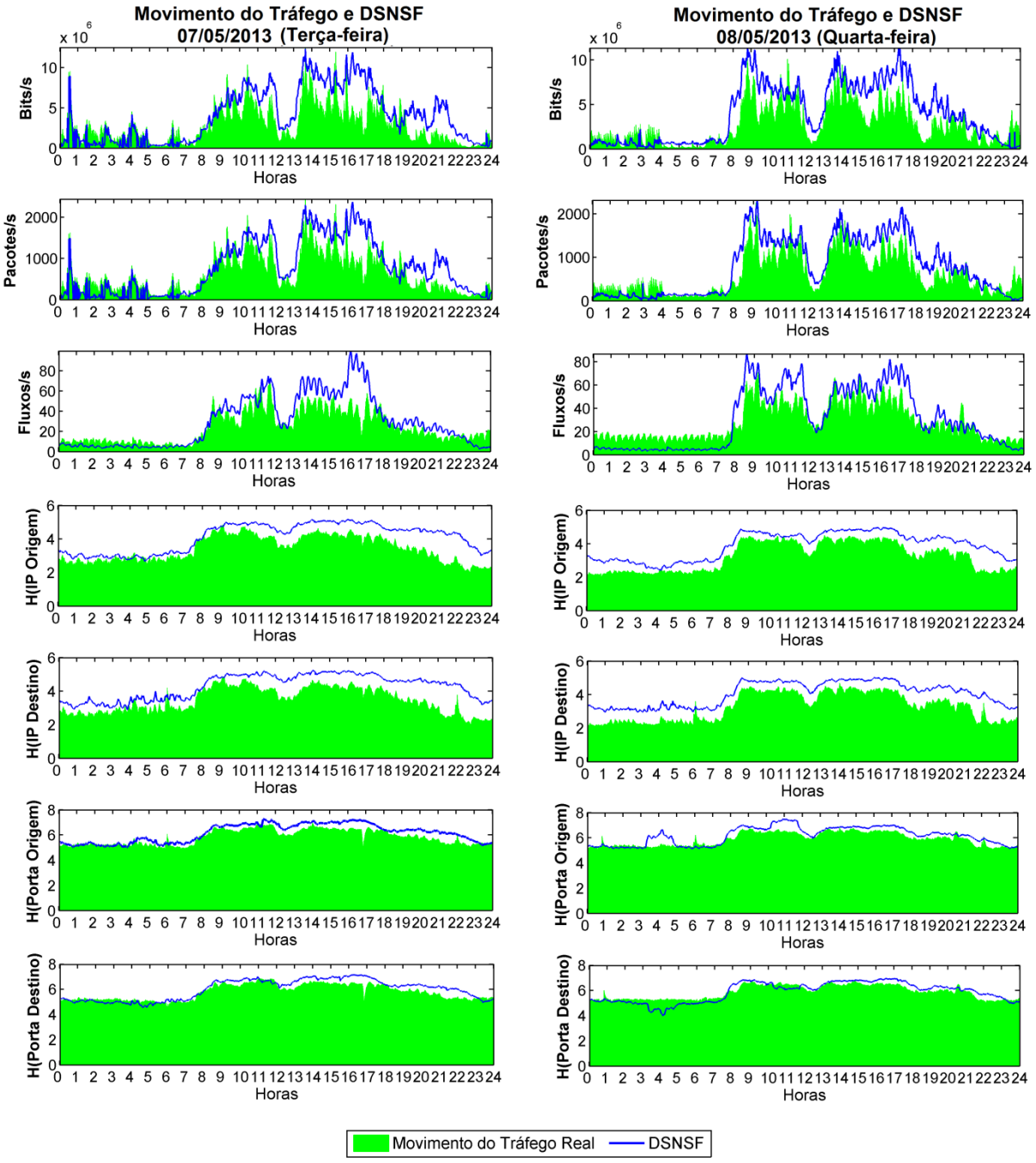

Figura 5.11 - DSNSF e movimento do tráfego dos dias 07 e 08 de maio.

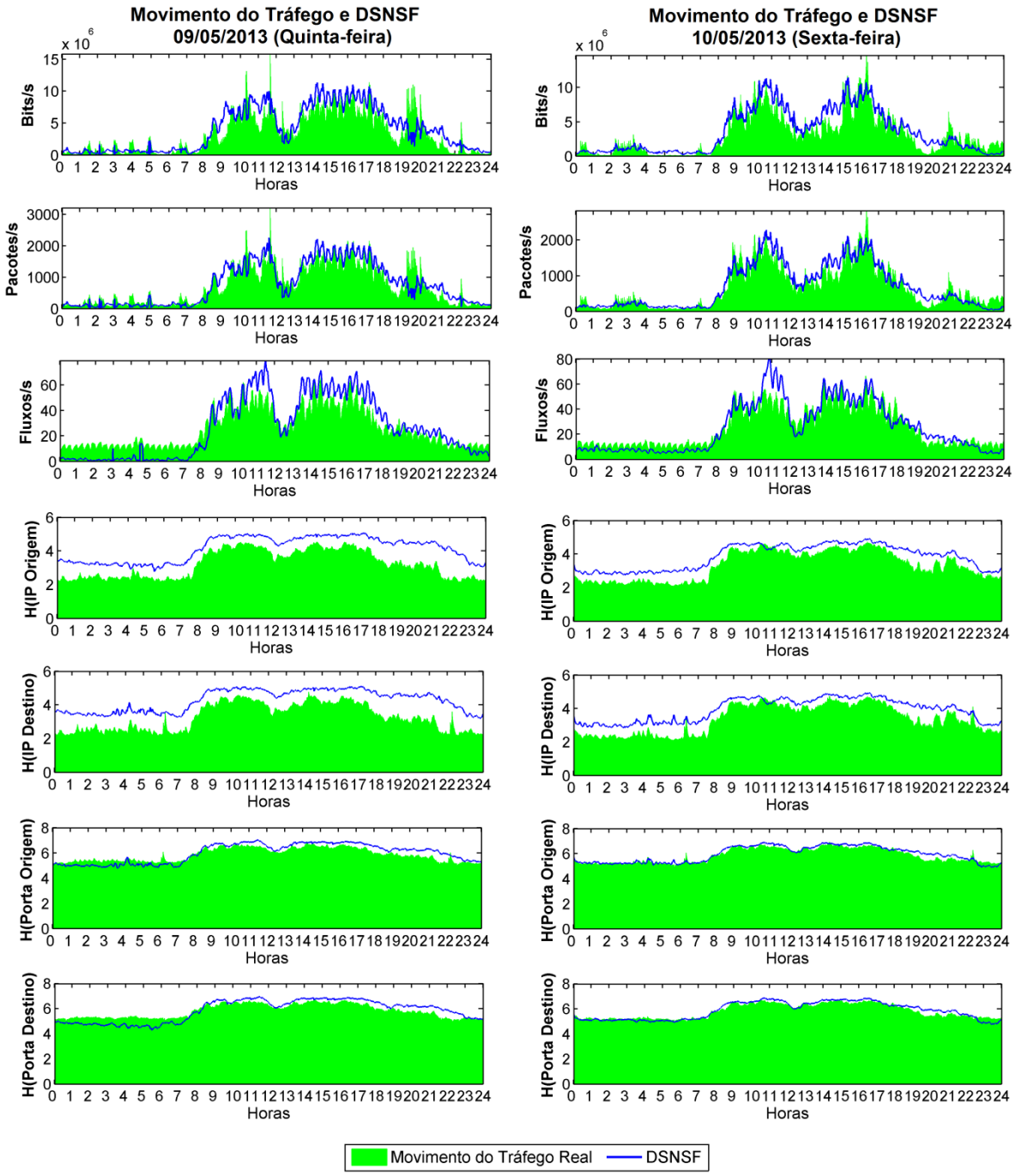

Figura 5.12 - DSNSF e movimento do tráfego dos dias 09 e 10 de maio.

O primeiro teste usado para verificar se o DSNSF é capaz de reconhecer as diversas características e peculiaridades do tráfego desse cenário é o NMSE. A Figura 5.13 ilustra os resultados para essa medida levando-se em conta as semanas analisadas. A média dos erros entre as sete dimensões do tráfego e o que foi verificada em cada um desses dias é apresentado. Ainda, novamente é utilizada a comparação entre diversos valores de γ para a abordagem de busca local.

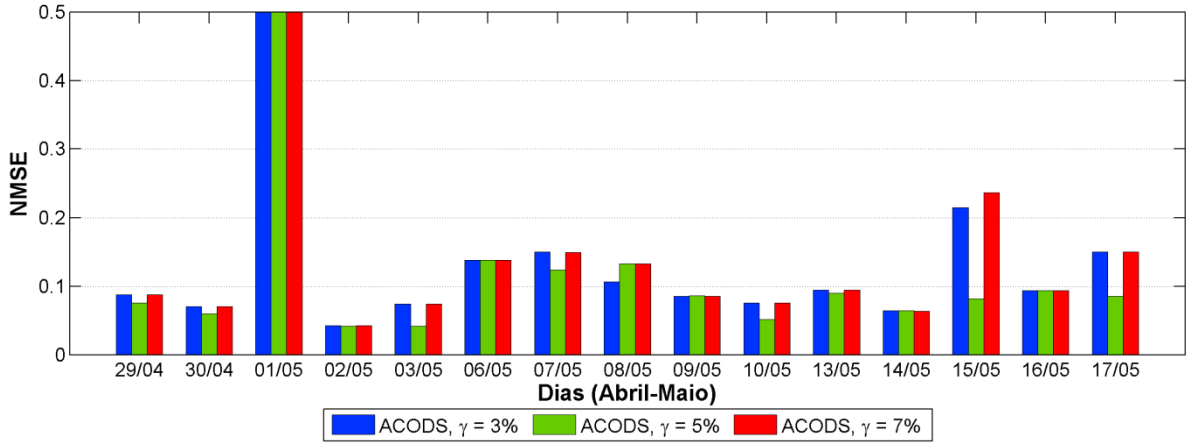

Figura 5.13 - Teste NMSE entre os DSNSF gerados e os movimentos reais de tráfego dos dias analisados.

Como pode ser observado, a maioria dos erros se manteve inferiores a 0,25 para os três valores assumidos pelo parâmetro γ. É possível verificar também que os melhores resultados foram obtidos quando esse parâmetro assumiu valor 5% e que em apenas uma ocorrência (dia 08 de maio) essa configuração ofereceu resultado pior e equivalente à busca local com $\gamma = 3\%$ e $\gamma = 7\%$, respectivamente. O dia que mais diferiu do padrão especificado pelo DSNSF foi 1 de maio, um feriado nacional. Embora para esse dia o teste de NMSE apresentasse erro próximo a 1,98, para melhor visualização dos resultados, o eixo y do gráfico foi ajustado para o valor 0,5.

Complementando a Figura 5.13, a Tabela 5.4 traz outra visão sobre os resultados da caracterização do tráfego. Os valores apresentados se referem à média calculada entre todos os dias para os atributos do fluxo. Dessa forma, é possível verificar que os atributos de volume apresentaram maiores erros, demonstrando a dificuldade de sua caracterização. Tal característica é influenciada diretamente pelo tamanho da rede analisada, em que apenas poucos usuários utilizando excessivamente a rede podem gerar grandes picos de tráfego, fazendo com que o comportamento analisado seja diferente do especificado pelo DSNSF.

Tabela 5.4 - Resultados do teste NMSE agrupados por atributos.

Atributo	$\gamma = 3\%$	$\gamma = 5\%$	$\gamma = 7\%$
Bits	0,6470	0,6033	0,6660
Pacotes	0,6662	0,6183	0,6719
Fluxos	0,2116	0,1802	0,2101
IP Origem	0,0284	0,0252	0,0277
IP Destino	0,0343	0,0303	0,0335
Porta Origem	0,0096	0,0097	0,0098
Porta Destino	0,0093	0,0093	0,0093

Os valores destacados na Tabela 5.4 representam os melhores valores encontrados para o teste NMSE. Como pode ser inferido pela Figura 5.13 e pela Tabela 5.4, o valor $\gamma = 5\%$ configura uma abordagem de busca local eficiente, capaz de melhorar o processo de criação de um perfil de comportamento normal do tráfego. Demais valores para γ foram analisados, entretanto, à medida que esse valor era incrementado, pior eram os resultados, consequência da eliminação de clusters necessários para a criação do DSNSF.

O gráfico da Figura 5.14 apresenta os resultados do teste de Bland-Altman para a rede da UTFPR. Novamente três valores são analisados para o parâmetro γ usado na busca local. Diferentemente da caracterização da rede demonstrado no cenário UEL, os resultados para UTFPR se mostraram modestos. Poucos dias atingiram taxas mais significativas do que 95% de concordância entre o DSNSF e o tráfego real, sendo todos eles conseguidos com $\gamma = 5\%$. Pode ser observado também que menores taxas são visualizadas na análise do dia 1 de maio. Devido ao feriado, o movimento do tráfego se manteve abaixo do esperado e consequentemente, diferiu do que era definido pelo DSNSF.

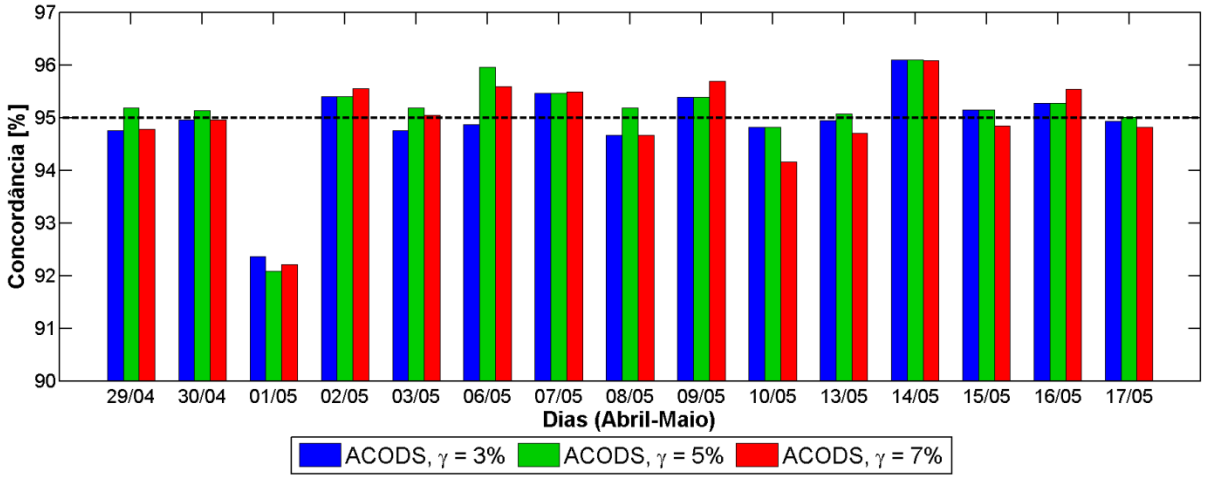

Figura 5.14 - Resultado do teste Bland-Altman entre os DSNSF gerados e os movimentos reais de tráfego dos dias analisados.

A Tabela 5.5 expõe os resultados do teste Bland-Altman, arranjados através das médias das taxas de concordâncias entre o DSNSF e o tráfego analisado. Essas médias foram calculadas para cada um dos sete atributos analisados.

Tabela 5.5 - Resultados do teste Bland-Altman agrupados por atributos.

Atributo	$\gamma = 3\%$	$\gamma = 5\%$	$\gamma = 7\%$
Bits	94,36	94,49	94,43
Pacotes	94,28	94,57	94,43
Fluxos	95,04	95,11	94,72
IP Origem	94,55	95,05	94,90
IP Destino	94,57	94,91	94,82
Porta Origem	95,48	95,33	95,36
Porta Destino	96,14	96,23	95,79

Como visto nas figuras que descrevem o movimento do tráfego para a rede UTFPR, os atributos *bits* e pacotes transmitidos apresentam comportamento mais instável que os demais. Essa propriedade também pode ser comprovada pela Tabela 5.5, em que as taxas de concordância para esses atributos não atingem 95%. Ainda, pode ser inferido que apenas para o atributo porta de origem, o valor $\gamma = 3\%$ garantiu um perfil de comportamento mais próximo ao que foi observado ao longo dos dias de análise. Tal exceção permite verificar que a entropia para esse atributo segue um padrão que pode ser facilmente extraído com o mínimo da interferência da busca local.

Levando-se em conta os erros para os distintos valores de γ, tanto no teste NMSE quanto no Bland-Altman, é observado que o atributo *bits* apresentou os piores valores. Embora as taxas de erro em relação ao valor adotado para o parâmetro γ variem em pequenas proporções como 0,13% e 0,7% para $\gamma = 3\%$ e $\gamma = 7\%$, respectivamente, cabe ressaltar que essa diferença tende a ser mais significativa à medida que as taxas de transferência das redes aumentam, uma vez que, esse valor pode representar uma alta variação do tráfego e caracterizar uma anomalia na qual grande quantidade de informação é comprometida.

Esse cenário ainda conta com a detecção de comportamentos anômalos. Dessa forma, é apresentada na Figura 5.15 a taxa de acurácia para as três semanas avaliadas. Como pode ser observado, os resultados se mantiveram ligeiramente inferiores aos alcançados durante a análise da rede UEL, pois a dificuldade de caracterização do tráfego da rede UTFPR torna a detecção pouco menos precisa. No entanto, embora a menor taxa de acurácia encontrada para a melhor abordagem de busca local seja 87,8%, a ADTW atingiu uma taxa média de 93,2% em relação à classificação correta dos intervalos anômalos.

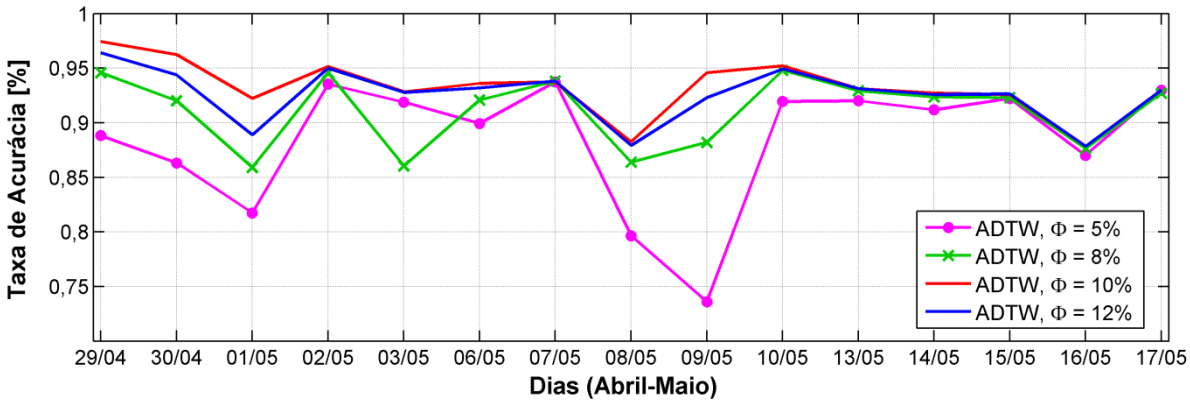

Figura 5.15 - Resultado do teste de acurácia para diversos valores de Φ.

Ainda sob essa análise, alguns aspectos que se fizeram notórios foram as características dos resultados de acurácia das diferentes redes para os variados valores de Φ. É possível inferir que a configuração $\Phi = 10\%$ apresenta o melhor resultado para o teste, provando que esse valor é válido tanto para esse ambiente quanto ao apresentado no cenário anterior. Porém, foi possível observar que durante o teste do tráfego gerado pela rede UEL, $\Phi = 8\%$ apresentou taxas próximas as melhores encontradas, enquanto $\Phi = 12\%$ obteve resultados muito inferiores. Para essa rede, quanto maior o limiar usado para detecção, menores são as taxas de verdadeiro-positivo e verdadeiro negativo e, consequentemente, piores são as taxas de acurácia. No cenário UTFPR, os resultados para $\Phi = 10\%$ e $\Phi = 12\%$ apresentam resultados equivalentes, demonstrando que até mesmo o tráfego normal varia intensamente em relação ao DSNSF e um limiar grande pode ser escolhido sem prejudicar a eficiência do sistema.

A Figura 5.16 mostra a curva ROC gerada para a detecção de comportamentos anômalos para os dados originados da rede UTFPR. Através da análise do gráfico fica evidente que os maiores valores testados para busca local apresentaram resultados semelhantes, porém com uma pequena vantagem quando utilizado $\Phi = 10\%$.

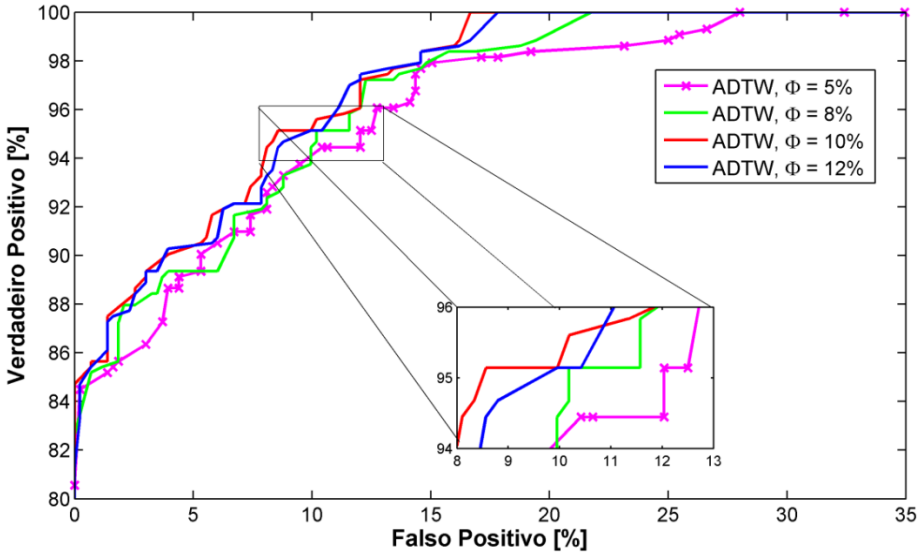

Figura 5.16 - Curva ROC para o cenário UTFPR.

Conclui-se ao fim deste cenário que o DSNSF construiu uma boa previsão em relação ao tráfego das três semanas de análise, conforme foi possível observar nos gráficos que representam os movimentos e as assinaturas geradas ao longo desses quinze dias. Por meio da avaliação estatística também foi possível confirmar a efetividade da ADTW na detecção de eventos anômalos. Portanto, foi demonstrado que o sistema é apto para realizar as tarefas para as quais foi projetado.

5.4 CENÁRIO 3: AVALIAÇÃO DA ABORDAGEM HEPTADIMENSIONAL

Com o objetivo de testar a eficácia do sistema também foram usadas anomalias sintéticas, isto é, tráfego gerado especificamente para simular certos comportamentos anômalos. A escolha das magnitudes de tais eventos é vital para que se produza um experimento realista. Desta forma, buscou-se a criação de ataques que causassem pequeno impacto ao comportamento do tráfego, de tal maneira que eles não pudessem ser detectados por uma métrica simples como contagem de *bits* ou pacotes. Em contrapartida, esses eventos deveriam ser suficientemente grandes para serem considerados prejudiciais à operação da rede.

Três tipos de ataques foram criados com diferentes intensidades, como mostrado na Tabela 5.6. O primeiro corresponde a um DDoS composto por solicitações geradas por múltiplas origens para um único endereço de destino. A segunda anomalia

compreende um ataque *port scan*, em que um único endereço de origem envia pacotes com a *flag* SYN habilitada às diferentes portas do destino com o objetivo de receber a confirmação, caso elas estejam ativas. O terceiro evento anômalo é um *flash crowd*, o que gera maior volume de tráfego de rede, proporcionando o aumento de *bits*, pacote e fluxos transmitidos. Para criar esses ataques foi utilizada a ferramenta Scorpius [70], desenvolvida pelo grupo Rigel de pesquisa em redes, situado no Departamento de Computação da Universidade Estadual de Londrina. Basicamente, esta aplicação injeta fluxos anômalos diretamente no tráfego exportado de acordo com o comportamento específico da anomalia desejada.

Tabela 5.6 - Características das anomalias sintéticas geradas para avaliar o sistema de detecção.

		Quantidade de IP Origem	IP Destino	Porta de Destino	Intervalos afetados	Período de injeção
DDoS	Evento 1	20	189.90.37.59	2935	139	29 de abril a 03 de maio
	Evento 2	10	189.90.221.116	7742	160	
Port Scan	Evento 1	40	189.90.115.60	20 a 25000	24	06 a 10 de maio
	Evento 2	30	189.90.240.65	20 a 32000	20	
Flash Crowd	Evento 1	10	189.90.250.32	4092	88	13 a 17 de maio
	Evento 2	5	189.90.250.21	9883	105	

Essas três anomalias são combinadas ao tráfego originado pela rede UEL e os horários escolhidos para que os eventos fossem incorporados correspondiam a intervalos que não apresentavam nenhuma anomalia. Na primeira semana de análise deste cenário, 299 intervalos foram preenchidos com a injeção do ataque DDoS. Ao longo da segunda semana o ataque *port scan* foi atribuído a 44 intervalos. Finalmente, a terceira semana teve 193 intervalos de um minuto afetados pelo ataque *flash crowd*. Como apresentado pela Tabela 5.6, o segundo evento de cada ataque tem uma intensidade inferior em relação ao primeiro, de modo que as características de volume são minimamente afetadas. O propósito dessas diferenças entre os eventos é de verificar se o ACODS pode construir uma assinatura digital que forneça uma previsão acurada do comportamento do tráfego. Além disso, espera-se avaliar, também, se tal assinatura é capaz de subsidiar a ADTW através do fornecimento de informações necessárias para o reconhecimento e classificação dos intervalos anômalos, independentemente da magnitude dos ataques gerados.

Esse cenário também se destina a verificar se os atributos descritivos contribuem para o reconhecimento de anomalias, apresentando melhorias em relação à detecção baseada somente no tráfego de *bits*, pacotes e fluxo. Assim, a Tabela 5.7, apresenta um comparativo entre os resultados da detecção utilizando a análise heptadimensional e a

abordagem baseada em volume. A precisão na detecção de anomalias de menor intensidade permaneceu satisfatória, porém com taxas inferiores às relatadas no reconhecimento de intervalos anômalos afetados pelos eventos de maiores proporções. O exemplo mais notório é o resultado do segundo ataque *port scan*. Nenhum dos intervalos em que os comportamentos anormais ocorreram é reconhecido através de detecção com baseada no volume do tráfego. O ataque *port scan* teve o menor índice de detecção, em que o ACODS conseguiu reconhecer 75% dos intervalos com essa anomalia. Por outro lado, os resultados para os ataques DDoS e *flash crowd* com menor intensidade atingiram 96,2% e 97,1%, respectivamente, utilizando a abordagem heptadimensional.

Tabela 5.7 - Comparação de anomalias detectadas utilizando as abordagens baseada em volume e análise heptadimensional do tráfego.

		Volume	7 dimensões
DDoS	Evento 1	135	139
	Evento 2	63	154
Port Scan	Evento 1	4	20
	Evento 2	0	15
Flash Crowd	Evento 1	84	86
	Evento 2	95	102
	(%) Intervalos Reconhecidos	71.08%	96.26%

Nesta avaliação, os resultados de detecção com base no volume permaneceram piores do que a abordagem heptadimensional. Utilizando essa última abordagem, as taxas de reconhecimento aumentaram cerca de 25,18%. Assim, verifica-se que a caracterização do tráfego normal, utilizando sete dimensões do fluxo IP é mais vantajosa do que apenas os três atributos fornecidos pela análise do volume do tráfego. Essa afirmação pode ser reforçada pela visualização da Figura 5.17. Ela compreende a segunda forma de relatório do sistema quando uma anomalia é detectada e sua função é demonstrar a relevância de cada atributo do fluxo para o reconhecimento dos ataques analisados.

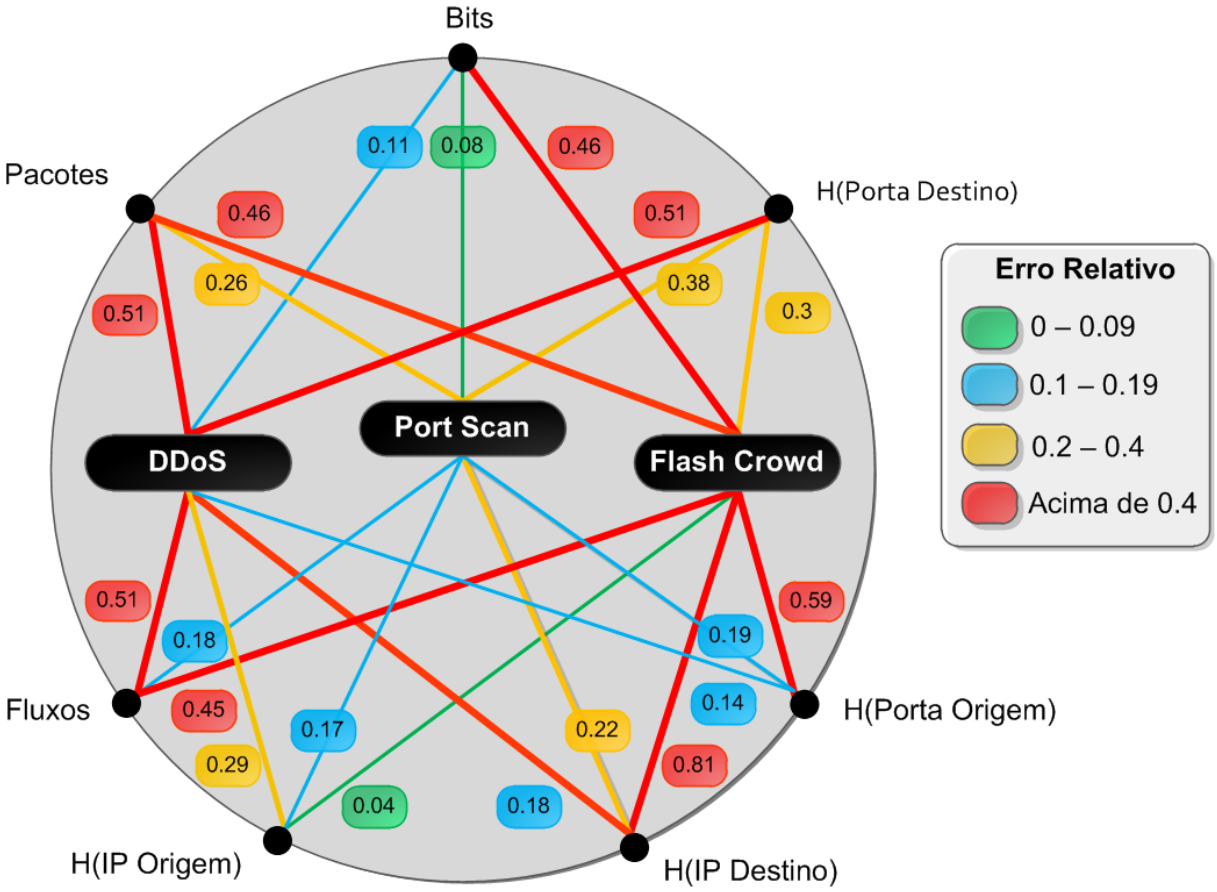

Figura 5.17 - Contribuição de cada atributo para gerar os comportamentos anômalos. Grandes valores para o fator F indicam que o atributo tem maior influência sobre a composição do ataque.

Na Figura 5.17 as linhas apresentam espessuras proporcionais à contribuição do atributo para composição do comportamento do ataque. Assim, ela demonstra a relevância de cada um dos atributos do fluxo para o reconhecimento das anomalias, ou seja, é possível verificar detalhadamente quais os atributos tiveram a maior variação comportamental comparado ao perfil fornecido pelo DSNSF. Por exemplo, a incidência dos atributos de volume é mais intensa durante um *flash crowd* do que na ocorrência de um *port scan*. Outro ponto importante a ser destacado é o tráfego anômalo gerado por esse último ataque. Por causa da pequena influência sobre o comportamento das sete dimensões, o *port scan* apresenta taxas de detecção ligeiramente mais baixas do que os demais ataques analisados.

Para a criação desse relatório, uma métrica quantitativa é estabelecida. O objetivo é fornecer uma medida que, primeiramente, mensure o desvio de comportamento do tráfego anômalo em relação ao padrão normal e, posteriormente, não utilize um valor

absoluto, uma vez que atributos de volume apresentariam valores exorbitantes, o que dificultaria a comparação com atributos descritivos (IP e portas), calculados com a entropia.

Para essa finalidade, um fator de importância é atribuído para cada atributo, relacionando-o a um determinado evento anômalo. Tal fator é calculado levando-se em conta o erro relativo entre o tráfego anômalo e a previsão gerada pelo DSNSF, como mostrado na Equação (5.3).

$$F_t = \frac{\sum_{t=1}^{T_a} \frac{|X_t - \Psi_t|}{\Psi_t}}{T_a} \tag{5.3}$$

Em que X é o perfil normal e T_a representa o total de intervalos anômalos. O fator F é calculado para cada intervalo t que compõe um determinado evento anômalo Ψ. Ao final, uma média entre os erros relativos da anomalia é calculada e apresentada.

Usando os campos do cabeçalho do pacote IP, a detecção de anomalias tem sua precisão aprimorada, permitindo uma classificação mais rigorosa dos comportamentos encontrados. Por exemplo, a distinção entre um ataque DDoS e um evento de *flash crowd* é difícil sem esses atributos descritivos. Ambas as anomalias mostram mudanças no tráfego relativo a *bits*, pacotes e fluxos e utilizando tais informações, apenas um diagnóstico impreciso é passível de ser realizado. Além disso, o ataque *port scan* não consegue uma boa taxa de detecção, utilizando apenas atributos de volume, como mostrou a Tabela 5.7. Porém, com a adição de informações sobre a entropia dos endereços IP e portas, a chance de sucesso é maior. Portanto, nota-se que um sistema cuja finalidade é auxiliar o administrador de rede na tomada de decisões, deve fornecer informações precisas sobre as atividades operacionais da rede, as quais podem ser adquiridas através da análise das sete dimensões de fluxo discutida neste trabalho.

5.5 CENÁRIO 4: COMPARAÇÃO COM K-MEANS

Na detecção baseada em perfis, a criação de um comportamento normal do tráfego é essencial para o desempenho do sistema. Por isso, uma comparação entre o DSNSF gerado pelo ACODS e a assinatura criada pelo tradicional método K-means é realizada para averiguar quão bem esses modelos conseguem extrair os diversos comportamentos do tráfego.

Ambas as abordagens são avaliadas sob as mesmas circunstâncias incluindo tamanho de janela de análise, número de clusters utilizados para clusterização e o mesmo período de teste.

K-means é um algoritmo de aprendizagem não-supervisionada para a partição de dados classificadores que divide uma população de tamanho N em K grupos [64]. É utilizado em vários campos de pesquisa por apresentar baixa complexidade computacional e praticidade em processar grandes amostras de dados. A seguir são mostrados os passos usados para execução do tradicional método de clusterização K-means.

Passo 1: Distribuir os elementos a serem clusterizados em um espaço de pesquisa. Também é necessário estabelecer os centros dos clusters (centróides) usados para o agrupamento dos dados.

Passo 2: Atribuir cada elemento ao cluster com o centróide mais próximo.

Passo 3: Quando os elementos estiverem alocados, recalcular a posição dos centros dos clusters.

Passo 4: Repetir os passos 2 e 3 até que o centróides não se movam ou até que o número máximo de iterações seja atingido.

Após a conclusão dos passos, o algoritmo retorna os índices que indicam a qual cluster cada elemento está associado. Além disso, como ocorre no ACODS, os valores do centróide, de cada cluster, ou seja, sua posição no plano também pode ser adquirida.

Um problema possível de ocorrer durante a execução do K-means é o cluster vazio, o qual acontece quando não ocorre a associação de nenhum elemento a um determinado cluster durante o processo de atribuição dos elementos aos clusters. Além de contradizer um dos princípios da clusterização, apresentado pela Equação (4.3), tal situação pode conduzir a solução a ótimos locais [71]. Aumentando-se o número de iterações pode-se ajudar a evitar esse problema.

Os erros absolutos das assinaturas geradas pelo ACODS e pelo método K-means são calculados através do teste NMSE e podem ser visualizados na Figura 5.18. Como pode ser observado, este teste procura avaliar também os diferentes valores atribuídos ao parâmetro γ para a DSNSF usando o método K-means.

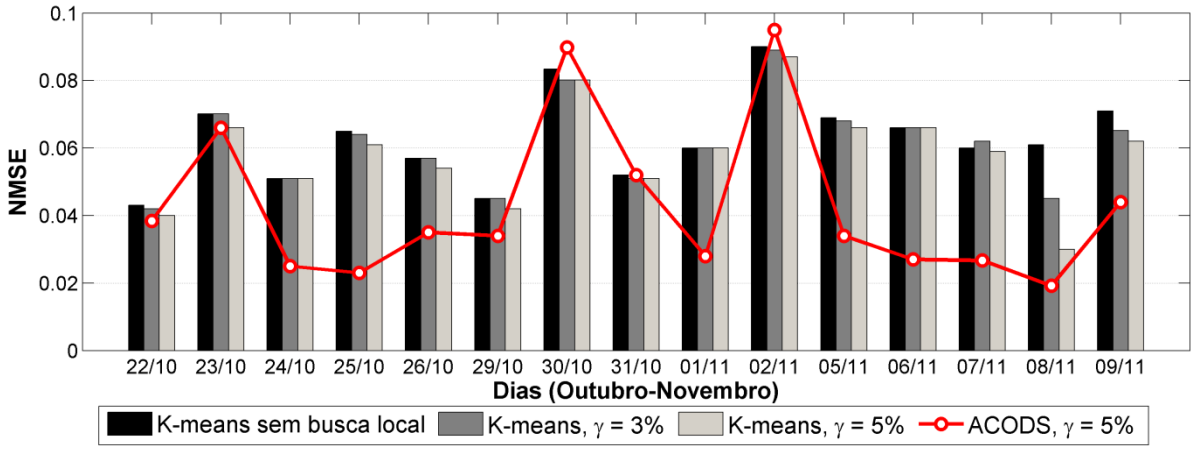

Figura 5.18 - Resultados para o teste NMSE comparando o melhor resultado do ACODS e as diversas assinaturas geradas pelo método K-means.

O melhor resultado expresso no cenário 1 pelo ACODS é comparado com os diversos resultados obtidos pelo K-means. Apenas para os dias 30 de outubro e 02 de novembro o valor do teste NMSE realizado sobre a assinatura do método K-means é inferior ao do ACODS. Também pode ser verificado que o valor atribuído à abordagem de busca local proporciona menores taxas de erros quando tem seu valor é igual a 5% para os DSNSF gerados pelo K-means.

O último teste de caracterização proposto apresenta o mesmo intuito do anterior, porém visa mensurar o grau de ajuste entre as assinaturas geradas pelo método K-means e o tráfego real, utilizando valores distintos para γ. Tais resultados são confrontados com o melhor resultado obtido pelo modelo ACODS. A Figura 5.19 apresenta os valores do teste Bland-Altman.

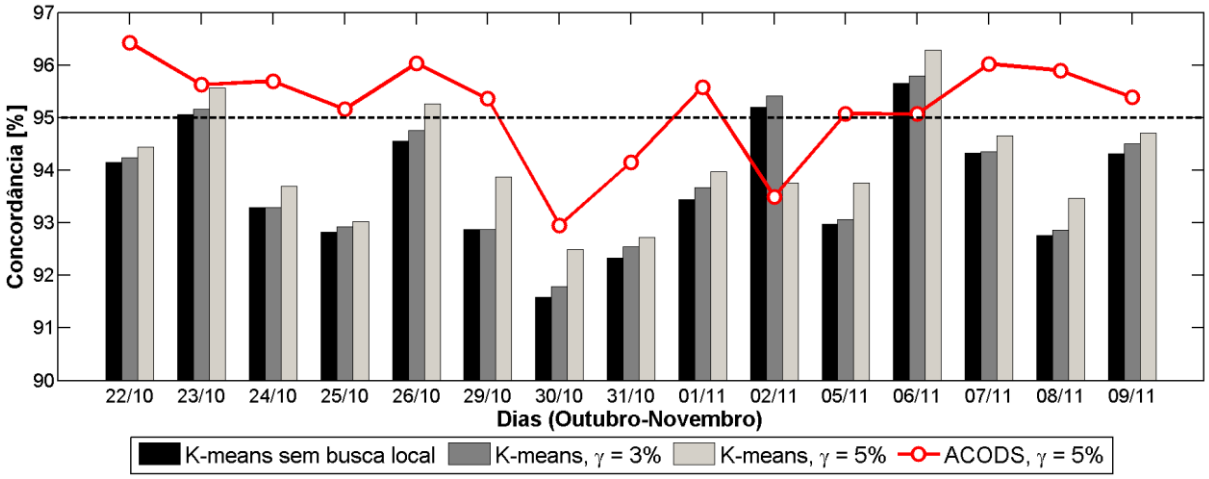

Figura 5.19 - Resultados para o teste Bland-Altman comparando o melhor resultado do ACODS e as diversas assinaturas geradas pelo método K-means.

O método K-means gerou várias assinaturas que apresentaram concordâncias inferiores à 95%, correspondendo a caracterizações de tráfego não satisfatórias. Através do teste Bland-Altman, novamente é comprovado que o ACODS conseguiu melhores resultados para a extração de padrões de comportamentos do tráfego e criação do DSNSF. Contudo, o DSNSF gerado pelo K-means obteve erros inferiores ao ACODS para os dias em que o tráfego não apresentou o comportamento previsto, conforme vinha acontecendo ao longo das semanas. Para melhor averiguação, a Figura 5.20 demonstra as assinaturas para o atributo *bits*/s de ambos os métodos, e estas são comparadas ao tráfego dos dias de comportamento incomum. Além disso, também são mostrados os dias pertencentes à semana anterior à esses dias excepcionais, os quais fizeram parte da base de dados necessários para a geração das assinaturas dos dias 30 de outubro e 2 de novembro de 2012.

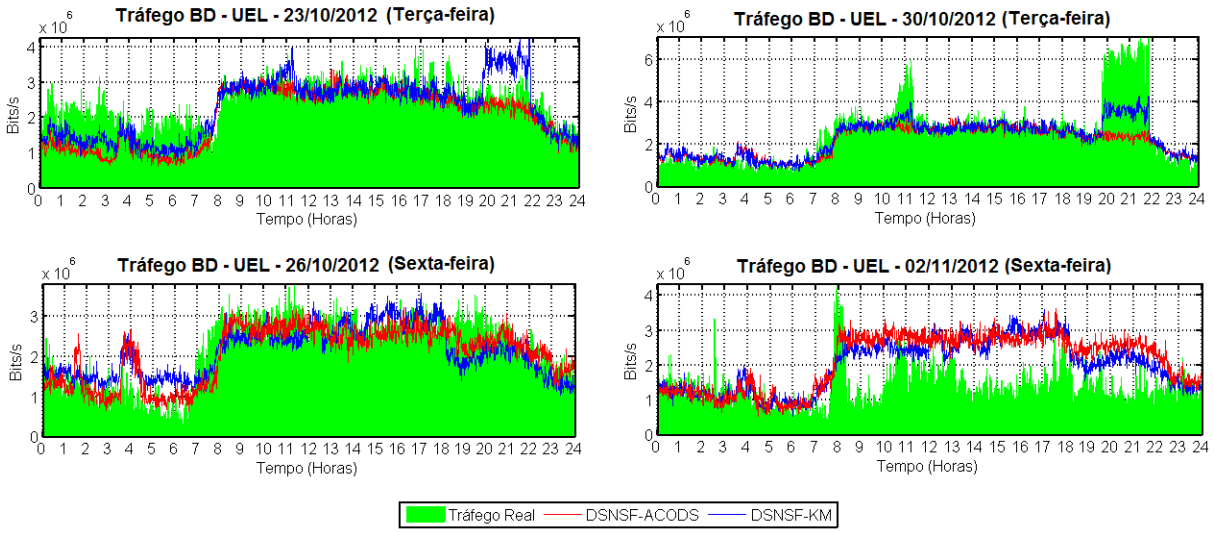

Figura 5.20 - Comparação entre as assinaturas geradas pelo ACODS e K-means aplicadas aos dias de tráfego incomum.

De acordo com os gráficos de movimento, pode-se inferir que o DSNSF gerado pelo método K-means apresenta grandes discrepâncias em relação à assinatura gerada pelo sistema ACODS, principalmente no intervalo de 19 as 22 horas das terças-feiras analisadas. Como verificado nos testes desse mesmo cenário, o DSNSF criado pelo ACODS apresentou melhores resultados durante a avaliação do dia 23 de outubro. Isso ocorre devido ao fato da sua proximidade em relação ao tráfego avaliado nesse dia. Em contrapartida, a assinatura gerada pelo método K-means é mais precisa em caracterizar o comportamento do dia 30 de outubro, sobretudo no intervalo entre as 19 as 22 horas. Porém, fica evidente que o evento ocorrido nesse período não é legítimo, portanto, a assinatura se ajusta a padrões que não dizem respeito ao perfil normal da rede.

Através da análise do movimento das sextas-feiras, dia 26 de outubro e 02 de novembro, confirma-se que ambos os métodos geraram assinaturas semelhantes para o atributo *bits*/s. Entretanto, a assinatura definida pelo K-means apresentou valores inferiores aos do DSNSF-ACO, tornando-se mais ajustável ao comportamento do tráfego durante um dia de feriado, em que o uso dos recursos da rede está abaixo do esperado para um dia comum.

O próximo passo da análise comparativa é verificar a capacidade das assinaturas de ambos os métodos em detectar anomalias. Para esse propósito, tanto o DSNSF gerado pelo ACODS quanto o construído pelo K-means são submetidos ao método de detecção ADTW, sob as mesmas circunstâncias incluindo tamanho de janela de análise e o mesmo período de teste.

A Figura 5.21 traz o resultado da taxa de acurácia para o DSNSF gerado pelo K-means, juntamente com uma comparação com o melhor resultado obtido por meio do ACODS. Mais uma vez, o resultado da detecção realizada com diferentes valores para o parâmetro Φ é demonstrado. É possível observar que os resultados da acurácia atingidos com $\Phi = 10\%$ e $\Phi = 12\%$, utilizando o método K-means, permaneceram próximos na maioria dos dias analisados. Entretanto, a diferença entre os dois resultados fica evidente quando comparadas as taxa verdadeiro-positivos e falso-positivos. Ainda sobre a acurácia, pode ser inferido que o sistema ACODS apresentou resultados melhores que os do K-means.

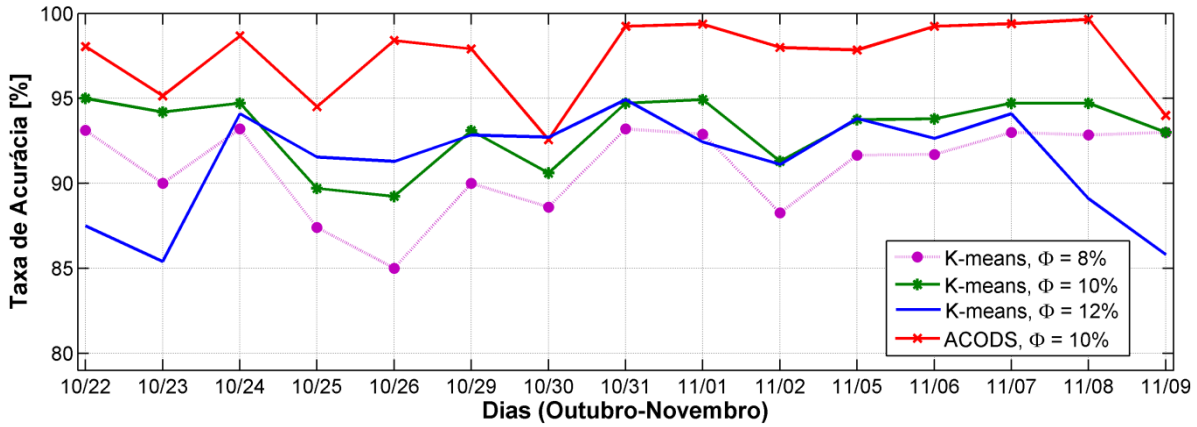

Figura 5.21 - Comparação entre os resultados do teste de acurácia para os DSNSF gerados pelo K-means e ACODS.

A Figura 5.22 apresenta o resultado da taxa de reconhecimento de anomalias em contraste com a taxa de falsos-positivos para a assinatura digital criado pelo método de clusterização K-means. Para fins de comparação, o melhor resultado obtido pelo ACODS no

cenário 1 é mostrado. Pode-se notar que o sistema apresentado neste trabalho obteve uma taxa maior de verdadeiro-positivos, com taxas de falso-positivos menores do que o K-means.

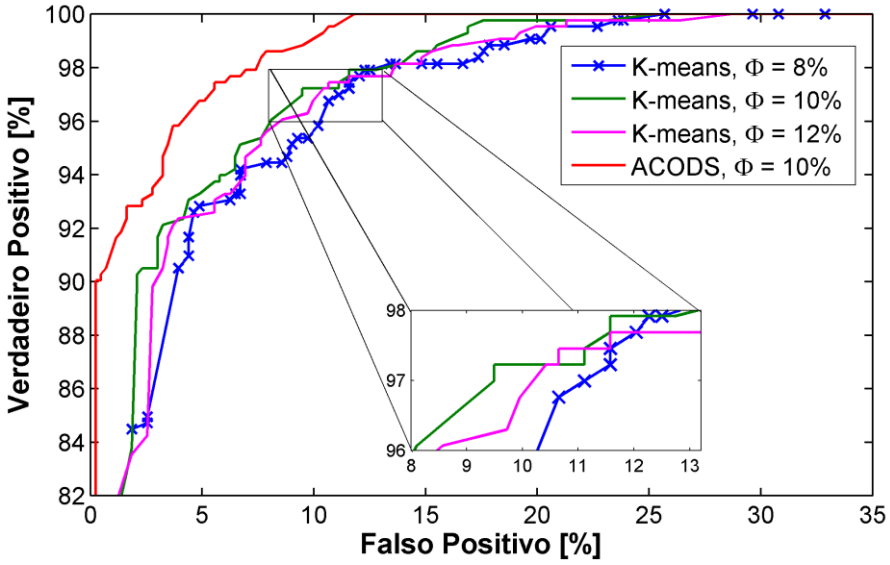

Figura 5.22 - Comparação entre as curvas ROC para os DSNSF gerado pelo K-means e ACODS. O melhor trade-off para ambos os métodos é alcançada quando Φ = 10%.

Apesar do método K-means apresentar boa taxa de acurácia usando $\Phi = 12\%$, o melhor resultado para detecção de eventos anômalos foi conseguido quando a ADTW utilizou $\Phi = 10\%$. Portanto, é possível inferir que o aumento do limiar de comportamento normal do tráfego, definido pelo parâmetro Φ, desfavorece a taxa de verdadeiros-positivos, da mesma forma que prejudica a taxa de falso-positivos, pois somente eventos de grande amplitude passam a ser detectados.

5.5.1 Análise de Complexidade

A complexidade computacional do método discutido é apresentada como a notação assintótica baseada na quantidade de instruções executadas. A complexidade do sistema ACODS é dada em primeiro lugar pela divisão de um conjunto de dados iniciais de E elementos em K centros de dimensão A, resultando em $O(EKA)$. Usando a população de formigas para auxiliar na busca dos melhores centros de agrupamento de dados e, como todas elas são comparadas umas as outras para encontrar a solução final, uma complexidade quadrática é adicionada, culminando em $O(EKAM^2)$. Tomando-se o número de iterações I como critério de parada do algoritmo de criação da assinatura digital, tem-se a complexidade

final $O(EKAM^2I)$. Para gerar um DSNSF de 24 horas, este processo é repetido 8640 vezes. Apesar de um número máximo de interações I ser definido, ACODS converge rapidamente para a solução. Quanto à ADTW, a complexidade computacional é o mesmo que do algoritmo tradicional *Dynamic Time Warping*, ou seja, $O(E^2)$ [57].

A escolha da construção do sistema com base em uma metaheurística é influenciada basicamente por duas questões: i) o tempo exigido para criação do DSNSF multidimensional é considerado primordial? ii) É preciso atingir boas soluções de clusterização com um custo baixo de processamento? Ambas as perguntas são importantes para aplicação abordada nesse trabalho, pois tratam do desempenho e da eficiência do sistema, respectivamente.

Com a finalidade de responder essas duas questões, foram observados os tempos gastos para geração do DSNSF baseado em sete dimensões para o ACODS e comparados com o K-means durante o intervalo de um minuto. As especificações de *hardware* e *software* do equipamento em que os testes foram executados são as seguintes: processador de dois núcleos com frequência 2,2 GHz, 3 GB de memória RAM, sistema operacional Windows Seven (32 *bits*). Os DSNSFs foram gerados por meio do aplicativo MATLAB (versão R2008b), utilizando a linguagem de programação que recebe o mesmo nome.

A Figura 5.23 demonstra a relação entre a convergência das soluções, medida através da função objetivo (Equação 4.5) e o número de iterações necessárias para cada método atingir esse valor. Por questões de simplicidade, são demonstrados os resultados pertencentes ao intervalo em que ambos os métodos obtiveram a convergência com o menor número de iterações durante a criação dos perfis de comportamentos gerados para análise desse cenário.

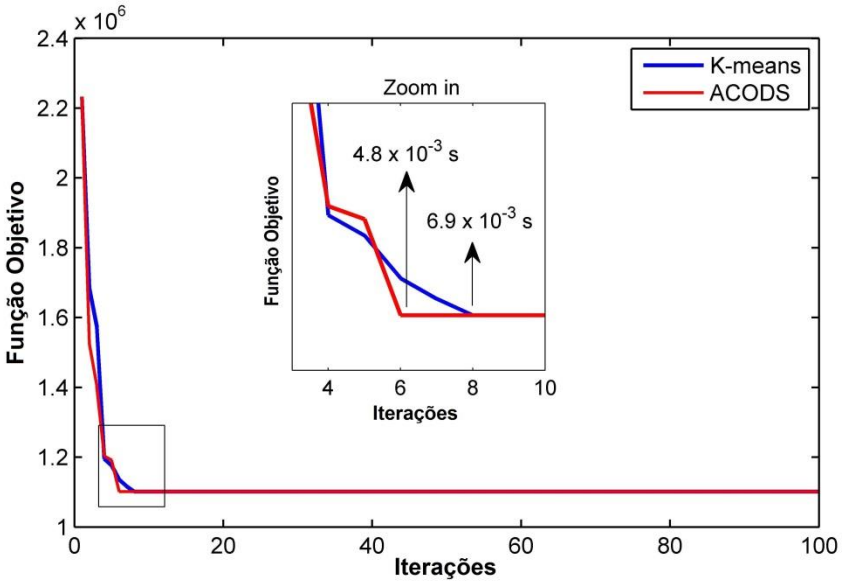

Figura 5.23 - Comparação do tempo necessário para a convergência de soluções. Pequenos valores para a função objetivo caracterizar um melhor agrupamento de dados.

É possível notar que o ACODS converge na sexta iteração enquanto o K-means alcança o mesmo estado apenas duas iterações depois. O resultado dessa convergência antecipada faz que com o sistema desenvolvido atinja o resultado desejado em apenas 4,8 x 10^{-3} segundos e a partir desse período não é possível encontrar nenhuma solução mais promissora para a clusterização dos dados. Embora esse exemplo apresente o melhor caso encontrado durante a análise, levando-se em consideração a qualidade da solução e o tempo gasto para encontrá-la, apenas pequenas variações foram observadas nos demais intervalos de outros dias.

Devido ao maior número de tarefas executadas pelo ACODS, em alguns casos K-means convergiu mais rapidamente, porém a solução criada não representava um ótimo DSNSF, o que explica os resultados melhores para caracterização do tráfego normal da rede apresentados pelo ACODS. Portanto, é passível de ser concluído que as rotinas extras como a abordagem de busca local e a atualização de feromônio que tornam a execução do ACODS mais complexa, contribuem para uma rápida convergência de soluções de qualidade. Dessa forma, o sistema apresentado se equipara ao K-means em tempo de execução, porém, oferece soluções mais promissoras que compõem um DSNSF capaz de auxiliar o administrador da rede de forma eficiente.

6 CONCLUSÃO

Monitorar o comportamento do tráfego tornou-se crucial para assegurar a efetividade da gerência de redes. No entanto, é impossível executar um acompanhamento manual do tráfego em sistemas de rede que estão constantemente crescendo em tamanho e complexidade. Dessa forma, este trabalho teve como objetivo tratar de tal problema, fornecendo uma ferramenta capaz de caracterizar o tráfego de um segmento de rede e detectar eventos anômalos, proporcionando informações atualizadas sobre o uso de recursos de rede para que os administradores possam mantê-la em pleno funcionamento.

Este trabalho apresentou os benefícios obtidos pela combinação de um modelo heurístico bio-inspirado e um algoritmo de mineração de dados utilizados para reconhecimento de padrões do tráfego. Dessa forma, foi possível o desenvolvimento de uma ferramenta para a detecção de anomalias que utiliza a clusterização juntamente com uma adaptação da metaheurística Ant Colony Optimization (ACO), resultando no sistema *Ant Colony Optimization for Digital Signature* (ACODS). Através da simulação de uma colônia de formigas em tarefas do cotidiano, este sistema analisa o histórico do tráfego e por meio da sua caracterização, descreve o comportamento normal do tráfego de rede.

O sistema desenvolvido foi avaliado em dois ambientes reais de rede e um simulado, mostrando-se apto para a tarefa de criação do perfil normal do tráfego e detecção de anomalias. Também foi possível verificar que a análise multidimensional de fluxos IP é eficiente para a caracterização, permitindo uma abordagem alternativa aos trabalhos em que somente atributos de volume são utilizados. Além disso, ao se analisar os atributos endereços IP e portas, um diagnóstico detalhado do comportamento da rede pode ser fornecido ao administrador, incluindo a localização de agentes e eventos maliciosos.

A utilização de protocolos de exportação de fluxos como o IPFIX, NetFlow e sFlow, além de proporcionar uma vasta gama de atributos referente ao tráfego de rede, torna possível a personalização das análises dos fluxos IP de acordo com critérios exigidos pelo administrador e requeridos pelos serviços prestados pela rede. Essa característica, combinada ao monitoramento proativo do tráfego realizado pelo ACODS, possibilitou a geração de alarmes indicativos de ocorrência de eventos que diferiram do perfil normal de comportamento da rede. Um exemplo notório foi a detecção de um evento *flash crowd*, que por meio do relatório disponibilizado pelo sistema, foi possível verificar que essa anomalia foi desencadeada devido à divulgação do resultado do concurso público da polícia civil. O

sistema ainda apresentou significativas taxas de detecção para as anomalias simuladas DDoS e *port scan,* em contraste com as baixas taxas de falsos alarmes.

Durante os testes, o tradicional método de clusterização K-means foi utilizado para extrair os perfis normais de comportamento da rede com o intuito de compará-los às assinaturas geradas pelo ACODS. O sistema apresentado demonstrou melhores resultados para geração do DSNSF devido a três características. A primeira é a capacidade de auto-organização dos agentes, a qual contribui para a construção rápida de boas soluções de clusterização. Dessa forma, foi possível observar que o ACODS convergiu para a solução final utilizando um menor número de iterações. A segunda também é relacionada ao comportamento dos agentes. Enquanto o K-means produz uma solução para clusterização a cada iteração, no ACODS cada agente está apto a realizar essa tarefa. Entretanto, melhores soluções são alcançadas por meio da interação coletiva entre todas as formigas, resultando em um processo de aprendizagem distribuído. Essa característica faz com que todos os agentes trabalhem cooperativamente na construção da caracterização do tráfego.

Ainda durante a análise, foi verificado que o K-means eventualmente fez uso de muitas iterações para resolver o problema de cluster nulo. A terceira característica do ACODS resolve esse problema. Através da evaporação do feromônio, soluções que levam a este evento são excluídas do espaço de busca ao longo das iterações. Além desse benefício, esse recurso evita convergências precipitadas, as quais limitam a exploração de soluções possíveis para extração de padrões do tráfego.

Outro aspecto importante a ser salientado com uso da metaheurística ACODS é a aplicação da abordagem de busca local na geração do DSNSF. Quando aplicada, essa abordagem possibilita a eliminação de comportamentos do tráfego que não são habituais ou não apresentam periodicidade na sua ocorrência. Provou-se que, até um limite especificado para a exclusão destes comportamentos, a caracterização do tráfego é favorecida. Juntamente com essa abordagem, para garantir que comportamentos legítimos que não se encontravam no DSNSF fossem erroneamente interpretados como anomalias, um modelo de detecção flexível foi usado.

A ADTW permitiu avaliar o DSNSF e o tráfego analisado para garantir melhores taxas de acurácia na detecção de anomalias, em detrimento da taxa de falsos-positivos. Através do alinhamento das séries temporais, é possível reconhecer comportamentos legítimos diferentes daqueles descritos pela caracterização por causa de deslocamentos temporais. Além disso, a ADTW fornece um limiar que identifica comportamentos anômalos, ao levar em conta a amplitude e duração desses eventos durante a

análise de tráfego. Esta técnica ainda contribui para redução de notificação de falsas anomalias, pois relaciona os comportamentos dos atributos visando encontrar padrões anômalos no tráfego.

Os resultados obtidos demonstraram que o ACODS é eficiente tanto para a caracterização de tráfego quanto para a detecção de anomalias. Por meio da automatização do processo de detecção e geração de alarmes, baseados nos limites definidos pelas assinaturas digitais, a responsabilidade atribuída ao administrador de monitorar visualmente o tráfego de vários segmentos de rede ao mesmo tempo pode ser excluída em alguns casos. As vantagens decorrentes dessa praticidade são a exclusão do erro derivado de operadores humanos, além da possibilidade de direcionar todos os esforços para os problemas que realmente merecem atenção. Desta forma, a abordagem apresentada neste trabalho se mostra adequada para auxiliar o gerenciamento de redes, detectando anomalias de tráfego e, consequentemente, contribuindo para o aumento da disponibilidade e confiabilidade para redes e os serviços prestados. Portanto, é possível concluir que o ACODS pode vir a ser utilizado como referência para a construção de um sistema autônomo futuro, capaz de agir e combater por conta própria os eventos anômalos detectados.

Os trabalhos futuros incluem o aprimoramento da correlação dos atributos do tráfego na composição da assinatura de ataques, visando a criação de um modelo que leve em consideração a arquitetura da rede para o reconhecimento do caminho de propagação da anomalia. Também será estudada a viabilidade de incluir dias dos finais de semana e novos atributos na análise realizada pelo sistema de caracterização e detecção. É pretendido averiguar a influência da amostragem de pacotes durante a caracterização do tráfego, bem como utilizar mais cenários, ataques e comparações com outros sistemas de detecção para consolidar a validação do ACODS.

Trabalhos publicados pelo Autor

1. CARVALHO, L. F.; ASSIS, M. V. O.; FERNANDES Jr., G.; RODRIGUES, J. J. P. C.; PROENÇA JR, Mario Lemes. **Digital Signature of Network Segment using PCA, ACO and Holt-Winters for Network Managemen**t. In: 15th IEEE International Conference on e-Health Networking, Application & Services (IEEE Healthcom 2013), 2013, Lisbon. 15th IEEE International Conference on e-Health Networking, Application & Services (IEEE Healthcom 2013). Lisbon, 2013. **(Qualis B4)**.

2. CARVALHO, L. F.; RODRIGUES, J. J. P. C.; BARBON, S. J.; PROENÇA JR, Mario Lemes. **Using Ant Colony Optimization Metaheuristic and Dynamic Time Warping for Anomaly Detection**. In: 21st International Conference on Software Telecomunications and Computer Networks (SoftCOM 2013), 2013, Split-Primosten. International Conference on Software Telecomunications and Computer Networks (SoftCOM), 2013. **(Qualis B4)**.

3. ASSIS, M. V. O.; CARVALHO, L. F.; RODRIGUES, J. J. P. C.; PROENÇA JR, Mario Lemes. **Holt-Winters Statistical Forecasting and ACO Metaheuristic for Traffic Characterization**. In: IEEE International Conference on Communications (ICC 2013), 2013, Budapest. IEEE International Conference on Communications, 2013. **(Qualis A2)**.

4. CARVALHO, L. F.; ZACARON, A. M.; ADANIYA, M. H. A. C. ; PROENÇA JR, Mario Lemes. **Ant Colony Optimization for Creating Digital Signature of Network Segments using Flow Analysis**. In: XXXI International Conference of the Chilean Computer Science Society (SCCC'2012), 2012, Valparaíso. Proceedings of XXXI International Conference of the Chilean Computer Science Society (SCCC'2012), 2012. **(Qualis B3)**.

5. ZACARON, A. M.; CARVALHO, L. F.; ADANIYA, M. H. A. C.; ABRAO, T.; PROENÇA JR, Mario Lemes. **Digital Signature of Network Segment using Flow Analysis**. In: The International Joint Conference on e-Business and Telecommunications (ICETE 2012) / DCNET 2012, 2012, Rome. DCNET 2012 Proceedings of the International Conference on Data Communication Networking, 2012. **(Qualis B4)**.

6. ZACARON, A. M.; CARVALHO, L. F.; ADANIYA, M. H. A. C.; ABRAO, T.; PROENÇA JR, Mario Lemes. **Assinatura Digital de Segmento de Rede Utilizando Análise de Fluxos e Clusterização K-means**. In: SEMISH - 39th Seminar on Hardware and Software, 2012, Curitiba. XXX Congresso da Sociedade Brasileira de Computação, 2012. **(Qualis B4)**.

REFERÊNCIAS

[1] SYSTEMS, C. Netflow for Accounting, Analysis and Attack. Disponível em: < http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html >. Acesso em: Setembro de 2013.

[2] SYSTEMS, C. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017**:** 34 p. 2013.

[3] ZARPELÃO, B. B. Detecção de Anomalias em Redes de Computadores. Tese de Doutorado. Faculdade de Engenharia Elétrica e de Computação (FEEC), Universidade Estadual de Campinas (UNICAMP), 2010.

[4] PROENÇA, M. L. Baseline Aplicado a Gerência de Redes. Tese de Doutorado. Faculdade de Engenharia Elétrica e de Computação (FEEC), Universidade Estadual de Campinas (UNICAMP), Campinas, 2005.

[5] SECURITY, P. PandLabs Annual Report 2012. Disponível em: < http://press.pandasecurity.com/wp-content/uploads/2013/02/PandaLabs-Annual-Report-2012.pdf >. Acesso em: Dezembro de 2013.

[6] HERRERO, Á.; CORCHADO, E.; GASTALDO, P.; ZUNINO, R. Neural projection techniques for the visual inspection of network traffic. *Neurocomputing***,** v. 72, n. 16–18, p. 3649-3658, 2009. ISSN 0925-2312.

[7] JIANG, J.; PAPAVASSILIOU, S. Enhancing network traffic prediction and anomaly detection via statistical network traffic separation and combination strategies. *Computer Communications***,** v. 29, n. 10, p. 1627-1638, 2006. ISSN 0140-3664.

[8] SHON, T.; KOVAH, X.; MOON, J. Applying genetic algorithm for classifying anomalous TCP/IP packets. *Neurocomputing***,** v. 69, n. 16–18, p. 2429-2433, 2006. ISSN 0925-2312.

[9] PATCHA, A.; PARK, J.-M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks***,** v. 51, n. 12, p. 3448-3470, 2007. ISSN 1389-1286.

[10] THOTTAN, M.; CHUANYI, J. Anomaly detection in IP networks. *IEEE Transactions on Signal Processing,***,** v. 51, n. 8, p. 2191-2204, 2003. ISSN 1053-587X.

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

[12] GROSSMAN, R. L. Data Mining: Challenges and Opportunities for Data Mining During the Next Decade 2000.

[13] CORRAL, G.; ARMENGOL, E.; FORNELLS, A.; GOLOBARDES, E. Explanations of unsupervised learning clustering applied to data security analysis. *Neurocomputing***,** v. 72, n. 13–15, p. 2754-2762, 2009. ISSN 0925-2312.

[14] MAZEL, J.; CASAS, P.; LABIT, Y.; OWEZARSKI, P. Sub-Space clustering, Inter-Clustering Results Association & anomaly correlation for unsupervised network anomaly detection. *(2011) 7th International Conference on Network and Service Management (CNSM)* 2011. 1-8 p.

[15] ROCHA, E.; SALVADOR, P.; NOGUEIRA, A. A multi-variate classification approach for the detection of illicit traffic. *(2011) 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2011. 1-6 p.

[16] LU, K.; WU, D.; FAN, J.; TODOROVIC, S.; NUCCI, A. Robust and efficient detection of DDoS attacks for large-scale internet. *Computer Networks***,** v. 51, n. 18, p. 5036-5056, 2007. ISSN 1389-1286.

[17] KIM, S. K.; LEE, S. H.; SEO, S. W. An automatic portscan detection system with adaptive threshold setting. *Journal of Communications and Networks***,** v. 12, n. 1, p. 74-85, 2010. ISSN 1229-2370.

[18] KIM, H.-A.; KARP, B. Autograph: toward automated, distributed worm signature detection. Proceedings of the 13th conference on USENIX Security Symposium - Volume 13. San Diego, CA: *USENIX Association***:** 19-19 p. 2004.

[19] BYUNGSEUNG, K.; SAEWOONG, B.; HYOGON, K. FDF: Frequency Detection-Based Filtering of Scanning Worms. *(2006) IEEE International Conference on Communications (ICC)*, 2006. 2124-2129 p.

[20] LIMA, M. F.; SAMPAIO, L. D. H.; ZARPELÃO, B. B.; RODRIGUES, J. J. P. C.; ABRAO, T.; PROEN; X00E; A, M. L. Networking Anomaly Detection Using DSNs and Particle Swarm Optimization with Re-Clustering. *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010. 1-6 p.

[21] 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*, 2005. 290-295 p.

[22] ADANIYA, M. H. A. C.; LIMA, M. F.; RODRIGUES, J. J. P. C.; ABRAO, T.; PROENCA, M. L. Anomaly detection using DSNS and Firefly Harmonic Clustering Algorithm. *Communications (ICC), 2012 IEEE International Conference on*, 2012. 1183-1187 p.

[23] ZACARON, A. M.; CARVALHO, L. F.; ADANIYA, M. H. A. C.; ABRÃO, T.; JR., M. L. P. Digital Signature of Network Segment using Flow Analysis. DCNET/ICE-B/OPTICS. OBAIDAT, M. S.;SEVILLANO, J. L.;ZHANG, Z.;MARCA, D. A.;VAN SINDEREN, M.;MARZO, J.-L. e NICOPOLITIDIS, P.: *SciTePress***:** 35-40 p. 2012.

[24] CASAS, P.; VATON, S.; FILLATRE, L.; NIKIFOROV, I. Optimal volume anomaly detection and isolation in large-scale IP networks using coarse-grained measurements. *Computer Networks***,** v. 54, n. 11, p. 1750-1766, 2010. ISSN 1389-1286.

[25] AMARAL, A. A.; ZARPELÃO, B. B.; MENDES, L. d. S.; RODRIGUES, J. J. P. C.; PROENÇA JUNIOR, M. L. Inference of network anomaly propagation using spatio-temporal correlation. *Journal of Network and Computer Applications***,** v. 35, n. 6, p. 1781-1792, 2012. ISSN 1084-8045.

[26] HUNT, R. SNMP, SNMPv2 and CMIP — the technologies for multivendor network management. *Computer Communications***,** v. 20, n. 2, p. 73-88, 1997. ISSN 0140-3664.

[27] KENYON, T. 9 - Network Management. In: KENYON, T. (Ed.). Data Networks. Burlington: Digital Press, 2002. p.633-711. ISBN 978-1-55558-271-5.

[28] PERKINS, D.; MCGINNIS, E. Understanding SNMP MIBs. Prentice-Hall, 1997.

[29] CASE, J.; FEDOR, M.; SCHOFFSTALL, M.; DAVIN, J. A Simple Network Management Protocol (SNMP) RFC 1157.

[30] CASE, J.; MCCLOGHRIE, K.; ROSE, M.; WALDBUSSER, S. Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2). RFC 1905.

[31] CASE, J.; MUNDY, R.; PARTAIN, D.; STEWART, B. Introduction and Applicability Statements for Internet Standard Management Framework RFC 3410.

[32] QUITTEK, J.; ZSEBY, T.; CLAISE, B.; ZANDER, S. Requirements for IP Flow Information Export (IPFIX). RFC 3917.

[33] CLAISE, B. Cisco Systems NetFlow Services Export Version 9. RFC 3954.

[34] CLAISE, B.; WOLTER, R. Network management: Accounting and Performance Strategies. *White Paper*. EUA. 2007

[35] SYSTEMS, C. Introduction to Cisco IOS NetFlow. Disponível em: < http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html >. Acesso em: Setembro de 2013.

[36] SYSTEMS, C. NetFlow Version 9 Flow-Record Format. Disponível em: < http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html >. Acesso em: Setembro de 2013.

[37] CLAISE, B.; JOHNSON, A.; QUITTEK, J. Packet Sampling (PSAMP) Protocol Specifications. RFC 5476.

[38] QUITTEK, J.; BRYANT, S.; CLAISE, B.; AITKEN, P.; MEYER, J. Information Model for IP Flow Information Export. RFC 5102.

[39] PHAAL, P.; PANCHEN, S.; MCKEE, N. InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. RFC 3176.

[40] CORPORATION, I. Traffic Monitoring using sFlow. Disponível em: < http:// www.sflow.org/sFlowOverview.pdf >. Acesso em: Setembro de 2013.

[41] LAKHINA, A.; CROVELLA, M.; DIOT, C. Mining anomalies using traffic feature distributions. Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications. Philadelphia, Pennsylvania, USA: *ACM***:** 217-228 p. 2005.

[42] SHUYING, C.; XUESONG, Q.; ZHIPENG, G.; KE, L.; FENG, Q. A flow-based anomaly detection method using sketch and combinations of traffic features. *Network and Service Management (CNSM), 2010 International Conference on*, 2010. 302-305 p.

[43] HUI, F. A Novel Clustering Algorithm with Ant Colony Optimization. *Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. PACIIA '08.* , 2008. 66-69 p.

[44] ELHDHILI, M. E.; BEN AZZOUZ, L.; KAMOUN, F. CASAN: Clustering algorithm for security in ad hoc networks. *Computer Communications***,** v. 31, n. 13, p. 2972-2980, 2008. ISSN 0140-3664.

[45] SÀNCHEZ-ARTIGAS, M.; GARCÍA-LÓPEZ, P.; GÓMEZ-SKARMETA, A. F.; SANTA, J. TR-clustering: Alleviating the impact of false clustering on P2P overlay networks. *Computer Networks***,** v. 52, n. 17, p. 3185-3204, 2008. ISSN 1389-1286.

[46] YUN, Y.; KE, C. Temporal Data Clustering via Weighted Clustering Ensemble with Different Representations. *IEEE Transactions on Knowledge and Data Engineering***,** v. 23, n. 2, p. 307-320, 2011. ISSN 1041-4347.

[47] DENEUBOURG; ARON, S.; GOSS, S.; PASTEELS, J. M. The self-organizing exploratory pattern of the argentine ant. *Journal of Insect Behavior***,** v. 3, n. 2, p. 159-168, 1990. ISSN 0892-7553.

[48] DORIGO, M.; CARO, G.; GAMBARDELLA, L. Ant Algorithms for Discrete Optimization. *Artificial Life***,** v. 5, n. 2, p. 137-172, 1999. ISSN 1064-5462.

[49] DORIGO, M. S., Thomas. Ant Colony Optimization: *Massachusetts Institute of Technology***:** 39 p. 2004.

[50] DORIGO, M.; BIRATTARI, M.; STUTZLE, T. Ant colony optimization artificial ants as a computational intelligence technique. *IEEE Comput. Intell. Mag.***,** v. 1, n. 4, p. 28-39, 2006.

[51] KOLIAS, C.; KAMBOURAKIS, G.; MARAGOUDAKIS, M. Swarm intelligence in intrusion detection: A survey. *Computers & Security***,** v. 30, n. 8, p. 625-642, 2011. ISSN 0167-4048.

[52] HONG, J.; QINGSONG, Y.; YU, G. An improved ant colony clustering algorithm. *Biomedical Engineering and Informatics (BMEI), 2010 3rd International Conference on*, 2010. 2368-2372 p.

[53] SHELOKAR, P. S.; JAYARAMAN, V. K.; KULKARNI, B. D. An ant colony approach for clustering. *Analytica Chimica Acta***,** v. 509, n. 2, p. 187-195, 2004.

[54] BAO-JIANG, Z. An Ant Colony Clustering Algorithm. *(2007) International Conference on Machine Learning and Cybernetics,* , 2007. 3933-3938 p.

[55] DUNN, J. C. A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters. *Journal of Cybernetics***,** v. 3, n. 3, p. 32-57, 1973. ISSN 0022-0280.

[56] ROUSSEEUW, P. J. Silhouettes: A graphical aid to the interpretation and validation of cluster analysis. *Journal of Computational and Applied Mathematics***,** v. 20, n. 0, p. 53-65, 1987. ISSN 0377-0427.

[57] ESLING, P.; AGON, C. Time-series data mining. *ACM Comput. Surv.***,** v. 45, n. 1, p. 1-34, 2012. ISSN 0360-0300.

[58] SAKOE, H.; CHIBA, S. Dynamic programming algorithm optimization for spoken word recognition. *IEEE Transactions on Acoustics, Speech and Signal Processing***,** v. 26, n. 1, p. 43-49, 1978. ISSN 0096-3518.

[59] MYERS, C.; RABINER, L.; ROSENBERG, A. E. Performance tradeoffs in dynamic time warping algorithms for isolated word recognition. *IEEE Transactions on Acoustics, Speech and Signal Processing,***,** v. 28, n. 6, p. 623-635, 1980. ISSN 0096-3518.

[60] JUNIOR, S. B. Dynamic Time Warping baseado na Transformada Wavelet. Dissertação de Mestrado. Departamento de Física e Informática, Universidade de São Paulo, 2007.

[61] SOULE, A.; KAV; SALAMATIAN; TAFT, N. Combining filtering and statistical methods for anomaly detection. Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. Berkeley, CA: *USENIX Association***:** 31-31 p. 2005.

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

[63] HAAG, P. NFDUMP. Disponível em: < http://nfdump.sourceforge.net >.

[64] MACQUEEN, J. Some methods for classification and analysis of multivariate observations. *Proc. Fifth Berkeley Symp. on Math. Statist. and Prob.*: Univ. of Calif. Press, 1967. 281-297 p.

[65] 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, 1993. ISSN 0960-1686.

[66] ALTMAN, D. G.; BLAND, J. M. Measurement in Medicine: The Analysis of Method Comparison Studies. *The Statistician***,** v. 32, n. 3, p. 307-317, 1983. ISSN 00390526.

[67] 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.

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

[69] LEI, J. Z.; GHORBANI, A. A. Improved competitive learning neural networks for network intrusion and fraud detection. *Neurocomputing***,** v. 75, n. 1, p. 135-145, 2012. ISSN 0925-2312.

[70] ASSIS, M. V. O. Scorpius - sFlow Anomaly Simulator. Disponível em: < http://redes.dc.uel.br/scorpius >. Acesso em: Março de 2014.

[71] FANG, C.; JIN, W.; MA, J. -Means algorithms for clustering analysis with frequency sensitive discrepancy metrics. *Pattern Recognition Letters***,** v. 34, n. 5, p. 580-586, 2013. ISSN 0167-8655.