Capítulo

3

Tráfego Internet não Desejado: Conceitos, Caracterização e Soluções

Eduardo Feitosa[1,2], Eduardo Souto[2], Djamel Sadok[1].

[1]Centro de Informática – Grupo de Pesquisa em Redes e Telecomunicações (GPRT)
Universidade Federal de Pernambuco
Caixa Postal 7851 – Recife – PE - Brasil

[2]Departamento de Ciência da Computação (DCC)
Universidade Federal do Amazonas
69077000 - Manaus - AM - Brasil

{elf, jamel}@cin.ufpe.br, esouto@ufam.edu.br

Abstract

In today's Internet architecture, the unwanted traffic generated by technological trends in network, new applications and services, and security breaches has affected a large portion of the Internet. This chapter presents the unwanted traffic universe including definitions, classification, and the reasons that explain its growth. It also points out the shortcomings of the existent solutions for detection of unwanted traffic. Lastly, this chapter presents potential solutions and a list of research topics and open problems on unwanted Internet traffic.

Resumo

Na atual arquitetura da Internet, o tráfego não desejado gerado por tendências tecnológicas em redes, novas aplicações e serviços, e violações de segurança tem afetado uma porção cada vez maior da Internet. Este capítulo apresenta o universo do tráfego não desejado incluindo definições, classificação e os motivos que explicam seu surpreendente crescimento. Além disso, aponta as deficiências das soluções existentes e recentes para detecção de tráfego indesejado. Por fim, este capítulo apresenta potenciais soluções e enumera temas de pesquisa em aberto sobre tráfego não desejado na Internet.

3.1. Introdução

Uma breve análise do tráfego Internet comprova o crescente aumento no transporte do tráfego considerado desconhecido, não solicitado, improdutivo e muitas vezes ilegítimo, em outras palavras, tráfego não desejado. Originado através de atividades como, por exemplo, mensagens eletrônicas não solicitadas (*spam*); atividades fraudulentas como *phishing*[1] e *pharming*[2]; ataques de negação de serviço (do inglês *Distributed Denial of Service* - DDoS); proliferação de vírus e *worms*; *backscatter*[3], entre outros, o tráfego não desejado pode ser considerado uma pandemia cujas conseqüências refletem-se no crescimento dos prejuízos financeiros dos usuários da Internet.

Exemplos de perdas financeiras podem ser encontrados em todo o mundo. Em 2006, os prejuízos ocasionados por *worms* foram de aproximadamente US$ 245 milhões, somente entre provedores de acesso norte-americanos [Morin, 2006]. O instituto de segurança americano CSI (*Computer Security Institute*) [Richardson, 2007], depois de entrevistar 194 empresas nos Estados Unidos, contabilizou perdas superiores a US$ 66 milhões ocasionadas pelo tráfego não produtivo gerado principalmente por fraudes, vírus, *worms*, *spyware* e intrusões em 2007. No Brasil, o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) contabilizou o número de incidentes relacionados às tentativas de fraude em 45.298 em 2007 [CERT.br, 2008] enquanto que, no mesmo período, o CAIS (Centro de Atendimento a Incidentes de Segurança) da RNP (Rede Nacional de Pesquisa) registrou cerca de 4000 tentativas de fraudes através de *spam* e *phishing*.

Parte desses prejuízos se deve a ineficiência das atuais soluções em identificar, reduzir e interromper o tráfego não desejado. Tipicamente, a efetividade fornecida pelas soluções existentes só é percebida após a ocorrência de algum dano. Além disso, a alta taxa de alarmes falsos e a falta de cooperação com outras soluções ou mesmo com a infra-estrutura de rede são fatores considerados incentivadores do aumento do tráfego não desejado. Como mencionado em [Oliveira et al., 2007], as soluções usadas para detectar e reduzir os efeitos de ataques DDoS tais como filtragem, limitação de banda, IP *traceback* e esquemas de marcação de pacotes são difíceis de implementar porque necessitam de mudanças na infra-estrutura da Internet. Ao mesmo tempo, soluções tradicionais como firewall e VPN (*Virtual Private Network*) são ineficazes contra códigos maliciosos e *spam*.

Outro ponto relacionado à ineficácia das atuais soluções é a definição do que é tráfego não desejado. Uma vez que normalmente parte deste tipo de tráfego é o resultado de atividades recreativas como o download de músicas e vídeos e jogos on-line. Como exemplos de aplicações utilizadas nas atividades recreativas temos: as aplicações P2P como Emule, Bit Torrent e Kazaa; as aplicações utilizadas na

---

[1] *Phishing* é um tipo de fraude eletrônica caracterizada pela tentativa de obter informações pessoais privilegiadas (por exemplo, números de cartões de créditos e senhas) através de sites falsos ou mensagens eletrônicas forjadas.

[2] *Pharming* é o termo atribuído ao ataque baseado no envenenamento de cache DNS que, consiste em corromper o DNS em uma rede de computadores, fazendo com que a URL de um site passe a apontar para um servidor diferente do original.

[3] *Backscatter* é o tráfego recebido de vítimas que estão respondendo a ataques de negação de serviço.

comunicação instantânea como Skype, MSN e Google Talk; e aplicações de tempo real como rádio e TV via Internet como Joost, Justin.TV[4], entre outros. Muitas das soluções existentes não reconhecem ou são configuradas para não detectar o tráfego gerado por essas atividades.

3.1.1. Definições

O termo "tráfego não desejado" foi introduzido na década de 80 e sempre esteve relacionado com atividades maliciosas como vírus, *worms*, intrusões e ataques em baixa escala. Já a nomenclatura que o tipifica como qualquer tráfego Internet não solicitado, não produtivo, não desejado e ilegítimo é recente.

O trabalho de Pang et al. [Pang et al., 2004] define tráfego não desejado como sendo um tráfego não produtivo composto por uma parte maliciosa (causada pelo tráfego de *backscatter* associado a atividades maliciosas como varreduras por vulnerabilidades, *worms*, mensagens de *spam*, etc.) e uma parte benigna (causada por má configuração de roteadores, *flash crowds*, etc.). Soto [Soto, 2005] complementa essa definição, afirmando que o tráfego não desejado também pode ser gerado pelo tráfego "corrompido" devido a ruído ou interferências em linhas de transmissão da rede.

Em [Xu et al., 2005], tráfego não desejado é caracterizado como aquele malicioso ou não produtivo cuja finalidade é comprometer computadores (*hosts*) vulneráveis, propagar códigos maliciosos, proliferar mensagens de *spam* e negar serviços. Outras nomenclaturas para definir tráfego não desejado são: tráfego lixo (*junk traffic*), tráfego de fundo (*background*) e tráfego anormal.

Em linhas gerais, a definição mais genérica sobre tráfego não desejado é qualquer tipo de tráfego de rede não requisitado e/ou inesperado, cujo único propósito é consumir recursos computacionais da rede, desperdiçar tempo e dinheiro dos usuários e empresas e que pode gerar algum tipo de vantagem ou benefício (lucro) para seus criadores.

Entretanto, não existe um consenso sobre o que é ou não tráfego indesejado. Comumente, essa definição depende do contexto em que está localizada e/ou da aplicação que está sendo utilizada. Por exemplo, a China trata o tráfego gerado pelo SkypeOut[5] (especificamente chamadas feitas de computadores para telefones comuns) como ilegal porque afeta a receita das operadores de telefonia. Seguindo a mesma linha de raciocínio, provedores de serviço Internet, empresas de telecomunicações, empresas públicas e privadas têm limitado o uso de aplicações *peer-to-peer* (P2P) alegando que este tipo de tráfego não é produtivo e é potencialmente empregado para proliferação de vírus e distribuição de códigos maliciosos, além de ferir e quebrar as leis de direitos autorais. Na linha de aplicações consideradas "proibidas" estão IRC (*Internet Relay Chat*), sites de relacionamento (Orkut, MySpace, Facebook, entre outros), mensagens instantâneas (MSN, Google Talk, ICQ) e jogos on-line.

[4] http://www.justin.tv
[5] http://www.skype.com

3.1.2. Discussões

Tráfego não desejado e não solicitado não é nenhuma novidade na Internet. No entanto, nos últimos 10 anos, este tipo de tráfego cresceu de forma surpreendente em volume de informação e sofisticação, atingindo níveis considerados alarmantes. Mas como explicar essa explosão? Fatores como a filosofia aberta da Internet (sem centros de controle), a existência de uma indústria ilícita por trás da produção e a proliferação de tráfego indesejado, a pouca importância atribuídas às questões de segurança, entre outros podem ajudar a explicar o significativo aumento do tráfego não desejado.

A preocupação com este tipo de tráfego é tamanha que congressos e workshops como o SRUTI (*Steps to Reducing Unwanted Traffic on the Internet*) [SRUTI, 2005], que desde 2005 vem sendo realizado para discutir os problemas e apresentar novas soluções. Até o momento, o evento mais importante nesta área foi o workshop do IAB (*Internet Architecture Board*) sobre tráfego não desejado, realizado em Março de 2006. Seu objetivo foi o de promover o intercâmbio de informações e experiências entre operadores, fabricantes, desenvolvedores e pesquisadores. Outro objetivo foi levantar projetos e tópicos de pesquisa que provavelmente serão geridos pelo IAB, IETF (*Internet Engennering Task Force*), IRTF (*Internet Research Tack Force*) e pela comunidade no desenvolvimento de soluções contra o tráfego não desejado. O resultado do workshop foi descrito na RFC (*Request for Comments*) 4948 [Anderson et al., 2007] que relata os tipos de tráfego não desejado encontrados na Internet, suas principais causas, as soluções existentes e as ações a serem tomadas para resolver o problema.

3.1.3. Organização do Capítulo

Diante do exposto, torna-se claro que o tráfego não desejado apresenta-se como um dos principais problemas de segurança e que precisa de soluções que contribuam para redução de seu atual nível, embora que ainda não seja trivial produzi-las. Quais os tipos de tráfego não desejado estão disponíveis na Internet? Qual é o objetivo de cada um? Quais são e onde estão as principais fontes de tráfego? O que precisa ser feito para atenuar os efeitos destes tipos de tráfego? Estas perguntas precisam ser respondidas cuidadosamente se quisermos continuar a utilizar a Internet. Os autores deste minicurso partilham da opinião de que a descoberta e interceptação precoce do tráfego não desejado é o modo mais seguro de garantir danos limitados.

O restante deste capítulo está organizado da seguinte forma. A seção 3.2 caracteriza o tráfego não desejado apresentando as principais vulnerabilidades da Internet que permitem sua geração e proliferação. Além disso, também são descritos os principais tipos de ataques, atividades e aplicações relacionados ao tráfego indesejado. Esta seção finaliza com a apresentação de algumas taxonomias. A seção 3.3 apresenta as soluções existentes contra o tráfego não desejado. Tais soluções são divididas em tradicionais (por exemplo, firewall, honeypots e ferramentas de medição de tráfego) e as baseadas na análise do tráfego. Em ambos os casos, as vantagens e desvantagens de cada solução são comentadas. A seção 3.4 discute soluções consideradas potencias e/ou futuras. Esta seção tem o intuito de apresentar ferramentas, aplicações e soluções disponíveis (implementadas) apontadas como promissoras na contenção do tráfego não desejado, mas cuja implantação exige mudanças na infra-estrutura da Internet ou apenas vontade e incentivo para fazê-la. Além disso, os autores deste minicurso apresentam

uma nova proposta nesta seção. Por fim, a seção 3.5 apresenta os comentários finais sobre o tema e aponta algumas questões em aberto.

3.2. Caracterização de Tráfego não Desejado

A atual estratégia de pesquisa sobre tráfego não desejado é baseada em três passos:

i) Adquirir conhecimento sobre as origens e os diferentes tipos de tráfego não desejado;

ii) Avaliar o impacto e a efetividade das soluções existentes; e

iii) Desenvolver novas contramedidas eficazes contra o tráfego não desejado.

Esta seção foca no primeiro passo, descrevendo as principais vulnerabilidades da Internet que contribuem para a geração de anomalias de tráfego e ataques a sua infra-estrutura. Além disso, os principais tipos de tráfego não desejado são apresentados, classificados e exemplificados.

3.2.1. Vulnerabilidades e Problemas Conhecidos

O tráfego não desejado está presente na Internet desde seu surgimento. Vírus, má configuração de dispositivos e serviços, ataques DoS e intrusões eram incidentes típicos, causados por pessoas que tentavam chamar atenção ou provar suas habilidades para o mundo. Com o passar dos anos, tais incidentes foram sendo adaptados e/ou substituídos por atividades abusivas e maliciosas em larga escala (por exemplo, *spam*, *worms*, etc.)

Existem diversas explicações para essa "evolução", até certo ponto natural, dos incidentes e a conseqüente massificação do tráfego não desejado. Na visão deste minicurso, os mais importantes são:

1. **A natureza aberta (sem controle) da Internet**

   A Internet é uma das poucas plataformas operacionais que funcionam sem centros de controle. Fato este que acabou contribuindo para seu efetivo sucesso. Contudo, essa característica impõe uma série de limitações técnicas e problemas, especialmente de segurança. A identificação de um atacante é um bom exemplo. Em um ambiente distribuído e diversificado como a Internet, a tarefa de descobrir um atacante é extremamente difícil, visto que a comunicação pode ser feita entre computadores localizados em qualquer lugar do mundo. Além disso, a pilha de protocolos TCP/IP que possibilita essa comunicação não disponibiliza qualquer mecanismo de auditoria que permita o acompanhamento das ações realizadas por um atacante. Como resultado, não existe um limite bem definido sobre o que um computador pode fazer e também não existe qualquer tipo de registro "disponível" do que um computador fez após um incidente.

2. **A veracidade dos endereços de origem**

   Muitos dos ataques encontrados na Internet caracterizam-se pela existência de endereços IP de origem forjados (falsificados). Uma vez que a "falta de controle" é característica funcional da Internet, cabe a cada elemento da rede que recebe pacotes com origens questionáveis ou desconhecidas decidir se aceita ou não, sob pena de bloquear tráfego requisitado e legítimo ou permitir ataques de negação de serviço. Atualmente, existem *Botnets* ou redes zumbi que são

formadas por um conjunto de computadores infectados por códigos maliciosos que permitem que esses computadores sejam controlados remotamente para a realização de diversos ataques. Portanto, a questão vai além da diferenciação da veracidade dos endereços IP de origem.

3. **O mau uso dos protocolos na Internet**

   Devido ao fato de sistemas de segurança e firewall bloquearem portas não usadas, o protocolo HTTP (*Hyper Text Tranfer Protocol*), usado inicialmente para acessar sites web, agora é constantemente empregado como protocolo de transporte genérico para aplicações que tem pouca ou nenhuma relação com a web como, por exemplo, comunicação VoIP e compartilhamento de arquivos. A explicação é simples, o HTTP tem caminho liberado em quase todos os firewalls. Assim, é mais fácil reaproveitar a infra-estrutura de comunicação do HTTP em novas aplicações ao invés de projetar aplicações seguras e que negociam passagem pelos filtros de segurança e firewall. O resultado é que a mesma infra-estrutura Internet utilizada para realizar tarefas cotidianas como acessar sites web, ler mensagens de correio eletrônico, conversar com pessoas e até fazer compras, também é utilizada para divulgar o tráfego não desejado.

4. **Computadores e sistemas comprometidos**

   A existência de enormes quantidades de computadores e sistemas comprometidos capazes ou efetivamente usados em atividades maliciosas serve como campo fértil para a proliferação do tráfego não desejado. Basicamente, o que acontece é que existe uma enorme quantidade de usuários (pessoas e empresas) novatos ingressando no ambiente da Internet, onde grande parte desses usuários não é preparada ou não está interessada em questões de segurança. Associado a este fato, diariamente são descobertas vulnerabilidades em sistemas operacionais, plataformas e aplicações. A soma desses dois fatos torna a Internet um local adequado e convidativo para o tráfego não desejado. Exemplos como, o aparecimento do grande número de *worms* que exploram erros de programação e falhas de segurança em sistemas operacionais e aplicativos (por exemplo, Code Red[6] e Code-Red II[7]), sites e e-mails falsificados que instalam códigos maliciosos no computador das vítimas e aplicações P2P que ajudam a disseminar vírus são noticiados quase que diariamente no mundo todo. Além disso, já faz um bom tempo que as atividades maliciosas não são realizadas por "iniciantes curiosos" utilizando *script kiddies*[8]. Atualmente, atacantes e criminosos contratam programadores profissionais para desenvolver ferramentas avançadas para comprometer computadores e sistemas. O pior é que muitas dessas ferramentas estão disponíveis na Internet para melhorias (código aberto) e para uso por novos atacantes.

5. **Autenticação**

---

[6] http://www.cert.org/advisories/CA-2001-19.html
[7] http://www.cert.org/advisories/CA-2001-23.html
[8] Códigos genéricos usados por atacantes iniciantes para realizar ataques e intrusões

> Considere o seguinte (e cada vez mais comum) cenário: "um usuário com um *smartphone* está conectado a rede sem fio da empresa onde trabalha. Ao se deslocar para uma reunião fora da sede, o seu aparelho passa a fazer parte da rede corporativa da operadora de telefonia celular GPRS (*General Packet Radio Service*). Ao parar para tomar um café, é interligado a uma rede pública através de um *hotspot*. Ao chegar à reunião, o aparelho é novamente adicionado à rede da empresa". Apesar de existirem soluções mais simplificadas que permitam toda essa mobilidade, o atual processo de autenticação de usuários e dispositivos conectados a redes ainda é demasiadamente complexo para ser considerado viável ou fácil de usar. Geralmente, os mecanismos de autenticação são vinculados ao tipo de meio físico utilizados, onde são empregadas diferentes credenciais, semânticas e bases de dados de autenticação (diversas tecnologias). É nesta verdadeira torre de babel de protocolos e serviços que atacantes investem para conseguir se infiltrar em computadores, sistemas e redes e, conseqüentemente, obter lucro.

Seja de forma isolada ou através da combinação, o fato é que todos esses fatores têm contribuído inevitavelmente para a proliferação do tráfego não desejado tanto em diversidade quanto em volume. Contudo, existe um aspecto mais preocupante sobre tudo isso: a existência de um verdadeiro mercado de submundo (um mercado negro) fortemente estabelecido dentro da Internet responsável por financiar grande parte das atividades ilícitas com o único objetivo de tentar obter ganhos financeiros. Davies [Davies, 2007] afirma que esta "economia informal" está enraizada como uma espécie de cultura dentro da Internet, sendo capaz de movimentar bilhões de dólares ao redor do mundo e que sua erradicação é praticamente impossível. O IAB considera este mercado como "*a raiz de todos os males da Internet*".

A base deste mercado negro são os servidores de IRC que muitas vezes são usados para gerenciar e executar atividades ilícitas como o roubo e a venda de número de contas, senhas de bancos e números de cartões de crédito e, a proliferação de códigos maliciosos. Parte do lucro obtido é reinvestido em atividades ilícitas incluindo a contratação de escritores profissionais para redação de mensagens de *spam* bem elaboradas, programadores para o desenvolvimento de novos e mais robustos vírus, *worms* e *spywares*, além de especialistas em web (programadores e projetistas) para a criação de sites mais sofisticados para atividade de *phishing*.

Para completar esse quadro nada animador, devido à própria arquitetura da Internet, não existe um modo simplificado de atribuir responsabilidade ou punição para atividades não intencionais ou maliciosas. Tomando como exemplo um ataque de negação de serviço distribuído, onde uma grande quantidade de computadores previamente comprometidos é utilizada para espalhar o ataque através da rede passando por diferentes caminhos e *backbones* até atingir a vítima. Uma vez que existe um grande número de elementos envolvidos (computadores, redes de acesso, *backbones*, roteadores e vítimas) não fica claro quem tem a responsabilidade pelo problema. Além disso, a ausência de um sistema legal em muitos países, incluindo o Brasil, que forneça proteção contra crimes na Internet ou que regule a conduta dos usuários também tem contribuído para o crescimento do tráfego malicioso, não produtivo e não desejado na Internet. Mesmo quando existe alguma jurisdição sobre crimes, como é o caso dos Estados

Unidos e Inglaterra, as leis geralmente penalizam as violações somente quando um crime tiver ocorrido.

3.2.2. Tipos de Tráfego não Desejado

Para melhorar a compreensão dos leitores sobre o assunto, esta seção apresenta os principais tipos ataques, anomalias e aplicativos relacionados com o tráfego não desejado ou não solicitado.

3.2.2.1. Ataques de Negação de Serviço

De acordo com a definição do CERT (*Computer Emergency Response Team*) [CERT, 2008], um ataque de negação de serviço consiste em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador ou rede. Em outras palavras, tentar tornar indisponíveis recursos ou serviços oferecidos por um servidor ou rede. Não existe a tentativa de roubar ou se apropriar de dados sigilosos de usuários como números de cartões de crédito e senhas de contas, mas sim a tentativa de parar serviços que são oferecidos a usuários legítimos. Geralmente, ataques de negação de serviço consumem recursos como memória, poder de processamento, espaço em disco e, principalmente, largura de banda através do envio de uma quantidade de pacotes (solicitações) maior do que o serviço pode suportar.

Os ataques de negação de serviço geralmente são executados de forma distribuída (DDoS) para aumentar ou superdimensionar sua potência. Um ataque deste tipo é mais elaborado e utiliza uma espécie de arquitetura (classe) social composta por:

- **Atacante**: O responsável por coordenar o ataque.
- **Mestre**: Computador intermediário localizado entre o atacante e os computadores zumbis, que recebe os parâmetros (ordens) para o ataque. Cada mestre controla um certo número (centenas ou milhares) de zumbis.
- **Zumbi**: Computador que efetivamente realiza o ataque.

A Figura 3.1 exemplifica a estrutura de um ataque de negação de serviço distribuído (DDoS).

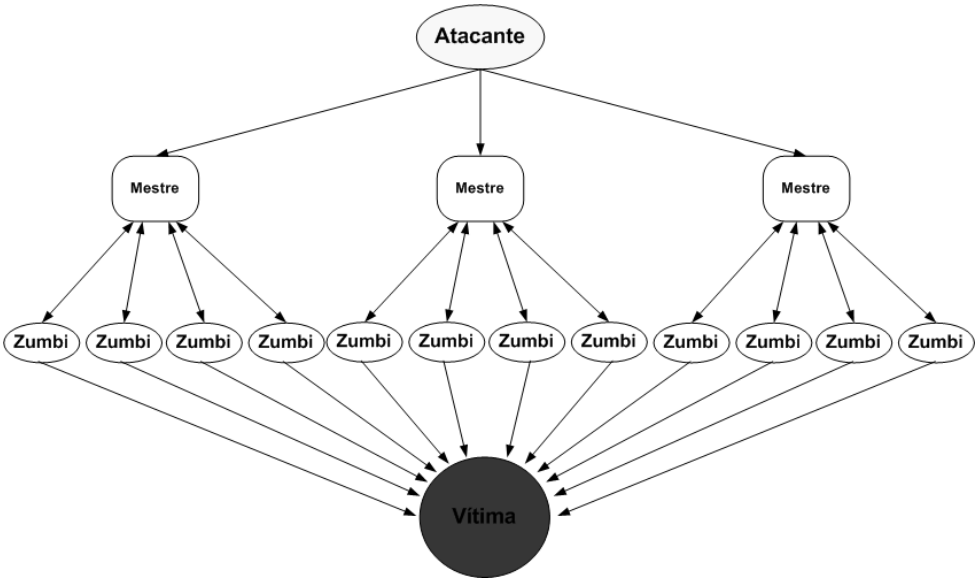

Figura 3.1. Estrutura de um ataque de negação de serviço distribuído.

Os principais tipos de ataque de negação de serviço baseiam-se em algumas características da pilha de protocolos TCP/IP, podendo, assim, afetar praticamente todos os computadores. A forma mais conhecida de ataque é a inundação (*flooding*). Normalmente, utilizam o processo de estabelecimento de conexão do protocolo de transporte TCP (*three-way handshake*), onde um pedido de conexão é enviado ao servidor através de um pacote TCP com a flag SYN (*Synchronize*). Se o servidor atender ao pedido de conexão, responde com um pacote TCP com a flag ACK (*Acknowledgement*). Desta forma, um ataque desse tipo (*SYN Flooding*) envia uma grande quantidade de pedidos de conexão até que o servidor não possa mais aceitar novos pedidos. Existem variantes do ataque de inundação para os protocolos ICMP e UDP como, por exemplo, ICMP *Unreachable*, *Smurf*[9], *Fraggle* e UDP *Packet Storm*[10].

Outra modalidade são os ataques por refletores, chamados de ataques lógicos, que também executam inundações. Neste tipo de ataque, uma estação intermediária (refletor) é colocada entre o atacante e a vítima, para redirecionar o ataque diretamente para a vítima. Para tanto, o atacante envia uma requisição para o refletor onde o endereço de origem enviado é na realidade o endereço da vítima. Um exemplo desse tipo de ataque é o *Smurf*.

O *backscatter*, tráfego recebido de vítimas que estão respondendo a ataques de negação de serviço, também está inserido nesta categoria. Como é caracterizado pelo tráfego de resposta dos ataques, alguns tipos de pacotes envolvidos no *backscatter* são TCP SYN/ACK, TCP RST/ACK e certos tipos de ICMP como *Echo Reply* e *Destination Unreachable*. Normalmente, tráfego *backscatter* tem seu endereço IP de origem forjado para representar espaços de endereçamento não usados.

[9] http://www.cert.org/advisories/CA-1998-01.html
[10] http://www.cert.org/advisories/CA-1996-01.html

Informações mais detalhadas sobre ataques de negação de serviço e variantes podem ser encontradas em [Laufer et al., 2005] e [Mirkovic et al., 2004].

3.2.2.2. Ataques ao DNS

O DNS (*Domain Name System*) é uma base de dados hierárquica distribuída que fornece informações fundamentais para operação da Internet como a tradução de nomes dos computadores para endereços IP. Devido a sua importância na estrutura da Internet, qualquer falha tem o potencial de afetar um grande número de usuários. Além da negação de serviço, os ataques ao DNS estão relacionados com a falta de autenticação e integridade dos dados.

O principal tipo de ataque relacionado ao tráfego não desejado é o envenenamento de cache (do inglês *cache poisoning*). Basicamente consiste em corromper a base de informação do serviço DNS, alterando ou adicionando dados sobre os endereços dos servidores. A finalidade é redirecionar conexões legítimas para servidores sobre o domínio dos atacantes (sites e endereços falsos). A principal consequência desse tipo de ataque é o *pharming* e seu principal alvo são páginas de instituições financeiras. Segundo [Hyatt, 2006], os atacantes usam *pharming* por quatros razões: identificar dados pessoais para efetuar roubos, distribuição de códigos maliciosos, disseminação de informações falsas e ataques *man-in-the-middle*.

3.2.2.3. Ataques ao Roteamento

O roteamento da Internet é baseado em um sistema distribuído composto por diversos roteadores, agrupados em domínios de gerência chamados sistemas autônomos (do inglês *Autonomous System* - AS). Dessa forma, o roteamento ocorre de duas maneiras: internamente (intra) ou externamente (inter) aos domínios. Em relação aos ataques ocorridos intra-domínios, apesar de relevantes, tendem a não produzir grandes efeitos, uma vez que a quantidade de elementos envolvidos é normalmente reduzida. Ataques ao roteamento entre domínios diferentes são mais preocupantes porque podem afetar todo o tráfego da Internet.

O grande alvo do tráfego não desejado em relação ao roteamento é o BGP (*Border Gateway Protocol*), um protocolo projetado para o roteamento inter domínios. Segundo [Arbor Networks, 2005], o BGP é um dos cinco pontos mais vulneráveis da Internet. De modo geral, ataques ao BGP interferem no roteamento modificando as rotas do tráfego Internet, mas não afetam a entrega de pacotes normais. Os principais ataques ao BGP são:

- **Redirecionamento**: ocorre quando o tráfego destinado a um determinado endereço, domínio ou rede é forçado a tomar um caminho diferente até um destino forjado. O objetivo deste ataque é personificar o verdadeiro destino para receber dados confidenciais. Comumente, este tipo de ataque é usado em atividades de *phishing* e principalmente fonte de *spam*
- **Subversão**: é um caso especial de redirecionamento, onde o atacante força o tráfego a passar através de certos enlaces com o objetivo de escutar ou modificar os dados. Em ataques de subversão o tráfego é repassado ao destino correto, tornando o ataque mais difícil de detectar.

3.2.2.4. SPAM

Alguns autores consideram *spam* como sendo toda mensagem comercial não solicitada (do inglês *Unsolicited Commercial E-mail* - UCE). Outros consideram *spam* como sendo mensagens não solicitadas enviadas de forma massiva (do inglês *Unsolicited Bulk E-mail* - UBE). De forma geral, o termo *spam* refere-se ao envio de mensagens não solicitadas de correio eletrônico a um grande número de usuários. Uma definição mais aprofundada sobre *spam* é apresentada em [Taveira et al., 2006].

O *spam* pode ser classificado de acordo com seu conteúdo em: boatos, correntes, propaganda ou comerciais, golpes, estelionatos e códigos maliciosos. Os boatos (*hoaxes*) tentam impressionar os usuários através de estórias falsas e assim garantir sua divulgação. Exemplos incluem mensagens do tipo roubo de rins, desaparecimento de crianças, difamação de empresas, a Amazônia como território mundial, etc. As correntes (*chain letters*) são mensagens que prometem algum de tipo de lucro financeiro ao leitor se este repassar a mensagem a um determinado número de usuários. As mensagens de propaganda são as mais comuns e mais divulgadas. O melhor exemplo são os comerciais de produtos farmacêuticos para homens. Os golpes (*scam*) representam mensagens enganosas que afirmar que o leitor foi "agraciado" com algum produto ou que tem a oportunidade de "se dar bem". Exemplos corriqueiros incluem sorteios, novos empregos, chance de ter o próprio negócio, etc. As mensagens de estelionato (*phishing*) são aquelas escondidas, ou melhor, ocultas em *spams* comerciais que visam obter informações pessoais (contas de banco e senhas, por exemplo) para serem usadas em fraudes ou compras pela Internet. Normalmente, induzem o leitor a acessar a URL indicada na mensagem ou preencher algum tipo de formulário. O tipo mais perigoso de *spam* é aquele que contém códigos maliciosos que tentam enganar o leitor a executar um determinado programa enviado junto com a mensagem. O resultado é a instalação de vírus, *worms* e cavalos de tróia, sempre visando alguma tentativa de fraude ou ataques de negação de serviço.

Além desses tipos, existem variações como SPIT e SPIM. SPIT (*Spam via Internet Telephony*) é o envio de mensagens não solicitadas a usuários de telefonia VoIP. SPIM (*Spam via Instant Messages*) representa o envio de mensagens através de aplicativos para troca de mensagens instantâneas.

O fato é que *spam* é ou tornou-se uma verdadeira praga na Internet. O Radicati Group [Radicati Group, 2006] estimou perdas mundiais equivalentes a US $ 198 bilhões relacionadas às mensagens de *spam* em 2007. Além disso, projetou que o número de mensagens de *spam* atingirá 79% do volume mundial de mensagens de correio eletrônico em 2010.

3.2.2.5. Códigos Maliciosos

Códigos maliciosos representam o tráfego empregado para causar danos, inicialmente, em computadores e, por conseguinte, em redes sem o consentimento do usuário. Normalmente, esses códigos maliciosos roubam dados, permitem acesso não autorizado, vasculham sistemas (*exploits*) e utilizam computadores e redes comprometidas (*botnets*) para proliferar mais tráfego não desejado. Os principais exemplares de códigos maliciosos são:

- **Vírus**: são programas que modificam a operação normal de um computador, sem permissão e conhecimento do usuário. Assim como um vírus biológico, um vírus de computador se replica e se espalha introduzindo cópias suas em outros códigos ou programas executáveis. Tipicamente, o ciclo de vida de um vírus tem quatro fases: *(i)* dormente, permanece desativado esperando um sinal para acordar, tal como uma data; *(ii)* propagação ou replicação; *(iii)* ativação (é ativado para executar sua "função"); e *(iv)* execução [Heidari, 2004]. Ao contrário de um *worm*, um vírus não pode infectar outros computadores sem auxílio externo.
- **Worms**: é um programa auto-replicante que é capaz de se auto-propagar através da rede explorando principalmente falhas de segurança em serviços. A taxa de propagação dos *worms* é muito rápida e pode ameaçar a infra-estrutura da Internet uma vez que cada máquina infectada torna-se um potencial atacante. De modo geral, prejudicam a rede consumindo largura de banda. A ativação de um *worm* pode ser tão rápida quanto sua velocidade de propagação. Entretanto, alguns podem esperar dias ou semanas até se tornarem ativos. O processo de ativação pode ser direto, através da execução por um usuário humano, programado ou ainda auto-ativado. Informações mais detalhadas sobre *worms* podem ser encontradas em [Weaver et al., 2003].
- **Cavalo de Tróia (*Trojan Horse*)**: são programas que uma vez ativados, executam funções escondidas e não desejadas como, por exemplo, varreduras de endereços IP e porta (TCP SYN) de alta carga, envio de grande volume de *spam*, ataques DDoS ou até mesmo adicionar o computador em uma *botnet*. Diferente dos *worms*, um cavalo de tróia não se auto-propaga, depende da interferência e curiosidade humana para se propagar. Atualmente, cavalos de tróia são conhecidos como "*gimme*", uma gíria para "*give me*", em referência as mensagens de *spam* que prometem lucro ou conteúdo picante.
- **Spyware**: são programas espiões que automaticamente recolhem informações sobre o usuário e os transmite para seus "instaladores". Geralmente, os dados monitorados referem-se aos habítos de compras na Internet ou a informações confidenciais como contas bancárias e senhas pessoais. Tais dados são, então, vendidos para terceiros ou usados para roubos e fraudes. Os *spywares* são aperfeiçoados constantemente de forma a dificultar sua detecção e remoção. Além dos próprios *spywares*, na categoria de programas espiões também estão o *adware* e o *keylogger*. *Adware*, também usado para definir *spyware*, é um programa que exibe automaticamente publicidade. *Keylogger* é um programa que captura os dados digitados no teclado e os envia ao atacante.

3.2.2.6. Aplicações Recreativas

O tráfego não desejado gerado por esta classe de aplicações é motivado pelo real crescimento da Internet, ou seja, representa a convergência natural entre os diversos tipos de dados, especialmente os multimídia, associado com a demanda dos novos usuários. Exemplos desse tipo de tráfego incluem rádio e televisão via Internet, compartilhamento de arquivos, mensagens instantâneas, jogos on-line interativos e multimídia.

A relação das aplicações recreativas com o tráfego não desejado não é percebida facilmente. Por exemplo, jogos on-line, IPTV e rádio via Internet não são relacionados diretamente a atividades maliciosas, mas o tráfego gerado pelos seu usuários espalhados pelo mundo é responsável por um grande consumo de largura de banda em determinadas redes, especialmente as de borda. Outro bom exemplo são as redes sociais[11] que também não estão diretamente relacionadas a atividades maliciosas, mas contribuem para o tráfego não desejado proliferando vírus, *worms* e *spywares*. Além disso, afetam a produtividade de empresas, uma vez que os funcionários que participam delas "dedicam" parte de seu tempo de trabalho para manter todos os seus contatos atualizados.

Por outro lado, o compartilhamento de arquivos via aplicações P2P é uma fonte reconhecida de tráfego não desejado responsável pela proliferação de códigos maliciosos e principal incentivador da pirataria, uma vez que fere as leis de direitos autorais ao "divulgar" conteúdo restrito. Um fato que chama atenção é o rápido crescimento do tráfego gerado por este tipo de aplicação desde 2003, o que tem exigido cada vez mais recursos das redes. Um estudo da empresa alemã Ipoque [Schulze e Mochalski, 2007] mostra que em 2007, o tráfego da Internet gerado pelo compartilhamento de arquivos via P2P correspondeu a algo entre 49% e 83% do volume mundial. Em certos períodos do dia, como as madrugadas, esse índice se aproximava dos 95%.

3.2.3. Classificação do Tráfego não Desejado

Para compreender o universo do tráfego não desejado, o modo mais usual é a categorização (classificação) dos tipos comuns. A primeira classificação formal sobre o assunto foi especificada em [Anderson et al., 2007] que define três categorias:

- **Perturbantes** (do inglês *nuisance*): como o próprio nome diz, representa o tráfego de fundo que "atrapalha" o uso da largura de banda e outros recursos como poder de processamento e espaço de armazenamento. Exemplos típicos incluem mensagens de *spam* e o compartilhamento de arquivos P2P. Estes tipos de tráfego normalmente transportam códigos maliciosos ou iludem os usuários a acessar sites não confiáveis e ferem ou quebram as leis de direitos autorais. Nesta categoria também se encaixam os *pop-up spams*, aplicações tipicamente perturbadoras que exibem janelas de mensagens em sistemas operacionais Windows tais como "ocorreu um erro" e "máquina comprometida". Apesar de pouco discutida, segundo [Krishnamurthy, 2006], esse tipo de aplicação é responsável por enviar centenas de milhares de mensagens a cada hora. Ataques DDoS também podem ser incluídos nessa categoria.
- **Maliciosos**: representam o tráfego responsável por divulgar e espalhar códigos maliciosos incluindo vírus, *worms*, *spywares*, etc. Tipicamente, esta classe se categoriza por apresentar um pequeno volume de tráfego, mas também por provocar altas perdas financeiras as vítimas. Normalmente, muitas empresas não

[11] Redes sociais representam a interação entre seres humanos através da formação de grupos ou relacionamentos. Devido à facilidade, alcance e disponibilidade, a Internet é um verdadeiro campo fértil para esse tipo de "serviço". MySpace, Facebook e Orkut são grandes expoentes de redes sociais. Apesar de ser classificado como mundo virtual, o Second Life também pode ser enquadrado nessa categoria.

"respeitam" esse tipo de tráfego até que algum grave incidente de segurança aconteça. É neste momento, na hora de "colocar a casa em ordem", que operadores e gerentes de rede se deparam com soluções custosas, específicas, que necessitam de especialistas e consomem tempo da equipe de operação e gerenciamento.

- **Desconhecido**: representam todo tráfego que mesmo quando pertencente a uma das categorias acima, por algum motivo não pode ser classificado com tal (tráfego malicioso criptografado ou misturado com tráfego legitimo, por exemplo) ou que ninguém conhece suas intenções ou origens. *Worms* silenciosos (*quiet worms*) são bons exemplos. Tais *malwares* abrem *backdoors* nas vítimas e ficam dormentes por um longo tempo.

Outra forma de caracterização do tráfego não desejado, mencionada por [Soto, 2005], é a classificação de sua origem em: primárias e secundárias. Origens primárias correspondem a toda requisição inicial de comunicação como pacotes TCP SYN, UDP e ICMP *Echo Request*. Nesta categoria se encaixam aplicações P2P, mensagens de *spam*, vírus e *worms*, intrusões e ataques massivos. Já as origens secundárias correspondem ao tráfego de resposta como, por exemplo, pacotes TCP SYN/ACK, TCP RST/ACK e ICMP *Echo Response*. Esta categoria inclui todo o tráfego gerador por *backscatter*, ataques de baixa intensidade ou baixa carga, e tráfego "benigno" como, por exemplo, falhas transitórias, interrupções, má configuração de equipamentos, *flash crowds*[12], entre outros.

3.3. Soluções Existentes

Como mencionado anteriormente, a Internet pode ser vista como uma das poucas plataformas operacionais existentes sem centros de controle. Essa característica serviu tanto como fator de sucesso, o que ajuda a explicar o rápido e exponencial crescimento da Internet, quanto serviu de ponto de fraco e que resultou no tráfego não desejado. Na tentativa de lidar com o lado negativo desse cenário, vários esquemas e soluções têm sido desenvolvidos e usados para identificar e minimizar o tráfego não desejado.

Nesta seção são apresentadas as soluções usadas na detecção e limitação do tráfego não desejado baseado nas vulnerabilidades mencionadas anteriormente. Para facilitar o entendimento, primeiro são discutidas as soluções consideradas tradicionais como firewall, sistemas de detecção de intrusão, honeypots, softwares "anti-alguma coisa", ferramentas de medição de tráfego e controle de acesso. Em seguida, serão apresentadas soluções baseadas na análise de tráfego.

3.3.1. Soluções Tradicionais

3.3.1.1. Firewall

O mecanismo para detecção e controle de tráfego indesejado mais empregado no mundo é o firewall. Neste documento, o termo "firewall" refere se a dispositivos (hardware ou

[12] O termo *flash crowd* refere-se à situação quando milhares de usuários acessam simultaneamente um site popular. Exemplos comuns incluem liquidações em grandes empresas, divulgação de catástrofes, eventos esportivos, entre outros. O resultado pode ser a interrupção do serviço devido ao grande número de acessos.

software) que aprovam ou negam a troca de tráfego entre redes. Basicamente, firewalls utilizam regras (filtros) que definem o que deve ser feito. Desta forma, todo o tráfego que entra ou sai da rede ou máquina é comparado com as regras e o resultado é uma ação, geralmente permitir ou negar o tráfego.

Não existe um consenso sobre a classificação dos tipos de firewall. A mais usual considera três tipos: filtro de pacotes, filtro de estados e filtros de aplicação (gateways). O **filtro de pacote** é um firewall que compara as informações do cabeçalho de cada pacote (endereços IP, portas e protocolo) com as regras definidas para decidir qual ação tomar. Foi o primeiro tipo a ser criado e ainda hoje é bastante utilizado por ser simples e fácil de configurar. Os exemplos mais comuns são as listas de controle de acesso (do inglês *Access Control List* – ACL) e o *ipchain* (integrado ao Kernel 2.2 dos sistemas operacionais Linux). Contudo, são vulneráveis a ataques com endereços IP forjados (bastante usado para geração de tráfego não desejado) e ineficazes contra tráfego criptografado.

Os **filtros de estado** mantêm registros do estado das conexões de rede (TCP e UDP) que estão ativas. A diferença quanto ao filtro de pacotes é que a filtragem pode ser baseada na tabela de estados de conexões estabelecidas e não apenas no cabeçalho. Em outras palavras, o estado das conexões é monitorado a todo o momento, o que permite que a tomada de ação seja definida de acordo com os estados anteriores mantidos em tabela. Existem três tipos de estados: NEW (novas conexões), ESTABLISHED (conexões estabelecidas) e RELATED (conexões relacionadas a outras já existentes). O *iptables*[13] é solução mais conhecida de firewall de estados. Questões de complexidade e custo são apontadas como desvantagem desse tipo de firewall. Atualmente, soluções de filtro de estados incorporaram a inspeção profunda de pacotes (do inglês *Deep Packet Inspection* – DPI) para verificar o tráfego na perspectiva da tabela de estado de conexões legítimas. Além disso, técnicas de identificação de tráfego também são utilizadas para procurar possíveis ataques ou anomalias.

Os **gateways de aplicação (*application-level gateways*)** são bastante utilizados no controle de tráfego indesejado uma vez que operam na camada de aplicação vasculhando o conteúdo dos pacotes a procura de indícios de anomalias como, por exemplo, seqüências de caracteres específicos (palavras ou frases) que indicam a presença de ataques, código maliciosos e até mesmo de determinadas aplicações como SMTP (*Simple Mail Transfer Protocol*), FTP (*File Transfer Protocolo*), HTTP, P2P, MSN, etc. Normalmente, funcionam como intermediários (*proxies*) de um determinado serviço, recebendo solicitações de conexão e gerando uma nova requisição para o servidor de destino. A resposta do serviço é recebida pelo firewall e avaliada para checar sua conformidade antes de ser repassada a quem originou a solicitação. Os tipos de filtros de aplicação mais comuns são voltados para correio eletrônico (anti-*spam*) e web (*Squid*[14], por exemplo). A principal vantagem desse tipo de firewall é a capacidade de avaliar tráfego bem específico e transações criptografadas. Por outro lado, cada novo serviço necessita de um *proxy* específico. Além disso, seu uso geralmente insere mudanças de desempenho no tráfego.

[13] http://www.iptables.org
[14] http://www.squid-cache.org

Com a proliferação do tráfego não desejado nos últimos anos, as soluções de firewall, até então destinadas a proteger o perímetro da rede, passaram a ser desenvolvidas para uso pessoal. ZoneAlarm[15] e Sygate[16] são firewall conhecidos voltados para o sistema operacional Windows. Já usuários Linux podem contar com o IPTables, inclusive para trabalhar na rede.

3.3.1.2. IDS

Os sistemas de detecção de intrusos ou simplesmente IDS (do inglês *Intrusion Detection System*), como o próprio nome diz, são sistemas (hardware ou software) que tentam descobrir quando um alvo está sob algum tipo de tentativa de acesso não autorizado, ou seja, alguma tentativa de intrusão. Normalmente, os IDS são compostos por sensores que geram eventos e alarmes de segurança que são enviados para uma estação de gerenciamento.

Os IDS podem ser classificados de acordo como a tecnologia de análise (assinaturas e anomalias) ou em relação ao local de aplicação (baseados em rede ou em *host*). Tradicionalmente, as técnicas usadas para analisar os dados coletados buscando detectar intrusões podem ser classificadas em dois grupos: detecção de assinatura e detecção de anomalia. A estratégia baseada em assinatura identifica padrões que correspondem ao tráfego de rede ou dados da aplicação e os compara com uma base de padrões (assinaturas) de ataques conhecidos. Desta forma, ataques conhecidos são detectados com bastante rapidez e com baixa taxa de erro (falsos positivos). Por outro lado, ataques desconhecidos não são detectados. A estratégia baseada na detecção de anomalia funciona com base na construção de perfis de comportamento para aquilo que é considerado como atividade normal. Desvios da normalidade são então tratados como ameaças. Assim, os sistemas de detecção de intrusão baseados em anomalia são capazes de se adaptar a novas classes de anomalias bem com detectar ataques desconhecidos (ataques "zero-day"). Uma forma de detectar intrusões é através da análise de seqüências de chamadas de sistema executadas pelos processos, pois estas constituem uma rica fonte de informação sobre a atividade de um sistema.

Em relação ao local de aplicação, existem duas abordagens básicas para a detecção de intrusão: detectores baseados em rede (do inglês *Network-based IDS* - NIDS), que analisam o tráfego de rede dos sistemas monitorados; e detectores baseados em *host* (do inglês *Host-based IDS* - HIDS), que monitoram as atividades locais em um computador, como processos iniciados, conexões de rede estabelecidas e chamadas de sistema executadas. Os NIDS são geralmente empregados em pontos estratégicos da rede para monitorar o tráfego de entrada e saída de todos os dispositivos em uma rede. Podem produzir alarmes para atividades suspeitas e atuar em conjunto com um firewall para automaticamente bloquear o tráfego analisado como malicioso ou anormal. Snort [Snort, 2008] e Bro [Paxson, 1998] são exemplos de sistemas de detecção de intrusão baseados na análise do tráfego de rede. Já os HIDS coletam dados do sistema onde estão instalados. Assim, os sensores ficam instalados na máquina que está sendo monitorada. A maior deficiência dos detectores baseados em *host* é sua relativa fragilidade, uma vez

[15] http://www.zonealarm.com
[16] http://www.symantec.com/norton/sygate/index.jps

que podem ser desativados ou modificados por um intruso bem sucedido, para esconder sua presença e suas atividades. Esse problema é conhecido como subversão.

O principal problema dos IDSs é a precisão. Como existe uma constante mutação seja no tráfego de rede seja nos padrões de assinatura, a detecção de intrusão se torna cada vez mais difícil e sujeita a erros. Segundo Kumar e Stafford [Kumar e Stafford, 1994], uma atividade intrusiva pode ser classificada como verdadeiros positivos, verdadeiros negativos, falsos positivos e falsos negativos. A Figura 3.2 resume os quatro casos possíveis. Os dois primeiros, verdadeiro positivo e verdadeiro negativo correspondem, respectivamente, a correta detecção de uma intrusão e a correta detecção de um evento normal. Já um falso positivo ocorre quando um evento normal é classificado como anômalo. O resultado é que uma atividade maliciosa pode, no futuro, não ser detectada devido a todos os falsos positivos anteriores. O pior caso é falso negativo, onde o tráfego normal é classificado como anômalo.

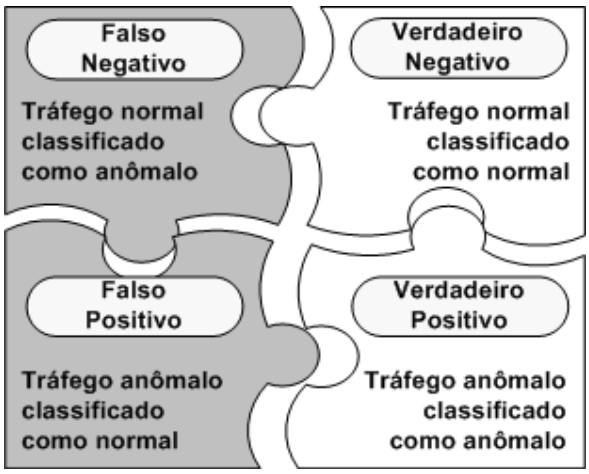

Figura 3.2. Possíveis classificações de um evento.

Por definição, os sistemas de detecção de intrusão são passivos, ou seja, apenas detectam e registram eventos. Contudo, devido à evolução das técnicas de intrusão e a necessidade de tomar decisões de forma mais rápida e precisa, sentiu-se a necessidade de atuar de forma reativa. Surgiram, então, os sistemas de prevenção de intrusão (do inglês *Intrusion Prevention System* - IPS). Um IPS é um sistema com as mesmas funcionalidades de um IDS, mas com a capacidade de automaticamente interagir com outros elementos de segurança para bloquear ou limitar um determinado tráfego malicioso. Além da capacidade de reação, os IPS são projetados para operar on-line e assim permitem prevenção em tempo real. Por fim, algumas implementações de IPS agregam mecanismos DPI para analisar protocolos da camada de aplicação e assim fornecer resultados mais precisos. Fabricantes como Cisco[17] e ISS[18] possuem soluções avançadas de IPS. No âmbito de ferramentas gratuitas, Snort e Untangle IPS[19] são bons exemplos.

[17] http://www.cisco.com/
[18] http://www.iss.net/
[19] http://www.untangle.com/

Existem também os APS (*Anomaly Prevention Systems*) cuja idéia é considerar cada tipo de anomalia separadamente através da criação de um perfil do comportamento do tráfego [Feroul et al., 2005]. Além disso, APS tem características que permitem que seja aplicado fora do perímetro da rede (*backbones*, por exemplo) enquanto IDS e IPS são voltados à segurança interna da rede.

3.3.1.3. Honeypots

A terceira classe de sistemas tradicionais contra o tráfego não desejado são os *honeypots*. O termo "*honeypot*" refere-se a uma ferramenta de segurança cuja função principal é colher informações sobre ataques e atacantes. Em outras palavras, é um software ou sistema que possui falhas reais ou virtuais de segurança, implementadas propositalmente, com a única finalidade de ser invadido, sondado e atacado para que os mecanismos utilizados na invasão possam ser estudados. Segundo [Spitzner, 2002], um *honeypot* é um recurso de rede cuja função é ser atacado e comprometido (invadido). Significa dizer que poderá ser testado, atacado e invadido. Os *honeypots* não fazem nenhum tipo de prevenção, mas fornecem informações adicionais de valor inestimável. Em relação ao tráfego não desejado, *honeypots* têm sido usados para anunciar espaços de endereçamento não alocados ou não permitidos, além de recolher informações sobre os originadores do tráfego de tais endereços.

Os *honeypots* são classificados de acordo com seu nível de atuação em: de baixa interatividade e de alta interatividade. *Honeypots* de baixa interatividade são ferramentas instaladas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir. Desta forma, o sistema operacional real deste tipo de *honeypot* deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. Também são chamados de *honeypots* de produção porque atuam como elementos de distração até que medidas efetivas possam ser tomadas. São normalmente utilizados para proteger empresas. O exemplo mais conhecido de *honeypot* de baixa interatividade conhecido é o honeyd [Provos, 2004] [Provos, 2008].

Honeypots de alta interatividade são máquinas completas que implementam sistemas operacionais e serviços reais comprometidos e são utilizadas quando se deseja compreender detalhadamente os mecanismos e vulnerabilidades exploradas. Normalmente, ficam localizados no perímetro externo da rede como em uma região de entrada ou zona desmilitarizada. Diferentemente dos *honeypots* de baixa interatividade, esses oferecem um maior risco e demandam pessoal especializado, tempo e dinheiro. São chamados de *honeypots* de pesquisa. As *honeynets* são exemplos de honeypots de alta interatividade [Honeynet Project, 2006].

Uma *honeynet* é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes [Hoepers et al., 2003]. Uma vez que é projetada para ser atingida e não existem sistemas ou aplicações de produção em uma *honeynet*, todo tráfego que chega é presumido ser malicioso ou resultado de uma configuração incorreta dos serviços da rede. De modo geral, uma *honeynet* é uma rede composta por um ou mais *honeypots* e um *honeywall* (Figura 3.3). O *honeywall* é um gateway que separa os *honeypots* do resto da rede e, por isso é o elemento central de uma *honeynet*.

Em resumo, os *honeypots* podem ser usados para caracterizar o tráfego não desejado com o propósito de advertir previamente operadores e gerentes de rede (além de outros dispositivos tais com firewalls e NIDS) de ataques e anomalias e fornecer tendências que os ajudem a melhorar a segurança da rede. O trabalho de Krishnamurthy [Krishnamurhty, 2004] propõe uma solução usando *honeypots* móveis que permite detectar a origem de ataques o mais perto possível.

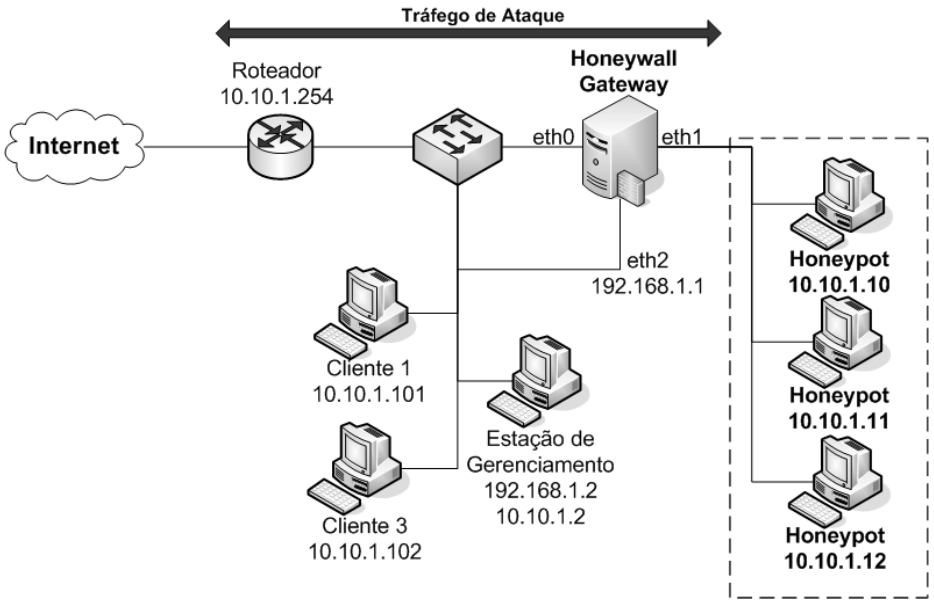

Figura 3.3. Exemplo de arquitetura Honeynet.

3.3.1.4. Software Anti-*

Na categoria de soluções contra o tráfego não desejado estão os software e programas desenvolvidos para detectar e eliminar potenciais ameaças aos computadores e redes como, por exemplo, antivírus, anti-*spyware*, anti-*phishing* e anti-*spam*.

Antivírus são programas que detectam e removem vírus de computador. Uma vez que novos vírus e variantes de vírus conhecidos são "lançados" quase que diariamente, um software antivírus deve manter-se automaticamente ou ser mantido sempre atualizado. Geralmente, os fabricantes de antivírus distribuem atualizações e "vacinas" para vírus específicos gratuitamente. Como existe um grande número de soluções antivírus, o que as diferencia são os métodos de detecção, funcionalidades oferecidas e o preço. Entre os exemplo de antivírus comerciais pode-se citar Norton, McAfee e Trend Micro enquanto que Avast, AVG e Vírus Shield apresentam antivírus gratuitos.

Já os anti-*spywares* são usados no combate a programas e códigos espiões como *spyware*, adware, *keyloggers*. Assim como os antivírus, também existem dezenas de soluções *anti-spyware* divididas em comerciais e gratuitas. Ad-Aware SE, Spybot e Windows Defender são exemplos de soluções não comerciais. Spyware Doctor, HijackThis e Spy Sweeper são soluções comerciais. Entretanto, algumas soluções anti-

spyware são famosas por divulgar *spywares* tais como Spyware Quake, Antivirus Gold, PSGuard, Malware Alarm, entre outros.

Softwares anti-*phishing* visam bloquear possíveis tentativas de fraude através de sites web ou mensagens de correio eletrônico. Normalmente, este tipo de solução é apresentado na forma de barras de tarefas (*toolbar*) integradas ou integráveis com navegadores web (Firefox 2.0, IE 7.0, Opera, por exemplo) ou clientes de correio eletrônico (Mozilla Thunderbird e Microsoft Mail), fornecendo informações como o nome "real" do domínio do site web ou se o SSL (*Secure Sockets Layer*) está ativo. Apesar de auxiliar os usuários, existem críticas as atuais soluções anti-*phishing* [Wu et al., 2006] como, por exemplo, a localização das barras de tarefas e das informações exibidas não ajuda os usuários, e a falta de sugestões sobre o que fazer quando uma tentativa de *phishing* é detectada, uma vez que hoje os indicadores apenas mostram o que está errado.

As soluções anti-*spam* também se enquadram nesta categoria. Basicamente, a detecção de *spam* é baseada na filtragem de mensagens não solicitadas através dos campos do cabeçalho ou do conteúdo da mensagem. A filtragem de cabeçalho verifica o endereço de origem, nome do remetente e assunto de uma mensagem para validá-la ou não. Este tipo de solução anti-*spam* é mais simples e sujeita a erros de configuração, uma vez que é preciso definir regras do que se quer ou não receber, ou seja, quais endereços, remetentes e assuntos são indesejados. As listas negras (*blacklist*) são exemplos de filtragem de cabeçalho. Já a filtragem baseada no conteúdo da mensagem é a mais utilizada. Normalmente esta técnica realiza buscas por palavras chaves tais como "viagra" no conteúdo das mensagens. Quando configurados corretamente, a filtragem baseada em conteúdo é bem eficiente, mas também podem cometer erros (barrar "especialista" porque contém "cialis", por exemplo). Além disso, a inspeção de conteúdo não verifica a origem da mensagem. Atualmente, o uso de filtros com mecanismo de auto-aprendizagem tem sido muito utilizado.

Para finalizar, atualmente existe uma tendência em agregar softwares pessoais como antivírus e anti-*phishing* na forma de pacotes. Por exemplo, a solução gratuita avast! antivírus 4.x Home Edition integra antivírus, anti-*spyware* e *anti-rootkit*[20] para máquinas Windows. O *google pack* oferece antivírus e anti-*spyware*.

3.3.1.5. Ferramentas de Medição de Tráfego

O monitoramento de tráfego é uma atividade essencial para o gerenciamento de redes e pode ser realizado através da observação dos pacotes ou fluxos.

Medição baseada em Pacotes

A análise baseada em pacote consiste da captura e análise do cabeçalho dos pacotes. Exemplos de informações importantes obtidas no cabeçalho do pacote são o endereço IP de origem (srcIP), o endereço IP de destino (dstIP), a porta de origem (srcPrt), a porta de destino (dstPrt) e o número do protocolo.

[20] Root Kit são ferramentas que visam obter acesso de administrador em um computador ou sistema.

Existem várias ferramentas de captura de pacotes (*sniffers*) disponíveis na Internet. Por exemplo, o TCPdump[21] é uma famosa ferramenta que permite inspecionar os pacotes da rede e fazer uma análise estatística de arquivos coletados (*traces*). Junto com o *Ethereal* (*Wireshark*)[22], que adiciona uma interface amigável para o TCPdump, essas ferramentas fornecem meios para identificação da aplicação baseada no conteúdo do pacote (*payload*).

Além da inspeção do cabeçalho do pacote, outra técnica é a inspeção profunda dos pacotes (DPI) que proporciona a identificação da aplicação permitindo analisar o conteúdo dos pacotes ao longo de uma série de operações. Como resultado, a análise DPI pode ser usada para encontrar protocolos não conformes, vírus, *spam*, invasões e assim por diante. A Figura 3.4 ilustra a inspeção de pacotes e a análise DPI.

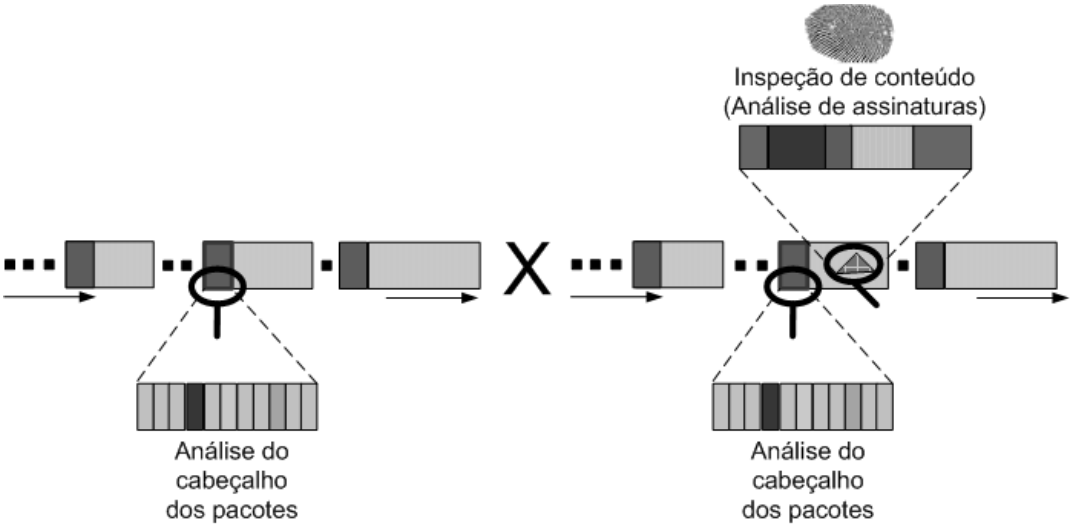

Figura 3.4. Inspeção de pacotes x análise DPI

Apesar de DPI proporcionar uma melhor solução do que filtragens, muitos pesquisadores argumentam que esta técnica fere a neutralidade da Internet, uma vez que pode ser usado para monopolizar o tráfego. Por exemplo, a China desenvolveu o "Grande Firewall da China", uma ferramenta DPI, para acompanhar todas as entradas e saídas de tráfego [OpenNet, 2004]. Este mecanismo é muito sofisticado e eficaz. Prova disso é sua capacidade de bloquear o tráfego Skype e o acesso a diversos sites incluindo o YouTube.

Medição baseada em Fluxo

As ferramentas baseadas em fluxo tentam reduzir o volume do tráfego analisado da rede através da agregação de pacotes em fluxos de informação. Nesse caso, regras de agregação são necessárias para combinar pacotes em fluxos. Comumente são utilizados cinco campos do cabeçalho dos pacotes no processo de formação de um fluxo: o endereço IP de origem (srcIP), o endereço IP de destino (dstIP), a porta de origem (srcPrt), a porta de destino (dstPrt) e o protocolo da camada de transporte. A Figura 3.5

[21] http://www.tcpdump.org/
[22] http://www.wireshark.org/

mostra um exemplo do processo de agregação de pacotes em fluxos baseado no srcIP e dstPrt. Normalmente, este processo é bastante empregado em ferramentas construídas para modelar o tráfego de rede. Exemplos de ferramentas que lidar com fluxos são Cisco Netflow[23] [Cisco, 2006] (o padrão de facto) e Juniper JFlow[24] [Juniper, 2008]

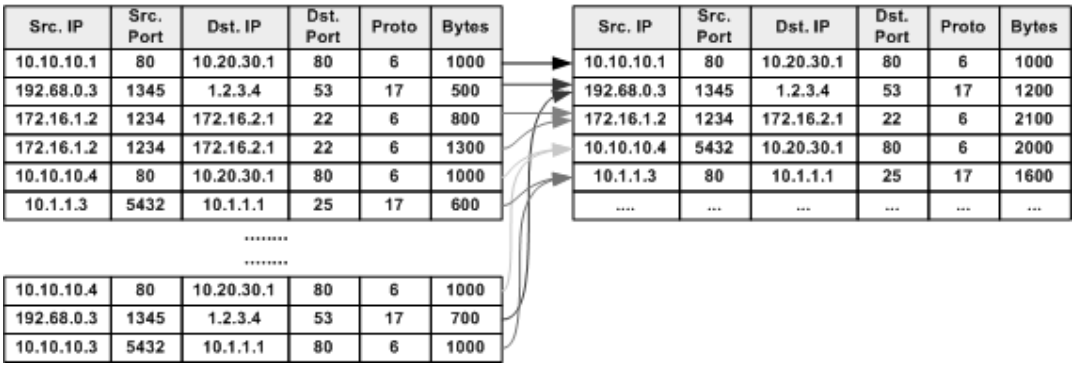

Figura 3.5. Exemplo do processo de agregação de fluxos.

3.3.1.6. Gerenciamento do Controle de Acesso

Atualmente, os produtos de segurança (antivírus, firewalls, IDS, etc.) são projetados como peças independentes de equipamentos ou software. A idéia básica do gerenciamento do controle de acesso é coordenar os mecanismos de segurança sob um computador ou rede. Neste cenário, a rede ou o computador são vistos como um único sistema ao invés de sistemas separados.

A idéia é reforçar a política de segurança regulamentando o acesso a rede pelos computadores. Por exemplo, um computador deve fornecer informações sobre o seu estado de segurança como o atual estado do antivírus, o nível de atualização de seu sistema operacional, etc. Através dessas informações, o sistema de controle de acesso poderá decidir se o computador está seguro e em conformidade com as políticas de segurança antes que seja permitido o acesso aos recursos da rede. Este cuidado no controle de acesso de computadores confiáveis ajuda a garantir que a "saúde" da rede inteira seja preservada.

O controle de acesso de rede pode ser visto como uma automação do processo manual usado pelos administradores do sistema para identificar e isolar as vulnerabilidades dentro de suas redes. O administrador pode manualmente inspecionar a configuração do computador para verificar se um usuário está em conformidade com as políticas de segurança. Os computadores também podem ser testados usando ferramentas (*scanners*) que identificam possíveis fraquezas. Contudo, a maior dificuldade encontrada é manter atualizados os diversos computadores da rede e os softwares usados pelos usuários. Por esta razão, a automação deste processo é altamente desejável, especialmente para grandes organizações.

---

[23] http://www.cisco.com/warp/public/732/netflow/

[24] http://www.juniper.net/techpubs/software/erx/junose80/swconfig-ip-services/html/ip-jflow-stats-config2.html

Neste cenário, recentemente têm sido propostas várias abordagens para fornecer controle de acesso. Algumas são descritas a seguir.

Safe Access

O Safe Access (SA) [StillSecure, 2008] é uma solução de controle de acesso que visa proteger a rede através de testes sistemáticos de conformidade dos computadores com as políticas de segurança definidas pela organização. Os computadores que não estão em conformidade são automaticamente isolados da rede. A utilização do SA inicia com a definição das aplicações e serviços que são permitidos aos usuários, bem como as ações que deverão ser tomadas para computadores que não estão conformes.

As políticas de acesso atualmente consistem de testes individuais para avaliar o estado de segurança de cada computador. A ferramenta SA interroga os computadores tentando obter acesso a rede. Diferente das outras abordagens, não é necessário instalar um agente nos computadores. O acesso seguro é verificado através da utilização de programas como antivírus e firewalls. Além disso, o SA inclui uma API (*application-programming interface*) que permite a interação com outros programas, por exemplo, um novo antivírus.

Testes específicos avaliam o sistema operacional verificando se as atualizações (*hotfixes* e *patches*) foram instaladas; garantem que o antivírus e outras aplicações de segurança estão atualizadas; detectam a presença de código maliciosos (vírus, *worms*, cavalos de tróia); e checam a existência de potenciais aplicações que podem colocar em risco a segurança do sistema como aplicações que compartilham arquivos e *spywares*. Baseados nos resultados dos testes os computadores são permitidos ou negado o acesso a rede

Cisco NAC

A Cisco tem alistado companhias de antivírus como a McAfee, Symantec e a Trend Micro para compor seu sistema de controle de admissão[25] de rede denominado NAC (*Network Admission Control*) [Cisco, 2008] cuja finalidade é validar o acesso a rede somente de dispositvos confiáveis e em conformidade com as políticas de segurança, visando proteger a rede de vulnerabilidades introduzidas por dispositivos que não estão em conformidade.

Como mostrado na Figura 3.6, a arquitetua NAC é formada por agentes denominados *Cisco Trust Agents*, dispositivos de acesso a rede, o servidor de controle de acesso seguro (ACS – *Access Control Server*) e servidores específicos como de antivírus. O agente Cisco é um pequeno software programado para se comunicar com o ACS e que atua como um IPS baseado em *host* e um firewall distribuído que identifica e bloqueia o tráfego com comportamento malicioso. Além disso, o agente tem a função de manter o sistema operacional atualizado. Os dispositivos de acesso a rede (roteadores, switches e pontos de acesso sem fio) intermediam a comunicação entre os agentes e o ACS. Nessa comunicação, o protocolo IEEE 802.1x é utilizado para gerenciar o acesso as portas físicas e aplicar as decisões tomadas pelo ACS sobre a admissão de um

[25] Apesar de empregado na solução da Cisco, o termo *controle de admissão* não é inteiramente apropriado. Controle de admissão tem sido usado no contexto de controle de tráfego referindo-se a aceitação ou rejeição do tráfego visando prevenir o congestionamento na rede.

computador. Exemplos de decisões tomadas por um ACS são desconectar o computador da rede ou mudá-lo para outra rede.

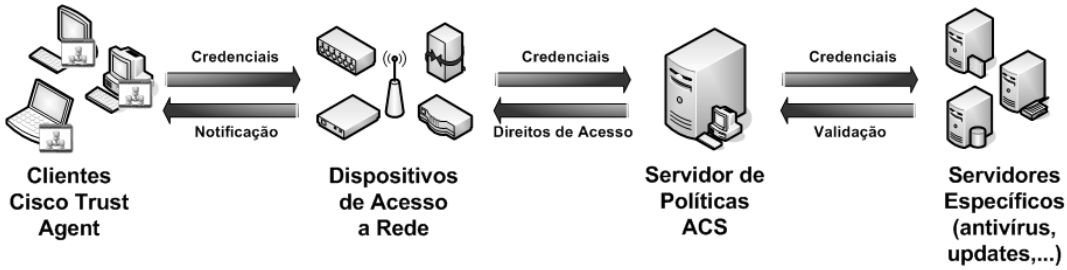

Figura 3.6. Arquitetura NAC.

Para o processo de admissão, o agente coleta informações do estado de segurança de múltiplos programas instalados nos clientes como antivírus, *firewalls* e outras aplicações de segurança. Após a coleta de informações de segurança, o agente envia suas credenciais e essas informações para os dispositivos de acesso a rede que as encaminharão para o ACS. Após o servidor de políticas (ACS) tomar uma decisão sobre a admissão de um computador, os dispositivos de acesso a rede aplicam a decisão de controle.

NAP

A Microsoft tem alistado vários parceiros como companhias de antivírus, vendedores de equipamentos de rede e integradores de sistema para compor uma solução de segurança denominada NAP (*Network Access Protection*) [Microsoft, 2008]. A idéia básica do NAP é detectar o estado de segurança de um computador que está tentando se conectar a rede e restringir o acesso deste até que as políticas de requisitos para conexão da rede sejam atendidas. O NAP realiza este objetivo através de um conjunto de funções:

- **Inspeção**: quando um computador tenta conectar-se a rede, o seu estado de segurança é validado em função das políticas de acesso definidas pelo administrador do sistema.
- **Isolamento**: computadores que não estejam em conformidade têm seu acesso negado ou restringido, dependendo das políticas estabelecidas.
- **Remediação**: problemas identificados são resolvidos tornando os computadores em conformidade com as políticas de acesso.

Como mostrado na Figura 3.7, os elementos na arquitetura NAP incluem:

- Servidores VPN que permitem conexões de acesso remoto baseada em VPN para uma rede privada;
- Servidores DHCP que fornecem configurações de endereço IP para os computadores;
- Serviço de diretório usado para armazenar as contas dos usuários e suas credenciais;
- Rede de quarentena para computadores que não estão em conformidade e necessitam ser remediados;

- Servidor NPS (*Network Policy Server*) que contém recursos tais como assinaturas de antivírus e atualizações de software. Estes recursos são usados para manter os computadores em conformidade com as políticas de segurança e fornecer remediação para os computadores não conformes.

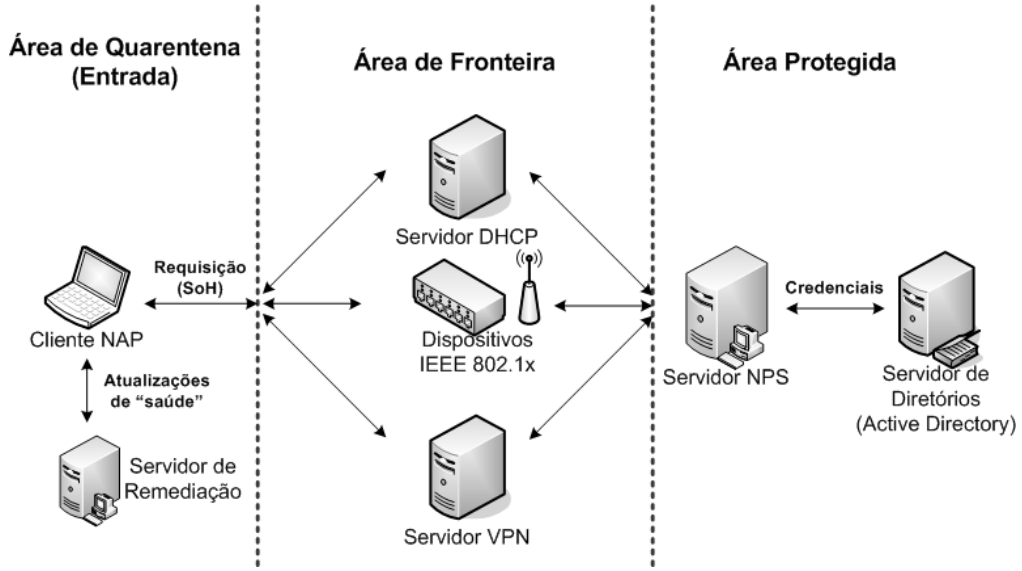

Figura 3.7. Exemplo da arquitetura NAP.

Na rede NAP, um computador age como um cliente DHCP que usa mensagens para requisitar um endereço de IP válido para um servidor DHCP. Neste caso, a requisição deve incluir um indicador do seu estado atual do sistema denominado de SoH (*Statement of Health*). Um computador sem um SoH é automaticamente designado como não conforme. Se o SoH é válido, o servidor DHCP atribui um endereço IP que permite ao computador o acesso a rede. Se o SoH não é válido, o computador é dito não conforme e o servidor DHCP isola-o computador em uma rede de quarentena.

Ao ser designado para a rede de quarentena, o computador reporta ao servidor de políticas requerendo atualizações. O servidor de políticas fornece ao computador as atualizações necessárias (por exemplo, assinaturas de antivírus e atualizações de softwares) para torná-lo em conformidade com as políticas. Após atualizar o seu SoH, o computador pode enviar uma outra requisição para o servidor DHCP que encaminha o SoH atualizado para o servidor NPS, responsável por validar o SoH enviado. Após essa validação, o DHCP permite o acesso normal à rede.

3.3.2. Soluções Baseadas na Análise do Tráfego

3.3.2.1. Técnicas Avançadas para Classificação de Tráfego

Uma das questões desafiadoras resultante das atuais soluções contra o tráfego não desejado é a necessidade prévia de uma análise manual para detectar corretamente o tráfego desconhecido e indesejado. Entretanto, considerando o rápido crescimento do número de novos serviços e aplicações, esse tipo de procedimento é muitas vezes impraticável.

Neste contexto, as abordagens de análise de tráfego têm atraído interesse especial nos últimos anos e apresentado resultados promissores contra este tipo de tráfego, especialmente para enlaces de alta velocidade. Técnicas para caracterizar o tráfego Internet, métodos para descobrir o tráfego gerado por aplicações, abordagens para desenvolver sistemas de detecção de anomalia mais precisos e soluções específicas para lidar com certos tipos de tráfego não solicitados (por exemplo, *spam* e P2P) surgiram como tentativa de tornar automática, rápida e precisa identificação e redução do tráfego não desejado.

Esta seção apresenta algumas das mais relevantes técnicas e metodologias baseadas em modelos estatísticos, matemáticos e na análise comportamental do tráfego Internet e que podem ser direta ou indiretamente aplicadas na análise do tráfego não desejado.

Modelos Estatísticos e Matemáticos

Modelos estatísticos têm sido empregados para construir modelos de séries temporais do tráfego da Internet e, conseqüentemente, procedimentos capazes de detectar anomalias.

Como argumentado no trabalho proposto por Scherrer et al.[Scherrer et al., 2007], o tráfego de rede consiste de um processo de chegada de pacotes IP que pode ser modelado usando processos pontuais não estacionários ou processos pontuais Markovianos. Entretanto, devido ao tamanho do volume de dados, especialmente em enlaces de alta velocidade, tais modelos geram grandes conjuntos de dados e necessitam de um alto poder computacional para seu processamento. Além disso, muitas das distribuições estatísticas não produzem bons resultados na medição das margens (distribuição marginal). Em linhas gerais, uma distribuição marginal é utilizada quando se tem interesse em informações de ma determinada váriavel (um dado do tráfego da rede como, por exemplo, endereço IP de origem). Ela sumariza as freqüências obtidas para cada nível. Por exemplo, na Tabela 3.1, as distribuições marginais são observadas nos totais das linhas e colunas (em itálico).

Table 3.1. Exemplo de distribuição marginal.

Y\X	0	1	2	3	P(y)
0	1/8	2/8	1/8	0	*1/2*
1	0	1/8	2/8	1/8	*1/2*
P(x)	*1/8*	*3/8*	*3/8*	*1/8*	*1*

É por este motivo que distribuições estatísticas não Gaussianas, em especial a distribuição Gama, vêm sendo aplicadas na busca de métodos mais rápidos e eficientes.

Por sua vez, os modelos matemáticos, especialmente *wavelets*, têm sido empregados na detecção de anomalias porque capturam correlações temporais complexas através de múltiplas escalas de tempo e encontram variações no comportamento do tráfego de rede. *Wavelets* são funções matemáticas que dividem os dados (sinais) em diferentes componentes de acordo com uma escala de interesse, permitindo realizar análises locais em uma área específica do sinal, como mostra a Figura 3.8.

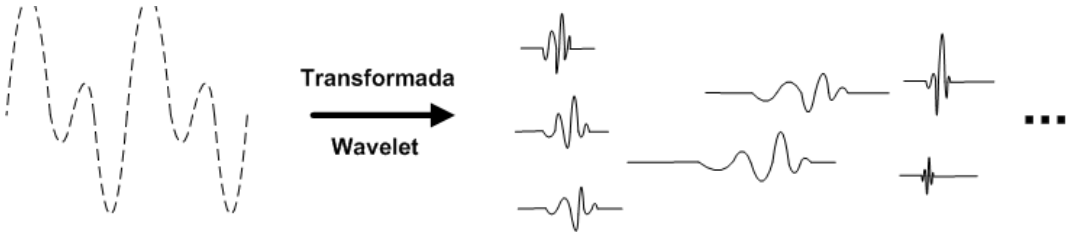

Figura 3.8. Processo de decomposição do sinal usando wavelet.

A seguir são detalhados dois trabalhos baseados nos modelos estatísticos e matemáticos e que podem ser facilmente utilizados para identificação e caracterização de tráfego indesejado.

Extracting Hidden Anomalies using Sketch and Non Gaussian Multiresolution Statistical Detection Procedures

O trabalho de Dewaele et al. [Dewaele et al., 2007] introduz um procedimento especialmente elaborado para detecção de anomalias de baixa intensidade ocultas no tráfego Internet. Essa técnica combina o uso de *Sketches* e um modelo estatístico não gaussiano (que não segue a distribuição normal) para descobrir anomalias no tráfego de dados. *Sketches* são estruturas de dados (geralmente tabelas *hash*) utilizadas para representar (sumarizar) dados massivos de tráfego em vetores bidimensionais que requerem baixo poder de processamento. Isto possibilita a redução do volume de informação e a medição do comportamento do tráfego. A distribuição Gama serve para extrair a função de distribuição marginal do tráfego para cada *sketch*. Desta forma, é possível capturar pequenas correlações entre as estruturas do tráfego. O processo de detecção faz uso da distância de Mahalanobis [Mahalanobis, 1930], uma medida estatística usada para determinar similaridades entre um conjunto de amostras desconhecidas e outro de amostras conhecidas, para executar comparações entre sketches e assim determinar comportamentos anômalos.

O procedimento de detecção e análise, exemplificado na Figura 3.9, consiste dos seguintes passos: geração dos *sketches*, agregação multiresolução, modelagem não gaussiana, referência, distâncias estatísticas e detecção de anomalias.

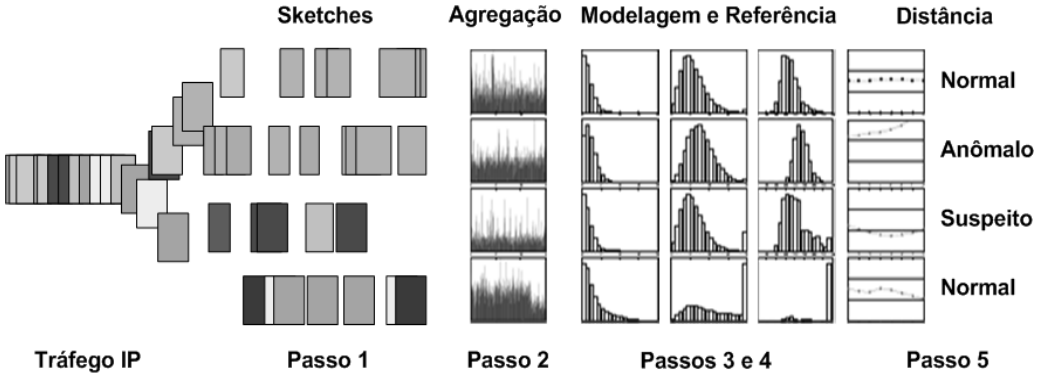

Figura 3.9. Processo de detecção de análise.

1. **Geração dos sketches**

Os *sketches* são usados para dividir os pacotes dentro de subgrupos de acordo com uma janela de tempo deslizante. Para cada fatia de tempo, somente o tempo de chegada, os endereços IP e as portas são analizados. Como resultado, tabelas *hash* são geradas representando segmentos do tráfego original, onde o endereço IP de origem ou destino é usado como chave da tabela hash.

2. **Agregação multiresolução**

   Na agregação multiresolução, os segmentos de tráfego gerado são colocados juntos para formar séries temporais que são agregadas de acordo com uma determinada escala.

3. **Modelagem não gaussiana**

   A distribuição Gama é usada para descrever as distribuições marginais das séries temporais agregadas. Em outras palavras, para cada agregação, os parâmetros α e β são estimados para serem usados para calcular a referência e a distância estatística. A escolha pela distribuição Gama e sua adequação são explicadas em [Abry et al., 2007] [Scherrer et al., 2006] [Scherrer et al., 2007].

4. **Referência**

   A média dos comportamentos e a variabilidade típica são estimadas para cada elemento da tabela *hash* usando estimadores de média e variância. Apesar da simplicidade, a junção dos *sketches* e referências permite a definição dos padrões de comportamento normal e anômalo. Anomalias podem ser encontradas observando mudanças no padrão estatístico através da comparação de *sketches* em um mesmo intervalo de tempo.

5. **Distância estatística**

   A distância de Mahalanobis é usada para medir o comportamento anômalo das referências. Cada distância calculada é comparada com um limiar (*threshold*). Se a distância de referência é menor ou igual ao limiar, o segmento é considerado normal. Caso contrário, é classificado como anômalo.

6. **Detecção de anomalias**

   A detecção de anomalias é realizada comparando *sketches* (chaves da tabela *hash*) com atributos (endereço IP de origem e destino e número das portas) registrados em uma lista durante o processo de detecção.

A validação deste procedimento foi realizada usando o repositório de tráfego do MAWI[26]. Foram investigadas duas anomalias de tráfego: ataques de inundação de baixa intensidade e varreduras curtas. Os resultados demonstram que o procedimento é capaz de descobrir anomalias como pacotes elefante, *flash crowds*, ataques DDoS (inundação TCP SYN e ICMP), varreduras de IP e porta, tráfego P2P, *worms*, entre outros.

Apesar de esse procedimento ser considerado um trabalho em progresso, os resultados iniciais são bastante promissores. Primeiro, nenhum tipo de conhecimento

[26] MAWI é um repositório de tráfego, integrante do projeto WIDE, que tem armazenado coleções de pacotes desde 2001 nos enlaces trans-pacíficos entre o Japão e os Estados Unidos. Maiores informações em http://mawi.wide.ad.jp/mawi/

prévio do tráfego e de suas características é necessário. Segundo, é capaz de detectar tanto anomalias com curto tempo de vida (curta duração) quanto as mais demoradas. Terceiro, requer baixo poder computacional e pode ser implementado em tempo real. Por fim, a janela de detecção pode trabalhar tanto em tempo menores (inferior a um minuto) quanto em tempos maiores (superior a dez minutos).

Como limitações, a técnica pode apresentar problemas de idenficação (falso positivo). Por exemplo, o serviço DNS pode ser considerado ilegítimo por apresentar um único padrão de tráfego. Uma sugestão para resolver o problema é a adição de filtros para excluir padrões conhecidos durante a fase de análise.

Anomaly Detection of Network Traffic based on Wavelet Packet

Gao et al. [Gao et al, 2006] descrevem um novo método de detecção de anomalias de rede baseado em transformadas *wavelet*. Os autores argumentam que existem algumas questões que precisam ser observadas para aplicação de *wavelet* em métodos de detecção de anomalias. Primeiro, a maioria dos métodos usa análise de multiresolução, que é somente adequada para anomalias de baixa freqüência. Segundo, os resultados podem ser incorretos quando somente uma escala é analisada. Terceiro, as transformadas *wavelet* demandam de um alto poder computacional e, conseqüentemente, podem ser consideradas inapropriadas para operações em tempo real.

Para superar estes problemas, os autores propõem o uso da análise de pacotes de *wavelet*, a qual possui a capacidade de decompor o sinal oferecido uma diversa faixa de possibilidades para análise. Em linhas gerais, em análises *wavelet*, um sinal é dividido em aproximação e detalhe. Esta aproximação é então dividida em uma aproximação de segundo nível e detalhe, e o processo se repete. Para uma decomposição de nível *n*, há *n +1* caminhos possíveis para decompor ou codificar o sinal. A Figura 3.10 ilustra esse processo.

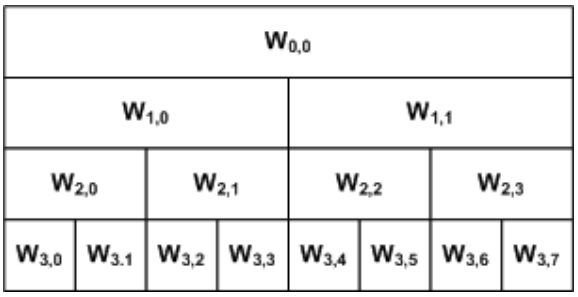

Figura 3.10. Processo de decomposição do sinal.

O método de detecção proposto é capaz de ajustar o processo de decomposição adaptativamente e exibir a mesma capacidade de detecção para anomalias de baixa, média e alta freqüência. Para alcançar este objetivo, o método proposto emprega um estágio de detecção inicial para verificar em cada escala através de um algoritmo de detecção estatístico se existem anomalias indicadas pela análise de pacotes de *wavelet*. No caso onde uma anomalia é percebida, uma nova decomposição de pacotes de *wavelet* é feita e este passo é executado novamente. Os níveis de decomposição são auto-adaptativos. Caso exista uma anomalia, a reconstrução dos pacotes de *wavelet* e a

confirmação do estágio de anomalia são usadas para reconstruir os sinais das escalas e checar se a reconstrução do sinal é anômala.

Metodologias Baseadas na Análise do Comportamento

Metodologias baseadas no comportamento tentam automaticamente identificar perfis de tráfego em redes de *backbone*. O objetivo por trás dessas abordagens é fornecer um entendimento plausível sobre o padrão de comunicação dos computadores e serviços. Na detecção de anomalias, a análise do comportamento é caracterizada através do processamento de grandes volumes de tráfego.

A seguir são apresentados recentes trabalhos baseados no padrão de comportamento dos computadors. Tais trabalhos foram projetados para identificar e classificar tráfegos não desejados em redes de *backbones*.

Traffic Classification on the Fly

A técnica proposta por Bernaille et al. [Bernaille et al., 2006] executa a análise do fluxo através da observação dos cinco primeiros pacotes de uma conexão TCP para identificar a aplicação. Ao contrário de outras técnicas, onde a classificação das aplicações ocorre somente após o final do fluxo TCP, esta técnica utiliza apenas o tamanho dos primeiros pacotes de uma conexão para classificar o tráfego. A idéia da classificação "*on the Fly*" é identificar com precisão a aplicação associada a um fluxo TCP o mais cedo possível. Essa técnica utiliza o conceito de clusters não supervisionados para descobrir grupos de fluxos que compartilham um comportamento de comunicação comum.

De modo geral, a classificação "*on the Fly*" é dividida em duas fases: aprendizagem *off-line* e classificação de tráfego *on-line*. A primeira fase é utilizada para aprender e detectar comportamentos comuns através de um conjunto de dados de treinamento. No fim desta fase, os fluxos TCP são agrupados de acordo com seus comportamentos. A fase classificação emprega estes fluxos agregados para descobrir qual a aplicação está associada a cada fluxo TCP.

Em resumo, a classificação "*on the Fly*" obtém mais informação do que a inspeção DPI sem desrespeitar a privacidade do pacote e ferir qualquer restrição legal. Os resultados apontam uma precisão acima de 80% para aplicações TCP bem conhecidas. Entretanto, a técnica também apresenta alguns problemas como pacotes entregues fora de ordem mudarão a representação espacial do fluxo que irá impactar na qualidade da classificação. Além disso, aplicações com comportamento inicial semelhante poderão ser classificadas com o mesmo rótulo.

BLINC: Multilevel Traffic Classification in the Dark

Karagiannis et al. [Karagiannis et al., 2005] apresentaram uma nova metodologia para classificar fluxos de tráfego de acordo com o tipo de aplicação. Diferente de outras propostas que analisam cada fluxo separadamente, o metódo proposto observa todos os fluxos gerados por computadores específicos. Além disso, o BLINC não examina o conteúdo dos pacotes, não assume que portas bem conhecida representam de maneira confiável as aplicações e somente usa informações obtidas pelos coletores de fluxo, o que explica o termo "*in the dark*".

A classificação do BLINC é baseada no padrão de comportamento dos computadores na camada de transporte. Esses padrões são analisados em três níveis de

detalhamento: social, funcional e aplicação. O nível social revela a popularidade do computador. Neste nível é investigado o comportamento do computador em relação as suas comunicações com outros computadores. Assim, somente os endereços IP de origem e destino são utilizados como mostrado na Figura 3.11.

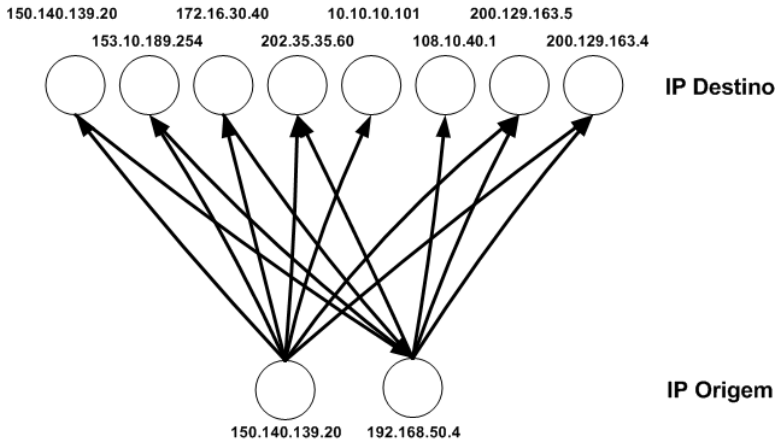

Figura 3.11. Representação visual do nível social através de grafo bipartido.

O nível funcional investiga o que o computador faz. Neste nível é analizado se atua como provedor ou consumidor de um serviço ou se participa de comunicações colaborativas. São avaliados os endereços IP de origem e destino e a porta de origem. Por último, o nível de aplicação captura a interação dos computadores na camada de transporte para identificar aplicações e suas origens. De acordo com Karagiannis [Karagiannis et al., 2005], um *graphlet* pode ser usado para representar as características dos fluxo correspondentes a diferentes aplicações pela captura do relacionamento entre o uso das portas de origem e destino. A Figura 3.12 mostra *graphlets* usado para identificar os fluxos de ataques DDoS a partir de respostas das vítimas.

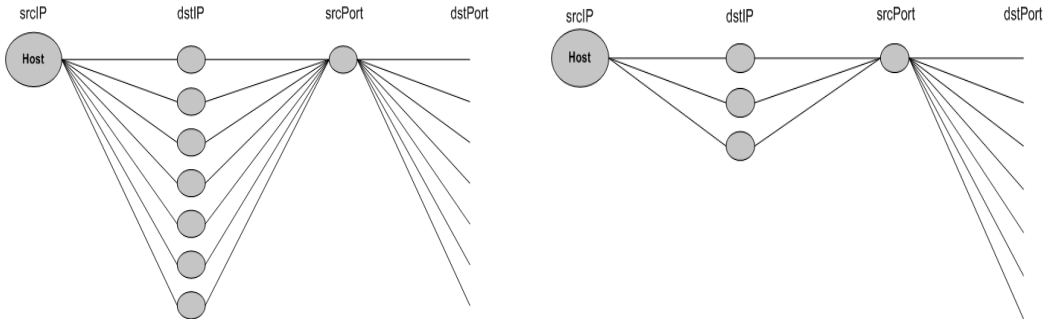

Figura 3.12. Representação visual das interações no nível social através de graphlets.

Os endereços IP e portas são associados na classificação com heurísticas (por exemplo, número de pacotes ou bytes transferidos) para refinar a classificação. A Figura 3.12 apresenta um exemplo onde a cardinalidade dos conjuntos de endereço IP destino

(a) em comparação com o conjunto de portas de destino (b) varia e pode indicar uma aplicação ou um ataque.

Em resumo, este método afirma ser capaz de classificar entre 80% e 90% do tráfego com mais de 95% de exatidão, além de detectar aplicações maliciosas e não conhecidas. A desvantagem é que requer uma grande quantidade de fluxos de dados completos (terminados) para executar as análises.

Profiling Internet backbone Traffic: Behavior Models and Applications

A metodologia proposta por Xu et al. [Xu et al., 2005a] objetiva identificar anomalias de tráfego. O método usa mineração de dados e técnicas de informação teórica para automaticamente descobrir padrões de comportamento significantes no tráfego de dados. A metodologia (aqui denominada de *profiling*) automaticamente descobre comportamentos do tráfego massivo e fornece meios plausíveis para entender e rapidamente reconhecer tráfego anômalo. A metodologia trabalha examinando os padrões de comunicação dos computadores (endereços e portas) que são responsáveis por um significativo número de fluxos em um determinado período de tempo.

O processo do *profiling* basicamente inclui a extração de clusters significativos e a classificação do comportamento deles baseado no relacionamento entre os clusters. Por exemplo, para um dado endereço IP (srcIP) *i*, o processo do *profiling* inclui a extração dos fluxos com srcIP *i* dentro de um cluster (denominado de cluster srcIP) e a caracterização do padrões de comunicação (ou seja, comportamento) usando medições de teoria da informação (entropia) sobre as três dimensões de fluxos restantes, ou seja, endereço IP de destino (dstIP), porta de origem (srcPrt) e porta de destino (dstPrt). A Figura 3.13 ilustra os passos da metodologia.

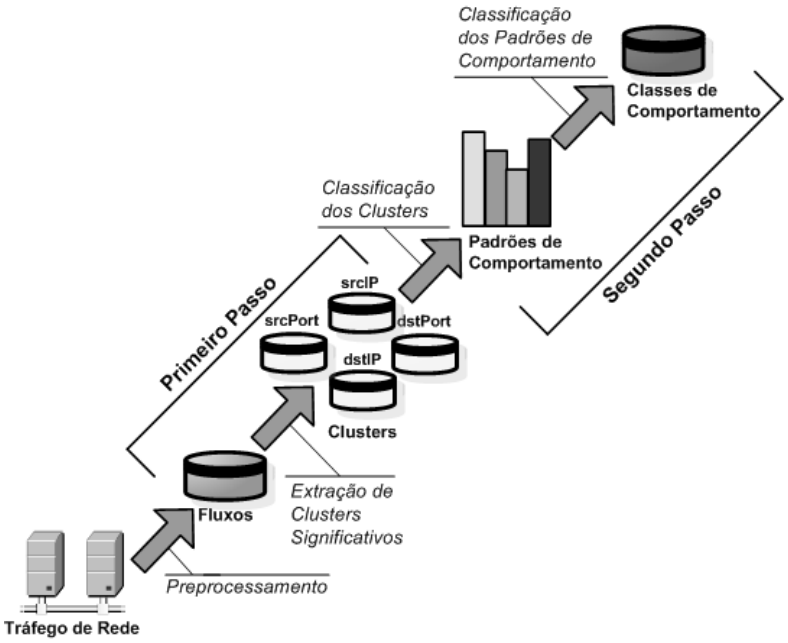

Figura 3.13. Etapas do método Profiling

O primeiro passo da metodologia é analisar um conjunto de fluxos baseado nas tuplas bem conhecidas para decidir sobre um espaço característico de interesse. O

objetivo é extrair os clusters significativos de dimensões específicas, isto é, endereços IP de origem e destino e portas de origem e destino. Então, os clusters mais significativos são extraídos de uma dimensão fixa (por exemplo, endereço IP de origem) e o conceito de entropia é usado para medir a quantidade de incerteza relativa (do inglês *Relative Uncertainly* – RU) contida nos dados.

Com os clusters extraídos, o segundo passo é descobrir ligações entre os clusters, ou seja, encontrar modelos de comportamento comuns para o perfil do tráfego. Para alcançar este objetivo, a metodologia propõe uma classificação do comportamento baseado nos padrões de comunicação dos computadores de usuários finais e serviços. Desta forma, para cada cluster, uma RU é computada e usada como métrica para criar classes de comportamento (do inglês *Behavior Classes* – BC). Entre essas classes é possível identificar qual delas representa tráfego anômalo ou indesejado.

Em resumo, esta metodologia é uma ferramenta muito poderosa para detectar anomalias, *exploits* de segurança não conhecidas, criar o perfil do tráfego não desejado, registrar o crescimento de novos serviços e aplicações. Também é flexível e capaz de automaticamente descobrir outros padrões de comportamento significantes. O trabalho em [Xu et al., 2005b] demonstra a habilidade para detectar as mais variadas anomalias massivas tais como varreduras de IP e portas, ataques DoS e DDoS, entre outros. O aspecto negativo é que esta metodologia não é apropriada para o tráfego amplo de rede e sim para enlaces únicos. Além disso, os resultados apresentados não são encorajadores para ataques de baixa intensidade.

Mining Anomalies Using Traffic Feature Distributions

Lahkina et al. [Lakhina et al., 2005] propõem uma metodologia baseada na distribuição características dos pacotes capaz de detectar anomalias de alto e baixo volume. Os autores argumentam que a análise dos fluxos de origem e destino (OD) pode revelar um conjunto geral e diversificado de anomalias, especialmente as maliciosas. O método proposto utiliza o conceito de entropia para fazer observações e extrair informações úteis em relação a dispersões na distribuição do tráfego. A metodologia *mining* está organizada em duas etapas: a distribuição do tráfego e a metodologia de diagnóstico.

Na primeira etapa são extraídos os campos dos cabeçalhos dos pacotes para procurar por eventuais anomalias causadas por mudanças (dispersões) na distribuição endereços ou portas observadas. Por exemplo, durante uma varredura de portas (port scan), a distribuição das portas de destino será bem mais dispersa do que durante uma condição normal de tráfego. São analisados quatro campos do cabeçalho IP dos pacotes: os endereços IP origem e destino e as portas de origem e destino (srcIP, dstIP, srcPrt, e dstPrt). Os autores afirmam que é possível capturar o grau de dispersão ou concentração de uma distribuição usando entropia, uma vez que anomalias como, por exemplo, os port scans, podem ser vistas claramente em termos de entropia, em comparação com o volume de tráfego.

A segunda etapa, denominada de diagnóstico, usa os resultados da aplicação da entropia sobre a distribuição para fazer um diagnóstico e classificar anomalias. Em seguida, um método chamado *Multiway Subspace* é usado para detectar anomalias, oferecendo uma estratégia de classificação não supervisionada. O método *Multiway Subspace* é derivado do método de subespaço proposto em [Dunia e Qin, 1998], e cujos

resultados na análise de tráfego podem ser encontrados em [Lakhina et al., 2004b]. A idéia por trás deste método é identificar as variações correlacionadas com múltiplas características de tráfego (no caso os campos do cabeçalho IP), o que provavelmente pode indicar uma anomalia. A classificação não supervisionada utiliza uma abordagem para a construção de grupos (clusters), onde os dados são analisados para detectar anomalias. A operação ocorre em duas fases. Primeiro, as anomalias bem conhecidas são agregadas de forma a adquirir conhecimento sobre suas origens. Assim, os grupos são rotulados com base em seus tipos. Em seguida, a classificação é feita pela agregação das anomalias desconhecidas.

Como resultado, a metodologia mining é capaz de detectar ataques DoS e DDoS, *flash crowds*, varreduras de endereços e porta, *worms*, interrupções e anomalias desconhecidas. Além disso, o método *Multiway Subspace* proposto também demonstra adequação a manipular enormes volumes de fluxo OD e, conseqüentemente, para descobrir anomalias.

Em resumo, o uso da entropia na detecção de variações do tráfego de rede causados pelas mais diversas anomalias é a principal vantagem desta metodologia. A complexidade e o alto poder computacional para implementar a metodologia são a principal desvantagem. Além disso, o tempo de construir séries temporais (fluxos OD) é grande, podendo ser da ordem de alguns minutos.

3.3.4. Considerações

Apesar dos avanços na detecção do tráfego não desejado, especialmente sobre *backbones* de alta velocidade, estas abordagens ou apresentam um caro custo computacional (complexidade) e mudanças na infra-estrutura ou resultados imprecisos.

No entanto, é possível perceber tendências para futuras soluções. Em primeiro lugar, análise gerada através da agregação do tráfego em fluxos permite a exibição dos pontos de penetração (origem) e saída (destino) do tráfego de forma simples, sem a perda de dados. Em segundo lugar, apesar de não apresentar uma precisão superior, técnicas de detecção baseadas no comportamento obtém mais tipos de tráfego indesejado e extraem mais dados correlacionados sobre o tráfego. Por último, esta seção capta a essência do debate e análise sobre técnicas de detecção de tráfego não desejado, mostrando que é possível ver uma "luz no fim do túnel" no que diz respeito a soluções automáticas, rápidas e precisas.

3.4. Potenciais Soluções

O tema tráfego não desejado vem ganhando destaque no mundo todo. A principal prova deste fato é o número de pesquisas e trabalhos publicados nos últimos anos, alguns deles apresentados neste minicurso. No entanto, a própria evolução tecnológica e a filosofia aberta da Internet tem imposto novos desafios a atividade de “controle” do tráfego não desejado.

Nesta seção serão apresentadas algumas abordagens e soluções consideradas pelos autores deste minicurso como potenciais e futuras.

3.4.1. Filtragem avançada

Como visto na seção 3.3.1.1, o uso de filtros de tráfego não é suficiente para lidar com o atual estágio do tráfego indesejado. A fim de resolver este problema, pesquisadores têm proposto mecanismos e sistemas avançados de filtragem. Atualmente, as melhores práticas nesta área estão descritas em dois documentos: BCP 38 (RFC 2827) [Ferguson e Senie, 2000] e BCP 84 (RFC 3704) [Baker e Savola, 2004].

Basicamente, o BCP 38 (*Best Current Pratice*) recomenda que os provedores de Internet filtrem pacotes IP, na entrada de suas redes, provenientes de seus clientes e que descartem aqueles pacotes cujo endereço IP não tenha sido alocado a esses clientes. Na verdade, muitos provedores de acesso possuem roteadores que suportam as medidas citadas no BCP 38.

O BCP 84 apresenta outras implementações de filtragem na entrada da rede como, por exemplo, *Strict Reverse Path Forwarding* (SRPF), *Feasible Path Reverse Path Forwarding* (Feasible FPR), *Loose Reverse Path Forwarding* (Loose FPR) e *Loose Reverse Path Forwarding Ignoring Default Routes*, que oferecem configuração automática e dinâmica de filtros de entrada ao núcleo e borda das redes.

Pesquisadores e especialistas defendem que a implantação global do BCP 38 e BCP 84 permitirá efetivamente bloquear ataques DDoS baseados em endereços IP de origem forjados. Contudo, a implantação deste tipo de proteção tem sido bastante questionada, especialmente por provedores de acesso Internet. Primeiro, o custo financeiro aumentaria devido à necessidade de pessoal técnico especializado. Segundo, para essa solução ser efetiva, necessita da implantação em todas as redes existentes. Além disso, qualquer eventual bloqueio de tráfego legítimo devido a erros acidentais na configuração desses filtros seria problemático e esse temor é usado com motivo (desculpa) para o BCP 38 e o BPC 84 não serem divulgados hoje em dia. Para finalizar, devido à alta versatilidade de alguns tipos de tráfego não desejado especificamente aqueles que trafegam sobre o protocolo HTTP, essas soluções podem apresentar uma baixa taxa de efetividade na luta contra o tráfego indesejado.

3.4.2. Investigação do Espaço de Endereços IP

Alguns tipos de tráfego indesejado usam espaços de endereço IP não atribuídos (não utilizados) para executar atividades como varredura de vulnerabilidades, ataques DoS e DDoS, divulgação de vírus e *worms*, entre outras. Neste contexto, algumas soluções têm sido apresentadas com o objetivo de monitorar o tráfego considerado não esperado.

Internet Motion Sensor (IMS)[27] [Cooke et al., 2004] [Bailey et al., 2005] é um sistema de vigilância distribuída, de nível mundial, cujo objetivo é identificar e monitorar o tráfego proveniente de espaços de endereçamento IP roteáveis não atribuídos e não anunciados comumente chamados de *darknets*. De acordo com [Anderson et al., 2006], atualmente a IMS controla cerca de 17 milhões de prefixos (/8, /16 e /24), cerca de 1.2% do espaço do endereço IPv4 espalhados ao redor do mundo em ISPs, organizações, empresas e universidades. A Figura 3.14 ilustra a arquitetura da rede IMS. Apesar de não ser considerada uma solução contra o tráfego não desejado, IMS é

[27] http://ims.eecs.umich.edu.

uma ferramenta eficaz para auxílio que pode ser emprega para combater este tipo de tráfego, seja através da identificação das origens quanto da compreensão dos mecanismos utilizados.

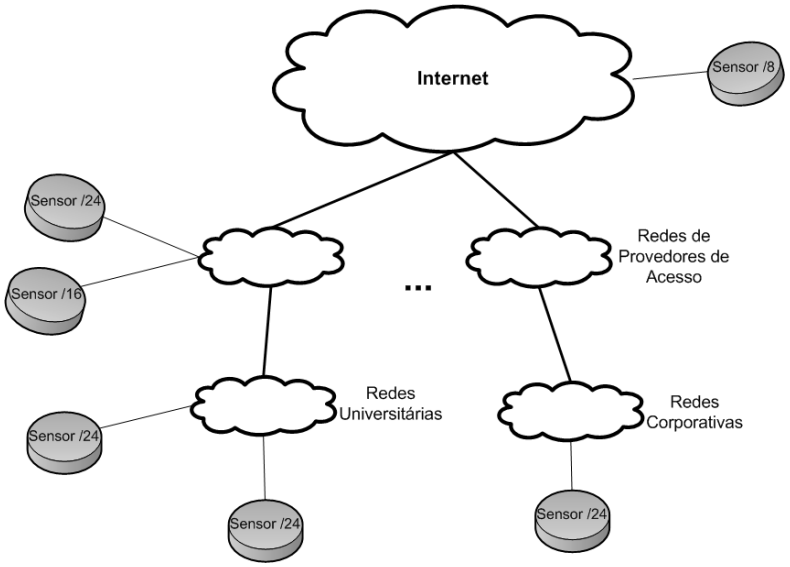

Figura 3.14. Arquitetura da rede IMS.

Outra solução semelhante são as Redes Telescópio (Network Telescopes) [Moore, 2002] [Moore et al., 2004]. Estas redes são compostas por monitores que observam o tráfego encaminhado para espaços de endereços IP não utilizados e registram eventos como a propagação de vírus na Internet. A idéia é manter os sensores ativos para "escutar" todo o tráfego enviado para estes espaços de endereçamento. Desta forma, é possível ver exatamente todos os eventos em seu "estado bruto", ou seja, sem quaisquer interferências de tráfego.

3.4.3. Lightweight Internet Permit System

Uma questão chave em relação ao tráfego não desejado é falsificação do endereço IP. Soluções como IPSec, SSL, VPN e esquemas de filtragem mais rígidos não apresentam qualquer tratamento para lidar com a falsificação de endereços IPs. Soluções mais robustas têm sido propostas, mas dependem de mudanças, algumas profundas, na infra-estrutura da Internet. Como se sabe que tais mudanças não são desejáveis e dificilmente não ocorrerão rapidamente.

É neste contexto o método LIPS (*Lightweight Internet Permit System*) [Choi et al., 2005] se propõe a identificar e bloquear o tráfego não desejado. LIPS fornece um mecanismo que permite a responsabilização do tráfego através da rápida autenticação de pacotes (*fast packet authentication*), ou seja, pacotes de tráfego não desejados são bloqueados e suas origens identificadas.

LIPS funciona como um mecanismo eficiente de filtragem de tráfego. Quando um computador origem quer se comunicar com um computador destino, primeiro requisita uma autorização de acesso ao destino. Se a autorização for concedida, um passaporte é enviado ao computador origem que o utiliza para enviar dados ao computador destino. Apenas pacotes com autorizações de acesso serão aceitos até ao

destino. Esta arquitetura simples é escalável e fornece uma possibilidade de estabelecer responsabilização ao tráfego entre redes e computadores, além de garantir o melhor aprovisionamento dos recursos Internet sem sacrificar a sua natureza dinâmica e aberta. Além disso, LIPS também simplifica e facilita à detecção precoce de ataques e intrusões a rede, uma vez que exige autorizações de acesso válidas antes de permitir quaisquer pacotes possam ser aceitos e processados.

LIPS opera de dois modos. A base do LIPS é modo *Host*, onde um computador se comunica diretamente com outro. Esse modo é aplicável para comunicações em pequena escala, mas também é usado em grande escala (inúmeros computadores) na presença de um gateway LIPS. O outro modo é o de *Gateway*, onde os computadores LIPS são organizados em zonas de segurança com base em domínios administrativos. O uso de zonas de autorização permite autenticar o acesso de pacotes entre zonas. Cada zona tem um servidor de licenças (*Permit Server*) para gerenciar as licenças entre zonas e um gateway de segurança (*Security Gateway*) para validar os pacotes entre zonas baseado nos pacotes permitidos dentro da zona (internos). Uma vez que uma zona de inter-licenciamento é estabelecida entre duas zonas, as comunicações subsequentes seguirão a autenticação entre elas. Desta forma, haverá uma redução no overhead de licenciamento.

Os autores argumentam que a solução LIPS é escalável e flexível, visto que pode ser implantada de forma incremental (não é necessário que ambos os lados de uma conexão tenham LIPS). Além disso, nenhuma modificação nos programas ou na arquitetura Internet é necessária e não há necessidade de chave criptográficas pesadas porque não há troca de chaves.

3.4.4. SHRED

Atualmente, as diversas soluções para lidar com o envio e a recepção de mensagens de *spam* são baseadas no uso de esquemas de filtragem, análise de tráfego e comportamento [Gomes et al., 2005], uso de *honeypots* [Andreolini et al., 2005] e até mesmo em mudanças no protocolo SMTP [Duan et al., 2005]. Uma idéia, não muito inovadora, é o uso de métodos que permitam punir os *spammers* através de cobranças financeiras. Nesta linha de soluções, uma proposta interessante é SHRED.

Spam Harassment Reduction via Economic Disincentives (SHRED) [Krishnamurthy e Blackmond, 2003] é um esquema que visa diminuir o volume do tráfego de *spam* através da punição monetária dos *spammers*. A idéia central é utilizar selos ou marcas (*stamp)* para inserir desincentivos econômicos para usuários que geram ou propagam *spam*.

O esquema proposto utiliza dois conceitos econômicos: passivo contingente com tempo de expiração e limite de crédito. O primeiro se refere ao fato de que uma dívida possa ser gerada baseada em uma ação externa dentro de um tempo limite. O segundo conceito refere-se ao limite de crédito pré-definido para cada usuário. No esquema SHRED, os selos representam o endividamento e possuem um valor monetário associado. Os selos são pré-alocados para os provedores de acesso através de um dos muitas autoridades de marcação eletrônica (do inglês *Eletronic Stamp Authorities* – ESA) que participam do serviço SHRED. Os selos são colados automaticamente a cada

mensagem enviada pelo provedor de acesso, de forma transparente e em nome do remetente.

A arquitetura SHRED é formada pelo remetente, seu provedor de acesso, uma ou mais ESA, provedor de acesso do destinatário e o destinatário. A Figura 3.15 ilustra a arquitetura.

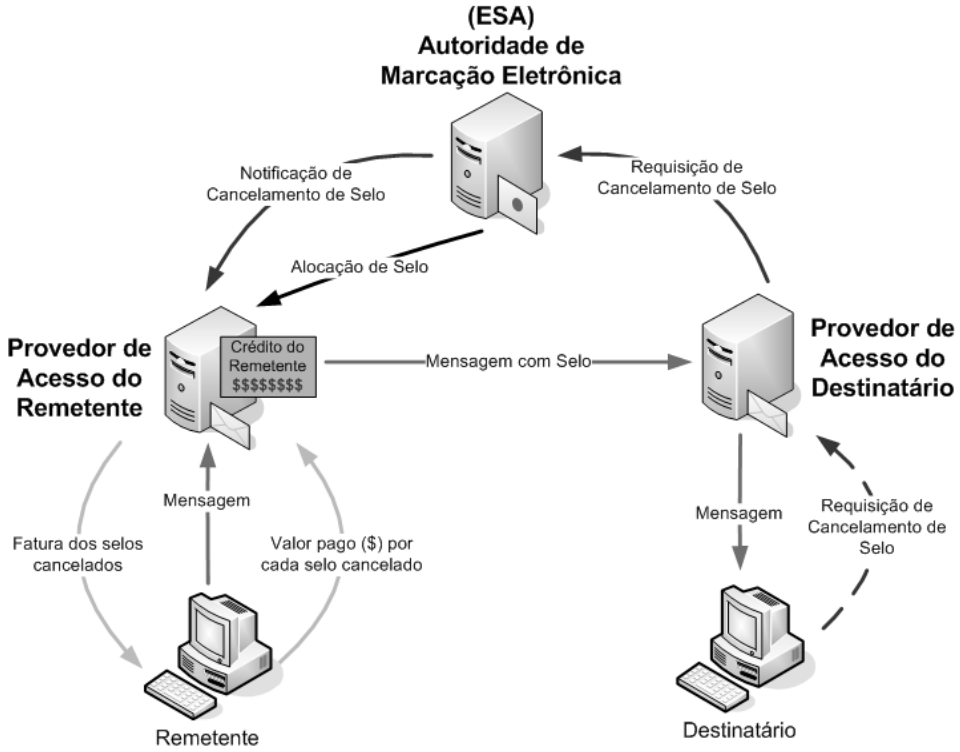

Figura 3.15. Arquitetura SHRED.

O processo de funcionamento é descrito a seguir. Quando o remetente envia um e-mail, seu provedor de acesso adicionará um selo como uma espécie de cabeçalho SMTP e reduzirá o crédito a sua disposição. Os selos têm um tempo de expiração associado a eles e incluem identificações do provedor de acesso de origem e do ESA que emitiu o selo. O provedor de acesso manterá o estado de todos os selos adicionados até que expirem. Quando o provedor de acesso do destinatário recebe o e-mail, verifica se o destinário recebe mensagens com selo. Em caso negativo, a mensagem é processada e entregue de forma tradicional. Em caso positivo, o provedor de acesso do destinatário valida o selo localmente e o repassa ao destinatário. Podem ser tomadas duas ações:

- Se ao ler a mensagem, o destinatário considerá-la indesejada, o selo pode ser cancelado se ainda estiver dentro do tempo de expiração. O cancelamento do selo pode ser feito atráves de uma interface de usuário, acessando uma URL anexada à mensagem ou enviando um e-mail para o administrador. Também podem ser utilizados filtros para realizar esta tarefa de maneira automática. Em seguida, o provedor de acesso do destinatário transmite mensagens canceladas para o ESA através de um canal privado e seguro. O provedor de acesso de

remetente recebe as mensagens com selo cancelado e cobra do remetente por cada selo.

- Se a mensagem recebida pelo destinatário estiver em conformidade ou o selo não for cancelado antes que o seu tempo de expiração seja atingido, o provedor de acesso do remetente incrementa seu limite de crédito.

Em resumo, SHRED pode ser utilizado para complementar os mais variados tipos de filtros de mensagens de correio eletrônico existentes. Contudo, não existe um resultado sobre a efetividade da solução visto que a mesma não foi colocada em operação.

3.4.5. OADS

Os serviços Internet funcionaram por um longo tempo através de um acordo informal e da boa fé dos usuários. Embora exista a falta de controle centralizado ou dono, a Internet é uma das poucas, se não for a única, infra-estrutura auto governada que funciona razoavelmente bem sobre esse paradigma. Hoje, este modelo de confiança está sobre intenso ataque como resultado da diversidade de comunidades que formam a Internet. Será possível manter esse "estilo de vida"? A qual preço? O que precisa ser feito? A proposta apresentada aqui, pelos autores deste minicurso, é chamada de sistemas de detecção de anomalias orientado a orquestração (*Orchestration oriented Anomaly Detection System* – OADS)

A orquestração não é mais uma metafora moderna que descreve uma atividade de gerenciamento de segurança bem conhecida. Analogamente a um maestro que mantém o ritmo, conduzindo os diferentes músicos, gerentes de segurança organizam a harmonia e ritmo de vários instrumentos (sistemas) de detecção de anomalia (sistemas de remediação, firewall, antivírus, aplicações de análise de tráfego, etc.) para atingir o efeito desejado, tornando a rede cada vez mais segura.

Esta proposta empresta o conceito introduzido na arquitetura orientada a serviços (do ingles *Service-Oriented Architecture* - SOA) [Erl, 2004], especificamente o de orquestração de serviços, e introduz uma nova metodologia para detecção de anomalias baseada na orquestração dos serviços de segurança.

A idéia por trás da orquestração é o gerenciamento automático da execução de diferentes detectors de anomalia. Em outras palavras, permite a colaboração e harmonização entre as diferentes técnicas e mecanismos contra atividades maliciosas. Colaboração permite que dois ou mais processos trabalhem em conjunto em direção a um objetivo comum sem um líder. Na música, isso ocorre quando músicos trabalham no mesmo álbum ou música. No contexto de segurança, a colaboração é vista como um facilitador de relações entre os diferentes detectores de anomalia. Por exemplo, dois ou mais detectores podem compartilhar a mesma base de tráfego para realizar análises ou o resultado elaborado por um detector pode ser usado como entrada para outro. A harmonia significa que dois ou mais sons diferentes estão próximos. Estendendo o conceito a área de segurança de rede, pode se dizer que a harmonia é permitir que um serviço de qualquer origem, empregando qualquer tecnologia, trabalhe bem como em uma orquestra.

Em comparação com as atuais metodologias, orquestração destaca-se por tornar possíveis interações entre os mais diversificados sistemas de detecção de anomalias. A metodologia OADS harmoniza bases de informação de tráfego, sistemas detectores de anomalia (ADS) e um mecanismo (*engine*) de orquestração. A Figura 3.16 ilustra a organização da metodologia OADS.

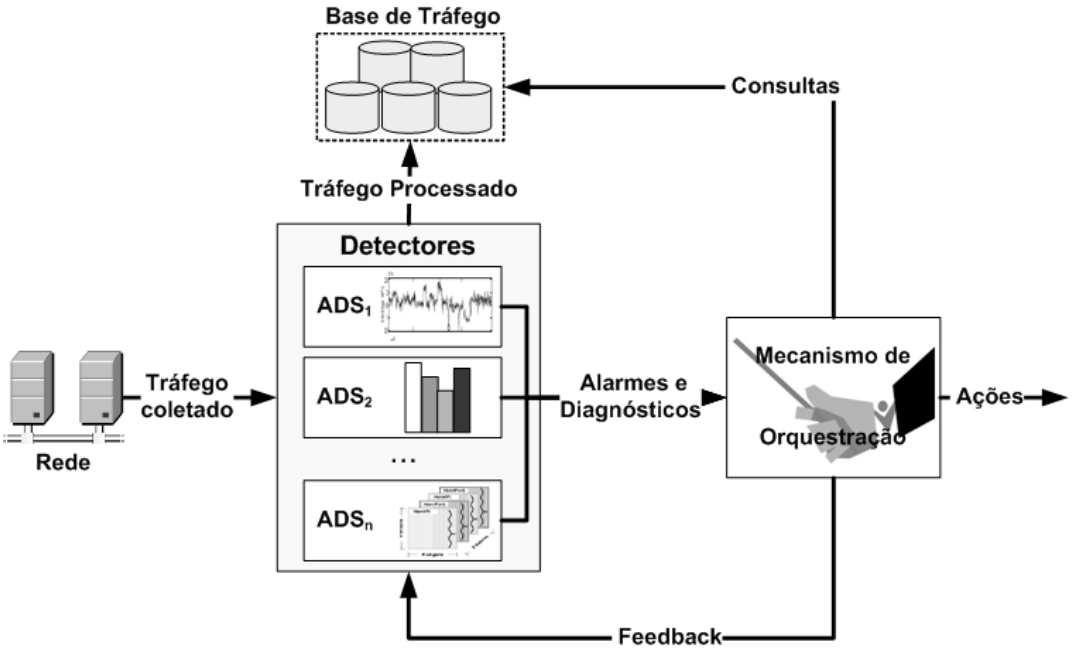

Figura 3.16. Modelo OADS.

- **Bases de tráfego**: armazena o tráfego processado pelos detectores de anomalia. A idéia por trás deste componente é permitir que o mecanismo de orquestração possa obter informações para ajudá-lo a decidir se existe um evento anômalo acontecendo e qual tratamento deve ser dado a este evento. A base de tráfego deve ser maleável para suportar diferentes tipos de tráfego (processado ou não) tais como fluxos OD, pacotes completos, *sketches*, níveis de agregação, clusters, etc.
- **Sistemas detectores de anomalia (ADS)**: atuam como sensores abastecendo o mecanismo de orquestração com informações relevantes (alarmes e diagnósticos), ajudando-o a tomar decisões corretas. Em OADS, os ADS podem e devem colaborar entre si. Por exemplo, a técnica Profiling [Xu et al., 2005] somente reconhece anomalias que geram um grande volume de tráfego. Deste modo, esta técnica pode ser empregada para disponibilizar seus fluxos processados do tráfego para outro detector capaz de encontrar ataques de baixa carga, aumentando assim a probabilidade de descobrir anomalias não percebidas e, conseqüentemente, expandir o nível de segurança da rede.
- **Mecanismo de orquestração**: é responsável por tomar decisões sobre eventos suspeitos ou anômalos baseado principalmente em alarmes disparados pelos diferentes sistemas de detecção de anomalias. Em linhas gerais, a avaliação realizada pelo mecanismo de orquestração leva em consideração as

características como a precisão, o tempo de detecção e o grau de sensibilidade de cada elemento. Além dos alarmes, o conhecimento prévio obtido da observação de anomalias anteriores e dos sinais registrados na base de informação do tráfego também pode ser usado para tomar decisões. A implementação do mecanismo de orquestração pode utilizar desde simples esquemas como um algoritmo de votação ou nívies de prioridade até soluções mais elaboradas e complexas tais como redes neurais e logica fuzzy [Zhi-tang et al., 2005] [Xiang et al., 2006]. Como benefício, o mecanismo de orquestração auxília o adminitrador da rede nas tarefas repetitivas e rotineiras de configuração e avaliação.

Para resumir, a orquestração consiste na captura de regras e sequências de como e quando as diferentes técnicas irão colaborar entre si para fornecer um serviço mais seguro. Em outras palavras, orquestração consiste em criar um modelo de processos executável que implementa um novo serviço através da harmonização de serviços pré-existentes. Os autores deste minicurso acreditam que o estilo de comunicação colaborativa entre os serviços de segurança representa um significativo passo em direção a desenvolvimento de sistema de autodefesa.

3.5. Conclusões

O tráfego não desejado pode ser considerado a verdadeira "pedra no sapato" da Internet. Embora os tipos e suas conseqüências sejam conhecidos, questões como a definição e as formas de minimizar seus efeitos ainda são motivos de discussão. A existência de uma "indústria do mal" motivada e evoluída, aliada ao surgimento de novos serviços e aplicações, a constante evolução tecnológica e ao *boom* populacional de novos (e freqüentemente despreparados) usuários impõe novos desafios na atividade de detectar e limitar o tráfego não desejado.

Este capítulo procurou introduzir o leitor no universo do tráfego Internet não desejado. Em primeiro lugar, o problema foi contextualizado e foram apresentadas definições e discussões sobre o assunto. As causas foram explicadas e os principais tipos de tráfego não desejado foram exemplificados. Em seguida foram discutidas as principais soluções desenvolvidas para lidar com o tráfego não desejado. Por último, foram apresenta algumas potencias e futuras soluções que estão à espera de serem implantadas ou ainda não estão em uso. Para estimular ainda mais o leitor, serão discutidas algumas questões em aberto e, por fim, serão feitas as observações finais.

3.5.1. Questões de pesquisa em aberto

Até o momento, a batalha com o tráfego não desejado tem apresentado soluções apenas reativas. Recentemente, o uso de análise de tráfego para identificar anomalias (principalmente ataques) tem recebido grande estímulo. Entretanto, um grande esforço ainda se faz necessário para encontrar alternativas inteligentes que não somente identifiquem, mas que também ajudem a reduzir este tipo de tráfego.

Algumas questões sobre o tráfego não desejado que ainda estão em aberto serão discutidas a seguir:

- Algumas vezes, novas aplicações e serviços impõem mudanças no gerenciamento e na capacidade dos enlaces das redes como, por exemplo, VoIP, IPTV, jogos em redes, entre outros. Contudo, as redes não estão preparadas para

atender imediatamente todos os novos requisitos exigidos por estes serviços. A solução atual é "não fazer nada" e deixar que essas novas aplicações sejam penalizadas com o não atendimento de seus requisitos ou mesmo com seu total bloqueio até que seu perfil de tráfego seja entendido e criado. A solução ideal é a construção rápida e precisa dos perfis de tráfego dessas novas aplicações e serviços.

- Muitas das recentes tecnologias de rede proporcionam alta largura de banda. Se por um lado, isso permite o aumento da capacidade de tráfego da rede, por outro impõem uma alta carga sobre o gerenciamento da rede. Soluções como amostragens não atingem um nível de precisão adequado. As atuais pesquisas nesta área têm proposto o uso do tráfego agregado tais como análise fluxos de origem e destino (OD) [Lahkina et al., 2004a], a análise do componente principal *(Principal Component Analysis* – PCA) [Crovella e Krishnamurthy, 2006] e o uso de *sketches* [Li et al., 2006] [Abry et al., 2007]. Entretanto, os resultados ainda podem ser melhorados

- Uma vez que as soluções baseadas na análise do tráfego podem levar minutos ou até mesmo dias para descobrir indícios de tráfego não desejado, o tempo de detecção é muito importante. Tempos curtos indicam uma melhor precisão, mas anomalias de baixa carga tendem a não serem detectados. A solução usual é observar estatísticas de períodos de tempo maiores, mesmo que isso implique em grandes latências. Juntamente com as medidas de tomada de ações (por exemplo, aplicação de novas regras ao firewall), o tempo total resultante pode ser relativamente longo a ponto de permitir danos irreversíveis.

- Embora a diversidade de novas aplicações e serviços só aumente e conseqüentemente estimule o tráfego não desejado, a quantidade de soluções de detecção existentes não acompanha esse crescimento. Primeiro porque existem diferentes tipos ou classes de tráfego não desejado. Segundo, esses tráfegos diferem em termos de duração, objetivo e gravidade. Em resumo, as soluções são obrigadas a recorrer a uma variedade de metodologias e técnicas para resolver todas essas questões.

- Uma vez que os usuários (clientes) de banda larga permanecem longos períodos de tempo conectados, é importante conhecer o perfil do tráfego "normal" para esses usuários. Será que existe uma tendência em direção ao uso maior de tráfego para determinadas aplicações? Como é que estas aplicações irão se comportar ? Como se comportam hoje com o número crescente de usuários?

- Com o aumento do número de usuários e computadores ligados na Internet, é importante conhecer quais são os computadores vulneráveis na rede. Será que simplesmente notificar os usuários que seus computadores têm vulnerabilidades e ameaças de segurança é suficiente e eficiente? Porque soluções automatizadas que permitem adequar esses computadores comprometidos tais como NAC [Cisco, 2008] e NAP [Microsoft, 2008] não são muito utilizadas?

3.5.2. Observações Finais

Hoje em dia, a Internet transporta uma grande quantidade de tráfego indesejado. Seja através da deturpação da filosofia aberta da Internet ou mesmo da exploração de diversas vulnerabilidades, o fato é que as conseqüências são altamente prejudiciais. A capacidade de causar danos financeiros é tamanha que esse tipo de tráfego é encontrado até em redes 3G [Ricciato, 2006] e [Ricciato et al., 2006].

A existência de uma economia de submundo financiando e lucrando com esse tipo de tráfego, a falta de normas e leis que responsabilizem e punam os culpados e as limitadas ferramentas empregadas contribuem para a proliferação e perpetuação do tráfego não desejado.

Atualmente, não existe uma lâmpada mágica que forneça a resposta definitiva contra o tráfego Internet não desejado, mas algumas ações podem e devem ser tomadas:

- Aumentar o número de pesquisas nessa área visando, inicialmente, resolver problemas específicos. O apoio de agências governamentais, órgãos de fomento à pesquisa e a própria iniciativa privada devem servir de fontes financiadoras.
- Estimular a realização de eventos, workshops, conferências sobre o tráfego não desejado. Tais encontros servem como ponto de partida para troca de conhecimentos e o surgimento de novas parcerias.
- Desenvolver um modelo jurídico de alcance global para facilitar a captura, o julgamento e a punição aos criadores e incentivadores do tráfego indesejado. Este trabalho deve ser conduzido por especialistas de modo a garantir da melhor forma a flexibilidade da Internet.
- Aumentar o desenvolvimento e uso de soluções contra o tráfego não desejado, uma vez que mesmo que não encerrem o problema, podem diminuir seu volume.
- Por fim, educar os usuários Internet para torná-los mais conscientes dos riscos existentes para seus computadores e sistemas, e torná-los clientes mais exigentes na questão de segurança junto a suas operadoras.

3.6. Referências

[Abry et al., 2007] Abry, P., Borgnat, P., e Dewaele, G. (2007) Sketch based anomaly detection, identification and performance evaluation. *IEEE/IPSJ SAINT Measurement Workshop*, páginas 80-84.

[Anderson et al., 2007] Anderson, L., Davies, E., and Zhang, L. (2007) *Report from the IAB workshop on Unwanted Traffic March 9-10 2006*. RFC 4948. Internet Engineering Task Force.

[Andreolini et al., 2005] Andreolini, M., Bulgarelli, A., Colajanni, M., e Mazzoni, F. (2005) HoneySpam: Honeypots Fighting Spam at the Source. Em *International Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'05)*, páginas 77-83.

[Arbor Networks, 2005] Arbor Networks. (2005) *Worldwide ISP Security Report*. http://www.arbornetworks.com.

[Arbor Networks, 2008] Arbor Networks. (2008) *PeakFlow*. http://www.arbornetworks.com.

[Bailey et al., 2005] Bailey, M., Cooke, E., Jahanian, F., Nazario, J., Watson, D. (2005) The Internet Motion Sensor: A Distributed Blackhole Monitoring System. Em *12th Annual Network and Distributed System Security Symposium*.

[Baker e Savola, 2004] Baker, F., e Savola, P. (2004) *Ingress Filtering for Multihomed Networks*. BCP 84. RFC 3704. Internet Engineering Task Force.

[Bernaille et al., 2006] Bernaille, L., Teixeira, R., Akodjenou, I., Soule, A., e Salamatian, K. (2006) Traffic Classification on the Fly. *ACM SIGCOMM Computer. Communication Review,* 36(2), páginas 23-26, Abril. ACM Press.

[CERT, 2008] CERT – Computer Emergency Response Team. (2008) *Denial of Service Attacks*. http://www.cert.org/tech_tips/denail_of_service.html

[CERT.br, 2008] CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2008) *Estatísticas do CERT.br*. http://www.cert.br/stats/incidentes/

[Choi et al., 2005] Choi, C., Dong, Y., e Zhang, Z. (2005) LIPS: Lightweight Internet Permit System for Stopping Unwanted Packets. *Lecture Notes in Computer Science*, páginas 178-190. Springer.

[Cisco, 2006] Cisco Systems. (2006) *Introduction to Cisco IOS NetFlow - A Technical Overview*. White Paper.http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml.

[Cisco, 2008] Cisco Systems. (2008) *Network Admission Control*. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

[Clark, 1988] Clark, D. (1988) The design philosophy of the DARPA Internet protocols. Em *ACM SIGCOMM*, 1988.

[Cooke et al., 2004] Cooke, E., Bailey, M., Watson, D., Jahanian, F., e Nazario, J. *The Internet Motion Sensor: A Distributed Blackhole Monitoring System*. Technical Report CSE-TR-491-04, University of Michigan, Eletrical Engineering and Computer Science.

[Crovella e Krishnamurthy, 2006] Crovella, M., e Krishnamurthy, B. (2006) *Internet Measurement: Infrastructure, Traffic and Applications*. John Wiley & Sons, Inc., Nova Yorque, NY, USA.

[Davies, 2007] Davies, E. (2007) *Unwanted Traffic*. IETF Journal, volume 3, Dezembro. http://www.isoc.org/tools/blogs/ietfjournal/?p=172

[Dewaele et al., 2007] Dewaele, G., Fukuda, K., Borgnat, P., Abry, P., e Cho, K. (2007) Extracting Hidden Anomalies using Sketch and Non Gaussian Multiresolution Statistical Detection Procedures. *ACM SIGCOMM Workshop on Large-Scale Attack Defense* (LSAD), páginas 145-152.

[Duan et al., 2005] Duan, Z., Gopalan, K., e Dong, Y. (2005) Push vs. Pull: Implications of Protocol Design on Controlling Unwanted Traffic. Em *International Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'05)*.

[Dunia e Qin, 1998] Dunia, R., e Qin, S. J. (1998) A subspace approach to multidimensional fault identification and reconstruction. *American Institute of Chemical Engineers (AIChE) Journal*, páginas 1813–1831.

[Eichin e Rochlis, 1989] Eichin, M. e Rochlis, J. (1988) With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988. Em *IEEE Computer Society Symposium on Security and Privacy*.

[Erl, 2004] Erl, T. (2004) *Service-Oriented Architecture*: A Field Guide to Integrating XML and Web Services. Prentice Hall PTR, Upper Saddle River, NJ, USA.

[Ferguson e Senie, 2000] Ferguson, P., e Senie, D. (2000) *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. BCP 38. RFC 2827. Internet Engineering Task Force.

[Feroul et al., 2005] Feroul, M., Roth, M., McGibney, J., Scheffler, T., e Waller, A. (2005) *Anomaly Detection System Study*. SEINIT Project. http://www.seinit.org/documents/Deliverables/SEINIT_D2.5_PU.pdf.

[Gao et al., 2006] Gao, J., Hu, G., Yao, X., e Chang, R. (2006) Anomaly Detection of Network Traffic Based on Wavelet Packet. Em *Asia-Pacific Conference on Communications (APPC'06)*.

[Gomes et al., 2005] Gomes, L. H., Castro, F., Almeida, V., Almeida, J., e Almeida, R. (2005) Improving Spam Detection Based on Structural Similarity. Em *International Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'05),* páginas 89-95.

[Heidari, 2004] Heidari, M. (2004) *Malicious Codes in Depth*. http://www.securitydocs.com.

[Hoepers et al., 2003] Hoepers, C., Stending-Jenssen, K. e Montes, A. (2003) *Honeynets Applied to the CSIRT Scenario*. http://www.honeynet.org.br/papers/hnbr-first2003.pdf

[Honeynet Project, 2006] The Honeynet Project. (2006) *Know Your Enemy: Honeynets*. http://www.honeynet.org/papers/honeynet/index.html.

[Hyatt, 2006] Hyatt, R. (2006). Keeping DNS trustworthy. *The ISSA Journal*, páginas. 37-38.

[Juniper, 2008] Juniper. (2008) *Juniper JFlow*. http://www.juniper.net/techpubs/software/erx/junose80/swconfig-ip-services/html/ip-jflow-stats-config2.html

[Krishnamurthy, 2006] Krishnamurthy, B. (2006) *Unwanted traffic: Important problems, research approaches*. IAB Workshop. http://www.research.att.com/~bala/papers

[Karagiannis et al., 2005] Karagiannis, T., Papagiannaki, K., e Faloutsos, M. (2005) BLINC: Multilevel traffic classification in the dark. *ACM SIGCOMM Computer Communication Review,* 35(4), páginas 229-240. ACM Press.

[Kumar e Spaffor, 1994] Kumar, S., e Spafford, E.H. (1994) *An application of pattern matching in intrusion detection*. The COAST Project, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA, Technical Report CSD-TR-94-013.

[Krishnamurthy e Blackmond, 2003] Krishnamurthy, B., e Blackmond, E. (2003) *SHRED: Spam Harassment Reduction via Economic Disincentives*. White Papers. AT&T. http://www.research.att.com/~bala/papers/

[Lakhina et al., 2004a] Lakhina, A., Papagiannaki, K., Crovella, M., Diot, C., Kolaczyk, E. D., e Taft, N. (2004) Structural Analysis of Network Traffic Flows. *ACM SIGMETRICS Performance Evaluation Review*, volume. 32, páginas 61-72.

[Lakhina et al., 2004b] Lakhina, A., Crovella, M., e Diot, C. (2004) Diagnosing Network-Wide Traffic Anomalies. Em *ACM SIGCOMM*, páginas 219-230.

[Lakhina et al., 2005] Lakhina, A., Crovella, M., e Diot, C. (2005) Mining anomalies using traffic feature distributions. *ACM SIGCOMM Computer Communication Review,* 35(4), páginas 217-228. ACM Press.

[Laufer et al., 2005] Laufer, R., Moraes, I., Velloso, P., Bicudo, M., Campista, M., Cunha, D., Costa, L., e Duarte, O. (2005) Negação de Serviço: Ataques e Contramedidas. *Livro Texto dos Mini-cursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais* (SBSeg'2005). Florianópolis, Brasil.

[Li et al., 2006] Li, X., Bian, F., Crovella, M., Diot, C., Govindan, R., Iannaccone, G., e Lahkina, A. (2006) Detection and Identification of Network Anomalies using Sketch Subspaces. Em *6th ACM SIGCOMM on Internet Measurement Conference* (IMC´06), páginas 147-152. Rio de Janeiro, Brasil. ACM Press.

[Mahalanobis, 1930] Mahalanobis, P. C. (1930) On tests and measures of groups divergence. *Journal of the Asiatic Society of Bengal*, volume 26.

[Microsoft, 2008] Microsoft. (2008) *Network Access Protection*. http://technet.microsoft.com/en-us/network/bb545879.aspx

[Mirkovic et al., 2004] Mirkovic, J., Martin, J., e Reiher, P. (2004) A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communications Review*, 34(2), páginas 39–53. ACM Press.

[Moore, 2002] Moore, D. (2002) Network Telescopes: Observing Small or Distant Security Events. Em *11th USENIX Security Symposium*.

[Moore et al., 2004] Moore, D., Shannon, C., Voelkery, G. M., e Savagey, S. (2004) *Network Telescopes:* Technical Report. Cooperative Association for Internet Data Analysis.CAIDA. http://www.caida.org/outreach/papers/2004/tr-2004-04

[Morin, 2006] Morin, M. (2006) The Financial Impact of Attack Traffic on Broadband Networks. *IEC Annual Review of Broadband Communications*, páginas 11–14.

[Oliveira et al., 2007] Oliveira, E. L., Aschoff, R., Lins, B., Feitosa, E., Sadok, D. (2007) Avaliação de Proteção contra Ataques de Negação de Serviço Distribuídos (DDoS) utilizando Lista de IPs Confiáveis. *VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (VII SBSEG). Rio de Janeiro, Brasil.

[OpenNet, 2004] OpenNet. (2004) *Internet Filtering in China in 2004-2005: A County Study*. http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf.

[Pang et al., 2004] Pang, R., Yegneswaran, V., Barford, P., Paxon, V., e Peterson, L. (2004) Characteristics of Internet Background Radiation. Em *4th ACM SIGCOMM on Internet Measurement Conference* (IMC' 04). ACM Press.

[Paxson, 1998] Paxson, V. (1998) Bro: A System for Detecting Network Intruders in Real-Time. Em *8th USENIX Security Symposium*.

[Procera Networks, 2007] Procera Networks. (2007) *PacketLogic Hardware Platform*. http://www.proceranetworks.com/products/packetlogic-hardware-platforms.html.

[Provos, 2004] Provos, N. (2004) A Virtual Honeypot Framework. Em *13th USENIX Security Symposium*.

[Provos, 2008] Provos, N. (2008) *Honeyd*. http://www.honeyd.org.

[Radicati Group, 2006] Radicati Group. (2006) Corporate Email Market 2006-2010. http://www.radicati.com.

[Research Alliance, 2008] Research Alliance. (2008) *The Honeynet Project*. http://www.honeynet.org/alliance/

[Ricciato, 2006] Ricciato, F. (2006) Unwanted traffic in 3G networks. *ACM SIGCOMM Computer Communications Review*, 36(2), páginas 53 – 5l. ACM Press.

[Ricciato et al., 2006] Ricciato, F., Hasenleithner, E., Svoboda, P., and Fleischer, W. (2006) On the impact of unwanted traffic onto a 3G network. Em *Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing* (SecPerU 2006).

[Richardson, 2007] Richardson, R. (2007) CSI/FBI Computer Crime Survey. Em *Twelfth Annual Computer Crime and Security*, páginas 1-30.

[Scherrer et al., 2006] Scherrer, A., Larrieu, N., Borgnat, P., Owezarski, P., e Abry, P. (2006) Non Gaussian and Long Memory Statistical Modeling of Internet Traffic. Em *4th International Workshop on Internet Performance, Simulation, Monitoring and Measurement* (IPS-MoMe).

[Scherrer et al., 2007] Scherrer, A., Larrieu, N., Owezarski, P., Borgnat, P., e Abry, P. (2007) Non-Gaussian and Long Memory Statistical Characterizations for Internet Traffic with Anomalies. *IEEE Transactions on Dependable and Secure Computing*, volume 4, páginas 56-70.

[Schulze e Mochalski, 2007] Schulze, H. e Mochalski, K. (2007) *Internet Study 2007*. Ipoque. http://www.ipoque.com/userfiles/file/internet_study_2007.pdf

[Snort, 2008] Snort. (2008) *Snort IDS*. http://www.snort.org.

[Soto, 2005] Soto, P. (2005) *Identifying and Modeling Unwanted Traffic on the Internet*. Dissertação de Mestrador. Departamento de Engenharia Elétrica e Ciência da Computação, Massachusetts Institute of Technology (MIT).

[Spitzner, 2002] Spitzner, L. (2002) *Honeypots: Tracking Hackers*. Addison-Wesley Professional.

[SRUTI, 2005] USENIX. (2005) *International Workshop on Steps to Reducing Unwanted Traffic on the Internet*. http://www.usenix.org/events/sruti05/

[StillSecure, 2008] StillSecure. (2008) *Safe Access – Network access control solution*. http://www.stillsecure.com/safeaccess.

[Taveira et al., 2006] Taveira, D., Moraes, I., Rubinstein, M. e Duarte, O. (2006) Técnicas de Defesa Contra Spam. *Livro Texto dos Mini-cursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais* (SBSeg'2006). Santos, Brasil.

[Weaver et al., 2003] Weaver, N., Paxson, V., Staniford, S., e Cunningham. R. (2003) A Taxonomy of Computer Worms. Em *ACM Workshop on Rapid Malcode*.

[Wu et al, 2006] Wu, M., Miller, R.C., Little, G. (2006) Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. Em *Symposium On Usable Privacy and Security* (SOUPS), páginas 102-113.

[Xiang et al., 2006] Xiang, G., Min, W., e Rongchun, Z. (2006) Application of Fuzzy ART for Unsupervised Anomaly Detection System. Em *International Conference on Computational Intelligence and Security*, volume 1, páginas 621-624.

[Xu et al., 2005a] Xu, K., Zhang, Z-L., e Bhattacharrya, S. (2005) Profiling internet backbone traffic: Behavior models and applications. *ACM SIGCOMM Computer Communication Review,* 35(4), páginas 169-180. ACM Press.

[Xu et al., 2005b] Xu, K., Zhang, Z-L., e Bhattacharrya, S. (2005) Reducing unwanted traffic in a backbone Network. Em *International Workshop on Steps of Reducing Unwanted Traffic on the Internet* (SRUTI´05).

[Zhi-tang et al., 2005] Zhi-tang, L., Yao, L., e Li, W. (2005) A Novel Fuzzy Anomaly Detection Algorithm Based on Artificial Immune System. Em *8th International Conference on High-Performance Computing in Asia-Pacific Region* (HPCASIA'05), páginas 479-483.