UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

Aplicação da Análise Matemática no Rastreamento Reverso do Número IP para Uso em Redes TCP/IP sob Ataque de Negação-de-Serviço

MATEUS MOSCA VIANA

Orientador: Prof. José Neuman de Souza, Dr. (UFC-BR)

Julho 2007

UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

Tese de Doutorado

Aplicação da Análise Matemática no Rastreamento Reverso do Número IP para Uso em Redes TCP/IP sob Ataque de Negação-de-Serviço

Doutorando:
MATEUS MOSCA VIANA

Orientador:
Prof. José Neuman de Souza, Dr. (UFC-BR)

Tese submetida à Coordenação do Curso de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos exigidos para a obtenção do grau de Doutor em Engenharia de Teleinformática

Fortaleza - Ceará
Julho 2007

MATEUS MOSCA VIANA

Aplicação da Análise Matemática no Rastreamento Reverso do Número IP para Uso em Redes TCP/IP sob Ataque de Negação-de-Serviço

Esta Tese foi julgada adequada para a obtenção do título de Doutor em Engenharia de Teleinformática e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará.

MATEUS MOSCA VIANA

Aprovada por:

Prof. José Neuman de Souza, Dr.

Prof. Eduardo Bergamini, Dr.

Prof. Raimundo Hélio Leite, Dr.

Prof. Paulo César Cortez, Dr.

Prof. Giovanni Cordeiro Barroso, Dr.

FORTALEZA, CE - BRASIL
JULHO DE 2007

Agradecimentos

Não seria possível concluir o presente trabalho sem contar com a inestimável colaboração de algumas instituições e de muitas pessoas, pelas quais tenho eterna gratidão. Segue a relação:

- Programa de Pós-Graduação em Engenharia de Teleinformática (PPGETI), iniciativa ousada do Centro de Tecnologia da Universidade Federal do Ceará, nas pessoas de seu Coordenador, Professores e Funcionários.

- Instituto Atlântico, Instituição ímpar e pioneira no Estado do Ceará, nos ramos da pesquisa e do desenvolvimento nas áreas de Tecnologia da Informação e Telecomunicações, pela cortesia e atenção com as quais sempre me distinguiu. Além de permitir o uso das suas instalações, financiou o projeto com uma bolsa durante os dois primeiros anos do trabalho.

- Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico - FUNCAP, que completou o suporte financeiro do projeto nos três últimos semestres do trabalho, na pessoa do seu Presidente, Prof. José Vitorino, antigo colega da UFC, e do seu Corpo de Funcionários.

- Aos Professores Eduardo Bergamini, Raimundo Hélio Leite, Paulo César Cortez e Giovanni Cordeiro Barroso, pela gentileza e prontidão com que aceitaram a laboriosa tarefa de compor a Banca Examinadora, mesmo adicionando mais uma carga ao seu importante e pesado trabalho.

- À Professora Rossana Andrade e aos Professores Javam Machado e Helano de Souza Castro, de quem tive a honra de ser aluno em algumas disciplinas.

- Aos amigos e amigas do Instituto Atlântico, desde o seu primeiro Superintendente, Eduardo Bernal, e o atual José Eduardo, o gerente de Tecnologia Adriano Carvalho, todo o pessoal da GADF, o pessoal

do apoio e os amigos do corpo tecnológico. Especial agradecimento aos participantes do "Café Cultural" das sextas-feiras, que desejo representar na pessoa do Gilberto Coelho, que com seu talento incomum gentilmente desenhou as figuras que ilustram esta tese.

- Por fim, gostaria de destacar duas pessoas em especial que, desde o princípio, confiaram no meu trabalho e o apoiaram de modo incondicional. Refiro-me aos meus amigos, Professores João César Moura, primeiro Coordenador do PPGETI e José Neuman de Souza, meu orientador.

Resumo da Tese apresentada à PPGET/UFC como parte dos requisitos necessários para a obtenção do grau de Doutor em Engenharia (Dr.)

APLICAÇÃO DA ANÁLISE MATEMÁTICA NO RASTREAMENTO REVERSO DO NÚMERO IP, PARA USO EM REDES TCP/IP SOB ATAQUE DE NEGAÇÃO DE SERVIÇO

Mateus Mosca Viana

Julho/2007

Orientador: José Neuman de Souza

Programa: Pós-Graduação em Engenharia de Teleinformática

O ataque por negação de serviço ficou conhecido a partir do ano de 1988, tendo se tornado uma grave ameaça ao funcionamento das redes de computadores em todo o mundo. Quando essa modalidade de ataque está em curso a vítima recebe um incremento tão intenso na demanda pelos seus recursos computacionais, que os mesmos podem se tornar indisponíveis aos usuários. A despeito de existirem outras formas de ataques a redes de computadores, a negação-de-serviço tem sido alvo de particular interesse da comunidade científica dedicada no estudo da segurança de redes de computadores. Isto se deve à simplicidade com que este ataque pode ser desferido, aliada ao seu efeito devastador. Além disso, a dificuldade que a vítima terá em se defender, dependerá da forma como o ataque se processa, sendo as formas de ataque caracterizadas como "direta", "indireta", ou "distribuída".

Na literatura especializada em segurança existem trabalhos com variadas propostas para a abordagem deste problema, sendo predominante nas mesmas o caráter de estado-da-arte. A tendência que se acentua nas propostas é a da união de argumentos computacionais e matemáticos.

Nesta tese são analisados alguns trabalhos que apresentam contribuições relevantes para a resolução do problema em estudo. Junta-se a esta análise a apresentação de uma idéia original para o tratamento do problema, utilizando conceitos e ferramentas da Teoria das Variáveis Complexas. Com

efeito, através de um mapeamento do ambiente de ataque no espaço das variáveis complexas, desenvolve-se um método para a identificação do número IP de um atacante por meio do uso do conceito de "número de rotação de uma trajetória ao redor de um ponto". Este conceito é uma conseqüência do "Teorema Integral de Cauchy", um dos mais importantes resultados da Teoria das Variáveis Complexas.

Abstract of Thesis presented to PPGET/UFC as a partial fulfillment of the requirements for the degree of Doctor in Engineering (Dr.)

APPLICATION OF MATHEMATICAL ANALYSIS IN IP NUMBER BACKTRACKING TO USE IN TCP/IP NETWORKS UNDER DENIAL-of-SERVICE ATTACK

Mateus Mosca Viana

Julho/2007

Advisor: José Neuman de Souza

Department: Teleinformatics Engineering

The denial-of-service attack was unveiled in the year of 1988 and became a serious threat to the computer networks to carry on properly, around the world. When this kind of attack is going on the victim suffers so high increment in demanding computacional resources, that they may become unavailable to the true users.

Despite the fact that there exist other kind of computers network attacks, the denial-of-service attack is the target of a special interest by the scientific community, dedicated to computers network security. This is due to the simplicity in starting the attack, associated with its destructive effect. The difficulty in defending against this attack grows according to it is in a form "direct", "indirect", or "distributed".

In the specialized literature dealing with security there are papers with varied approaches to this problem and the main feature is the predominant state-of-art. The stressed trend in the arised proposes is the joining of mathematical and computational arguments.

In this thesis some papers are analysed with considerable contributions to the problem under study. An original idea dealing with this problem, based in concepts and tools of the Theory of Complex variables, is joined to this analysis. The mapping between the attack environment and the complex

variables space is the form by which one may construct a method to determine an attacker IP number, through the use of the "windind number of a path around a point". This concept is a consequence of the "Cauchy's Integral Theorem", one the the most important results in the Theory of complex Variables.

Lista de Figuras

Sumário

Capítulo 1

Introdução

Desde que as redes de computadores surgiram, na década de 1960, o uso da Tecnologia da Informação tem experimentado avanços significativos, cada vez mais permeados no âmbito da sociedade. Esse quadro se deve ao elevado grau de desenvolvimento científico e tecnológico que se conseguiu alcançar nesse período um pouco superior a quarenta anos. As conseqüências de natureza social, decorrentes do uso dos ítens tecnológicos dessa área do conhecimento, se refletem em profundas mudanças que têm ocorrido nos hábitos e nas vidas das pessoas.

Na verdade, além da fundamentação científica e do elevado grau de sofisticação tecnológica, um importante fator que induz à utilização das redes de computadores é a confiança que as pessoas depositam nas mesmas. E essa confiança decorre da certeza de se saber que é possível usar as redes de computadores sem o risco de se tornar vítima de algum ato ilícito. Em outras palavras, a confiança decorre da aparente segurança que as redes suscitam nos usuários. Isto significa que o cuidado com a segurança deixa de ser um ítem para o qual se exija uma justificativa estrita e passa a ser uma prática compulsória.

A seguir são apresentadas as diretrizes gerais que regulam o assunto abordado neste trabalho, cuja finalidade é nortear o entendimento do leitor.

1.1 Motivação e Delimitação do Estudo

O tema referente ao estudo da segurança em redes de computadores tem fascinado um público, cada vez mais numeroso, tanto de profissionais, quanto de usuários das mesmas. Na verdade, existe um constante desafio a todos os interessados em segurança, uma forma de contrapartida sombria que tem acompanhado todo o desenvolvimento das redes de computadores, desde as suas origens, até os dias atuais.

O desafio decorre do sistemático surgimento de novas formas de ataques às redes. Essa prática nociva tem crescido em importância à proporção que as relações sociais, cada vez mais, dependem de dispositivos remotos e interligados, para a demanda de serviços, para os negócios e para o lazer.

Variadas alternativas para o incremento da segurança têm surgido ao longo do tempo. Os exemplos mais relevantes, dentre essas alternativas, são aqueles que tratam do uso de senhas secretas, técnicas criptográficas e barreiras ao acesso, além da execução de rastreamento do atacante.

Este trabalho apresenta uma análise de algumas das mais significativas estratégias para rastreamento e identificação de atacantes a redes de computadores. O ataque em foco é aquele conhecido pela denominação de **negação-de-serviço**, cuja nomenclatura em Língua Inglesa é *Denial-of-Service* (DoS), ou a sua variante, que recebe o nome de *Distributed Denial-of-Service* (DDoS).

O desenvolvimento da análise leva em conta o aprofundamento dos aspectos matemáticos envolvidos em cada uma das estratégias, necessários para justificar os resultados utilizados pelos seus autores. A adoção deste comportamento permite avaliar as propostas quanto à sua validade sob o ponto de vista teórico.

Além da análise matemática realizada sobre propostas de outros autores, este trabalho também contém uma estratégia original para o problema do rastreamento e identificação de atacantes, baseada na Teoria da Análise Com-

plexa. Naturalmente, esta proposta é acompanhada de uma correspondente análise matemática que a justifica.

Os objetivos a serem atingidos por meio do presente trabalho são apresentados na próxima seção a seguir, de modo mais detalhado.

1.2 Objetivo Geral

Neste trabalho se encontram apresentadas algumas das mais relevantes abordagens para a solução do problema do rastreamento e identificação de atacantes, por negação-de-serviço, existentes na literatura especializada.

O objetivo que se procura atingir com a exposição destas propostas se divide em dois aspectos distintos. O primeiro trata da verificação da validade das propostas apresentadas, por meio do uso de ferramentas da análise matemática. O outro se constitui na formulação de uma nova proposta para tratar o referido problema por meio do uso de argumentos de natureza matemática, oriundos da Teoria das Variáveis Complexas.

Os objetivos específicos do trabalho se dividem entre os capítulos subseqüentes ao atual, nos quais se desenvolvem os detalhes analíticos das propostas consideradas. As próximas subseções se referem aos conteúdos destes capítulos.

1.2.1 *Origem do Problema*

As raízes históricas das origens dos ataques DoS e DDoS se confundem, em parte, com a própria origem das redes de computadores e da Internet. A apresentação deste posicionamento histórico é o objetivo do Capítulo 2, intitulado **Riscos nas Redes de Computadores**.

Nenhuma proposta para solução do problema do ataque é apresentada naquele capítulo, que cuida apenas do posicionamento do cenário tecnólogico das redes de computadores, no início dos anos 60, quando o Mundo experi-

mentava as aflições causadas pela **Guerra Fria**. Esta era a denominação do momento histórico durante o qual surgiu a **ARPANET**, a arquitetura de rede apresentada como solução para o problema de interrupção das comunicações, em decorrência de possíveis bombardeios a instalações militares.

Paradoxalmente, contudo, a robustez deste modelo de arquitetura de rede seria posta à prova depois da sua liberação para uso no meio civil, isto é, quando evoluiu para o que se conhece atualmente como **Internet**. Mesmo sendo praticamente à prova de interrupções, a grande rede veio a se tornar o ambiente no qual os ataques DoS e DDoS seriam algumas as mais temíveis ameaças que os seus usuários poderiam encontrar.

1.2.2 *Primeiras Contramedidas*

A capacidade de um atacante em disfarçar o endereço de origem de um ataque do tipo DoS, ou DDoS, motivou o surgimento de métodos indiretos para rastrear o local de onde é disparado. O Capítulo 3, cujo título é **Determinismo Computacional**, contém duas propostas primitivas para efetuar este rastreamento.

A primeira proposta se baseia na idéia de que todos os pacotes trafegando na rede devem ser marcados preventivamente. Uma análise matemática elementar mostra a existência de fundamento no fato de que, este procedimento determinístico pode trazer o risco de sobrecarregar o tráfego na rede. E esta sobrecarga ocorrerá, principalmente, se o procedimento for utilizado em larga escala.

Por outro lado, em ambientes restritos existe a possibilidade do uso desta abordagem, desde que se permita alguma degradação no desempenho do tráfego na rede. Essas conclusões tomam por base as condições atuais em que se encontra a tecnologia disponível para a transmissão de dados.

Quanto à outra alternativa proposta ainda no Capítulo 3, esta se apresenta como sendo uma atitude de caráter muito ofensivo. Trata-se de

um processo para detectar os elementos da trajetória de ataque por meio de um contra-ataque da vítima aos roteadores da rede, a partir dos que lhes sejam mais próximos. Mesmo que possa apresentar alguma eficácia esse método faz a vítima se comportar também como um atacante, o que é nocivo em um ambiente cooperativo como o de uma rede.

1.2.3 *Modelagem Determinística*

No Capítulo 4, cujo título é **Abordagem Matemática Determinística**, a abordagem se baseia na construção de um modelo matemático. Para esta finalidade são utilizados argumentos com base em métodos numéricos de interpolação e de resolução de equações lineares e resultados da Teoria dos Números. A base do modelo é o artigo de Dean, Franklin e Sttublefield, referência [21], publicado no ano de 2002.

O ponto central da proposta é a construção de um polinômio para representar a trajetória de ataque. Os seus coeficientes são os números IP dos roteadores desta trajetória e o grau de cada termo indica a distância, em "saltos", até a vítima. Para isto, é necessário montar um sistema de equações lineares, por meio do uso da técnica de interpolação polinomial.

Deve-se ter em conta que o conjunto numérico dos elementos usados na interpolação possui a estrutura algébrica de um corpo finito, pois estes elementos são componentes de números IP. Os mecanismos de cálculo numérico assumem um caráter singular, visto que não é comum na literatura habitual sobre métodos de interpolação e de resolução de equações, o tratamento de problemas sobre corpos numéricos finitos.

Apesar de o carácter do processo de rastreamento ser determinístico, a marcação de pacotes se faz de modo aleatório. Esta prática permite reduzir a quantidade de pacotes selecionados e, por conseguinte, a carga de processamento nos elementos da rede. Apesar de algumas restrições quanto à sua aplicação, na forma como se encontra, esta proposta se constitui em

significativa fonte de motivação aos interessados no desenvolvimento de soluções para o problema do rastreamento. Enfim, esse artigo se constituiu na inspiração inicial para a realização do presente trabalho.

1.2.4 *Modelagem Computacional*

O resultado da procura de um procedimento computacional, destinado a realizar o rastreamento do número IP, compõe o conteúdo do Capítulo 5, intitulado **Visão Computacional Probabilística**. O trabalho mais relevante da literatura especializada, e que segue esta direção, foi publicado no ano 2000 por Savage, Wetherall, Karlin e Anderson, conforme referência em [51].

Dois aspectos são destacados nesta metodologia proposta para o rastreamento. O primeiro diz respeito à forma de como se calcula o tamanho da amostra a ser utilizada, cujo fundamento é o **Problema do Coletor de Cupons**, oriundo da **Teoria das Probabilidades**, também conhecido pela denominação de *Coupon Collector´s Problem*, em Língua Inglesa. No apêndice B são apresentados mais detalhes que envolvem este problema, a título de esclarecimento adicional sobre o mesmo.

O outro aspecto a ser considerado diz respeito ao modo de realizar a marcação de um pacote, através da utilização de bits já existentes no pacote. Nenhum novo campo é acrescentado ao pacote, cujo tamanho permanece o mesmo de antes da marcação. Assim, não há qualquer contribuição no sentido de degradar o desempenho da rede, em virtude de sobrecarga.

Este trabalho tornou-se uma referência clássica para o estudo de métodos de rastreamento de número IP.

1.2.5 *Modelagem Probabilística*

O uso de métodos probabilísticos tem se tornado a principal estratégia para enfrentar o problema do rastreamento e identificação de atacantes. Os artigos de Micah Adler, vide [1, 44], que foram publicadas no ano de 2002, se constituem nos principais exemplos de como esta tendência ainda evolui. No Capítulo 6, cujo título é **Tratamento Matemático Probabilístico**, são apresentadas as idéias que constam nestas referências.

A fim de tornar mais pedagógica a apresentação, o processo de marcação e de rastreamento é mostrado primeiro na situação hipotética da existência de apenas uma trajetória de ataque. Somente esse caso é suficente para um vasto desenvolvimento da idéia presente nos artigos referidos, sendo explorada de modo intenso no presente trabalho.

Como uma extensão da idéia original, as referências também sugerem como passar para o caso em que o ataque é realizado através de múltiplas trajetórias. Esta situação mais geral é apenas citada neste trabalho, por se constituir em um vasto campo específico de pesquisa que transcende os objetivos aqui delineados.

1.2.6 *Análise Complexa*

Quanto ao Capítulo 7, isto é, **Uso da Análise Complexa no Rastreamento Reverso**, no mesmo se trata de uma proposta original do autor, referente a um novo ponto de vista sob o qual se pode vislumbrar o problema do rastreamento. As considerações são de natureza essencialmente teórica e pressupõem que o ataque ocorre ao longo de uma única trajetória. Outra suposição importante é a de que, em cada roteador, existe um programa destinado a marcar pacotes em trânsito com o seu número IP.

O objetivo que se tem em mente é mostrar a possibilidade de determinar o número IP de um roteador atacante, a partir da transferência do problema,

do ambiente de ataque para o espaço das variáveis complexas. A escolha do espaço das variáveis complexas como o ambiente adequado para resolver o problema, se fundamenta na riqueza de propriedades e de resultados existentes com respeito aos elementos componentes deste espaço.
O primeiro passo é a definição de uma função que transforma um número IP de um roteador, em um número complexo. Em seguida, associa-se a quantidade de pacotes marcada no roteador em estudo, com o número de voltas de um caminho fechado γ em torno do ponto complexo ω_k, imagem do roteador R_k. Utilizando-se o conceito de "número de rotação de um caminho em torno de um ponto", pode-se construir uma equação, cuja solução fornece o número IP procurado.

O destaque necessário sobre o que se conclui do presente trabalho será objeto de comentário na próxima subseção.

1.2.7 *Aspectos da Conclusão*

Ao longo do desenvolvimento de todo o trabalho existe o cuidado de se apresentarem conclusões específicas, ao final de cada um dos sete primeiros capítulos. Desse modo, se pode avaliar o que cada um desses capítulos representa no cenário geral do conhecimento sobre o problema do rastreamento reverso do número IP.

A finalidade da inclusão do Capítulo 8, intitulado **Conclusões e Trabalhos Futuros**, é permitir que se tenha uma referência a todos os pontos de convergência em cada um dos capítulos. Além disso, essa convergência não pode prescindir de um comentário de caráter geral, quando se defrontam os assuntos tratados ao longo de todo o trabalho.

O Capítulo 8 se encerra mostrando caminhos para desenvolvimentos ulteriores da pesquisa, nesse importante tópico da segurança das redes de computadores e de comunicações.

O enfoque da metodologia utilizada neste trabalho é apresentado na seção a seguir.

1.3 Percurso Metodológico

Tratando-se de uma incursão prospectiva sobre um problema cuja solução, a rigor, ainda se encontra no estado da arte, o presente trabalho foi conduzido por uma técnica que tem por base a pesquisa documental. Levando em conta a natureza do problema sendo estudado, as distintas referências que fazem parte do acervo consultado se dividem em dois grupos principais.

O primeiro grupo de documentos se constitui daqueles específicos sobre o problema do rastreamento reverso, quando considerado como uma contramedida aos ataques do tipo DoS e DDoS. Esse grupo é aquele no qual predominam os artigos científicos obtidos de publicações especializadas. A fonte primordial para a pesquisa desses documentos ainda é a Rede Internet. Já o outro grupo é aquele no qual se encontram as referências consideradas clássicas, no que concerne aos modelos e métodos matemáticos utilizados. Livros são os principais componentes deste acervo documental.

Enfim, o permanente confronto de idéias, necessário para o desenvolvimento do trabalho, somente pode progredir mediante o uso permanente do método dedutivo. Somente através da linha de raciocínio proporcionada por esse método seria possível aplicar, em situações específicas, as idéias gerais do conhecimento matemático.

A seguir, visando compor o cenário do problema em estudo, a próxima seção apresenta uma visão histórica das idéias que conduziram ao surgimento das redes de computadores.

1.4 Ambiente Histórico

O período histórico posterior ao término da Segunda Guerra Mundial, entre 1945 e meados dos anos 1970, recebeu a singular denominação de "Período da Guerra Fria". Isso foi em decorrência da beligerância diplomática ocorrida entre países do bloco ocidental, liderado pelos Estados Unidos da América, e

do bloco oriental, sob a liderança da então União Soviética. Havia uma real ameaça de ser deflagrada a tão temida "Terceira Guerra Mundial", pelos detentores de armamento nuclear, cujo acirramento maior se deu durante os anos 1960.

A utilização da tecnologia da Informática já era uma realidade no bloco ocidental, em particular nos ambientes militares e nos de pesquisa científica, sendo comuns as "redes centralizadas", cuja topologia é mostrada na Figura 1.1. A característica de tais redes era a de centralização em um só computador, ao qual estavam conectados "terminais de teleprocessamento", com a função única de serem periféricos para entrada ou saída remota de dados, sem nenhuma atividade de processamento independente.

A natureza das redes centralizadas tornava mandatório que, qualquer mensagem entre os usuários dos terminais deveria passar pelo computador central. Desse requisito decorriam dois importantes fatos.

Em primeiro lugar, o controle total da rede era exercido por quem co-

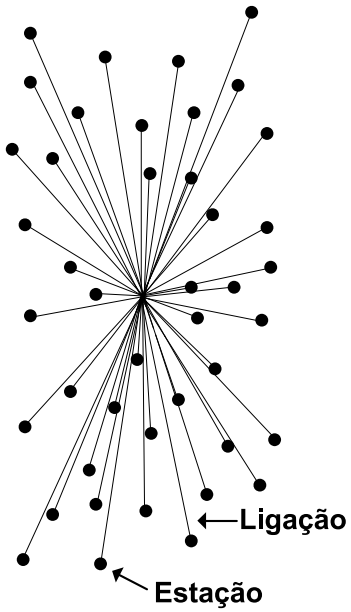

Figura 1.1: Rede Centralizada.

mandava o computador central. Sendo essa uma característica de natureza totalitária, sempre havia o risco de algum viés no modo como se utilizava

a rede, na possibilidade de que o interesse pessoal do controlador exercer alguma interferência.

Além disso, a centralização também expunha todo o sistema a uma situação de extrema vulnerabilidade. Com efeito, caso o computador central fosse desativado, a rede imediatamente pararia de funcionar, cessando toda a comunicação que se processava entre os usuários. A falta de comunicação preocupava, e preocupa, particularmente as autoridades militares, pois é um fato que pode significar a derrota em um campo de batalha, na época o principal motivo para o uso das redes de computadores.

Essa situação despertou o interesse de pesquisadores na procura de soluções capazes de neutralizar a vulnerabilidade existente nas redes centralizadas. A conseqüência mais notável da inovação surgida de tais esforços se constituiu nas bases da rede que hoje é conhecida como Internet.
Na próxima seção é apresentada a estrutura geral do presente trabalho, com uma descrição sucinta de cada um dos próximos capítulos.

1.5 Estrutura do Trabalho

A evolução da idéia de rede de computadores, até o estágio atual em que se encontra a Internet, bem como a abordagem dos aspectos intrínsecos referentes aos riscos do uso de redes de computadores, são os assuntos tratados no Capítulo 2. Efetuar a confrontação histórica dos fatos na linha do tempo permite o entendimento mais efetivo de todo o panorama do problema do rastreamento reverso, de que trata o trabalho. Ao mesmo tempo, a justificativa da escolha do tema do trabalho se torna mais clara, diante dessa mesma confrontação histórica.

Algumas das primeiras tentativas de defesa contra o ataque de negação de seviço compõem o conteúdo do Capítulo 3. Nota-se a predominância de um raciocínio puramente computacional, de caráter determinístico, no trato da ameaça. Uma rápida e simples análise matemática, desenvolvida sobre o

modelo de marcação determinística de pacotes, mostra que o modelo apresentado pode ser utilizado em ambientes e abrangência restrita.

A partir do Capítulo 4 o trabalho se concentra no assunto da pesquisa em foco, que é o rastreamento reverso do número IP. Com efeito, no próprio Capítulo 4 são tratados os aspectos referente a um método baseado em argumentos algébricos determinísticos. Por meio de tais argumentos, podem ser obtidos os dados necessários para a realização do rastreamento reverso do número IP. Este método, proposto por Dean, Franklin e Sttubfiled, vide [21], compreende o modo de como se faz a amostragem dos pacotes´para análise e a definição de quais campos precisam ser examinados. Em seguida, com os dados obtidos trata-se de construir um sistema de equações lineares, do qual se conhecem as soluções, mas as incógnitas são justamente os coeficientes. Todo o processo se conclui quando se determinam estes coeficientes, cujos valores são os números IP dos roteadores da trajetória de ataque. Esta visão de caráter matemático foi inspiradora do tema abordado no presente trabalho.

Dentre as técnicas que atualmente se sobressaem como promissoras na marcação de pacotes, destacam-se aquelas de caráter probabilístico. No Capítulo 5 se apresentam aspectos de um famoso trabalho devido a Savage, Wetherall, Karlin e Anderson, vide [51], que tem servido como base ao estudo de métodos para o rastreamento reverso do número IP. Nesse trabalho prevalece uma abordagem de caráter computacional, com acentuado viés probabilístico. O processo de seleção de pacotes toma por base um importante resultado da Teoria da Amostragem, conhecido como "Problema do Celetor de Cupons´´. O modo como se realiza o manuseio de bits do cabeçalho TCP/IP, para armazenar a marcação de pacotes, é um dos pontos centrais desta abordagem. Esta marcação se refere à identificação de um roteador da trajetória de ataque e se trata de um ponto crítico para qualquer contramedida ao ataque de negação de serviço.

Seguindo a linha da abordagem probabilística, no Capítulo 6 se encontra um estudo baseado no artigo de Adler, vide [1]. Este trabalho se concentra na

discusão de qual deve ser a quantidade de bitas necessária, no cabeçalho do protocolo TCP/IP, de modo que se possa utilizá-los no processo de marcação de pacotes. Trata-se de um promissor estudo de natureza teórica, através do qual se poderão estabelecer bases para a codificação necessária à identificação de números IP de roteadores em trajetórias de ataque.

Depois de todas as considerações nos capítulos anteriores, envolvendo trabalhos relevantes na abordagem do problema em foco, apresenta-se no Capítulo 7 uma proposta original.

Trata-se de uma visão inovadora, no que concerne ao modo de determinar quais são os roteadores de uma trajetória de ataque. Com efeito, o ambiente de ataque é transformado por meio de uma função em um subconjunto do espaço das variáveis complexas. Através desta transformação, algumas características do ataque são associadas a conceitos existentes no espaço das variáveis complexas. A riqueza de conteúdo teórico deste novo ambiente permite que se determine o número IP de um roteador, a partir de dados amostrados no ambiente de ataque original.

Trata-se, também, de um estudo teórico cuja pretensão imediata é permitir a ampliação do horizonte de conhecimento sobre o problema do rastreamento reverso. O passo seguinte será a implementação de modelos desta teoria, que contribuam para o desenvolvimento de soluções práticas para a defesa contra o ataque de negação de serviço.

Enfim, o Capítulo 8 contém conclusões e comentários sobre trabalhos futuros, relacionados com o problema do rastreamento reverso do número IP, em especial baseados na proposta do Capítulo 7. Alguns apêndices foram inseridos com o intúito de fornecer ao leitor do trabalho algumas referências rápidas sobre aspectos da Matemática utilizados no texto.

Capítulo 2

Riscos nas Redes de Computadores

Neste capítulo se apresentam as raízes históricas que mostram o surgimento e a evolução das redes de computadores. Ao lado do desenvolvimento científico e tecnológico experimentado as ameaças se configuram como um fato cotidiano, de modo que o uso de redes de computadores exige permanente vigilância.

2.1 O Cenário Inicial das Redes

Durante o ano de 1957 os estrategistas militares do ocidente, em particular dos Estados Unidos da América, foram surpreendidos com a notícia do lançamento de um satélite artificial, o *Sputinik 1*, pela então União Soviética. O importante feito científico foi interpretado, também, como uma ameaça real à segurança mundial, com a possibilidade da deflagração de uma guerra nuclear. A habilidade de um adversário colocar um satélite artificial em orbita da Terra, mostrava que o mesmo possuía veículos lançadores capazes de desfechar um ataque, com armas nucleares, em qualquer ponto do Planeta.

O governo dos Estados Unidos, entre outros aspectos, viu no acontecimento uma iminente ameaça à sobrevivência da rede de computadores para

comunicações militares, do sistema de defesa daquele País, vide [18]. Sendo formada pela interligação de redes centralizadas, dispersas por vasta área geográfica, existia um elevado risco da interrupção das comunicações naquela rede, como conseqüência de um possível ataque por mísseis. Na Figura 2.1 encontra-se a imagem da topologia da rede de comunicações, formada pela interligação de redes centralizadas.

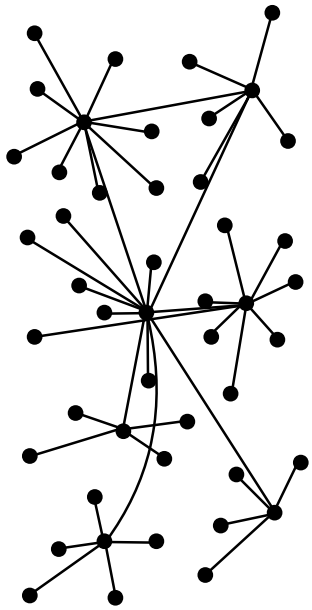

Figura 2.1: Interligação de Redes Centralizadas.

A resposta do Departamento de Defesa dos Estados Unidos foi dada ainda no mesmo ano de 1957, com a criação da *Advanced Research Projects Agency*(ARPA). A nova instituição tinha como principal objetivo contribuir para a aceleração do progresso científico e tecnológico do País. Parte do esforço foi direcionado para eliminar a vulnerabilidade existente no sistema de comunicações militares.

No ano de 1962, um engenheiro eletricista da *Rand Corporation*, de nome Paul Baran, apresentou uma idéia inovadora, baseada em uma nova concepção para a topologia das redes de computadores. Publicada em um relatório técnico da *Rand Corporation*, vide [5], surgia a idéia conhecida pela

denominação de **rede distribuída**. O modelo concebido por Paul Baran se caracterizava pelos dois aspectos seguintes: não existia uma autoridade central na rede; ocorria redundância nas ligações entre os computadores. Pode-se ver na Figura 2.2 a imagem esquemática de uma rede distribuída.

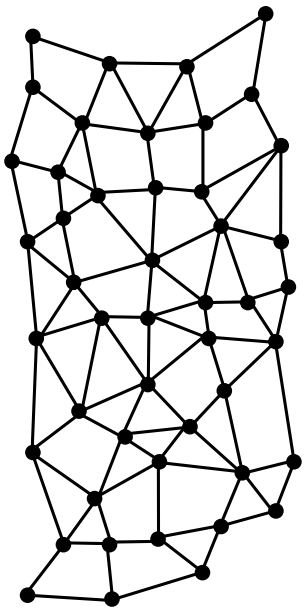

Figura 2.2: Rede Distribuída.

O fato de cada um dos computadores que formam os nós da rede se ligar a diversas rotas, por onde os dados das mensagens podem ser remetidos, garante a robustez da mesma. Na verdade, se um dos nós sofresse interrupção os outros continuariam a se comunicar através das rotas alernativas.

Uma outra importante contribuição surgiu em 1961, quando Leonard Kleinrock publicou o primeiro documento sobre a teoria da comutação de pacotes, vide [37]. Neste processo, atualmente ainda em uso, as mensagens são divididas em pedaços (pacotes) e só então enviadas de um computador para outro, até chegar ao seu destino. Quando todos os pacotes de uma mesma mensagem chegam ao destino eles são reunidos e a mensagem original é reconstruída. Um fato interessante é que, entre a origem e o destino, um pacote pode seguir por um caminho diferente daqueles usados por quaisquer outros. Essas idéias foram aproveitadas no projeto de uma rede resistente a

ataques, conforme se verá na seção a seguir.

2.1.1 *ARPANET*

Foi durante o ano de 1962 que a ARPA tomou a iniciativa de contratar pesquisadores, para a elaboração de planos destinados à construção de uma rede de computadores, capaz de permitir o intercâmbio de dados. Havia a intenção de que, por meio da rede, as pessoas pudessem trabalhar em conjunto, além de também compartilhar recursos escassos, mesmo separadas por grandes distâncias geográficas.

Escolheu-se para a construção dessa rede o modelo proposto por Paul Baran, vide [5], e que lançou a idéia de comunicação digital via comutação de pacotes, numa série de pesquisas sigilosas realizadas na *Rand Corporation*, vide [17]. A idéia era que, nem o funcionamento da rede, nem as comunicações entre processos em curso, deveriam ser interrompidos no momento da ocorrência de uma avaria. Para que isto acontecesse seria necessário que alguma conexão física entre os dois processos permanecesse em funcionamento. Esta característica é a que estabelecia a robustez da rede.

O protótipo da rede, denominada ARPANET, estava pronto em dezembro de 1969 e para realizar o primeiro experimento com a mesma foram escolhidas quatro universidades, que seriam conectadas em janeiro de 1970. As instituições eram *University of California Los Angeles*, (UCLA), *Stanford Research Institute*, *University of California Santa Barbara* e *University of Utah*. O projeto da rede original deveria atender às comunidades acadêmica e militar dos Estados Unidos.

A fim de estabelecer a interligação entre computadores era necessário que se dispusesse de uma plataforma comum, independente de fabricante. A construção desta plataforma foi uma preocupação da *Defense Advanced Research Projects Agency*, a DARPA, que resultou na criação de um famoso protocolo, como se verá a seguir.

2.1.2 *TCP/IP*

Apesar do sucesso conseguido pela rede ARPANET a versão original ainda estava sujeita a freqüentes quedas, vide [3], p. 49. Ao mesmo tempo, a expansão se tornava dispendiosa devido a adaptações para os diferentes sistemas operacionais do novos computadores participantes. Essa situação motivou o início de uma pesquisa para criar um conjunto de protocolos mais confiáveis, resultando em meados dos anos 1970, no surgimento de um conjunto de protocolos que recebeu a denominação resumida de "TCP/IP", baseada nos nomes de dois dos principais protocolos do conjunto, a saber: *Transmission Control Protocol* e *Internet Protocol*.

O TCP/IP apresentava duas vantagens principais sobre outros protocolos então existentes. Tratava-se de um protocolo que não sobrecarregava o computador, ou seja era "leve". Além disso, o custo para a sua implementação era inferior ao de outros protocolos, vide [3], p. 49.

Em 1979 foi criado um grupo denominado *Internet Configuration Control Board*, ICCB, por Vint Cerf, um pesquisador da DARPA, vide [58] e [34], para a coordenação dos esforços de pesquisa através de diversos grupos de trabalho. Ao mesmo tempo, toda a documentação dos trabalhos desses grupos, sejam propostas para novos protocolos, ou alterações nos já existentes, é registrada por meio de artigos conhecidos como *Request For Comments*, os conhecidos RFC.

No ano de 1981 a DARPA publicou as especificações do protocolo TCP/IP, vide [20], e resolveu implementar tais especificações em um computador modelo VAX, fabricado pela empresa Digtal Equipment Corporation (DEC). A popularidade do TCP/IP cresceu ainda mais quando, em 1983, foi integrado à versão 4.2 do sistema operacional UNIX, da Berkely Software Distribution (UNIX BSD), vide [3], p. 49. O TCP/IP torna-se o protocolo padrão para a ARPANET no ano de 1983 vide [42].

Naquela mesma época, a DARPA propôs que a rede original fosse separada em duas, uma para uso do pessoal civil que trabalhou no seu desenvolvimento, denominada ARPANET, e outra para uso exclusivamente militar, a MILNET, vide [40], apêndice 7, p. 76. À interconexão dessas duas redes deu-se o nome de "Internet" (cuja origem vem da palavra *internetworking*). A *National Science Foundation*, (NSF), dos Estados Unidos expande em 1985 a Internet para toda a comunidade científica americana e, de 1986 a 1992, dá-se a expansão para a comunidade científica internacional.

Apesar de as condições que propiciaram a criação da Internet terem sido de inspiração bélica, uma importante conseqüência do surgimento dessa rede foi a possibilidade da democratização do uso da Computação. O sistema operacional UNIX, juntamente com o protocolo TCP/IP permitiam um tráfego fácil de mensagens comunicando equipamentos, com as mais diversas demandas por serviços.

No entanto, a vantagem da facilidade de uso oferecida pelo sistema operacional UNIX, em conjunto com o TCP/IP, tinha como contrapartida a vulnerabilidade a ataques de usuários maldosos. A próxima seção trata dos aspectos que envolvem ataques a computadores.

2.2 Os Ataques

A simples atitude de conectar um computador a uma rede de computadores é o primeiro passo para torná-lo vulnerável a ataques. Mas o que vem a ser um "ataque a um computador"?

No sentido mais geral diz-se que, um ataque a um computador é qualquer iniciativa tomada por alguém, que visa ter acesso a recursos do computador, sem a devida autorização. Os recursos visados podem ser de naturezas as mais variadas, tais como dispositivos físicos ligados ao computador, programas, registros em arquivos, linhas de comunicação, por exemplo.

Os ataques costumam ser desferidos a partir de localidades remotas, no

âmbito do espaço virtual, apesar de o conceito de ataque apresentado no parágrafo anterior não fazer referência à proximidade entre computador e atacante. Sob este ponto de vista, a expressão "localidade remota" difere do conceito geográfico habitual. No espaço virtual, dois computadores ligados a uma mesma rede são equipamentos remotos um com respeito ao outro, mesmo que geograficamente estejam em mesas vizinhas.

Existem duas palavras que traduzem o verdadeiro significado geral da segurança, seja em que ambiente for, e em particular nas redes de computadores. As palavras são: **autenticação** e **autorização**. Os ataques remotos são favorecidos em virtude da ocorrência de falha em algum dos dispositivos da rede que cuidam, seja da autenticação, seja da autorização, de uma solicitação de serviço. Na subseção a seguir tratam-se dos aspectos que compõem um ataque a uma rede de computadores.

2.2.1 *Estratégia de um Ataque*

Antes de realizar um ataque a uma rede de computadores, o atacante experiente desenvolve um planejamento metódico, através do cumprimento de algumas tarefas iniciais, vide [3], p. 522-535. Nenhuma destas tarefas tem a intenção de perturbar o alvo, o que pode colocá-lo em estado de alerta, mas apenas de colher dados necessários à execução do ataque. As tarefas são descritas a seguir:

- Delineação da aparência da rede -
  O exame dos servidores de nomes da rede é um excelente começo, visto que exibe a relação de todos os seus usuários, alguns dos quais poderam servir como disfarce para o atacante. Coletar dados referentes ao administrador de sistemas, também é uma prática que pode ser útil ao atacante, além da identificação do sistema operacional utilizado pelo alvo.

- Identificação de pontos vulneráveis -

  A partir dos dados coletados na tarefa anterior, deve-se proceder à identificação de pontos fracos do alvo. Dependendo da acuidade com que estes dados tenham sido obtidos, será possível a identificação dos dados pessoais do administrador do sistema, os seus hábitos e contas alternativas, entre outros aspectos. Também é possível identificar qual é a topologia da rede, quem são os servidores de domínio, quais as características dos equipamentos e dos sistemas de programação básico e aplicativo, bem como possíveis relações de confiança e as prováveis vulnerabilidades, vide [3], p. 522-525.

- Execução de teste -

  Cumpridas as duas tarefas anteriores, o atacante experiente deve simular um ataque à guisa de teste. Para tanto, deve obter uma máquina que funciona como exemplpo de alvo, cuja configuração se assemelha à do alvo verdadeiro. Esta simulação permite avaliar o ataque, tanto sob o ponto de vista do atacante, quanto da vítima.

2.2.2 *Categorias de Ataques*

Na literatura especializada os ataques são divididos em duas categorias gerais, a saber: **ataques passivos** e **ataques ativos**.

A categoria dos ataques passivos reúne todos aqueles ataques que têm por objetivo capturar dados da vítima, a partir da simples observação do seu comportamento. Estes ataques são "silenciosos", no sentido de que não interferem no funcionamento normal do equipamento da vítima. Os ataques passivos se apresentam em uma das duas modalidades descritas a seguir.

A primeira modalidade de ataque passivo consiste na **espionagem dos conteúdos de mensagens** e se trata de um assédio direto aos dados que estão trafegando. Os conteúdos espionados podem ser conversações telefônicas, mensagens de correio eletrônico, ou registros de arquivos sendo

transferidos. Em geral, só há efetividade na espreita quando os dados estão em texto puro. A observação de dados criptografados somente tem sentido se o atacante tem a possibilidade de decifrá-los.

A outra modalidade de ataque passivo é a **análise de tráfego de mensagens**, que consiste na observação de alguns aspectos das mensagens chegando na vítima, ou dela se originando. Os aspectos de interesse são a quantidade de mensagens chegando ou saindo, os tamanhos de pacotes, as origens e os destinos. O dados resultantes destas observações se tornam úteis na determinação da localização e da identificação de servidores de comunicação, além de permitir que seja esboçado o padrão de comportamento dos usuários que utilizam o equipamento sendo espionado. Enfim, as informações obtidas destas observações podem ser úteis nas suposições sobre a natureza da comunicação em curso, vide [54], p. 8. Convém notar que este tipo de ataque produz resultados úteis, mesmo quando as mensagens estão criptografadas.

Diferente da anterior, a categoria dos ataques ativos reune os ataques que causam algum tipo de prejuízo à vítima. Estes ataques são divididos em quatro tipos distintos, a saber: disfarce, retransmissão, modificação de mensagens e Negação-de-Serviço.

Um ataque do tipo **disfarce** ocorre quando o atacante finge ter outra identidade diferente da sua própria. A execução deste ataque, em geral, é realizada em conjunto com algum outro tipo de ataque ativo. À guisa de exemplo, suponha-se que um atacante A foi autenticado e obteve autorização para entrar em um ambiente, com um certo grau de privilégios. Esse atacante pode capturar uma seqüência de autorização de um outro usuário B mais privilegiado do que ele, transmitir essa seqüência ao servidor de acesso e obter uma autenticação com maior privilégio, fingindo ser justamente o usário B. Observe-se que foi utilizado o ataque da retransmissão, descrito logo a seguir, para completar o disfarce.

O ataque ativo da **retransmissão** é, em geral, utilizado como complemento a algum outro com intenções bem mais ambiciosas. A sua operação

consiste em capturar, através de um ataque passivo, uma seqüência de dados e em seguida retransmiti-la para obter algum efeito não autorizado, vide [54], p. 9.

Existem diversas manifestações do tipo de ataque conhecido como **modificação de mensagens** que se podem relacionar. Se uma mensagem original, "Enviar o relatório para o usuário A", é transformada em "Enviar o relatório para o usuário B", tem-se um claro exemplo de alteração de conteúdo, visto que uma parte da mesma está alterada. Por outro lado, se a mensagem "Enviar relatório primeiro para A e depois para B" for modificada para "Enviar relatório primeiro para B e depois para A", ocorre uma modificação que se refere à reordenação de conteúdo. Enfim, se a mensagem "Disparar processo às 15:00hs" for enviada somente às 16:00hs, ocorre a modificação por atraso da mensagem. Em qualquer das situações pode ser originado um efeito não autorizado, vide [54], p. 9.

Dentre todos os tipos de ataques, passivos ou ativos, descritos anteriormente, o de **negação-de-serviço** é certamente o que tem efeito dos mais nocivos. A finalidade deste ataque é a de inibir a utilização ou o gerenciamento de recursos de comunicação sem, contudo, danificar os referidos recursos. Como se pode ver, o ataque por negação-de-serviço atinge a base da expectativa de todo usuário de computadores, que é exatamente a disponibilidade de recursos. Incluem-se neste tipo os ataques que provocam a interrupção de conexão entre dois computadores, impedindo o acesso a um serviço. Uma outra modalidade de manifestação da negação-de-serviço é por meio da "inundação" de uma rede com uma grande quantidade de mensagens inúteis, de modo que o tráfego de mensagens legítimas seja interrompido, vide [14] e [54], p. 9.

De acordo com o que foi apresentado deve-se ter em mente que, tanto ataques passivos, quanto ataques ativos, são igualmente prejudiciais. A diferença entre os dois tipos se encontra no modo de detecção e de prevenção. Enquanto os ataques passivos são difíceis de serem detectados, existem mecanismos disponíveis para prevenir o seu sucesso. Por outro lado, os

ataques ativos são fáceis de serem detectados, por meio da observação dos seus efeitos. Contudo, a prevenção contra os efeitos de ataques ativos pode se constituir em uma tarefa difícil.

A próxima seção tratará do ataque ativo da Negação-de-Serviço, mostrando algumas particularidades do mesmo, visto se tratar do ponto central de estudo neste trabalho.

2.3 O Ataque por Negação-de-Serviço

Durante o mês de novembro do ano de 1988, na *Cornell University*, um estudante de pós-graduação construiu um programa que se auto reproduzia e o enviou para outros computadores pela Internet. Em virtude da habilidade de explorar algumas falhas do sistema operacional UNIX, o programa conseguiu penetrar em outros computadores da rede, vide [49].

Este programa ficou conhecido com o "verme da Internet" e não causava nenhum dano ao computador onde se instalava. Porém, era capaz de criar cópias de si mesmo com tanta rapidez que os computadores infectados ficavam sem utilidade. Existia a impressão de que se estivessem como se "inundados" pela grande quantidade de cópias e paravam de funcionar.

Naquela época, estimava-se que a Internet fosse constituída por cerca de 60.000 (sessenta mil) computadores. O verme da Internet conseguiu parar o funcionamento de uma quantidade estimada entre 2.100 (dois mil e cem) e 2.600 (dois mil e seiscentos) computadores. Esses números representavam um intervalo entre 3,5% e 4,3% de todos os computadores da grande rede. Se aplicados na atualidade, cuja quantidade de computadores está na ordem de dezenas de milhões, pode-se ter uma idéia do que poderia representar esse risco, vide [33].

Convém lembrar que, na época do incidente, o impacto sobre a Internet foi dramático. Além dos computadores infectados, que não podiam funcionar por razões de ordem técnica, o pânico motivou a desconexão de inúmeros

outros computadores, não atingidos pelo verme. Esse fato representou a primeira iniciativa de um ataque do tipo **Negação-de-Serviço**. Em Língua Inglesa utiliza-se a expressão *Denial-of-Service* (DoS), muito usual entre os que atuam na área de segurança.

2.3.1 *Descrição dos Ataques DoS e DDoS*

Um ataque por negação de serviço é um ataque ativo no qual um, ou mais, computadores investem contra uma vítima e tentam impedir que a mesma possa realizar o seu trabalho, conforme [30]. A relação de vítimas pode ser ampla, passando por servidores de rede, clientes, roteadores, conexões de rede, um usuário isolado, uma empresa que usa a Internet para prestar serviços, entre outras. Ainda conforme [30], ataques DoS podem também incluir a obtenção de acesso não autorizado a recursos alheios. Por vezes, o ataque DoS serve como a primeira etapa de exploração de vulnerabilidades para que seja desferido um ataque de outro tipo, vide [33].

O efeito devastador de um ataque DoS pode ser conseguido de maneira simples, por meio do acionamento de um serviço muito popular da Internet. Trata-se do envio maciço de mensagens através do correio elettrônico. Devido à sua popularidade na Internet, esse serviço é uma importante via para o ataque DoS. O que caracteriza ataque DoS por meio do serviço de correio eletrônico é a chegada de uma imensa quantidade de pacotes de mensagens, em geral idênticas, num curto período de tempo. O efeito que se faz sentir é o de uma verdadeira inundação de pacotes de mensagens, de modo a impedir que o equipamento alvo receba os pacotes legítimos que lhes são destinados. Deste modo, a confiabilidade do sistema fica comprometida.

A detecção de um ataque DoS é um aspecto que não será considerado neste trabalho, cuja ênfase se concentra nos modos de conseguir neutralizá-lo. No que concerne a este ponto, convém observar que existe uma modalidade do ataque DoS que é mais difícil de ser combatida. Trata-se do *Distributed*

Denial-of-Service, ou DDoS, uma variação do ataque DoS que é desfechada simulaneamenente a partir de múltiplos computadores. Naturalmente, os endereços dos computadores atacantes podem ser facilmente falsificados e esta falsificação é conhecida na literatura especializada pela denominação de *spoofing*. O DDoS se constitui em uma modalidade de ataque com elevada dificuldade na identificação do atacante, além de ser.

2.3.2 *Contramedida*

O foco do interesse de uma contramedida estabelecida como reação a ataques de quaisquer tipos a uma rede de computadores, ou a um computador específico, se constitui na necessidade de encontrar meios para neutralizar os efeitos de ataques. Em particular, no presente trabalho o tipo de ataque para o qual se analisam contramedidas é o ataque DoS.

A estratégia destinada a neutralizar essa modalidade de ataque é em princípio muito simples. Em primeiro lugar devem ser identificados os locais de onde se originam os pacotes nocivos. Em seguida, deve ser bloqueado o recebimento de qualquer pacote que proceda daqueles locais.

Esta identificação aparentemente é uma tarefa de fácil execução, uma vez que no cabeçalho do protocolo TCP/IP existe um campo cujo conteúdo é o endereço do equipamento de origem da mensagem, isto é, o campo **SOURCE IP ADDRESS**, conforme mostrado no datagrama da Figura 3.1. Em vista desse fato, seria suficiente examinar este campo e o problema estaria resolvido. Contudo, nunca é demais lembrar que o atacante costuma ser movido pela malícia de modo que, antes de despachar os pacotes que inundarão a máquina da vítima, ele poderá alterar os endereços de origem no cabeçalho TCP/IP de cada um. Esta atitude de disfarce tornará sem valor o resultado da inspeção daquele campo do cabeçalho do datagrama, para fins de determinação da origem de um ataque DoS. Sendo assim, o que se deve fazer é procurar outros modos para a identificação da origem dos pacotes atacantes. Uma estratégia que pode ser utilizada para esta

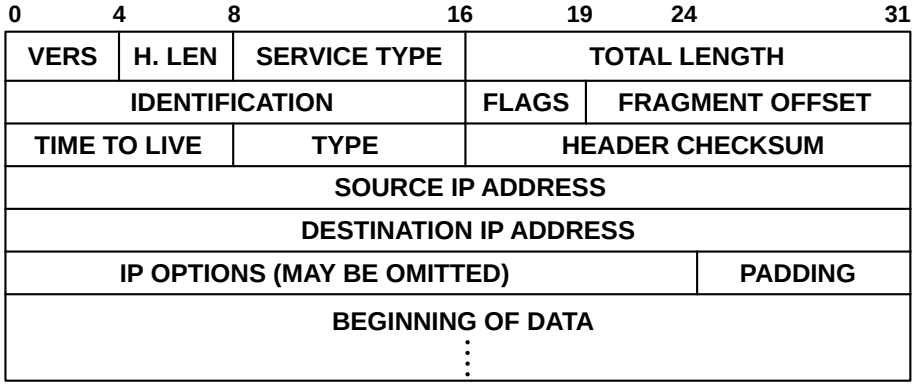

Figura 2.3: Formato do Cabeçalho do Datagrama do IP.

finalidade é a que procura a identificação da origem de um ataque por meio da recomposição da trajetória que os pacotes atacantes percorreram, fazendo o caminho inverso, desde a vítima até chegarem ao ponto de origem do ataque. Esta estratégia se baseia em uma técnica denominada **técnica do rastreamento reverso**.

A fim de que se possa realizar o referido rastreamento reverso é necessário que se obtenham informações acerca da trajetória, a partir das quais se possa inferir algum conhecimento produtivo sobre a natureza da mesma. Essas informações precisarão ser obtidas com a análise de dados observados nos pacotes que trafegaram pela trajetória de ataque e chegaram até à vítima.

2.3.3 *Rastreamento Reverso*

Sabe-se que o movimento de um pacote de mensagens ao longo da rede se assemelha a uma sucessão de "saltos´´ ("hops´´) de roteador para outro, desde o ponto onde o mesmo se originou, até o seu destino. Em cada roteador onde o pacote chega, o mesmo é submetido a um procedimento rotineiro existente no protocolo TCP/IP, e que pode ser resumido nas seguintes etapas, conforme [41]:

- Inspeção do cabeçalho do pacote para obter o campo **DESTINATION IP ADDRESS**.
- Consulta à tabela de endereços de roteadores, usando como argumento o campo **DESTINATION IP ADDRESS**.
- Envio do pacote ao próximo roteador, desde que haja sucesso na pesquisa à tabela.

Este procedimento é repetido no próximo roteador e assim por diante, até que o pacote chegue ao seu destino final.

A fim de criar um formalismo no trato dessa situação, será identificado como sendo R_k o roteador de uma trajetória de ataque que se encontra k-saltos distante da vítima. Por sua vez, a vítima será identificada como sendo R_0. Assim, pode-se representar uma trajetória de ataque que contém n roteadores como sendo uma cadeia de composta dos símbolos que identificam os roteadores, que se descreve como $C = (R_0R_1...R_n)$. O procedimento do rastreamento reverso tem como objetivo construir esta cadeia, a partir da qual será possível identificar o atacante e em conseqüência neutralizar o ataque.

Observando-se o cabeçalho do datagrama do IP, na Figura 3.1, pode-se verificar que um pacote trafegando pela Internet não mantém qualquer registro dos roteadores intermediários por onde passou. Na referida Figura 3.1, existem os campos **SOURCE IP ADDRESS** e **DESTINATION IP ADDRESS** que dizem respeito apenas aos endereços de origem e de destino do pacote, vide [16], p. 209-217. Logo, a simples inspeção dos pacotes atacantes, tal qual se apresentam, não é suficiente para para construir a cadeia de símbolos C, visto que não possuem dados dos quais se possam extrair informação para a construção da trajetória seguida pelo pacote.

A inexistência de mecanismos no protocolo TCP/IP para a identificação da trajetória percorrida por um pacote, torna necessária a procura por alternativas de onde se possam extrair subsídios para a construção da cadeia

de símbolos C. O próximo capítulo apresenta algumas idéias sobre métodos determinísticos que se propõem a fornecer tais subsídios, através dos quais se possa realizar o rastreamento reverso de número de IP para poder reagir a ataques por Negação-de-Serviço.

2.4 Contribuição do Capítulo

Ao longo do processo de construção do conhecimento sobre a segurança de sistemas, as propostas para solução têm surgido por meio de observação e experimentação. Tais soluções, em sua grande maioria, tratam de aspectos relacionados quase que unicamente com abordagens baseadas em algoritmos. O ataque por negação de serviço, DoS, bem como a sua variante DDoS, cuja facilidade e simplicidade de sua execução se alia aos efeitos devastadores que pode provocar, suscitou um problema referente à busca de contramedidas para o mesmo, que tem sido igualmente estudado sob esse ponto de vista.

A contribuição do presente capítulo se concentra, principalmente, no aspecto do posicionamento histórico em que se situa o referido problema. Abrange aspectos dos eventos ocorridos em um período no qual a Ciência da Computação experimentou um significativo avanço. E tudo o que foi exposto permite formar um quadro de desafios presentes e futuros, no que concerne ao uso de redes de computadores, seja para os leigos, seja para os especialistas na área de segurança.

Capítulo 3

Determinismo Computacional

O incidente provocado por Robert Morris, no final do ano de 1988, que veio a ser conhecido como o *Morris Worm*, vide [3], p. 749-753, foi caracterizado de modo detalhado no *Request For Comment* (RFC), cuja publicação é de dezembro de 1989, referida em [49]. Desde então, o ataque ficou conhecido como sendo do tipo DoS e muito se tem escrito sobre contramedidas destinadas a neutralizá-lo. As propostas para contramedidas que têm surgido tomam por base a idéia do rastreamento reverso do número IP, ou seja, a de procurar descobrir o número IP do atacante por meio de informações extraídas dos pacotes atacantes.

Os modos de como se pode extrair informações dos pacotes fazem a diferença entre a natureza de cada uma das propostas para contramedidas. Uma idéia primitiva para obter informações sobre o número IP do atacante estabelecia que todo pacote que chegasse a um roteador deveria ser "carimbado" com o número IP deste roteador. Trata-se de uma idéia que leva em conta somente o lado computacional do problema. Neste capítulo será estudada esta forma de contramedida, tanto pelo seu valor histórico, quanto para a avaliação da sua efetividade. Pode-se ver em [22] uma interessante referência a esta proposta de contramedida.

Já em [51] a proposta relaciona uma abordagem computacional com um modelo matemático de caráter probabilístico. Por sua vez, em [21] se pode

ver uma proposta para a identificação do número IP de um atacante, que se baseia em um modelo matemático determinístico, representado como um sistema de equações lineares. A proposta em [44] também apresenta um modelo matemático, porém de caráter probabilístico.

Além da proposta citada anteriormente, que se baseia em "carimbar" pacotes, neste capítulo também será apresentada uma outra abordagem, essencialmente de natureza computacional. Devido ao fato de lançar mão de uma atitude mais drástica, cujo resultado pode interferir de modo nocivo no funcionamento da rede, a sua utilização não é recomendável. No entanto, será descrita porque faz parte da história das contramedidas ao ataque DoS.

3.1 Marcação Determinística de Pacotes

Nesta seção apresenta-se um procedimento que pode ser agregado ao protocolo TCP/IP e cuja função é a coletar indícios que permitam identificar por quais roteadores um determinado pacote trafegou. Esse procedimento é de natureza puramente determinística e o resultado da sua utilização dá a certeza de que é possível realizar o rastreamento reverso do número IP, a partir dos indícios coletados. Em conseqüência, se poderá determinar a origem de um ataque do tipo DoS. Resta estabelecer o *modus operandi* ao qual se deve submeter cada pacote que chega a um roteador da trajetória de ataque, que é justamente o assunto tratado a seguir.

A fim de se determinar a trajetória de ataque no espaço virtual, tendo unicamente os roteadores como os elementos de referência neste espaço, será definido o seguinte procedimento ao qual deve ser submetido cada pacote que chega a um roteador:

- Inserção de um campo do tamanho de trinta e dois bits no pacote em trânsito.

- Gravação do endereço IP do roteador no novo campo referido no ítem anterior.

Este procedimento recebe a denominação de **marcação determinística de pacotes**.

Observe-se que a ordem em que os citados campos de trinta e dois bits são inseridos em um pacote é a mesma em que o pacote visita os roteadores. Deste modo, o rastreamento reverso poderia ser realizado por meio de uma simples inspeção dos campos que foram inseridos em um pacote. Basta considerar estes campos na ordem inversa em que foram agregados ao pacote, ou seja, do final para o começo.

O procedimento do rastreamento reverso torna-se uma operação simples e rápida. Contudo, a inserção de campos referentes ao procedimento de marcação aumenta o tamanho da carga total do pacote, de modo que o seu comprimento pode crescer de modo exagerado. Levando-se em conta que esse procedimento deva ser realizado com todos os pacotes trafegando pela rede, sob o ponto de vista da rede coo um todo pode-se chegar a uma situação caótica. A rede pode ter o seu funcionamento seriamente comprometido, ou até mesmo parar. Contudo, todas estas são conjecturas de natureza puramente qualitativa. A sua validade precisa ser comprovada através de métodos que levem em conta os aspectos quantitativos envolvidos no procedimento considerado.

De acordo com a Figura 3.1, pode-se ver que o cabeçalho do datagrama contém um campo denominado **TOTAL LENGTH**. Este campo tem o comprimento de dezesseis bits e a sua função é armazenar um valor numérico representando o tamanho total do pacote, em octetos. Isto significa que nenhum pacote pode ter o seu tamanho excedendo a 65.536 octetos, o que equivale a 16.384 palavras de trinta e dois bits. Lembrando que o cabeçalho ocupa cinco palavras, poderão ser utilizadas, no máximo, 16.379 palavras para o transporte de carga útil.

Durante o funcionamento do processo de marcação determinística de pa-

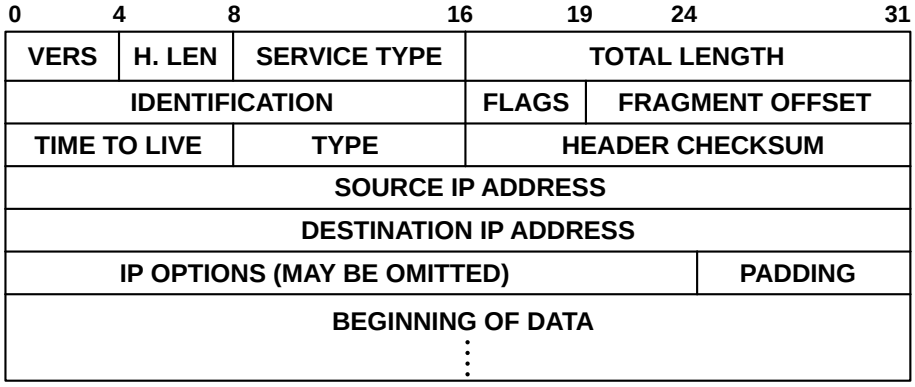

Figura 3.1: Formato do Cabeçalho do Datagrama do IP.

cotes, conforme foi visto, o pacote recebe a inserção de um novo campo cujo comprimento é de uma palavra, em cada roteador por onde passa. Este novo campo inserido recebe o número IP do roteador visitado. Naturalmente, esta prática contribui para que o espaço no pacote destinado à carga útil seja reduzido.

Considere-se um pacote qualquer que precisa de B palavras de trinta e dois bits para acomodar a carga útil que transporta. Lembrando que o cabeçalho de um pacote no protocolo TCP/IP possui o tamanho fixo de cinco palavras, o comprimento deste pacote, em palavras, será dado pela expressão $(5 + B)$. Desde que o comprimento de um pacote qualquer não pode ultrapassar o valor 16.384 palavras, pode-se ver que este é o valor máximo para a expressão anterior. Além disso, a mesma expressão permite concluir que o comprimento mínimo de um pacote é igual a 5 palavras. Este comentário pode ser resumido como segue:

- Se um pacote não transporta carga útil o valor de B é igual a zero palavras. Neste caso, o pacote contém apenas o cabeçalho TCP/IP e o seu comprimento total é iguala a 5 palavras.

- Se um pacote transporta a maior quantidade de carga útil possível, além do cabeçalho TCP/IP, então B assume o seu valor máximo, isto é, 16.379 palavras. Neste caso, o seu comprimento total é o máximo

possível e igual a 16.384 palavras.

As duas situação acima são inspiradoras para a definição de uma medida de eficiência para pacotes trafegando pela rede. Basta fazer a comparação do espaço ocupado pela carga útil, com o espaço total do pacote. Se o valor de B for pequeno em comparação com o comprimento do pacote, que é $5 + B$, isto se traduz como uma baixa eficiência no transporte de carga útil. Neste caso, o espaço ocupado pelos dados de controle, que compõem o cabeçalho do datagrama, representará uma parte significativa do comprimento total do pacote. Por outro lado, se o valor de B for grande em comparação com $5 + B$, a eficiência será igualmente elevada. Nesta outra situação, o espaço ocupado pelo cabeçalho do datagrama pouco significa com respeito ao comprimento total do pacote. Assim, quanto maior for o valor de B, melhor será o aproveitamento do pacote, no que concerne à sua eficiência para transportar a carga útil das mensagens.

Esta comparação entre a quantidade de palavras necessárias para conduzir a carga útil, B, com o tamanho total do pacote, $5 + B$, permite definir uma razão, denominada $\mathcal{E}$, para a medir a eficiência com que o pacote transporta a carga útil. Trata-se da seguinte expressão:

$$\mathcal{E} = \frac{B}{(5 + B)}. \tag{3.1}$$

Como se pode ver de (3.1), a eficiência de um pacote em transportar carga depende apenas do valor de B, pois o tamanho do cabeçalho é constante.

O procedimento de inserção de números IP de roteadores intermediários em um pacote que trafega por uma trajetória de ataque resultará no preenchimento de parte do espaço disponível para carga útil. Deste modo, a expressão (3.1) precisará ser modificada de modo a que possa representar, também, este efeito da inserção das palavras de 32-bits contendo números IP, ao longo da sua trajetória.

O acompanhamento de um pacote que se move ao longo de uma trajetória pode ser registrado pela seqüência dos números IP dos roteadores que

compõem esta trajetória. Deste modo, o movimento do pacote se assemelha a uma sucessão de "saltos", de um roteador para outro. Em vista desta interpretação, costuma-se medir em "saltos" a distância entre um roteador atacante e a vítima do ataque. Se um pacote tem origem em um roteador atacante, que se encontra a uma distância de n saltos da vítima, então a cada salto deverá ser inserida uma palavra de 32 bits ao espaço do pacote disponível para carga útil. Quando o pacote chega à vítima, a sua carga total foi acrescida de n palavras de 32 bits.

Nesta nova situação a carga que um pacote será constituída pelos seguintes elementos: cabeçalho com 5 palavras; carga útil com B palavras; área de marcação com n palavras. Assim, a carga total do pacote que chega à vítima será igual a $(5 + B + n)$ palavras de 32 bits e a expressão da eficiência do pacote será agora dada por

$$\mathcal{E}' = \frac{B}{(5 + B + n)}. \tag{3.2}$$

Comparando a expressão (3.1) com a (3.2), de imediato se conclui que $\mathcal{E}' \leq \mathcal{E}$, ocorrendo a igualdade apenas quando n é igual a zero, isto é, na ausência do processo de marcação. Essa desigualdade permite formular uma expressão (3.3) que compara as duas situações, como a seguir:

$$\frac{\mathcal{E}'}{\mathcal{E}} = \frac{1}{1 + \frac{n}{5+B}} \leq 1. \tag{3.3}$$

A fim de investigar a relação entre as duas medidas de eficiência deve-se estudar o comportamento das duas variáveis inteiras, n e B. A extensão do domínio dessas variáveis do conjunto dos números inteiros positivos para o conjunto dos números reais, permite que se possa ter uma visão mais ampla do seu comportamento, em um ambiente com maior variedade de recursos. Essa extensão de domínio é o conteúdo do assunto a ser abordado na subseção a seguir.

3.1.1 *Modelo Matemático Analítico*

Um rápido vislumbre sobre a expressão (3.3) é suficiente para motivar a definição de uma função, destinada a avaliar o impacto que este processo de marcação de pacotes pode causar no funcionamento de uma rede. Trata-se da função

$$\omega : \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R},$$

doravante denominada *função $\omega(x, y)$ da razão de eficiência.* As variáveis n e B da expressão (3.3), que significam as quantidades de números IP inseridos e de palavras usadas para carga útil, respectivamente, serão denominadas na função como x e y. Assim, a expressão da função para a razão de eficiência será a seguinte:

$$\omega(x, y) = \frac{1}{1 + \frac{x}{5+y}}. \tag{3.4}$$

As variáveis inteiras não negativas n e B, da expressão (3.2), foram substituídas pelas suas extensões contínuas, as variáveis reais x e y, respectivamente. A fim de se ter uma idéia geral do comportamento dessa função, definida em (3.4), convém observar o gráfico da mesma na Figura 3.2.

Pode-se ver no gráfico da Figura 3.2 o comportamento de cada uma das

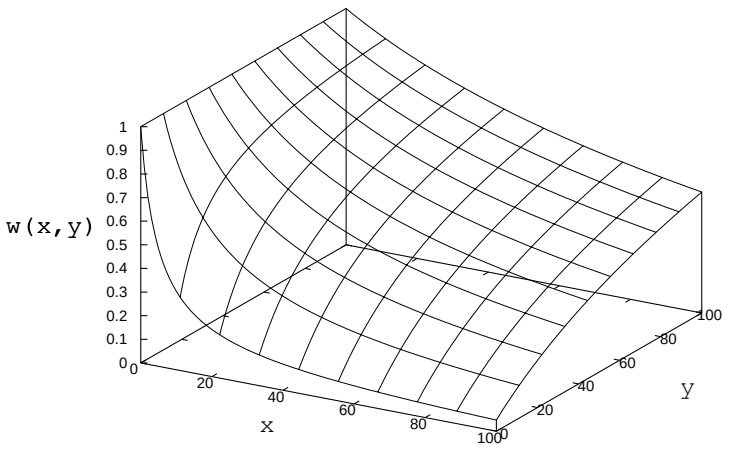

Figura 3.2: Função $\omega(x, y)$ da Razão de Eficiência

variáveis independentes, x e y, considerando cada uma no intervalo fechado $[0, 100]$. Com efeito, à proporção que a variável x cresce, diminui o valor da função $\omega(x, y)$. Por outro lado, o crescimento da função se dá no mesmo sentido que o da variável y.

Tais efeitos são esperados no fenômeno em estudo, pois a variável x representa o comprimento da trajetória, cujo crescimento aumenta a carga de controle do pacote, devido à inserção de novos campos com endereços dos roteadores. Desse modo, quando se aumenta a trajetória, a razão entre as eficiências no transporte de mensagens pelo pacote se reduz cada vez mais. A visão oferecida pela variável y já é outra pois, pressupondo um comprimento constante para a trajetória, mostra que a razão entre as eficiências cresce com o aumento da carga útil.

Estas observações podem ser mais bem analisadas se cada uma das variáveis for observada de modo individual, por meio da definição de duas novas funções auxiliares, decorrentes daquela definida na expressão (3.4). As próximas subseções apresentam tais visões individualizadas do comportamento da função da razão de eficiência,

3.1.2 *Variando o Comprimento da Trajetória*

Considerando a quantidade de palavras usadas para carga útil B, representada por y na expressão (3.4), como sendo igual à constante y_μ, pode-se definr uma nova função, $\omega_{y_\mu} : \mathbb{R}^+ \to \mathbb{R}$, apenas de uma variável real independente x, que representa a extensão contínua da quantidade de números IP inseridos num pacote, conforme a expressão abaixo:

$$\omega_{y_\mu}(x) = \frac{1}{1 + \frac{x}{5+y_\mu}}. \tag{3.5}$$

Esta nova função, denominada *função $\omega_{y_\mu}(x)$ da razão de eficiência*, permite estudar o fenômeno da marcação de pacotes considerando uma carga útil de tamanho constante. Tomando-se um valor constante, y_μ, para y pode-se

estudar o fenômeno da marcação de pacotes considerando uma carga útil de tamanho constante. O gráfico da nova função ω_{y_μ}, que depende do parâmetro y_μ, é mostrado na Figura 3.3, na qual se tomaram os valores 0, 1, 5, 50 e 100 para este parâmetro, a título de exemplo.

Observe-se que no gráfico da Figura 3.3 a curva na parte mais inferior é

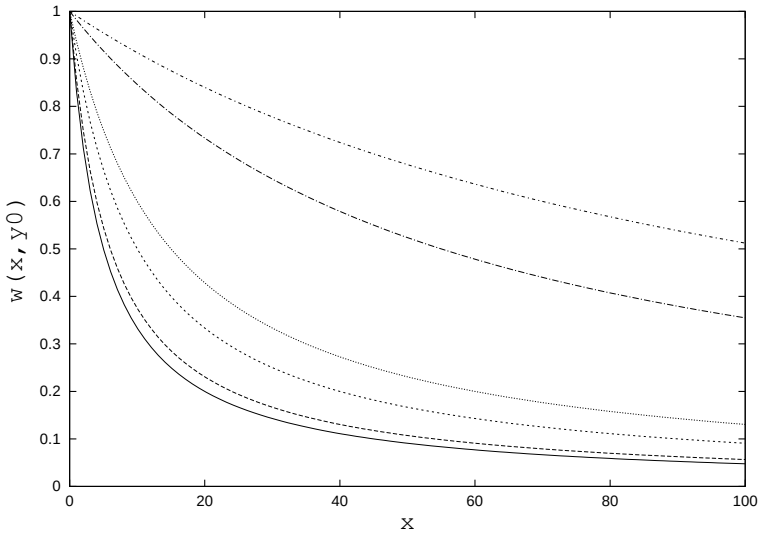

Figura 3.3: Função $\omega_{y_\mu}(x)$ da Razão de Eficiência

aquela cujo parâmetro y_μ recebe o valor zero. À proporção que o valor do parâmetro aumenta, a curva correspondente no gráfico se localiza mais distante do eixo horizontal.

O conjunto de curvas mostrado na Figura 3.3, que são gráficos da função $\omega_{y_\mu}(x)$, para diferentes valores do parâmetro y_μ será denominado Ω_y. Pode-se verificar no referido gráfico que, quanto maior for o valor atribuído ao parâmetro y_μ, mais suave será a forma como a curva referente a este parâmetro decresce, se comparada às que correspondem a valores menores do parâmetro. Não obstante o fato de que o parâmetro y_μ pertence ao conjunto $\mathbb{R}^+$, a curva que está na posição mais inferior representa o caso em que y_μ é tomado igual a zero. Esta é uma situação singular que, na prática, significa a ausência total de carga útil no pacote, mas é considerada aqui para efeito de referência como limite inferior. A função $\omega_0(x)$, cujo gráfico é

o limite inferior do conjunto Ω_y, corresponde àquela associada ao valor zero para y_μ e será denotada $l(x)$.

Por outro lado, a curva que corresponde ao limite superior do conjunto Ω_y aparentemente não é determinada, pois depende da capacidade de carga do pacote. Uma observação mais acurada na expressão (3.5), contudo, permite determinar o limite superior do conjunto Ω_y. Levando em conta que o menor valor que a variável x pode assumir é justamente igual a um, do ponto de vista prático é trivial concluir que a fração no denominador satisfaça à relação

$$\frac{x}{5 + y_\mu} > 0. \tag{3.6}$$

Logo, a função $\omega_{y_\mu}(x)$ será sempre inferior ao valor um e a curva limite superior é justamente a do gráfico da função $u(x) = 1$. Essa conclusão de natureza intuitiva pode ser estabelecida de modo rigoroso nos termos da seguinte

Proposição 3.1. *Seja Ω_y o conjunto de todas as funções $\omega_{y_\mu} : \mathbb{R}^+ \to \mathbb{R}$, tal que ω_{y_μ} é como na expressão (3.5), e $y_\mu \in \mathbb{R}^+$ é um parâmetro dado. Então, a função constante $u(x) = 1$ é o elemento maximal em Ω_y.*

Demonstração. Considere-se "$\leq$" como uma relação entre entre elementos do conjunto Ω_y tal que, para $\omega_{y_\mu}, \omega_{y_\nu} \in \Omega_y$, então $\omega_{y_\mu} \leq \omega_{y_\nu}$ desde que $y_\mu \leq y_\nu$. Levando em conta a ordem total no conjunto dos números naturais, $\mathbb{N}$, é trivial ver que, toda seqüência $\{\omega_{y_\mu} \mid y_\mu \in \mathfrak{I}\}$, sendo $\mathfrak{I} \subseteq \mathbb{N}$ um conjunto de índices, é uma cadeia. Além disso, pode-se facilmente ver que cada cadeia $\{\omega_{y_\mu} \mid y_\mu \in \mathfrak{I}\}$ é limitada superiormente pela função $u(x) = 1$. então, pelo Lema de Zorn segue que Ω_y tem um elemento maximal, ver [6], p. 142-145. Além disso, suponha-se que $\omega_{y_\varpi}(x) < u(x)$ é um elemento maximal. Desde que $0 < (1/y_\varpi) < 1$ considere-se $\zeta = (1/y_\varpi)/2$. Então, $0 < \zeta < (1/y_\varpi)$ e portanto $y_\varpi < (1/\zeta)$. Considerando $\lceil (1/\zeta) \rceil = y_\mu \in \mathfrak{I}$, tem-se $\omega_{y_\varpi}(x) \leq \omega_{y_\mu}(x)$, ou seja, existe uma outra função, $\omega_{y_\mu}(x)$, que também é elemento maximal em Ω_y. Logo, a função $u(x) = 1$ é o elemento maximal. □

O estudo do comportamento das funções $\omega_{y_\mu}(x)$ envolve ainda outros aspectos que, apesar de triviais, são significativos no que concerne ao entedimento das referidas funções. A proposição 3.2 a seguir resume tais aspectos.

Proposição 3.2. *A função da razão de eficiência $\omega_{y_\mu}(x)$ é monótona estritamente decrescente e se aproxima de zero quando a variável x cresce.*

Demonstração. Dado um valor y_μ do parâmetro y, considerem-se os valores da variável x, denominados x_1 e x_2, ambos maiores do que zero, tais que $x_1 < x_2$. Então, obviamente tem-se

$$\omega_{y_\mu}(x_1) = \frac{1}{1 + \frac{x_1}{5+y_\mu}} > \frac{1}{1 + \frac{x_2}{5+y_\mu}} = \omega_{y_\mu}(x_2), \tag{3.7}$$

donde $\omega_{y_\mu}(x)$ é monótona estritamente decrescente. Por outro lado, para cada valor de y_μ é também trivial ver que

$$\lim_{x\to\infty} \omega_{y_\mu}(x) = \lim_{x\to\infty} \left(\frac{1}{1 + \frac{x}{5+y_\mu}} \right) = 0. \tag{3.8}$$

Logo, fica demonstrada a proposição. □

O ato de observar a Figura 3.3 revela ainda uma peculiaridade na sua característica de ser monótona decrescente. Trata-se da velocidade com que cada curva se aproxima do eixo horizontal à proporção que a variável x cresce, definida pela expressão (3.9), da primeira derivada da função $\omega_{y_\mu}(x)$.

$$\frac{d\omega_{y_\mu}(x)}{dx} = -\frac{\frac{1}{5+y_\mu}}{(1 + \frac{x}{5+y_\mu})^2}. \tag{3.9}$$

Conforme os gráficos da Figura 3.3, pode-se constatar que as curvas correspondentes a valores mais elevados do parãmetro y_μ aproximam-se do eixo horizontal de modo mais lento do que aquelas referentes a valores menores do parâmetro. A expressão (3.9) indica de modo explícito essa dependência da derivada da função com respeito ao valor do parâmetro. Os gráficos na Figura 3.4, por seu turno, mostram as curvas correspondentes às funções derivadas das $\omega_{y_\mu}(x)$.

Quando o valor da variável x se encontra próximo de zero, pode-se notar que a curva cujo parâmetro é igual a zero, chamado aqui de y_0, fica abaixo de todas as outras. Contudo, à proporção que a variável x cresce, é possível verificar que ocorre a interseção entre a curva do parâmetro y_0 com as outras posteriores. O fato de todas as curvas da Figura 3.3 serem estritamente monótonas garante que as suas correspondentes na Figura 3.4 também o serão. Assim, essa propriedade estabelece que duas curvas distintas somente poderão se interceptar apenas uma vez, em um único ponto.

Esse comportamento converge com a idéia de que, o efeito nocivo provo-

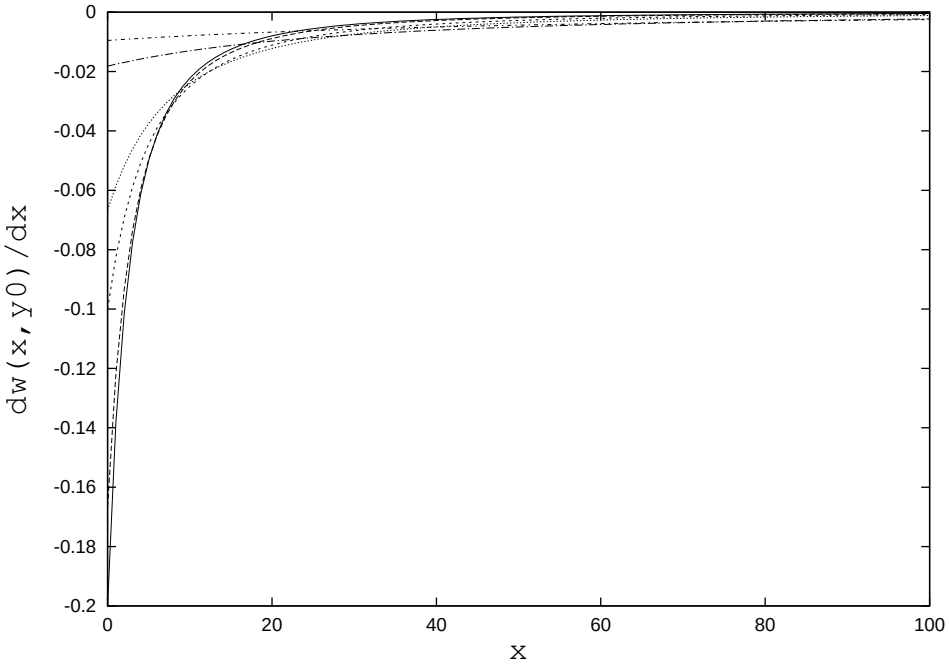

Figura 3.4: Derivada da Função $\omega_{y_\mu}(x)$ da Razão de Eficiência

cado sobre a razão de eficiência, por meio do crescimento da trajetória, pode ser retardado conforme seja ampliada a magnitude da carga útil no pacote. A fim de imprimir um tom mais formal com respeito ao comportamento da derivada da função $\omega_{y_\mu}(x)$, convém enunciar e demonstrar a proposição a seguir:

Proposição 3.3. *A primeira derivada de* $\omega_{y_\mu}(x)$ *é tal que*

$$\frac{d\omega_{y_\mu}}{dx} \in O(1/x^2).$$

Demonstração. Considere-se $\tau = (1/(5+y_\mu))$, o termo paramétrico que existe na expressão (3.9) e, desde que $y_\mu \in \mathbb{N}$, é óbvio concluir que $\tau \in]0,1[$. Então, a expressão (3.9) pode ser escrita como

$$\frac{d\omega_{y_\mu}(x)}{dx} = -\frac{\tau}{(1+\tau x)^2}. \tag{3.10}$$

Uma vez que as relações abaixo são válidas,

$$\left| -\frac{\tau}{(1+\tau x)^2} \right| < \left| -\frac{1}{(1+\tau x)^2} \right| < \left| -\frac{1}{(\tau x)^2} \right| = \left| \frac{1}{(\tau)^2} \right| \left| \frac{1}{(x)^2} \right|,$$

tem-se que a poposição está provada, isto é, conclui-se que $d\omega_{y_\mu}(x)/dx$ é assintoticamente limitada pela função $(1/x^2)$. □

Enfim, os resultados do estudo do comportamento das *Funções* $\omega_{y_\mu}(x)$ *da Razão de Eficiência* não apresentam nenhuma surpresa. Está claro que, o aumento da carga destinada ao controle do tráfego do pacote somente contribui para reduzir a eficiência do transporte de mensagens de interesse dos usuários da rede.

Complementando o estudo do comportamento da função que mede a razão de eficiência, esta subseção termina com alguns comentários sobre a natureza algébrica que existe no conjunto Ω_y.

3.1.3 *Uma Rápida Visão Algébrica - I*

Considerando os elementos $\omega_{y_\mu}(x)$, do conjunto Ω_y, pode-se definir um operação de adição entre os mesmos, baseada na adição existente no conjunto $\mathbb{R}$ dos números reais.

Definição 3.1. *Considerando o conjunto Ω_y das funções $\omega_{y_\mu}(x)$, a operação de adição $\oplus : \Omega_y \times \Omega_y \to \Omega_y$ é tal que $\omega_{y_\mu}(x) \oplus \omega_{y_\lambda}(x) = \omega_{y_\mu + y_\lambda}(x)$.*

Desde que a operação $\oplus$ foi definida a partir da operação de adição sobre os números reais, ambiente de onde provêm os elementos y_μ, é natural esperar que a mesma deva herdar algumas das propriedades dessa adição real. Com efeito, a proposição a seguir traduz essa expectativa.

Proposição 3.4. *A operação $\oplus : \Omega_y \times \Omega_y \to \Omega_y$ é associativa e possui elemento neutro.*

Demonstração. Desde que

$$(\omega_{y_\mu} \oplus \omega_{y_\nu}) \oplus \omega_{y_\lambda} = \omega_{y_\mu + y_\nu} \oplus \omega_{y_\lambda} = \omega_{(y_\mu + y_\nu) + y_\lambda}$$

$$= \omega_{y_\mu + (y_\nu + y_\lambda)} = \omega_{y_\mu} \oplus \omega_{y_\lambda + y_\nu} = \omega_{y_\mu} \oplus (\omega_{y_\nu} \oplus \omega_{y_\lambda}).$$

Logo, a operação $\oplus$ é associativa. Considerando $y_\nu = 0$, então tem-se que

$$\omega_{y_\mu} \oplus \omega_{y_\nu} = \omega_{y_\mu} \oplus \omega_0 = \omega_{y_\mu + 0} = \omega_{0 + y_\mu} = \omega_{y_\mu}$$

e, portanto, existe um elemento neutro para a operação $\oplus$, que é ω_0. □

A partir do que estabelece a Definição 3.1 e do resultado da Proposição 3.4, conclui-se que o par $(\Omega_y, \oplus)$ é um *monóide*, visto que atende aos requisitos que caracterizam essa estrutura algébrica, vide Apêndice C. Supondo que $\omega_{y_\mu}, \omega_{y_\lambda}, \omega_y \in \Omega_y$, considere-se a equação

$$\omega_y \oplus \omega_{y_\mu} = \omega_{y_\lambda}, \tag{3.11}$$

cuja incógnita é ω_y e os valores conhecidos são ω_{y_μ} e ω_{y_λ}. Desde que em um monóide não existe a garantia da existência de inverso para cada um dos elementos de Ω_y, segundo a operação $\oplus$, essa equação nem sempre apresenta solução em Ω_y.

A equação 3.11 pode ser utilizada na representação de dois problemas identificáveis em $(\Omega_y, \oplus)$. O primeiro pode ser apresentado na seguinte forma:

Enunciado 3.1. *Dado um certo tamanho x_k estabelecido para a trajetória, qual valor y deve ser acrescido à carga útil do pacote, de modo que a função ω_{y_μ} de razão de eficiência possa ser elevada para ω_{y_λ}?*

Naturalmente, o problema no Enunciado 3.1 pode ser modelado segundo a equação 3.11, para a qual existirá solução em $(\Omega_y, \oplus)$ desde que seja verdadeira a relação $y_\mu < y_\lambda$.

O outro problema que pode ser inferido se traduz por meio do seguinte

Enunciado 3.2. *Considerando que a rede opera de acordo com uma dada razão de eficiência ω_{y_μ}, qual deverá ser o valor y que, uma vez acrescido ao comprimento da carga útil do pacote, permitirá incrementar a magnitude da trajetória do valor x_r para o x_s, mantendo essa mesma razão de eficiência?*

De modo análogo ao comentário anterior, o enunciado 3.2 também se refere à resolução da equação que se obtém a partir da expressão (3.11).

3.1.4 *Variando a Magnitude da Carga Útil*

Nesta subseção o estudo da razão de eficiência $\omega(x, y)$, será procedido de acordo com um outro ponto de vista. Com efeito, agora a variável independente corresponderá à magnitude da carga útil transportada pelo pacote, y, enquanto a fixação do comprimento da trajetória, que é a variável x, será representado como o parâmetro x_ν.

Desse modo, a expressão para a função $\omega_{x_\nu}(y)$ da razão de eficiência terá a forma mostrada a seguir:

$$\omega_{x_\nu}(y) = \frac{1}{1 + \frac{x_\nu}{5+y}}. \tag{3.12}$$

De modo análogo ao que foi apresentado na subseção 3.1.2, o conjunto de todas as funções $\omega_{x_\nu} : \mathbb{R}^+ \to \mathbb{R}$, tal que ω_{x_ν} é definida como na expressão (3.12), e $x_\nu \in \mathbb{R}^+$, é chamado Ω_x.

Esta nova situação permite que se estude o comportamento da razão de eficiência a partir da visão de uma trajetória cujo comprimento é fixo. Em primeiro lugar, é importante observar os gráficos da função $\omega_{x_\nu}(y)$ de razão de eficiência , para alguns valores de x_ν, conforme se pode ver na Figura 3.5.

Sob o ponto de vista teórico pode-se considerar a situação em que $x_\nu = 0$.

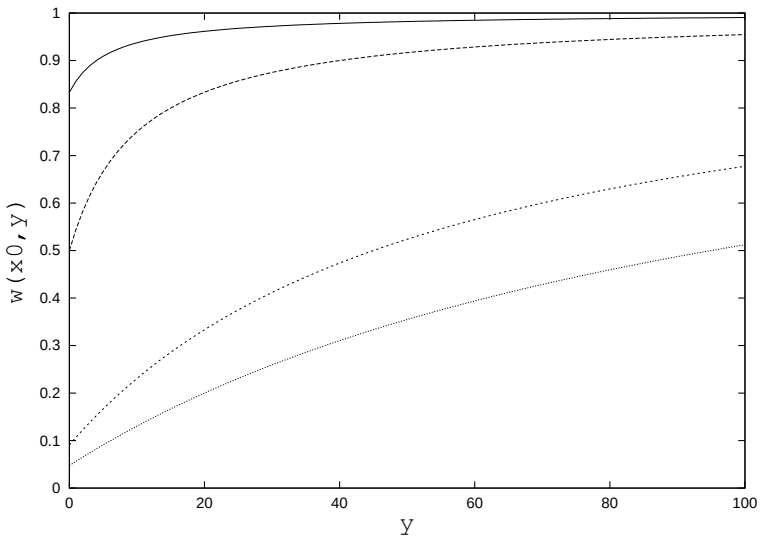

Figura 3.5: Função $\omega_{x_\nu}(y)$ da Razão de Eficiência

Naturalmente, na prática essa consideração corresponde ao fato de que a trajetória possui comprimento igual a zero, isto é, não há tráfego e, portanto, não há também problemas com a eficiência desse tráfego. Neste caso, o gráfico da função $\omega_{x_\nu}(y)$ é a linha horizontal cujos pontos têm, todos, a segunda coordenada igual a um.

Ainda no gráfico da Figura 3.5, pode-se ver que o crescimento do valor do parâmetro x_ν provoca a redução do valor da função $\omega_{x_\nu}(y)$ da razão de eficiência, para uma dada carga útil do pacote. Este crescimento do valor de x_ν desloca o ponto que é a interseção da linha do gráfico com o eixo vertical cada vez mais para valores próximos de zero. A despeito disso, uma função $\omega_{x_\nu}(y)$, para qualquer parâmetro $x_\nu > 0$ é sempre monótona crescente.

A propriedade de ser monótona crescente é facilmente verificada de modo formal através do cálculo e da análise da derivada da expressão (3.12) com

respeito a y, dada pela expressão:

$$\frac{d\omega_{x_\nu}(y)}{dy} = \frac{x_\nu}{(5+y+x_\nu)^2}. \tag{3.13}$$

Evidentemente a expressão (3.13) é estritamente positiva para valores de x_ν maiores do que zero, seguindo daí o fato de que $\omega_{x_\nu}(y)$ é uma função monótona. Por outro lado, à proporção que y cresce sem limite é fácil ver que

$$\lim_{y\to\infty} \omega_{x_\nu}(y) = \lim_{y\to\infty} \left(\frac{1}{1+\frac{x_\nu}{5+y}} \right) = 1 \tag{3.14}$$

e também que

$$\lim_{y\to\infty} \frac{d\omega_{x_\nu}(y)}{dy} = 0. \tag{3.15}$$

Logo, isto significa que a função $\omega_{x_\nu}(y)$ se aproxima assintoticamente da função $u(y) = 1$, para cada valor do parâmetro x_ν.

A partir das expressões (3.14) e (3.15) é possível concluir que, mantendo fixo o comprimento da trajetória, à proporção que se aumenta a carga útil de um pacote a função razão de eficiência converge para o valor um, fato que conincide com a intuição desenvolvida sobre o problema da marcação determinística de pacotes, por meio da inserção de números IP. Pode-se dizer mesmo que, o efeito nocivo da inserção de campos com números IP nessa modalidade de marcação de pacotes sofre progressiva atenuação, como resultado do aumento da carga útil do pacote. Naturalmente, essa afirmação é válida desde que sejam respeitados os limites físicos do ambiente onde se dá o fenômeno em estudo.

De modo análogo ao que se fez ao final do estudo da função $\omega_{y_\mu}(x)$ da razão de eficiência, cabe também aqui a inserção de comentários sobre a natureza algébrica que existe no conjunto Ω_x, cujo comportamento apresenta um caráter dual em relação ao conjunto Ω_y, anteriormente definido.

3.1.5 *Uma Rápida Visão Algébrica - II*

Considerando os elementos $\omega_{x_\nu}(y)$, do conjunto Ω_x, pode-se definir um operação de multiplicação entre os mesmos, baseada na multiplicação existente no conjunto $\mathbb{R}$ dos números reais, conforme a

Definição 3.2. *Considerando o conjunto Ω_x das funções $\omega_{x_\nu}(y)$, a operação de multiplicação $\odot : \Omega_x \times \Omega_x \to \Omega_x$ é tal que $\omega_{x_\nu}(y) \odot \omega_{x_\lambda}(y) = \omega_{x_\nu . x_\lambda}(y)$.*

Desde que a operação $\odot$ foi definida a partir da operação de multiplicação sobre os números reais, ambiente de onde provêm os elementos x_ν, é natural esperar que a mesma deva herdar algumas das propriedades dessa multiplicação real. Com efeito, a proposição a seguir traduz essa expectativa.

Proposição 3.5. *A operação $\odot : \Omega_x \times \Omega_x \to \Omega_x$ é associativa e possui elemento neutro.*

Demonstração. Desde que

$$(\omega_{x_\mu} \odot \omega_{x_\nu}) \odot \omega_{x_\lambda} = \omega_{x_\mu . x_\nu} \odot \omega_{x_\lambda} = \omega_{(x_\mu . x_\nu) . x_\lambda}$$

$$= \omega_{x_\mu . (x_\nu . x_\lambda)} = \omega_{x_\mu} \odot \omega_{x_\lambda . x_\nu} = \omega_{x_\mu} \odot (\omega_{x_\nu} \odot \omega_{x_\lambda}).$$

Logo, a operação $\odot$ é associativa. Considerando $x_\nu = 1$, então tem-se que

$$\omega_{x_\mu} \odot \omega_{x_\nu} = \omega_{x_\mu} \odot \omega_1 = \omega_{x_\mu . 1} = \omega_{1 . x_\mu} = \omega_{x_\mu}$$

e, portanto, existe um elemento neutro para a operação $\odot$, que é ω_1. □

A partir do que estabelece a Definição 3.2 e do resultado da Proposição 3.5, conclui-se que o par $(\Omega_x, \odot)$ é um *monóide*, visto que atende aos requisitos que caracterizam essa estrutura algébrica, vide Apêndice C. Supondo que $\omega_{x_\mu}, \omega_{x_\lambda}, \omega_x \in \Omega_x$, considere-se a equação

$$\omega_x \odot \omega_{x_\mu} = \omega_{x_\lambda}, \tag{3.16}$$

cuja incógnita é ω_x e os valores conhecidos são ω_{x_μ} e ω_{x_λ}. Desde que em um monóide não existe a garantia da existência de inverso para cada um dos elementos de Ω_x, segundo a operação $\odot$, essa equação nem sempre apresenta solução em Ω_x.

Por sua vez, a equação (3.16) pode ser utilizada na representação de um outro problema identificável em $(\Omega_x, \odot)$, que se pode enunciar como segue:

Enunciado 3.3. *Considerando uma dada carga útil y_k para um pacote, cujo valor da função de razão de eficiência é $\omega_{x_\lambda}(y_k)$, e o número $x_\mu < x_\lambda$, encontrar o número x que torne possível estabelecer a igualdade da expressão $\omega_x \odot \omega_{x_\mu} = \omega_{x_\lambda}$.*

Apesar de nenhum uso prático imediato estar explícito, o Enunciado 3.3 mostra que função $\omega_{x_\lambda}(y)$ de razão de eficiência, cujo parâmetro é o número x_λ, pode ser decomposta como duas mais simples, unidas pela operação $\odot$. Essa decomposição permite substituir o estudo de uma trajetória mais longa pelo de duas mais curtas.

3.1.6 *Variando Ambos os Elementos*

A fim de completar o atual estudo da função $\omega(x, y)$ de razão de eficiência, esta subseção trata da situação teórica em que as duas variáveis, simultaneamenste, crescem sem limite. A expressão (3.17), mostrada a seguir, resume o comportamento da referida função, nessa situação de crescimento ilimitado das variáveis:

$$\lim_{x,y\to\infty}\left(\frac{1}{1+\frac{x}{5+y}}\right) = \lim_{x,y\to\infty}\left(\frac{1}{1+\frac{1}{(5/x)+(y/x)}}\right) = \frac{1}{2}. \qquad (3.17)$$

O fato de que a expressão (3.17) convergir para o valor limite igual a $(1/2)$ se deve a que tanto x, quanto y, podem crescer sem limite. Com efeito, o crescimento ilimitado de x faz a fração $(5/x)$ convergir para zero. Ao mesmo

tempo, a fração (y/x) convergirá para o valor 1 (um), quando ambos os seus componentes crescem sem limite.

O valor da expressão (3.17) permite concluir que, quando se inserem campos de marcação, ao mesmo tempo que também cresce a carga útil por pacote, a eficiência com que a rede funciona cai para a metade daquela com respeito à situação sem a marcação. Esta é uma propriedade que pode levar o método da inserção de campos à consideração, como uma alternativa para a identificação de atacantes, em ambientes de dimensões mais restritas. Essa conclusão de natureza teórica, no entanto, somente será verdadeira desde que se respeitem os limites que o meio físico possa suportar.

A próxima seção apresenta uma outra contramedida a ataques do tipo DoS, que também se enquadra na classe das abordagens computacionais determinísticas. Apesar de sua extravagância, o uso dessa técnica pode ser justificado em situações especiais.

3.2 Rastreamento por Contra-Ataque

A fim de compreender como funciona a contramedida denominada *rastreamento por contra-ataque*, convém observar como funciona o diálogo entre um computador cliente, que demanda serviço, e um computador servidor, que provê o serviço demandado. Este é o assunto da próxima subseção.

3.2.1 *Conexão Cliente-Servidor*

No ambiente da arquitetura cliente-servidor a execução de serviços de alto nível requer funções capazes de criar uma infra-estrutura de comunicação entre rede de computadores. Essas funções devem garantir a interligação entre redes, mesmo que sejam heterogêneas, e são implementadas por meio de equipamentos (hardware) e de programas (software) apropriados.

A interligação entre redes se baseia no princípio da comunicação entre

computadores, que nada mais é do que um díálogo simples entre dois equipamentos. Um dos computadores é o *servidor*, isto é, aquele sempre pronto para receber alguma solicitação. O outro é o *cliente*, que a qualquer instante pode solicitar algum serviço.

Quando um computador cliente deseja estabelecer uma conexão com um computador servidor, o diálogo entre os mesmos segue um roteiro tal como o seguinte:

- O cliente envia uma mensagem SYN para o servidor.
- Ao receber a mensagem SYN o servidor responde com outra, SYN-ACK, de confirmação.
- Quando o cliente recebe a resposta do servidor, estabelece a conexão respondendo com ACK.

Uma vez concluído o diálogo supra, a conexão entre cliente e servidor fica estabelecida e os dados do serviço específico podem ser intercambiados entre os dois computadores.

Como se pode ver, o protocolo é de concepção bastante simples. Esse fato influencia não somente na facilidade de implementação do protocolo, como também na eficiência com que o mesmo opera a transmissão de dados. Contudo, ataques do tipo DoS costumam ser desfechados exatamente tirando proveito dessa simplicidade, conforme será apresentado na próxima subseção.

3.2.2 *O Congestionamento TCP-SYN*

A descrição do processo de comunicação entre dois computadores mostrou que, enquanto uma conexão está ativa, na memória de cada um dos computadores fica presente um registro com os dados identificadores dessa conexão. O computador cliente terá apenas um registro, enquanto o servidor terá um registro para cliente ao mesmo conectado, todos armazenados em uma tabela

na memória principal.

Naturalmente, existe uma capacidade máxima para esta tabela armazenar registros de clientes, acima da qual o funcionamento do servidor ficará comprometido, recusando novas solicitações. A esta situação de negar a permissão para inserir novos registros para identificar conexões se denomina *negação de serviço*.

Enquanto está sendo estabelecido o diálogo de conexão, e o servidor envia a mensagem SYN-ACK ao cliente, sabe-se que é criado um registro na tabela de conexões TCP, que permanece no estado "em aberto"até ser recebida uma mensagem ACK do cliente, que lhe corresponda. Naturalmente, essa espera não é indefinida e a tentativa de conexão falhará se não for completada no tempo apropriado.

O ataque decorrente da elevada intensidade de um fluxo TCP-SYN ocorre quando uma grande quantidade de mensagem SYN é enviada ao servidor, de modo que a tabela de conexões TCP fique repleta de registros "em aberto". A continuidade do fluxo atacante fará com que novos registros "em aberto"substituam os mais antigos, de modo que impedirá às mensagens verdadeiras chegar ao servidor. Em decorrência, o servidor negará serviço aos clientes verdadeiros.

Além desta forma de ataque, cujos detalhes podem ser vistos em [12], na próxima subseção será tratada uma outra, dentro da mesma modalidade de congestionamento.

3.2.3 *Ataque do Tipo Smurf*

Todas as mensagens enviadas para uma rede de computadores devem passar pelo conjunto de roteadores aos quais a mesma se liga. Uma grande quantidade de mensagens congestiona os roteadores, de modo que toda essa atividade resulta em perda de pacotes destinados à rede. Os ataques cujo objetivo é o congestionamento do tráfego em uma rede têm sido comunicados ao CERT por administradores de redes e provedores de serviços de Internet

desde o ano de 1998. Trata-se de uma modalidade de ataque do tipo DoS que utiliza o protocolo ICMP (*Internet Control Message Protocol*), através do qual são forjadas mensagens que, uma vez enviadas, requerem um eco como resposta.

Tais ataques resultam em uma grande quantidade de pacotes sendo enviados de variados locais remotos para a vítima e produzindo congestionamento na rede. A nomenclatura "ataque do Tipo Smurf" é oriunda de um programa denominado *Smurf*, segundo [13] utilizado por atacantes para executar ações dessa natureza.

A próxima subseção descreve os aspectos da técnica do rastreamento por contra-ataque, como uma forma de responder a um ataque do tipo DoS.

3.2.4 *Técnica de Contra-Ataque*

A fim de mitigar a tarefa de responder a um ataque do tipo DoS, Hal Burch e Bill Cheswick propuseram em [9], p. 313-315, uma contramedida para o ataque DoS. Trata-se de um método que se compõe de três etapas, respectivamente denominadas *1) Traçar Mapas*, *2) Localizar Fontes Intermediárias* e *3) Ligar Fontes Intermediárias*.

Uma importante característica do método é o fato de que o mesmo não requer auxílio ou intervenção de provedores de Internet para a sua aplicação. Além disso, ainda conforme Burch et alli, o rastreamento requer apenas alguns minutos, depois que a vítima percebe que está sob ataque. Cada uma dessas etapas tem o seu detalhamento mostrado a seguir.

- Etapa 1 - Traçar Mapa

  Nesta etapa deve ser traçado um mapa da Internet mostrando as trajetórias que partem da vítima, com os seus respectivos roteadores, e chegando às maiores distâncias possíveis da mesma. Existem técnicas destinadas à realização dessa tarefa, como mostrado em [27], p. 1-10 e [15], p. 1-6.

- Etapa 2 - Localizar Fontes Intermediárias de Ataque
  Em seguida, devem ser localizadas na rede as fontes de onde provem o ataque. Para isto, utiliza-se um serviço gerador de caracteres baseado no protocolo UDP, ver [47], por meio do qual envia-se uma curta rajada de caracteres a cada um dos roteadores localizados na Etapa 1 anterior. Caso um dos roteadores atingidos pela rajada de caracteres esteja na trajetória de ataque, o fluxo de pacotes atacantes sofrerá uma perturbação.

- Etapa 3 - Ligar Fontes Intermediárias de Ataque
  Uma vez localizadas as fontes intermediárias de ataque, deve-se utilizar o mapa construído na etapa 1 para se determinar quais outras fontes, ligadas à última localizada, precisam ser atingidas pela rajada de caracteres. Prossegue-se através da rede, de roteador em roteador, "podando-se" os ramos que não perturbam o ataque. Desse modo, restarão os ramos da árvore através dos quais ocorre o ataque DoS. Então, repete-se a etapa 2, até quando for possível estender o procedimento para a localização e fontes intermediárias de ataque. A interligação dos roteadores localizados como atacantes forma a trajetória de ataque.

A técnica descrita por meio das três etapas mostradas anteriormente aparenta ser de simples aplicação. Além disso, a menos do programa destinado a traçar o mapa da rede, os recursos usados não apresentam grande sofisticação tecnológica.

3.2.5 *Alguns Comentários*

Uma rápida reflexão sobre a natureza dessa contramedida, destinada ao rastreamento reverso do número IP, mostra que ela própria é um ataque

DoS. No que concerne à eficácia e à eficiciência, nada garante que a técnica se mostre adequada. De fato, segundo Burch et alli, ver [9], p. 313-315, apesar de a experiência ter funcionado em uma intranet, cujo ambiente está sob controle, não há certeza de que se possa obter resultados positivos se aplicada no âmbito da Internet. O que há de concreto, se essa técnica for extrapolada para a Internet, é a certeza do impacto desfavorável que causará no funcionamento da propria rede e nos usuários da mesma.

Deve-se ter em mente que a abordagem utilizada para o rastreamento reverso do número IP foi baseada unicamente em argumentos computacionais. Nos próximos capítulos serão apresentados argumentos com fundamentação matemática, que permitem extrair maior riqueza de detalhes, quando associados ao apelo computacional.

3.3 Observações Adicionais

No universo das propostas para a solução do problema do rastreamento reverso as primeiras abordagens foram de caráter puramente computacional. O desenvolvimento de um novo algoritmo sempre deverá sempre apresentar algum fato que justifique a sua utilização, tal como maior velocidade, menor complexidade computacional, ou ainda menor exigência de recursos de máquina.

Nas seções anteriores foram apresentadas abordagens de natureza estritamente computacional, com fundamentações de caráter primitivo. A primeira idéia que se tem é que ambas não resistiriam a uma análise mais aprofundada, quando se faz apenas uma rápida exposição do seu funcionamento. No entanto, esse aprofundamento analítico é exatamente a contribuição do presente capítulo ao estudo da abordagem computacional determinística.

Capítulo 4

Abordagem Matemática Determinística

Este capítulo apresenta uma proposta de contramedida ao problema do ataque do tipo DoS, via o uso do rastreamento reverso do número IP. A partir de um conjunto de suposições previamente estabelecidas surge um singular modelo matemático, baseado na técnica da interpolação.

O modelo proposto leva em conta apenas uma trajetória de ataque. Os roteadores ao longo desta trajetória são associados a pontos em um plano coordenado, por sobre os quais se pode interpolar um polinômio. Os coeficientes do polinômio interpolador serão os números IP de cada um dos roteadores da trajetória.

Deve ser ressaltada a elegância desta abordagem, que se utiliza de conceitos fundamentais da Matemática, em especial da Álgebra Abstrata e da Análise Numérica.

4.1 Apresentação do Problema

O modelo da interpolação polinomial é devido ao trabalho dos pesquisadores Drew Dean, Matt Franklin and Adam Sttublefield, conforme se pode ver em [21], p. 2-4. Tal qual outras abordagens, este modelo consid-

era a Figura 5.1 como sendo a topologia do ambiente onde se dá um ataque do tipo DoS.

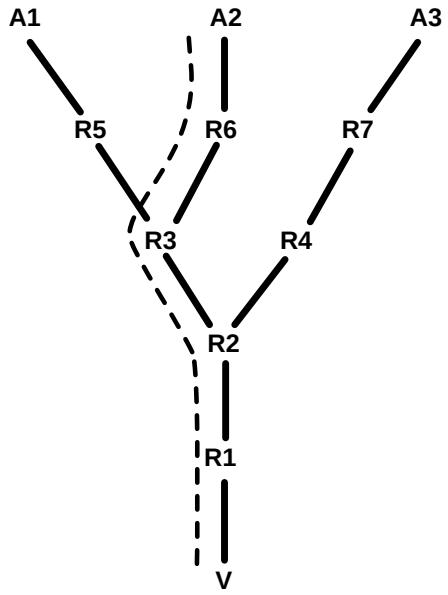

Figura 4.1: Ambiente de Ataque.

Os ataques podem partir de um, ou mais, agressores, enumerados como A_1, A_2, A_3, por exemplo, que se ligam à vítima, V, através das trajetórias representadas pelas linhas mais espessas. Os pacotes percorrem essas trajetórias, onde se encontram roteadores, $\{R_i | i = 1, \ldots, 7\}$. A linha tracejada destaca uma trajetória possível para o deslocamento dos pacotes de ataque.

Uma trajetória de ataque fica determinada quando se consegue descobrir quais são os números IP dos roteadores que a compõem. A trajetória destacada pela linha tracejada na figura Figura 5.1, por exemplo, é composta pelos roteadores R_1, R_2, R_3.

No âmbito do espaço virtual, a identificação de cada roteador se dá por meio de um número IP e esta forma de identificação não incorpora qualquer característica de natureza métrica. A partir dos números IP dos roteadores nem mesmo se pode estabelecer uma medida de distância de natureza topológica entre os mesmos. A possibilidade que existe é a de que, no ambiente da árvore como um todo, definir uma relação de adjacência

entre dois roteadores. Em especial, para dar subsídio ao presente estudo, considera-se essa relação de adjacência sobre uma trajetória de ataque, o que origina uma relação de ordem total.

Considere-se $\{R_i | i = 0, 1, \ldots, n\}$ o conjunto dos roteadores que compõem uma trajetória de ataque, sendo i um índice cujo valor cresce a partir do roteador mais próximo da vítima, em direção ao atacante. O que se deseja é associar cada um destes roteadores do ambiente de ataque a um par ordenado da forma (x_i, y_i), que se encontra no plano $\mathbb{R}^2$. Esta associação também deve permitir que se possa inferir o número IP dos roteadores R_i a partir das coordenadas do par ordenado.

Sabe-se da técnica da interpolação, ver [7], p. 85-86 e [26], p. 360-361, que uma vez de posse do conjunto $\{(x_i, y_i) | i = 0, 1, \ldots, n\}$, de $(n + 1)$ pares ordenados é possível construir um polinômio de grau n que passa por todos esses pontos, desde que algumas condições mínimas sejam satisfeitas.

A partir da observação do ambiente no qual ocorre um ataque do tipo DoS, é possível obter tais pares de pontos necessários ao processo de interpolação. O modelo proposto por Dean et alli, ver [21], é tal que os coeficientes que surgem no polinômio construído serão exatamente os números IP dos roteadores que constituem a trajetória de ataque. As próximas seções apresentam aspectos do detalhamento deste modelo para o rastreamento reverso do número IP.

4.2 Descrição da Interpolação

A motivação para o uso de um método de interpolação polinomial provém da facilidade que existe no manuseio de um polinômio, que é o tipo mais simples de função matemática. Os detalhes sobre métodos de interpolação podem ser encontrados em [10], p. 96-106 e em [48], p. 80-83. Todavia, a essência de um problema de interpolação polinomial se encontra no enunciado mostrado a seguir:

Enunciado 4.1. *Dado um conjunto de* $(n+1)$ *pontos* $\{(x_i, y_i)|i = 0, \ldots, n\}$ *em um plano, deseja-se construir um polinômio de grau* n*, cuja forma é,*

$$P(x) = \sum_{k=0}^{n} a_k.x^k = a_n.x^n + a_{n-1}.x^{n-1} + \ldots + a_2.x^2 + a_1.x + a_0, \qquad (4.1)$$

tal que o gráfico desse polinômio passe por todos os pontos do conjunto. Essa condição se traduz através das das $(n+1)$ *expressões seguintes:*

$$y_i = P(x_i), \quad i = 0, \ldots, n.$$

Conhecendo-se os valores dos $(n+1)$ pontos do conjunto definido como $\{(x_i, y_i)|i = 0, \ldots, n\}$, pode-se facilmente inferir da expressão (4.1) que a construção do polinômio $P(x)$ depende apenas de se descobrir os valores dos $(n+1)$ coeficientes que o constituem. Em outras palavras, é necessário calcular os valores dos a_k, para $k = 0, 1, \ldots, n$. Substituindo na expressão em (4.1), sucessivamente, os $(n+1)$ valores x_i e y_i, de cada ponto, serão obtidas $(n+1)$ expressões, conforme visto a seguir:

$$\begin{cases} y_0 = a_n.x_0^n + a_{n-1}.x_0^{n-1} + \ldots + a_2.x_0^2 + a_1.x_0 + a_0 \\ y_1 = a_n.x_1^n + a_{n-1}.x_1^{n-1} + \ldots + a_2.x_1^2 + a_1.x_1 + a_0 \\ y_2 = a_n.x_2^n + a_{n-1}.x_2^{n-1} + \ldots + a_2.x_2^2 + a_1.x_2 + a_0 \\ \qquad\qquad\qquad\qquad \vdots \\ y_n = a_n.x_n^n + a_{n-1}.x_n^{n-1} + \ldots + a_2.x_n^2 + a_1.x_n + a_0 \end{cases} \qquad (4.2)$$

O conjunto de expressões em (4.2) se contitui em um sistema de equações lineares com $n+1$ equações e $n+1$ incógnitas. Não se deve esquecer que as incógnitas são os elementos a_k, para $k = 0, 1, \ldots, n$. A fim de resolver o sistema de equações lineares em (4.2), e descobrir os valores das incógnitas, pode-se lançar mão de algum dentre vários métodos numéricos, conforme [10], p. 300-320, ou [48], p. 19-76.

Representando a expressão (4.2) por meio da notação de matrizes, como em (4.3), vê-se que a matriz do sistema é o que se costuma denominar *Matriz de Vandermonde*. Existem técnicas especiais destinadas a resolver sistemas

de equações lineares cuja matriz é dessa natureza, conforme descrito em [48].

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{n-1} \\ y_n \end{bmatrix} = \begin{bmatrix} x_0^n & x_0^{n-1} & \dots & x_0^2 & x_0 & 1 \\ x_1^n & x_1^{n-1} & \dots & x_1^2 & x_1 & 1 \\ x_2^n & x_2^{n-1} & \dots & x_2^2 & x_2 & 1 \\ & & \vdots & & & \\ x_{n-1}^n & x_{n-1}^{n-1} & \dots & x_{n-1}^2 & x_{n-1} & 1 \\ x_n^n & x_n^{n-1} & \dots & x_n^2 & x_n & 1 \end{bmatrix} . \begin{bmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ \vdots \\ a_1 \\ a_0 \end{bmatrix} \tag{4.3}$$

Ainda utilizando a notação matricial, vê-se na expressão (4.4) o vetor de incógnitas explicitado em função da Matriz de Vandermonde e do vetor de ordenadas dos pontos. Essa forma de expressão é lícita, pois os pontos são todos distintos e, em decorrência, a matriz de Vandemonde possui inversa.

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ a_n \end{bmatrix} = \begin{bmatrix} x_0^n & x_0^{n-1} & \dots & x_0^2 & x_0 & 1 \\ x_1^n & x_1^{n-1} & \dots & x_1^2 & x_1 & 1 \\ x_2^n & x_2^{n-1} & \dots & x_2^2 & x_2 & 1 \\ & & \vdots & & & \\ x_{n-1}^n & x_{n-1}^{n-1} & \dots & x_{n-1}^2 & x_{n-1} & 1 \\ x_n^n & x_n^{n-1} & \dots & x_n^2 & x_n & 1 \end{bmatrix}^{(-1)} . \begin{bmatrix} y_n \\ y_{n-1} \\ y_{n-2} \\ \vdots \\ y_1 \\ y_0 \end{bmatrix} \tag{4.4}$$

Apenas para fins de estabelecer o aspecto formal dos cálculos mostrados anteriormente, recomenda-se a leitura do Apêndice D. Naquele apêndice se encontra um teorema que estabelece as condições necessárias para que se possa interpolar um polinômio por um conjunto de pontos. Naturalmente, tais condições precisam ser satisfeitas no desenvolvimento acima.

4.3 Coleta dos Dados

Para que seja possível construir um sistema de equações tal como o (4.2) é necessário obter um conjunto de pares ordenados, $\{(x_i, y_i)|i = 0, 1, \dots, n\}$, a partir da trajetória de ataque. Contudo, cada elemento residindo no espaço virtual é identificado unicamente por meio do seu número IP. Assim, para efeito de aplicar um método de interpolação é necessário que seja definida uma função, denominada Ψ, do ambiente de ataque, A, no espaço bidimensional $\mathbb{R}^2$, de modo que o número IP de cada roteador possa ser representado

por meio de um par ordenado.

A função $\Psi : A \rightarrow \mathbb{R}^2$, que associa um número IP de um roteador R_i a um par ordenado (x_i, y_i), isto é $\Psi(IP_i) = (x_i, y_i)$, precisa satisfazer a uma condição fundamental. Se IP_i e IP_j são números IP de dois roteadores distintos R_i e R_j, então tem-se que $\Psi(IP_i) \neq \Psi(IP_j)$. Em outras palavras, a função Ψ deve ser uma injeção.

O aprofundamento sobre as características desta função Ψ se encontra na próxima subseção.

4.3.1 *Comentários sobre a Função* Ψ

A fim de que se possa transformar o número IP_i de um roteador R_i em um par ordenado (x_i, y_i) é preciso definir a função Ψ de modo explícito. Considerando que o roteador R_i se encontra em uma trajetória de ataque, o seu número IP_i pode contribuir com a expressão de uma das coordenadas do par ordenado (x_i, y_i), que será a sua imagem pela função Ψ. A coordenada mais adequada deste par ordenado para receber esta contribuição é a y_i, visto que os números IP dos roteadores ao longo de uma trajetória de ataque não necessariamente obedecem a uma relação de ordem. Resta definir como se deve especificar a coordenada x_i, para completar o par ordenado que, naturalmente, deve obedecer a uma relação de ordem total.

A observação de um ambiente de ataque do tipo DoS mostra que, por mais intenso ou amplo que se apresente esse ataque, o mesmo pode ser entendido como um fato de abrangência local. Este entendimento permite que se defina um sistema local de coordenadas, ainda no espaço virtual, capaz de determinar os elementos que dão suporte ao ataque.

A perspectiva de se definir um sistema local de coordenadas torna a vítima uma referência canônica para essa finalidade. A partir da mesma ao longo de uma trajetória de ataque, qualquer um dos roteadores pode ser localizado considerando a quantidade de roteadores que existe entre o próprio e a vítima. Partindo do fato de que a localização de um pacote

viajando na rede só é determinada quando ele chega em um roteador, o seu deslocamento se assemelha a uma seqüência de *saltos* entre roteadores. Deste modo, pode-se medir a distância entre um roteador R_i e a vítima, R_0, como sendo a quantidade de saltos executados pelo pacote, desde que sai de R_i até chegar a R_0, por sobre a trajetória de ataque.

Deve-se ter em mente que essa forma de medir distância no ambiente de ataque tem carácter estritamente topológico. E o fundamento para a abordagem proposta é a existência de uma relação de ordem total entre as coordenadas x_i.

Antes de propor um modo de coletar os dados convém lembrar um importante resultado oriundo da da Álgebra Abstrata. Conforme se pode ver em [6], p. 77, um polinômio estará perfeitamente determinado quando se conhecem o seu grau e os seus coeficientes.

Com esse resultado em mente, pode-se construir um sistema de equações lineares, tal como em (4.2), cuja solução permite encontrar os valores dos coeficientes do polinômio interpolador procurado. Contudo, em nenhum momento falou-se sobre como se deve fazer para determinar o grau do polinômio. Naturalmente, essa tarefa deve ser incorporada, também, ao processo de coleta de dados. Isso significa que a obtenção de cada um dos pares ordenados (x_i, y_i), juntamente com o grau do polinômio, deve ser realizada nos roteadores, à proporção que o pacote se desloca pela trajetória de ataque.

4.3.2 *Cálculo do Valor de um Polinômio*

A determinação de cada um dos pares ordenados (x_i, y_i) requer que se atribua um valor para a variável independente, x_i. Uma vez inserida em $P(x)$, essa variável independente produz $y_i = P(x_i)$, que é o valor do polinômio procurado.

Uma rápida inspeção na expressão (4.1) mostra que o cálculo de y_i possui complexidade $O(x^n)$, o que se constitui em uma significativa dificuldade op-

eracional. Contudo, uma simples transformação na expressão (4.1) permite reduzir esse grau de complexidade, conforme se pode ver em (4.5) a seguir:

$$P(x) = ((\ldots(a_n.x + a_{n-1}).x + \ldots + a_2).x + a_1).x + a_0. \qquad (4.5)$$

Essa é uma forma conveniente para efetuar o cálculo do valor do polinômio, para uma dada variável independente x. Na expressão (4.5) não existe a necessidade de efetuar cálculos com potências da variável x, para calcular o valor do polinômio. Além disso, e princIPalmente, evidencia cada operação a ser realizada entre os coeficientes e a variável independente x.

Convém ainda notar em (4.5) que, o cálculo do valor do polinômio obedece a uma curta e simples seqüência de operações, iniciada com a multIPlicação entre o coeficiente de maior índice, a_n, e a variável independente x. Em seguida, adiciona-se o próximo coeficiente, a_{n-1} ao produto anterior. Caso esse coeficiente adicionado seja a_0, o cálculo está concluído. Senão, repete-se o procedimento anterior. Em resumo, o procedimento de cálculo é nada mais do que um produto seguido por uma adição, cujo resultado vai sendo acumulado em um totalizador.

Dois fatos são particularmente importantes, no que concerne ao cálculo do valor de um polinômio descrito anteriormente. Em primeiro lugar, o procedimento de cálculo exige o manuseio dos coeficientes na ordem decrescente do seu índice. Além disso, o valor estabelecido para a variável independente deve ser um número pertencente ao domínio da função, que é um polinômio, o seu domínio é o corpo sobre o qual o polinômio está definido, vide [6], p. 79-82 e Apêndice C.

Enfim, o cálculo do valor de um polinômio pode ser sintetizado por meio do pseudocódigo mostrado a seguir:

```
/* PS010 - Pseudocódigo p/ Calcular Valor de Polinômio */;
/***********************************************/
/* y: acumulador do cálculo */;
/* k: índice dos coeficientes */;
/* x: variável independente */;
```

```
/************************************************/
y ← 0;
k ← n;
obter  x;
enquanto  k > 0, faça
    y ← y + a_k;
    y ← y * x;
    k ← k − 1;
y ← y + a_0;
/************************************************/
```

O desenvolvimento do procedimento no pseudocódigo PS010 levou em conta o fato de que o cálculo do polinômio deve ser executado em um único computador. Contudo, essa premissa precisa ser adequada ao ambiente onde o cálculo será de fato efetuado. A verdade é que cada um dos coeficientes a_k se encontra em um roteador diferente. Assim, o campo acumulador do cálculo deverá trafegar entre os roteadores de modo que, em cada roteador esse campo receba a adição do número IP e em seguida seja multiplicado pela variável independente, x_i. Em conseqüência, à proporção que o pacote se desloca ao longo da trajetória vai a cada salto compondo o valor de y_i, de modo que, ao atingir a vítima, o pacote entregará o par ordenado (x_i, y_i).

Depois de terem chegado $(n + 1)$ pares ordenados, com distintos valores de x_i, então será possível construir um sistema tal como (4.2). Conforme se pode ver em (4.4), podem ser obtidos os coeficientes do polinômio interpolador, ou seja, os números IP dos roteadores da trajetória de ataque.

As peculiaridades às quais deve se submeter o determinismo apresentado acima no cálculo do valor de um polinômio são o assunto da próxima subseção.

4.3.3 *Adaptação do Cálculo ao Espaço Virtual*

Observando o pseudocódigo PS010 pode-se ver que o mesma se compõem de três estruturas distintas de programação. A primeira se constitui das três primeiras instruções que se referem ao estabelecimento de valores iniciais para as variáveis y (acumulador do cálculo), k (índice dos coeficientes) e x (variável independente). Este grupo de instruções é executado apenas uma vez durante o processamento. A segunda estrutura é constituída pelo laço com três operações aritméticas, que se repetem ao longo da trajetória de ataque. Enfim, existe uma última estrutura, constituída por apenas uma instrução aritmética que é executada uma única vez, somente no roteador ligado ao destino do ataque.

Desde que as três instruções da primeira estrutura devem ser executadas no início do procedimento, e apenas uma vez, esse fato significa que as mesmas precisam ser acionadas no *primeiro roteador* da trajetória de ataque. Assim, um pacote que sai do atacante deverá ser submetido inicialmente às seguintes operações operações aritméticas, ao chegar no primeiro roteador:

- O campo acumulador, y, deve ser tornado igual a zero ($y \leftarrow 0$).
- O campo índice de coeficientes, k, deve ser tornado igual a n.
- A variável independente, x, deve ser obtida.

O problema que ocorre nesse ponto, quando se trata de implementar o pseudocódigo a partir do modelo na expressão (4.1), é a atribuição do valor n ao campo k. Esse é o grau do polinômio e que corresponde ao comprimento da trajetória, desconhecido pelo procedimento no primeiro roteador. Na verdade, o pseudocódigo precisa ser modificado nessa instrução. A operação conveniente seria a de tornar igual a zero o campo índice de coeficiente, isto é fazer $k \leftarrow 0$, e de incrementá-lo ao longo da trajetória. Desse modo, quando o alvo fosse atingido, seria conhecido o tamanho da trajetória e,

por conseguinte, o grau do polinômio interpolador. Para isso, o polinômio mostrado em (4.1) precisa ser modificado para a nova forma a seguir:

$$P(x) = \sum_{k=0}^{n} a_{n-k}.x^k = a_0.x^n + a_1.x^{n-1} + \ldots + a_2.x^2 + a_{n-1}.x + a_n. \quad (4.6)$$

Desse modo, a simplificação para o cálculo desse polinômio passa a ser vista como

$$P(x) = ((\ldots(a_0.x + a_1).x + \ldots + a_2).x + a_{n-1}).x + a_n. \quad (4.7)$$

Enfim, restaria ainda a necessidade de se obter o valor para a variável independente, x, que deve acompanhar o pacote até o seu destino. Esse valor pode ser obtido por meio de algum procedimento que contenha um algoritmo gerador de números aleatórios, no primeiro roteador.

Concluída a execução da primeira estrutura do pseudocódigo, a segunda estrutura deve ser executada ainda no primeiro roteador, antes de o pacote ser enviado para adiante. Mas essa estrutura também precisa sofrer modificações para funcionar no espaço virtual. Tratando-se de um laço, a primeira preocupação deve ser com o critério de parada, que em PS010 é a comparação da variável k com zero, isto é, $k > 0$. Naturalmente, com esse critério o procedimento nunca teria progresso, pois uma das modificações na primeira estrutura foi justamente tornar o valor inicial de k igual a zero. Levando em conta que o pacote contém o endereço de destino da mensagem, a comparação desse endereço como o de cada roteador ao longo da trajetória torna-se um critério de parada aceitável. Assim, a adaptação da segunda estrutura pode ser resumida como sendo:

- *enquanto o endereço de destino é diferente do atual*:

  Adicionar o número IP, a_0, ao acumulador y.

  MultIPlicar o acumulador y pela variável independente, x.

  Incrementar o índice de coeficientes, k, em uma unidade.

A segunda estrutura permanece sendo executada ao longo da trajetória de ataque, em cada um dos roteadores que a compõem. A única exceção

ocorre quando o pacote chega ao roteador de destino. Nessa ocasião, a única estrutura executada é a terceira do pseudocódigo, na qual só existe apenas uma instrução destinada a acumular o número IP do último roteador.

Como se pode ver, ao longo dos roteadores da trajetória de ataque a execução do pseudocódigo PS010 deve ocorrer de modo seletivo, apesar de que as três estruturas componentes podem funcionar em qualquer roteador da rede. A seguir se apresenta uma proposta para a implementação do pseudocódigo PS010, de acordo com o mecanismo de operação apropriado em cada uma das três situações em que um roteador pode se encontrar.

Roteador inicial (índice 0 no modelo) -

1. Criar um acumulador, y, cujo conteúdo inicial é igual a zero, isto é, $y \leftarrow 0$.
2. Criar um índice de coeficiente, k, cujo conteúdo inicial é igual a zero, isto é, $k \leftarrow 0$.
3. Gerar um valor aleatório x.
4. Atribuir ao acumulador y o total da soma $(y + a_0)$ (sendo a_0 o número IP do roteador R_0), isto é, $y \leftarrow y + a_0$
5. Atribuir ao acumulador y o produto do seu valor atual, y, por x, isto é, $y \leftarrow y.x$.
6. Enviar o par ordenado (x, y) para o próximo roteador.

Roteador intermediário (índice k no modelo, sendo $0 < k < n$) -

1. Atribuir ao acumulador y o total da soma $(y + a_k)$ (sendo a_k o número IP do roteador k), isto é, $y \leftarrow y + a_k$.
2. Atribuir ao acumulador y o produto do seu valor atual, y, por x, isto é, $y \leftarrow y.x$.

3. Incrementar o índice de coeficiente, k, em uma unidade, isto é, $k \leftarrow k + 1$.

4. Enviar o par ordenado (x, y) para o próximo roteador.

Roteador final (índice n no modelo) -

1. Atribuir ao acumulador y o total da soma $(y + a_n)$ (sendo a_n o número IP do roteador R_n), isto é, $y \leftarrow y + a_n$.

2. Incrementar o índice de coeficiente, k, em uma unidade, isto é, $k \leftarrow k + 1$.

3. Obter o par ordenado final, (x, y).

4. Obter o contador k.

A partir da implementação sugerida acima, cada pacote entregaria à vítima um par ordenado (x, y), contendo uma abcissa x e a sua correspondente ordenada, $y = P(x)$, além do grau do ploinômio, n, contido no contador k. A reunião de $(n+1)$ pares ordenados permitiria a inserção dos valores dos mesmo no sistema de equações lineares (4.2), e o conseqüente cálculo dos a_i, resolvendo o problema em estudo.

A proposta apresentada parte do princípio de que devem ser identificados três tipos distintos de roteadores em uma rede de computadores, a saber: roteador inicial, roteador intermediário e roteador final. No entanto, essa possibilidade não pode ser admitida, visto que os protocolos que configuram as redes de computadores não fazem distinção entre os roteadores que as compõem. Desse modo, não há como estabelecer qual é o tipo a que pertence cada um dos roteadores do ambiente de ataque. No máximo pode-se identificar qual é o último roteador da trajetória, pois todo pacote contém o endereço de destino da mensagem e, assim, pode identificar esse roteador.

Tal situação de impasse faz surgir a pergunta: o que se deve fazer para

coletar dados sobre a trajetória de ataque, ainda tomando por base a proposta anterior?

O problema se resume na identificação de qual deve ser o roteador inicial de uma determinada trajetória, pois a partir daí todos os outros roteadores estarão automaticamente identificados. Na ausência de um modo para determinar precisamente qual roteador é o primeiro de uma trajetória, a alternativa é recorrer a um procedimento aleatório, cuja execução deverá preceder a de todas as outras instruções.

Semelhante ao lançamento de uma moeda, tal procedimento funcionará como um mecanismo para a tomada de decisão, cuja natureza aleatória está associada à existência de uma probabilidade de sucesso, p. Desse modo, a partir do resultado retornado pelo mecanismo do procedimento, com probabilidade p um roteador poderá ser considerado o primeiro da trajetória.

O uso da abordagem aleatória insere no problema um aspecto de incerteza, que será comentado na próxima subseção.

4.3.4 *Incerteza sobre os Dados Coletados*

Observando-se a Figura 5.1, é fácil ver que a trajetória para chegar até à vítima poderia ser $R_6R_3R_2R_1$, se R_6 fosse escolhido como roteador inicial. No entanto, também poderiam ser detectadas trajetórias tais como $R_3R_2R_1$, R_2R_1, ou mesmo R_1, dependendo de o processo aleatório escolher R_3, R_2, ou R_1, como roteador inicial.

Essa variedade de trajetórias, que inclui a real e as "virtuais", à primeira vista, estabeleceria na vítima uma confusão, considerando a exagerada quantidade de pacotes que a mesma recebe. Os pacotes recebidos devem ser agrupados de modo que, em cada grupo, o valor do campo contador,k, seja o mesmo para todos os pacotes. Deste modo, será possível estabelecer o grau do polinômio interpolador, por meio da identificação do grupo cujo valor do campo contador é máximo.

A avaliação do grau de complexidade do problema em estudo deve ter

em conta um importante aspecto. Trata-se do fato de que, todas as considerações dos parágrafos anteriores desta subseção consideram que o ataque se dá através de um única trajetória. Essa é uma suposição bastante restritiva do problema em evidência, visto particularizar em demasia a situação da prática.

A proposta alternativa do pseudocódigo PS010, no entanto, apresenta um elemento útil no combate a ataques que ocorrem ao longo de múltiplas trajetórias, que é o já citado contador k, cujo conteúdo mostra a distância do roteador inicial onde o pacote foi marcado até a vítima. Ordenando os pacotes com respeito ao campo k, de modo decrescente, suponha-se que o maior valor de distância encontrado foi $k = d$. Além disso, supondo que N seja a quantidade de pontos com esse valor máximo do campo k, tais condições permitem chamar à memória um conhecido problema, cujo enunciado pode ser posto nos termos seguintes:

Enunciado 4.2. *(Lista de Decodificação de Reed-Solomon)- Dados* $(x_1, y_1), \ldots, (x_N, y_N)$ *pontos distintos, encontrar todos os polinômios de grau máximo igual a* d *que passem por, no mínimo, uma quantidade* m *desses pontos, que seja menor do que, ou igual a* N*.*

Segundo Dean, Franklin e Sttubfield, ver [21], p. 7-8, existe um algoritmo proposto por Guruswami e Sudan, em [28], p. 1-26, para a resolução desse problema no tempo $O(N^3)$, quando $N < m^2/d$. Ainda segundo os mesmos autores, foi desenvolvida uma implementação desse algoritmo por Olshevsky e Shokrollahi, ver [45], que reduz o tempo para $O(N^{2.5})$. Os detalhes desses desenvolvimentos não serão apresentadosse devido se encontram foram do objetivo do presente trabalho. Contudo, são relevantes os aspectos computacionais envolvidos e se constituem no assunto abordado na próxima seção.

4.4 Aspectos Computacionais

A descrição do procedimento de interpolação, mostrado na seção 4.2, revela a necessidade de se resolver um sistema de equações lineares, como forma para obter os coeficientes do polinômio interpolador. A importância do problema e o as conhecidas formas de solução, conforme se pode ver em[10], p. 300-320, e [48], p. 19-76, tornam atraente e elegante a abordagem proposta por Dean, Franklin e Sttubfield. Contudo, as condições do ambiente onde se dá o ataque DoS exigem adequações nos procedimentos aritméticos para o tratamento de sistemas de equações lineares, devido à natureza dos dados envolvidos no problema.

4.4.1 *Representação dos Dados*

Deve-se partir do princípio de que, sendo elementos do espaço virtual, os roteadores são identificados através de números IP. Sabe-se que a estrutura de tais números é formada por uma palavra de trinta e dois bits, conforme a Figura 4.2. Nesta palavra, cada um dos octetos é envolto por um par de parênteses e indexado, de modo a tomar a forma de um quadrupleto.

$$(\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0$$

Figura 4.2: Forma do Número IP.

Cada um dos octetos componente do número IP contém um número inteiro sem sinal, e que pode ser visto como pertencente ao conjunto $\mathbb{Z}_{256} = \{0, 1, \ldots, 255\}$. Esta é a raiz das modificações no procedimento de resolução do sistema de equações lineares.

O primeiro ponto a ser considerado diz respeito à natureza algébrica do conjunto $\mathbb{Z}_{256}$. Conforme o Apêndice C, seção C.4, verifica-se facilmente que $\mathbb{Z}_{256}$ não é um corpo e, portanto, não se aplica no mesmo a lei do cancelamento, vide Apêndice C, seção C.4. Este fato invalida o uso dos métodos

convencionais para a resolução de um sistema de equações lineares nesse conjunto.

Um modo de transpor essa dificuldade é encontrar um conjunto, que será denominado Λ, possuindo propriedades de corpo algébrico e que contenha $\mathbb{Z}_{256}$. Além disso, não deve existir qualquer outro corpo contido em Λ, que contenha $\mathbb{Z}_{256}$. Assim, Λ será o corpo "o mais próximo possível" de $\mathbb{Z}_{256}$.

O candidato canônico para ser Λ é o conjunto $\mathbb{Z}_{257}$. Em virtude da sua "proximidade" com $\mathbb{Z}_{256}$, para efeito de operações aritméticas pode-se identificar em $\mathbb{Z}_{257}$ as classes zero e 256. E isso se deve ao fato de que, na representação de um número IP, além da classe 256 equivaler à classe zero, o maior valor que pode ser representado em um número binário de oito bits é 255.

A fim de se resolver o problema correlato da interpolação, esse modo de representação dos dados, conforme a Figura 4.2, deverá ser inserido no modelo matemático mostrado em (4.4). Considerando o fato de que se trabalha sobre um corpo finito, o $\mathbb{Z}_{257}$, cuja forma sintética usada para representar o problema é a seguinte:

$$\overrightarrow{A} = X^{-1}.\ \overrightarrow{Y}\ (mod \quad 257). \tag{4.8}$$

Os cálculos necessários de serem efetuados para resolver uma equação matricial como a da expressão (4.8), deverão levar em conta essa natureza dos elementos dos vetores $\overrightarrow{A}$ e $\overrightarrow{Y}$. Ao mesmo tempo, existe a necessidade de se calcular a inversa da matriz X, que é uma Matriz de Vandermonde sobre um corpo finito. Deve-se ter em mente que, os elementos da matriz de Vandermonde **X**serão números aleatórios obtidos do conjunto $\mathbb{Z}_{257}$, cuidando-se para que a ocorrência de 256 seja convenientemente substituída pelo valor zero.

À guisa de ilustração, e ainda tomando a expressão (4.4) como a equação matricial a ser resolvida, tem-se que a_k, o elemento de ordem k do vetor $\overrightarrow{A}$,

se representa como sendo

$$a_k = ((aaa)_3.(aaa)_2.(aaa)_1.(aaa)_0)_k. \tag{4.9}$$

De modo análogo, se escreve o elemento y_k, do vetor $\overrightarrow{Y}$ de acordo com

$$y_k = ((yyy)_3.(yyy)_2.(yyy)_1.(yyy)_0)_k. \tag{4.10}$$

Representa-se o elemento da inversa da matriz $\mathbf{X}$, que se encontra na linha k e na coluna $(n-j)$, como sendo $(x_k^{n-j})^{-1}$. Naturalmente, este não é o valor inverso do elemento (x_k^{n-j}) da matriz $\mathbf{X}$ e sim a indicação do elemento que se encontra na interseção da linha k com a coluna $(n-j)$ da matriz $\mathbf{X}^{-1}$. A expressão (4.11) indica como o valor de cada elemento do vetor $\overrightarrow{A}$ pode ser obtido:

$$a_k = \sum_{j=0}^{n} (x_k^{n-j})^{-1}.y_j. \tag{4.11}$$

A fim de observar com mais acuidade os detalhes operacionais necessários para efetuar os cálculos na expressão (4.11), convém escrever a referida expressão como segue:

$$((aaa)_3.(aaa)_2.(aaa)_1.(aaa)_0)_k = \sum_{j=0}^{n} [(x_k^{n-j})^{-1}.((yyy)_3.(yyy)_2.(yyy)_1.(yyy)_0)_j] \tag{4.12}$$

O que se observa desse detalhamento é que cada um dos componentes da estrutura do número IP deve ser operado de modo independente dos demais. Por exemplo, para calcular o valor de uma das quatro componentes do elemento a_k, denominada aqui como $(aaa)_\lambda$, para $\lambda \in \{0, 1, 2, 3\}$, é necessário efetuar a soma de cada um dos produtos dos elementos da linha k, da matriz $\mathbf{X}^{-1}$, pelas componentes $(yyy)_\lambda$ que lhes são correspondentes, do vetor $\overrightarrow{Y}$, conforme se vê na expressão (4.13).

$$((aaa)_\lambda)_k = \sum_{j=0}^{n} [(x_k^{n-j})^{-1}.((yyy)_\lambda)_j]. \tag{4.13}$$

Como se pode ver, a expressão (4.13) mostra a natureza mais interna do tipo de cálculo que deve ser efetuado, no intuito de obter os números IP de uma trajetória de ataque. Deve-se ter em mente, também, que cada um dos elementos em (4.13) é um número pertencente ao conjunto $\mathbb{Z}_{257}$, sendo necessário respeitar as regras para efetuar operações aritméticas com os mesmos.

4.5 Comentário Final

A teoria sobre a resolução de sistemas de equações lineares é bastante conhecida, bem como os métodos numéricos utilizados nessa tarefa, desde que se trabalhe em um espaço vetorial sobre o corpo $\mathbb{R}$, dos números reais. O fato de o modelo proposto por Dean, Franklin e Sttubfield ter fundamento no uso dessa teoria é sem dúvida meritório.

A natureza do número IP, no entanto, mostra uma outra realidade, no que concerne às peculiaridades do cálculo aritmético com os elementos do conjuntos numéricos $\mathbb{Z}_{257}$. Apesar da aparente dificuldade de implementação de aspectos operacionais, deve-se atentar para a originalidade da idéia apresentada, como método de rastreamento e identificação de atacantes DoS.

Capítulo 5

Visão Computacional Probabilística

A publicação do famoso artigo de Savage, Wetherall, Karlin e Anderson, intitulado *Pratical Network support for IP Traceback*, no ano 2000, vide [51], se constituiu em um evento cuja importância se reflete sobre todos aqueles interessados no problema do rastreamento reverso do número IP. O trabalho propõe uma abordagem de natureza computacional, apoiada pelo uso de aspectos da Teoria das Probabilidades. Sob essas condições se desenvolve um conjunto de procedimentos destinados a compor as contramedidas para o devastador ataque de Negação-de-Serviço.

Os procedimentos são divididos em duas categorias, a saber: 1) a dos que tratam da coleta de dados dos pacotes; 2) a dos que se utilizam desses dados para a recomposição das trajetórias de ataque. Ao longo deste capítulo serão apresentados os aspectos gerais da proposta de Savage, bem como desenvolvidos comentários sobre os fundamentos matemáticos envolvidos na abordagem.

5.1 Apresentação

A aplicação de uma contramedida de rastreamento reverso, em um cenário de ataque por Negação-de-Serviço (Denial-of-Service), necessita de indícios capazes de identificar os roteadores componentes da trajetória de ataque. O modo mais direto de obter esses indícios é transportá-los dos roteadores até à vítima, por meio dos pacotes que trafegam na rede. Para isso, é necessário forçar que cada roteador grave uma marca identificadora nos pacotes trafegando pelos mesmos.

Caso um pacote recebesse uma marca, como um selo, em cada um dos roteadores por onde passasse, facilmente seria posível reconstituir a sua trajetória de ataque. Esta abordagem determinística permitiria registrar no pacote a trajetória seguida pelo mesmo, podendo ser facilmente reconstituída.

Contudo, a viabilidade do uso generalisado deste procedimento é questionável, vide Capítulo 3, em virtude de dois fatores principais. Em primeiro lugar, a marcação de pacotes seria um trabalho adicional que resultaria no imediato aumento da carga de serviço na rede. O outro fator, não menos crítico, diz respeito ao espaço necessário em um pacote para a inserção de todas as marcas necessárias. Neste caso, o tamanho de um pacote poderia se tornar muito grande, também comprometendo o desempenho da rede.

A informação necessária ao rastreamento para a identificação de um atacante deve ser obtida dos pacotes que chegam até a vítima. O procedimento de marcação de pacotes nos roteadores do ambiente de ataque é a forma de obter esta informação. A fim de que não se torne um problema para o tráfego na rede, a marcação deve ser realizada não no conjunto de todos os pacotes trafegando pela rede, porém em uma amostra deste conjunto.

Esta decisão faz surgir uma outra questão a ser resolvida, a saber: quais pacotes deverão ser marcados nos roteadores? Nesta situação é necesário apelar para uma forma de escolha que seja de natureza aleatória. Deste

modo, no elenco de programas para tratamento de pacotes em cada roteador deve ser incluído algum, capaz de selecionar pacotes e neles inserir marcação. Um programa desta natureza deve incluir algum mecanismo probabilístico, sendo p o valor da probabilidade de marcação.

Este procedimento recebe a denominação de "Marcação Probabilística de Pacotes", ou *Probability Packet Marking*, na Língua Inglesa. Essa última acepção deu origem à sigla PPM, através da qual essa abordagem é conhecida.

5.2 Coleta de Dados

A imagem topológica que retrata a situação de um computador sob ataque por negação de serviço, que aparece no Capítulo 4, é igual à figura Figura 5.1 mostrada abaixo.

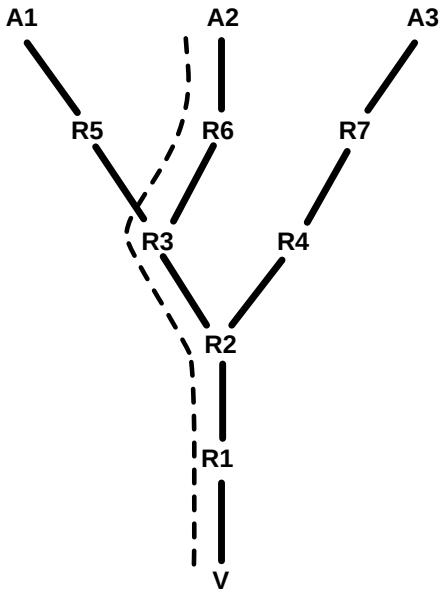

Figura 5.1: Ambiente de Ataque.

O processo de coleta de dados se constitui da gravação do número IP do roteador, em um pacote que está transitando por esse roteador. Supõe-se que o valor da probabilidade, p, seja igual em todos os roteadores do ambiente

de ataque. Desde que a marcação de pacotes ocorre com probabilidade p, se a quantidade total de pacotes trafegando pelo ambiente de ataque é igual a N, então a quantidade de pacotes marcados é igual a $p.N$.

O procedimento da coleta de dados precisa levar em conta os dois aspectos seguintes:

1. Como os pacotes devem ser selecionados;
2. Como os dados oriundos dos roteadores são armazenados.

Ambos os aspectos enmerados são objeto das próximas subseções.

5.2.1 *Seleção dos Pacotes*

O caráter aleatório da PPM pode fazer com que um pacote seja marcado mais de uma vez. À proporção que um pacote se desloca desde a sua origem até alcançar a vítima, o processo de marcação pode ser descrito pelo seguinte algoritmo:

/* Pseudocódigo $PS05 - 0100$ */
Para cada pacote recebido
    Gerar um número aleatório $x \in [0, 1)$
    Se $x < p$ *então*
        Marcar_pacote
    Fim_do_Se
Fim_do_Para

O funcionamento do algoritmo mostrado acima em cada roteador da rede, submete os pacotes que trafegam neste ambiente a uma seqüência de provas, que consiste no sucesso (S), ou fracasso (F), de marcar um pacote. Analisando

a situação da prova à qual cada pacote está submetido, podem ser extraídas da mesma as três propriedades seguintes:

1. Cada prova comporta apenas dois resultados possíveis, isto é, sucesso (S), ou fracasso (F).

2. A probabilidade de sucesso permanece constante em todas as provas.

3. Os resultados das provas são independentes uns dos outros.

Uma situação experimental na qual essas propriedades podem ser identificadas caracteriza o que se costuma denominar de um conjunto de *provas de Bernoulli*, ou um *experimento de Bernoulli*. Apesar da simplicidade da situação, os modelos matemáticos decorrentes desse experimento aleatório básico são largamente aplicáveis em vários ramos do conhecimento, conforme se pode ver em [25], p. 146-155, e [53], p. 145-152.

No caso em questão, a prova que resulta em sucesso corresponde àquela na qual o pacote recebe marcação, sendo considerado fracasso o caso contrário. Por seu turno, qualquer análise destinada à execução do rastreamento reverso deverá ser realizada apenas no subconjunto dos pacotes que recebeu marcação. A quantidade de elementos desse conjunto de pacotes será função da probabilidade p.

Quando um ataque está em curso, a quantidade dos pacotes atacantes deverá ser muito superior àquela dos roteadores do ambiente de ataque. Caso contrário, a situação não será caracterizada como um ataque DoS e não haverá problema a ser resolvido. Além disso, espera-se que o subconjunto dos pacotes que recebem marcação contenha indícios de todos os roteadores que compõem o ambiente de ataque. Esta é uma condição necessária para que seja possível efetuar o rastreamento para a identificação dos atacantes.

O fato de que mais de um pacote possa conter indícios de um mesmo roteador é semelhante à situação que se denomina *amostragem com reposição*. Segundo Feller, em [25], p. 28, *amostragem com reposição* é o processo de

obtenção de dados de uma população no qual o mesmo elemento pode ser selecionado mais de ma vez. Tal é o caso no experimento de marcação de pacotes, quando o mesmo roteador é identificado em mais de um pacote atacante.

Quanto ao desenvolvimento de uma análise que possibilite reconstruir as trajetórias de ataque é necessário que vítima disponha de informação suficiente acerca do ambiente de ataque. Esta informação deverá ser extraída dos dados sobre os roteadores, representados pelas marcações nos pacotes. Surge, então, a seguinte pergunta: qual é a quantidade mínima de informação necessária para que se possa reconstituir as trajetórias de ataque? Traduzindo noutros termos: qual é a quantidade mínima da pacotes marcados que a vítima deve receber, para que seja possível reconstituir as trajetórias de ataque?

Na próxima subseção será tratado o problema da reconstituição de trajetórias de ataque, enquanto a resposta à pergunta anterior ficará para a seção subseqüente.

5.2.2 *Reconstituição de Trajetórias*

Conforme se pode ver na Figura 5.1 uma trajetória de ataque está indicada como uma linha tracejada e pode ser escrita em forma vetorial como $(V, R_1, R_2, R_3, R_6, A)$. A relação de ordem implícita entre os elementos estabelece que, quanto mais à esquerda, mais próximo da vítima se encontra o roteador.

O movimento de um pacote ao longo de uma trajetória de ataque se processa como se o mesmo "saltasse" de um roteador para outro. Isto se deve ao fato de que o roteador é o único elemento da rede que pode perceber a presença de um pacote. Assim, a distância entre dois roteadores, R_λ e R_μ, por exemplo, pode ser medida em "saltos", que é a quantidade de roteadores existentes na trajetória entre os dois roteadores citados, mais um.

O algoritmo mostrado no pseudocódigo $P05 - 0100$ é tal que se podem

inferir sobre a PPM as seguintes propriedades:

1. Os roteadores são independentes no que concerne ao processo de marcação;
2. Cada pacote de mensagem pode ser, ou não, marcado;
3. A probabilidade de marcação, p, é a mesma em todo o ambiente de ataque.

Segundo o comentário na subseção 5.2.1, essas propriedades fazem do processo de marcação um experimento de Bernoulli. A conseqüência imediata desse fato é que, a probabilidade da vítima receber um pacote que tenha sido marcado por um roteador, que esteja a uma distância d da mesma, deve atender a duas condições:

1. A probabilidade de o pacote receber marcação em um roteador distante d-saltos da vítima é igual a p;
2. A probabilidade de o pacote não receber qualquer marcação nos $(d-1)$ roteadores restantes da trajetória é igual a $(1-p)^{d-1}$.

Logo, a função que resume as duas condições acima é dada pela expressão

$$f(d) = p(1-p)^{d-1}. \tag{5.1}$$

Como se pode ver, neste caso a seqüência de provas Bernoulli possui d elementos com apenas um sucesso e $(d-1)$ fracassos.

Observando a expressão da função (5.1) conclui-se trivialmente que a mesma é monótona decrescente [31] e essa monotonicidade permite estabelecer uma ordem parcial entre os roteadores. Por outro lado, o escalonamento dos roteadores de modo decrescente, tomando como referência a quantidade de pacotes que é recebida de cada um dos mesmos, permite construir uma tabela de freqüências. Desde que p é constante, à proporção que cresce a

distância do roteador até à vítima, d, o valor de $f(d)$ se reduz.

Assim, quanto maior for a freqüência associada a um roteador, mais próximo o mesmo se encontra da vítima. Logo, a reconstituição de trajetórias de ataque equivale à identificação de todos os conjuntos de roteadores que mantêm entre si, em cada conjunto, uma relação de ordem total.

Contudo, convém avaliar o grau de complexidade computacional presente nesse processo de reconstituição das trajetórias de ataque. Desde que todos os roteadores do ambiente de ataque estão representados nas marcações de pacotes, considerem-se $N_1, N_2, \ldots, N_d$ as quantidades desses pacotes marcados às distâncias $1, 2, \ldots, d$. Então a quantidade de trajetórias possíveis de serem construídas é dada pela expressão $T_0(N_1, N_2, \ldots, N_d) = N_1.N_2 \ldots N_d$.

A topologia do ambiente de ataque, conforme a Figura 5.1, sugere que a função $T_0(N_1, N_2, \ldots, N_d)$ se encontre na categoria das funções de complexidade fatorial, isto é, $T_0(N_1, N_2, \ldots, N_d) \in O(n!)$. A situação mais simples seria aquela na qual existisse somente uma trajetória a ser reconstruída e, nesse caso $T_0(N_1, N_2, \ldots, N_d) \in O(1)$).

A próxima seção tratará dos aspectos inerentes ao método de amostragem dos pacotes.

5.3 A Amostragem de Pacotes

Na subseção 5.2.1 foi formulada uma questão referente à quantidade mínima de pacotes marcados que a vítima deve receber, para que seja possível reconstituir as trajetórias de ataque. Uma vez que qualquer roteador pode marcar mais de um pacote fica caracterizado que o processo de amostragem é com repetição. O processo de amostragem com repetição aparece em diversas situações de natureza prática, quando falha a hipótese de independência entre os dados. Em tais circunstâncias, surge a necessidade do uso de técnicas apropriadas para a aquisição de dados.

Um interessante exemplo de uma situação de amostragem com repetição

é aquela ilustrada pelo clássico *Problema do Coletor de Cupons*, conhecido em Língua Inglesa pela denominação *Coupon Collector's Problem*, ou CCP.

Esse problema é apresentado aqui por meio de uma alegoria. Com efeito, o que se deseja é obter todos os N diferentes cupons de uma coleção que são distribuídos, com probabilidade p, como brindes no interior de caixas de cerais. Ao adquirir uma caixa, a priori o comprador não sabe se haverá cupom no seu interior, e mesmo que exista algum, também não sabe se será repetido. A questão central é determinar a quantidade mínima de caixas que devem ser adquiridas, de modo que a coleção de cupons possa ser completada. A resposta a essa questão exige algumas considerações de natureza teórica, apresentadas a seguir.

5.3.1 *Uso do Problema do Coletor de Cupons*

Nesta seção será mostrado como a marcação probabilística de pacotes pode ser modelada de acordo com a metodologia do problema do coletor de cupons. A fim de adequar esse Problema ao processo de marcação probabilística de pacotes será considerada uma alegoria como exemplo adequado para esta situação.

Considere-se um dispositivo formado por uma mesa possuindo diversos buracos no seu tampo, tendo um saco sob cada um dos buracos. Nesse dispositivo se pode praticar um jogo de arremesso de bolas, cujo objetivo é atingir os buracos. A cada arremesso de uma bola em direção a um buraco existem dois resultados possíveis, a saber:

1. A bola atinge o buraco, o que representa um sucesso.
2. A bola não atinge qualquer buraco, o que representa um fracasso.

Supondo que seja p a probabilidade de acertar um buraco, o que se deseja é estimar a quantidade mínima de bolas a ser arremessada, de modo que

cada um dos buracos seja atingido, pelo menos, por uma bola. Não há limite estabelecido para a quantidade disponível de bolas a ser arremessada.

Aplicando o princípio do arremesso das bolas nos buracos, ao cenário de um ataque do tipo DoS, pode-se associar os pacotes às bolas e os roteadores aos buracos. O fato de uma bola arremessada cair num buraco, se assemelha a um pacote que pode ser marcado em um roteador. As bolas que não caíram em algum buraco correspondem aos pacotes não marcados.

5.3.2 *Aspectos do Modelo*

O movimento de um pacote em uma trajetória com d roteadores, com o eventual registro da marcação de um pacote, pode ser representado por uma seqüência, formada pelos símbolos extraídos do conjunto F, S, posicionados lado-a-lado de modo que representem a ordem crescente da distância à vítima, a partir da extremidade esquerda da seqüência. Estes símbolos são utilizados para representar, respectivamente, as situações de fracasso(F), ou sucesso (S), de um determinado roteador marcar um pacote com probabilidade p.

Devido à natureza do experimento, qualquer seqüência poderá conter, no máximo, uma ocorrência do símbolo S. Neste caso, a posição do sucesso entre os elementos da seqüência indica a distância a que o roteador, que marcou o pacote, se encontra da vítima. Assim, esse processo de marcação de pacotes se caracteriza como um subconjunto de um experimento de Bernoulli, no qual ocorre um sucesso e $(d-1)$ fracassos. Isso significa que, no conjunto Ω dos pacotes que chega até a vítima, identificam-se dois subconjuntos, Ω_F, dos pacotes sem marcação, e Ω_S, dos pacotes com uma marcação. Estes conjuntos são tais que

- $\Omega_S \cup \Omega_F = \Omega$;
- $\Omega_S \cap \Omega_F = \emptyset$.

Em virtude de satisfazerem as propriedades acima, diz-se que os dois subconjuntos formam uma *partição* do conjunto Ω. Tomando todas as possíveis seqüências oriundas do experimento de Bernoulli com d elementos, sabe-se que a probabilidade de ocorrerem as seqüências com apenas um sucesso é dada por $d.p.(1-p)^{d-1}$, segundo [31]. Essa é a probabilidade de os d roteadores da trajetória de ataque poderem ser escolhidos para a marcação.

Considere-se a variável aleatória $X : \Omega \rightarrow N$, que associa a cada pacote recebido a quantidade de experimentos de Bernoulli necessárias para a obtenção de um sucesso [35]. Pela própria definição pode-se ver que $X(\omega)\epsilon N$, para $\omega \, \epsilon \, \Omega$, o que caracteriza X como uma variável aleatória discreta e não-negativa, com valores inteiros. Assim, dizer que $k = X(\omega)$ significa que o pacote ω foi marcado em um roteador que fica a uma distância k da vítima. A expressão da função de massa de probabilidade da variável aleatória X é dada por

$$p_X(k) = p.(1-p)^{k-1}, \tag{5.2}$$

pois a mesma se comporta de acordo com a distribuição geométrica. Observe-se que o parâmetro da distribuição é o valor p, isto é, a probabilidade de que ocorra um sucesso em um experimento de Bernoulli, ou seja, a marcação de um pacote por um roteador.

Para determinar quantos pacotes precisam ser utilizados na reconstituição da trajetória de ataque é necessário extrair uma amostra, com repetição, que contenha r elementos distintos. Para a determinação do tamanho da amostra que contenha r elementos distintos, denominada S_r, deve-se ter em mente o seguinte fato. Chamando S_{r+1} o tamanho da amostra necessário para se obter $(r+1)$ elementos distintos, então a variável

$$X_r = S_{r+1} - S_r \tag{5.3}$$

representa a quantidade de extrações necessárias de serem realizadas na população para se obter o $(r+1)$-ésimo elemento distinto, quando já existem

r elementos distintos. Em conseqüência $X_r - 1$ representará a quantidade de extrações realizadas na população depois de existirem r elementos distintos e antes de existirem $(r + 1)$ elementos também distintos, conforme [25].

Decorre da definição da variável X_r que

$$\begin{aligned} S_{r+1} &= S_r + X_r \\ &= S_{r-1} + X_{r-1} + X_r \\ &\vdots \\ &= S_1 + X_1 + X_2 + \ldots + X_{r-1} + X_r. \end{aligned} \tag{5.4}$$

A reconstituição parcial necessita que se obtenham exemplares dos pacotes atacantes com marcações distintas, correspondendo a cada um dos os roteadores que compõem essa parte da trajetória.

A variável S_k também pode ser interpretada como a quantidade de pacotes necessários de serem obtidos, para que sejam representados na vítima todos os pacotes da trajetória que vai até o k-ésimo roteador.

Desde que S_1 é a quantidade de extraçôes para que se obtenha o primeiro sucesso, e este ocorre justamente quando se obtém o primeiro elemento da amostra, quando ainda não pode haver repetição, conclui-se que $S_1 = 1$. Desse modo, a expressão para S_r pode ser escrita como segue:

$$S_r = 1 + X_1 + X_2 + \cdots + X_{r-1}, \tag{5.5}$$

Uma vez que se considere toda a trajetória, que tem comprimento d, sabe-se de (5.5) e do Apêndice B que o valor esperado para S_d satisfaz a expressão:

$$E[S_d] \leq d.(\ln d + O(1)). \tag{5.6}$$

Durante o período do ataque, a vítima recebe uma determinada quantidade de pacotes, representada por uma variável aleatória discreta $Y : \Omega \to N$. Da definição de S_d pode-se escrever que

$$E[S_d] = d.p.(1 - p)^{d-1}.E[Y]. \tag{5.7}$$

Substituindo (5.6) em (5.7), obtém-se a importante relação abaixo, prognosticada no trabalho de Savage, vide [51], isto é:

$$E[Y] \leq \frac{\ln d}{p.(1-p)^{d-1}}. \tag{5.8}$$

A relação mostrada em (5.8) é um limite superior para a quantidade de pacotes que deve ser recebida, de modo que possa ser garantida a representatividade da amostra, na reconstrução da trajetória de ataque. A tabela 1, conforme [57], mostra exemplos para essa razão limitante, considerando três valores distintos para a probabilidade de marcação p e trajetórias tendo comprimento $d \leq 10$.

Tabela 1 - Razão Limitante

d	p = 0,020	p = 0,100	p = 0,300
1	0,0	0,0	0,0
2	35,4	7,7	3,3
3	57,2	13,6	7,5
4	73,6	19,0	13,5
5	87,2	24,5	22,3
6	99,1	30,0	35,5
7	109,8	43,5	84,2
8	119,8	43,5	84,2
9	129,1	51,0	127,0
10	138,1	59,4	190,2

Algumas considerações teóricas adicionais podem ser encontradas no Apêndice E.

A principal contribuição do presente capítulo se concentra na formalização de alguns resultados de natureza matemática, utilizados pelos autores do artigo da referência [51]. Esta formalização pode servir como um balizamento a novas contribuições ao estudo do problema do rastreamento reverso.

Capítulo 6

Dimensionamento de Informação de Bit para o Rastreamento Reverso

A utilização da marcação probabilística de pacotes tem se mostrado uma interessante alternativa para encontrar a solução do problema do rastreamento reverso, desde a vítima até uma fonte anônima de ataque. Neste processo merece especial atenção a quantidade de bits que precisa ser alocada no cabeçalho TCP/IP para a finalidade da marcação de um pacote, pois o campo que eles formam deverá armazenar algum indício dessa trajetória.

Este capítulo trata do assunto apresentado no artigo de Mikah Adler, cujas referências são [1, 44], e que aborda a importância da quantidade desses bits no processo de marcação de pacotes. Além de levar em conta aspectos da Teoria da Codificação, o protocolo sugerido neste processo de marcação também utiliza alguns interessantes resultados relativos a limites de desigualdades de natureza probabilísticas.

6.1 Aspectos Preliminares

A Teoria da Informação estabelece que um vetor contendo b bits, possui a capacidade de representar até 2^b mensagem distintas, uma de cada vez,

conforme pode ser visto em [2, 8, 56]. Se o cabeçalho de um pacote é munido de um campo com tamanho de b bits, que é destinado a conter marcações que identifiquem trajetórias de ataque, então este campo poderá identificar até 2^b trajetórias distintas, cada uma delas representada por um número binário. Assim, o conjunto de pacotes que a vítima recebe é um elemento do conjunto de todos os 2^{2^b} possíveis subconjntos com trajetórias distintas.

Sabe-se do Capítulo 4 que, de acordo com a visão topológica da vítima, o ambiente de ataque é representado como uma árvore, na qual a vítima se encontra anexada à raiz. Por sua vez, também sabe-se que uma árvore qualquer pode ser transformada em uma árvore binária. Considerando a representação do ambiente de ataque na forma de uma árvore binária, cuja altura é igual a n, existem no máximo 2^n trajetórias de ataque possíveis de serem utilizadas, por atacantes que se encontram a uma distância de n saltos da vítima.

A fim de que seja possível identificar cada trajetória de ataque, com probabilidade igual a p, é necessário que a seguinte desigualdade seja satisfeita:

$$2^{2^b} \geq 2^n p. \tag{6.1}$$

Procedendo ao desenvolvimento da expressão 6.1, obtém-se

$$log_2\, 2^{2^b} \geq log_2\, 2^n p$$

$$\Rightarrow 2^b \geq n + log_2\, p,$$

donde finalmente se deduz que

$$b \geq log_2\,(n + log_2\, p). \tag{6.2}$$

Sendo b um número que representa a quantidade de bits em um campo do cabeçalho TCP/IP, então deve ser inteiro positivo. Logo, pode-se também escrever a expressão (6.2) como segue:

$$b = \lceil log_2\,(n + log_2\, p) \rceil. \tag{6.3}$$

Convém neste ponto comentar o significado da probabilidade p na expressão (6.2). Sabe-se da teoria que p se encontra no intervalo $[0, 1] \subset \mathbb{R}$.

Naturalmente, deve-se excluir a possibilidade de considerar o seu valor como sendo igual a zero pois, na prática, esse fato significaria a não existência da possibilidade de se marcar qualquer pacote, decorrendo daí a falência do método para reconstruir a trajetória de ataque.

Desde que a função logaritmo é monotonamente crescente o valor de $log_2\, p$ crescerá à proporção que o valor de p varia de zero até um. Isso implica em que o valor de $(n + log_2\, p)$ também crescerá de modo que, quando $p = 1$, o valor de b será igual a $log_2\, n$. Esse é o menor valor de b capaz de contemplar todas as possíveis variações que podem ser experimentadas pela probabilidade p. Significa que, a quantidade de b bits é suficiente para atender aos propósitos de marcação de pacotes.

Por outro lado, o fato de que $p = 1$ retrata a situação extrema na qual todos os roteadores marcariam todos os pacotes, com o risco de ocorrer uma sobrecarga no esforço computacional. Assim, convém escolher um valor para p capaz de permitir a obtenção de uma amostra representativa, sem os riscos de comprometer o tráfego na rede. Esse é o paradigma que predomina nos esquemas de rastreamento reverso propostos nos protocolos anteriores ao trabalho de Adler.

A abordagem proposta em [1, 44] apresenta uma nova nova técnica de marcação de pacotes enviados por uma mesma trajetória. Como se verá adiante, um dos aspectos mais interessantes dessa técnica é que a mesma pode ser efetiva ainda quando se tenha $b = 1$, isto é, a quantidade de bits reservados para a marcação de pacotes é igual a 1. Segundo o autor, neste caso existe uma contrapartida, que é a exagerada quantidade de pacotes necessária para a reconstrução da trajetória de ataque. Essa quantidade é representada por uma função de n, que se encontra na classe $O(2^{2n})$. O fato de esse protocolo ser bastante simples para ser utilizado na prática estimulou o estudo do caso em que os pacotes são enviados através de diversas trajetórias.

Nas próximas seções os detalhes da concepção do protocolo serão apresentados.

6.2 Características Simplificadoras

Conforme afirmado na seção 6.1, a topologia do ambiente de ataque se assemelha a uma árvore, cujo nó raiz é ligado à vítima. Os ataques são provenientes das folhas da árvore, de acordo com a estratégia do atacante.

Para a descrição dos aspectos do protocolo são formuladas algumas hipóteses simplificadoras, que posteriormente serão relaxadas, para dar maior robustez ao modelo. As hipóteses simplificadoras são declaradas nos ítens a seguir:

1. A árvore do ambiente de ataque é binária completa, com altura n. A vítima se encontra em um nó adicional ligado à raiz.

2. Cada nó diferente de uma folha é capaz de determinar de qual nó filho veio o pacote recebido.

3. A vítima tem pleno conhecimento da topologia do ambiente de ataque.

Apesar de parecer bastante restritiva, a primeira hipótese se faz necessária no momento, a fim de que se possa desenvolver as idéias do protocolo. A garantia única acerca do ambiente de ataque é que o mesmo tem a forma de árvore e que a vítima se posiciona em um nó adicional à raiz desta árvore. Cada pacote que é enviado do atacante para a vítima tem os valores dos b bits previamente definidos. No entanto, os nós intermediários podem alterar estes valores, via o processo de marcação.

Além dessa forma de comunicação entre os nós, nenhuma outra ocorre, bem como não há qualquer informação sobre o estado de algum nó intermediário. De fato, essa característica de ser um canal sem memória é típica da Internet, pois os nós intermediários não possuem memória, ao contrário do que ocorre com a vítima.

6.2.1 *Representação da Trajetória de Ataque*

Ao longo de uma trajetória de ataque a localização de qualquer nó é estabelecida com referência à posição da vítima. Desde que um pacote se desloca como se saltasse de um nó para outro, a distância de um nó até a vítima é medida em *saltos*, ou seja, conta-se a quantidade de nós existentes entre o nó, cuja distância se deseja avaliar, e a vítima. Adicionando-se uma unidade a esta quantidade de nós obtém-se a distância procurada.

Para a finalidade de desenvolvimento do assunto, o nó que se encontra a uma distância de k saltos da vítima será identificado pelo símbolo N_k. As hipóteses formuladas anteriormente permitem estabelecer como sendo N_0 a identificação da vítima, enquanto um atacante, que se encontra em uma folha da árvore, será denotado como N_{n+1}.

Cada pacote enviado pelo atacante para a vítima contém um campo com b-bits, cujos valores são originalmente definidos pelo atacante. No entanto, qualquer um dos nós intermediários pode alterar estes valores e nenhuma outra forma de comunicação existe entre os nós.

O processo de marcação probabilística de pacotes, que produz alterações no campo com b-bits destinado à marcação, leva em conta dois aspectos. O primeiro decorre da hipótese simplificadora segundo a qual um nó sabe de que filho veio o pacote, enquanto o outro depende apenas de um procedimento aleatório.

A árvore do ambiente de ataque é supostamente binária completa de altura n, de modo que o conteúdo do campo com b-bits forma uma cadeia binária, $B = B_1B_2 \ldots B_N$, que representa uma trajetória de ataque. Esta trajetória pode ser percorrida a partir da vítima a fim de se encontrar o atacante, desde que se leve em conta as seguintes regras, em cada nó N_k:

- $B_k = 0$, se a trajetória veio do filho à esquerda de N_k.
- $B_k = 1$, se a trajetória veio do filho à direita de N_k.

No caso em que o atacante escolher uma folha como ponto incial do ataque, a cadeia B identifica de modo único este ponto, desse modo resolvendo o problema do rastreamento reverso do número IP. Por outro lado, se o atacante escolher como ponto inicial do ataque um nó que não é uma folha da árvore, ele pode definir os valores dos bits iniciais do pacote, de modo a simular que o ataque provém de uma folha qualquer da árvore. Neste caso, a trajetória pareceria se estender além da sua origem verdadeira.

6.3 Protocolo para Única Trajetória de Ataque

Nesta seção se fará a suposição de que todos os pacotes de um ataque do tipo DoS sejam enviados para a vítima ao longo de uma mesma trajetória. Com o propósito de desenvolver um raciocínio de progressiva complexidade, a situação inicialmente considerada é aquela em que, o campo para marcação existente em cada pacote possui apenas um único bit, ou seja, $b = 1$.

De maneira análoga ao que foi apresentado na subseção 6.2.1, a cadeia binária, B, que neste caso terá apenas um único bit, deverá ser construída de modo que seja a representação da trajetória de ataque. Deve-se ter em conta que o atacante insere um conteúdo inicial no bit de marcação de um pacote, no momento de seu envio.

A idéia expressa por Micah Adler, nos seus trabalhos referidos em [1, 44], sugere que se poderá construir uma cadeia binária representando a trajetória de ataque a partir do número que indica a probabilidade p, de que a vítima receba pacotes com o bit de marcação contendo 1. O cálculo de uma estimativa do valor de p é simples de ser realizado. Basta calcular a razão entre a quantidade de pacotes recebidos com o bit de marcação contendo 1 e a quantidade total de pacotes recebidos. Contudo, antes de prosseguir com essa idéia, convém estabelecer os fundamentos que a tornam válida sob o

ponto de vista matemático.

6.3.1 *Alguns Resultados Importantes*

Considere-se um nó que pertence ao ambiente de ataque, cuja imagem se encontra apresentada na Figura 6.1.

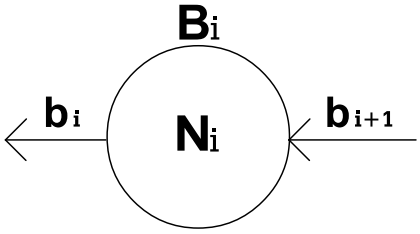

Figura 6.1: Nó do Ambiente de Ataque.

Como se pode ver, na Figura 6.1, o nó N_i possui um bit que lhe é inerente, B_i, em conseqüência da construção da árvore binária completa que compõe o ambiente de ataque. No que concerne ao tráfego de pacotes, por sua vez, devem ser considerados os bits, b_{i+1} e b_i, mostrados na figura. O bit b_{i+1} representa o bit de marcação encontrado no pacote que chega a N_i. Por sua vez, o bit b_i representa o bit de marcação depois que o pacote foi enviado pelo nó N_i.

Uma vez que os bits B_i e b_{i+1} podem ter conteúdos variados, naturalmente pertencentes ao conjunto $\{0, 1\}$, o conteúdo de b_i será determinado por meio de algum procedimento de natureza aleatória. Tal procedimento é semelhante a um experimento que consiste em lançar uma moeda para o alto e depois observar qual face ficou para cima, cuja descrição é mostrada no pseudocódigo a seguir:

/* Pseudocódigo $PS06 - 0100$ */
Se "cara"então
$b_i \leftarrow b_{i+1}$
Senão

$$b_i \leftarrow B_i$$

Fim_do_Se

O caráter aleatório do procedimento utilizado para a determinação do conteúdo de b_i traz à luz a necessidade de definir probabilidades, para cada um dos estados em que pode se encontrar o bit de marcação. Assim, define-se

$$p_{i+1} = \text{Prob}\{\text{conteúdo de } b_{i+1} = 1\}$$

e

$$p_i = \text{Prob}\{\text{conteúdo de } b_i = 1\}.$$

O que se pretende é a construção de uma cadeia de bits capaz de representar a trajetória de ataque. Deve ser levado em conta que a probabilidade de a vítima receber pacotes com bit de marcação igual a 1 é igual a p. Neste ponto, convém demonstrar um importante resultado envolvendo as probabilidades sucessivas do bit de marcação.

Lema 6.1. *Sendo p_{i+1} e p_i definidos como acima, e considerando o protocolo no pseudocódigo $PS06 - 0100$, então é válido dizer que*

$$p_i = B_i.\left(\frac{1}{2}\right) + \frac{p_{i+1}}{2}.$$

Demonstração. A fim de facilitar o desenvolvimento da demonstração, as definições das probabilidades p_{i+1} e p_i serão simplificadas para $p_{i+1} = \text{Prob}\{b_{i+1} = 1\}$ e $p_i = \text{Prob}\{b_i = 1\}$. Da Teoria da Probabilidade tem-se a expressão seguinte:

$$\begin{aligned}
\text{Prob}\{b_i = 1\} &= \text{Prob}\{b_i = 1 \text{ e } b_{i+1} = 0\} + \text{Prob}\{b_i = 1 \text{ e } b_{i+1} = 1\} \\
&= \text{Prob}\{b_{i+1} = 0\}.\text{Prob}\{b_i = 1 | b_{i+1} = 0\} \\
&+ \text{Prob}\{b_{i+1} = 1\}.\text{Prob}\{b_i = 1 | b_{i+1} = 1\} \\
&= (1 - p_{i+1}).\text{Prob}\{b_i = 1 | b_{i+1} = 0\} \\
&+ p_{i+1}.\text{Prob}\{b_i = 1 | b_{i+1} = 1\}. \qquad (6.4)
\end{aligned}$$

De acordo com o pseudocódigo $PS06-0100$, o valor de cada uma das duas probabilidades condicionais dependerá do conteúdo do bit B_i. Com efeito, observem-se as duas situações distintas e complementares apresentadas a seguir.

- Caso $B_i = 0$, então $\text{Prob}\{b_i = 1 | b_{i+1} = 0\} = 0$, pois qualquer que seja o resultado do lançamento da moeda o bit b_i sempre será marcado com o valor 0. Por outro lado, $\text{Prob}\{b_i = 1 | b_{i+1} = 1\} = (1/2)$, pois o conteúdo de b_i poderá ser 0 ou 1, dependendo apenas do resultado do lançamento da moeda. Logo, pode-se escrever

$$p_i = (1 - p_{i+1}).0 + p_{i+1}.(1/2) = (p_{i+1}/2).$$

- Caso $B_i = 1$, então $\text{Prob}\{b_i = 1 | b_{i+1} = 0\} = (1/2)$, pois o conteúdo de b_i poderá ser 0 ou 1, dependendo apenas do resultado do lançamento da moeda. Por outro lado, $\text{Prob}\{b_i = 1 | b_{i+1} = 1\} = 1$, visto que o conteúdo de b_i será sempre igual a 1, ficando independente do lançamento da moeda. Logo, pode-se escrever

$$p_i = (1 - p_{i+1}).(1/2) + p_{i+1}.1 = (1/2) + (p_{i+1}/2).$$

Compondo as duas expressões anteriores para p_i em uma única, juntamente com o valor do conteúdo de B_i, facilmente conclui-se que

$$p_i = B_i.\left(\frac{1}{2}\right) + \frac{p_{i+1}}{2}.$$

□

No aspecto dinãmico resultante do protocolo sugerido para no processo de marcação de pacotes existe o predomínio da simplicidade. Contudo, deve-se levar em conta o fato de que o conteúdo inicial do bit de marcação do pacote é estabelecido pelo atacante. O próximo teorema apresenta um importante resultado, a partir do qual se tem uma ferramenta para a execução do rastreamento reverso.

Teorema 6.1. *Considerem-se uma trajetória de ataque de comprimento* n *e* $p = Prob\{$*vítima receber um pacote cujo bit de marcação contém 1*$\}$*. Então, ocorrerá uma das duas situações seguintes:*

- *Se o conteúdo inicial do bit de marcação do pacote contém* 0*, então*

$$p = \sum_{i=1}^{n} B_i.\left(\frac{1}{2}\right)^i;$$

- *Se o conteúdo inicial do bit de marcação do pacote contém* 1*, então*

$$p = \left(\frac{1}{2}\right)^n + \sum_{i=1}^{n} B_i.\left(\frac{1}{2}\right)^i.$$

Demonstração. Sendo N_n o último nó da trajetória de ataque, o mesmo recebe um pacote do atacante, cujo bit de marcação é denominado b_{n+1}. Segundo essa mesma notação, define-se $p_{n+1} = \text{Prob}\{\text{conteúdo de } b_{n+1} = 1\}$.

- Se o conteúdo de b_{n+1} é igual a 0, então $p_{n+1} = 0$. A partir do lema 6.1 pode-se escrever o seguinte:

$$p_n = B_n.\left(\frac{1}{2}\right) + \frac{p_{n+1}}{2} = B_n.\left(\frac{1}{2}\right).$$

De modo análogo, tem-se

$$p_{n-1} = B_{n-1}.\left(\frac{1}{2}\right) + \frac{p_n}{2} = B_{n-1}.\left(\frac{1}{2}\right) + B_n.\left(\frac{1}{2}\right)^2$$

$$p_{n-2} = B_{n-2}.\left(\frac{1}{2}\right) + \frac{p_{n-1}}{2} = B_{n-2}.\left(\frac{1}{2}\right) + B_{n-1}.\left(\frac{1}{2}\right)^2 + B_n.\left(\frac{1}{2}\right)^3.$$

Em cada uma das expressões é fácil ver que a soma entre o índice da probabilidade à esquerda do sinal de igualdade, com o expoente do último termo à direita, é sempre igual a $(n + 1)$. De acordo com a Figura 6.1, a probabilidade de a vítima receber um pacote com bit de marcação contendo 1 é denotada como sendo p_1. Neste caso, o expoente

do termo mais à direita da expressão para essa probabilidade deve ser igual a n, donde se conclui que

$$\begin{aligned} p_1 &= B_1.\left(\frac{1}{2}\right) + B_2.\left(\frac{1}{2}\right)^2 + \ldots + B_{n-1}.\left(\frac{1}{2}\right)^{n-1} + B_n.\left(\frac{1}{2}\right)^n \\ &= \sum_{i=1}^{n} B_i.\left(\frac{1}{2}\right)^i \end{aligned}$$

- Por outro lado, Se o conteúdo de b_{n+1} é igual a 1, então $p_{n+1} = 1$. Novamente o lema 6.1 permite escrever a expressão seguinte:

$$p_n = B_n.\left(\frac{1}{2}\right) + \frac{p_{n+1}}{2} = B_n.\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right).$$

De modo análogo ao raciocínio para o caso anterior pode-se constatar que, o cálculo de cada novo valor da probabilidade, p_k, envolve o acréscimo de um termo da forma $B_k.\left(\frac{1}{2}\right)$, bem como multiplica por $(1/2)$ o valor anterior da probabilidade, p_{k+1}. A aplicação de subtituições sucessivas permite que se obtenha o valor de p_1 como sendo

$$\begin{aligned} p_1 &= B_1.\left(\frac{1}{2}\right) + B_2.\left(\frac{1}{2}\right)^2 + \ldots + B_{n-1}.\left(\frac{1}{2}\right)^{n-1} + B_n.\left(\frac{1}{2}\right)^n + \left(\frac{1}{2}\right)^n \\ &= \left(\frac{1}{2}\right)^n + \sum_{i=1}^{n} B_i.\left(\frac{1}{2}\right)^i \end{aligned}$$

□

O teorema 6.1 anterior mostra de maneira clara como se pode proceder para representar uma trajetória de ataque, a partir do valor da probabilidade de a vítima receber um pacote com o bit de marcação contendo 1. Contudo, não se pode garantir unicidade nessa representação, visto que a mesma depende do conteúdo inicial do bit de marcação. Na verdade, a diferença entre as duas expressões se encontra apenas no termo $(1/2)^n$, cujo valor tende a ser pequeno, à proporção que n cresce.

Ainda segundo Adler, em [1, 44], existe um modo simples a partir do qual, com elevada probabilidade, se pode construir uma cadeia de bits única que representará a trajetória de ataque.

6.3.2 *Construção da Cadeia*

Os resultados da subseção 6.3.1 permitem relacionar a probabilidade p com o valor de cada bit B_i, inerente a um nó N_i. Decorre daquela teoria que, a cadeia binária que representa a trajetória de ataque será construída por meio da conversão do valor da probabilidade p para binário. Para isso é preciso reduzir a incerteza na obtenção dos elementos que comporão essa cadeia. De fato, o teorema 6.1 estabelece que a cadeia binária determinada a partir dessa conversão depende do conteúdo inicial do bit de marcação e, portanto, não é única.

Nesta subseção será apresentada uma proposta para a redução desta incerteza, conforme elaborada por Adler e encontrada em [1, 44], que se baseia em um processo cuja fundamentação é mostrada no lema a seguir.

Lema 6.2. *Considerem-se um conjunto de bits,* $B_1, \ldots, B_\lambda$*, e um protocolo pelo qual a vítima é capaz de determinar números* p*,* σ *e* $c_1, \ldots, c_\lambda$*, pertencentes ao conjunto* $\{x \in \mathbb{R} | 0 \leq x \leq 1\}$*, que satisfazem às seguintes condições:*

1. $|p - \sum_{j=1}^{\lambda} c_j.B_j| \leq \sigma$.
2. *Para todos os* $1 \leq i \leq (\lambda - 1)$, $c_i > 2\sigma + \sum_{j=i+1}^{\lambda} c_j$.
3. $c_\lambda > 2\sigma$.

Então, por meio desses números reais a vítima será capaz de determinar os bits $B_1, \ldots, B_\lambda$*, de maneira única.*

Demonstração. A primeira condição estabelece que o valor da probabilidade é aproximado pela combinação de bits, tanto quanto seja desejado. O somatório mostrado ali reflete a representação de um número fracionário na base binária visto que, pela segunda condição, qualquer c_i é superior à soma de todos os outros restantes. Por fim a terceira condição estabelece que o último componente do número fracionário é maior do que zero. A estratégia

da demonstração se baseia no fato de que, caso a vítima conheça $B_1, \ldots, B_{i-1}$, para qualquer $1 \leq i \leq (\lambda - 1)$, então ela poderá determinar B_i. Para tanto, define-se $p\prime = p - \sum_{j=1}^{i-1} c_j B_j = \sum_{j=i}^{\lambda} c_j B_j$. Da primeira condição tem-se que

$$|p - \sum_{j=1}^{\lambda} c_j.B_j| \leq \sigma$$

$$\Rightarrow |(p - \sum_{j=1}^{i-1} c_j.B_j) - \sum_{j=i}^{\lambda} c_j.B_j| \leq \sigma$$

$$\Rightarrow |p\prime - \sum_{j=i}^{\lambda} c_j.B_j| \leq \sigma$$

$$\Rightarrow p\prime - \sum_{j=i}^{\lambda} c_j.B_j \geq -\sigma$$

$$\Rightarrow p\prime = \sum_{j=i}^{\lambda} c_j.B_j - \sigma = c_i.B_i + \left(\sum_{j=i+1}^{\lambda} c_j.B_j \right) - \sigma \geq c_i.B_i - \sigma.$$

Naturalmente, se $p\prime \geq c_i - \sigma$ então este deve ser o caso em que $B_i = 1$. Por outro lado, caso se constate que $p\prime \leq c_i - \sigma$, então este deve ser o caso em que $B_i = 0$. Assim, os valores de B_i podem ser determinados através de um "método guloso", começando com B_1 e prosseguindo bit-a-bit até o B_λ. □

No pseudocódigo $PS06 - 0200$ vê-se um algoritmo, denominado DECODE, que pode ser usado determinação dos elementos da cadeia, conforme sugerido por Adler em [1, 44]. Apesar do seu aspecto simples e objetivo, o algoritmo DECODE sofre a influência do viés causado pelo conteúdo inicial do bit de marcação. A fim de neutralizar este efeito nocivo dentro de limites de erro aceitáveis, as referências [1, 44] sugerem um interessante procedimento. Considerando um nó genérico N_i, as probabilidades associadas com o mesmo, no envio de bits, serão as seguintes:

- A probabilidade de enviar o bit B_i é sempre igual a $(1/2)$.
- A probabilidade de enviar um bit 1 recebido de N_{i+1} é igual a $(1/2 - \epsilon)$, sendo ϵ uma constante tal que $0 < \epsilon < (1/2)$.

- A probabilidade de enviar um bit 0 recebido de N_{i+1} é igual a ϵ).

/* Pseudocódigo $PS06 - 0200$ */
DECODE$(p, \sigma, c_1, \ldots, c_\lambda)$
Se $p \geq c_1 - \sigma$ *então*
$A_1 \leftarrow 1$
Senão
$A_1 \leftarrow 0$
Fim_do_Se
Para $i = 2, \ldots, \lambda$
$p\prime \leftarrow p - \sum_{j=1}^{i-1} c_j.A_j$
Se $p\prime \geq c_i - \sigma$ *então*
$A_1 \leftarrow 1$
Senão
$A_1 \leftarrow 0$
Fim_do_Se
Fim_do_Para
Retorna $\{A_1, \ldots, A_\lambda\}$

Considerando $r = (1/2) - \epsilon$ para fins de simplificação e δ, um número tal que $0 \leq \delta \leq 1$, um parâmetro do protocolo para delimitar a probabilidade, o **Protocolo de Bit Único** é definido como segue:

- Obter um amostra com $F = \frac{6.ln(2/\delta)}{\epsilon^2.r^{2n}}$ pacotes.
- Obter x, a quantidade de pacotes da amostra com bit de marcação contendo 1.
- Calcular a estimativa da probabilidade, dada pela expressão $p = x/F - r^n/2$.
- Calcular o valor de σ, dado pela expressão $\sigma = r^n/2 + \epsilon.r^n$.

- Retornar $\{A_1, \ldots, A_n\}$ =DECODE$(p, \sigma, \frac{1}{2}, \frac{r}{2}, \frac{r^2}{2}, \ldots, \frac{r^{n-1}}{2})$.

Apesar de o protocolo de bit único se apresentar como uma alternativa para a solução do problema do rastreamento reverso, torna-se necessário demonstrar a sua validade. Antes de proceder a qualquer demonstração, no entanto, convém estabelecer a seguinte

Definição 6.1. *Para $t \in \{0, 1\}$, chama-se p_i^t à probabilidade de que o nó N_i receba um bit de marcação contendo* 1*, dado que o atacante estabeleceu como sendo t o conteúdo inicial desse bit.*

O lema 6.3, a seguir, será importante na demonstração da validade do protocolo.

Lema 6.3. *Sendo $t \in \{0, 1\}$, então decorre que $p_0^t = t.r^n + \sum_{i=1}^{n} B_i \frac{r^{i-1}}{2}$.*

Demonstração. Uma pequena generalização do lema 6.1 permite escrever que $p_{i-1}^t = r.p_i^t$, quando $B_i = 0$. No caso em que $B_i = 1$, o mesmo lema mostra que $p_{i-1}^t = (1/2) + r.p_i^t$. Sintetizando essas duas expressões, tem-se que

$$p_{i-1}^t = B_i.(1/2) + r.p_i^t.$$

Considerando estágios mais anteriores nessas expressões da probabilidade, e usando a expressão anterior, facilmente se conclui que

$$p_{i-2}^t = B_{i-1}.(1/2) + B_i.(r/2) + r.p_i^t.$$

Prosseguindo de modo indutivo obtém-se o resultado procurado. □

Enfim, a validade do protocolo de bit único pode ser constatada por meio do teorema 6.2, enunciado e demonstrado a seguir.

Teorema 6.2. *A vítima é capaz de determinar, com probabilidade $(1-\delta)$, os elementos corretos da cadeia, $B_1, \ldots, B_n$, por meio do protocolo de bit único.*

Demonstração. Observando o lema 6.3 nota-se que

$$|p - p_0^0| > r^n(\frac{1}{2} - \epsilon)$$

e sendo δ o erro admissível de ser cometido, então

$$Prob\left\{|p - p_0^0| > r^n\left(\frac{1}{2} - \epsilon\right)\right\} \leq \delta.$$

Quando se tem $|p - p_0^0| \leq r^n(\frac{1}{2} - \epsilon)$, então a aproximação se emcontra dentro da região de aceitação e a primeira condição do lema 6.3 está satisfeita. A definição $r = (1/2) - \epsilon$ permite o seguinte desenvolvimento:

$$r.\left(\frac{1}{2} + \epsilon\right) = \frac{1}{4} - \epsilon^2 < \frac{1}{4}$$

$$\Rightarrow r^n.\left(\frac{1}{2} + \epsilon\right) < \frac{r^n}{4} \Rightarrow \frac{r^{n-1}}{2} > 2.r^n\left(\frac{1}{2} + \epsilon\right),$$

que comprova a validade da terceira condição do Lema 6.3. Por fim, a própria escolha dos valores para os c_i comprovam a validade da segunda condição. Portanto, pelo lema 6.3 conclui-se que a vítima é capaz de determinar toda a cadeia de bits com probabilidade igual a $1 - \delta$. □

Neste ponto deve-se ter em conta uma importante indagação: qual deve ser o tamanho da amostra de pacotes necessária de ser recebida pela vítima, de modo que se possa aplicar o modelo apresentado?

Contudo a resposta se encontra na descrição do protocolo pois, quando foi estabelecido o valor de F, que é o tamanho da amostra, observa-se de imediato que esse problema pertence à classe $O(2^n)$.

6.4 Múltiplas Trajetórias de Ataque

Esta seção se propõe apenas a comentar, de modo geral, o caso no qual os pacotes enviados à vítima percorrerão múltiplas trajetórias de ataque. Toma-se como base o mesmo modelo de protocolo apresentado na situação em que se levou em conta apenas uma única trajetória de ataque.

Naturalmente, algumas características adicionais precisam ser levadas em consideração, a fim de que se possa entender o funcionamento do modelo com múltiplas trajetórias de ataque. A primeira delas diz respeito a um novo parâmetro, denominado k, que representa a quantidade máxima de nós iniciais escolhida pelo atacante. Um outro parâmetro, denotado por α, costuma ser utilizado no modelo de múltiplas trajetórias. Trata-se de um parâmetro que estabelece a quantidade mínima de pacotes que deve ser enviada por uma trajetória, a fm de que a mesma possa ser determinada.//

O aprofundamento deste assunto se encontra fora do escopo do presente trabalho.

6.5 Conclusões e Contribuições

No presente capítulo foi apresentada uma abordagem para o problema do rastreamento reverso para a identificação do número IP, baseada no dimensionamento da informação de bits. No caso em que e considera apenas uma única trajetória de ataque, a idéia envolvida é simples, pois se baseia na determinação desta trajetória de ataque a partir da representação binária de um valor de probabilidade.

O caso com mais de uma trajetória, contudo, envolve aspectos mais complexos de concepção da proposta. Em ambos os casos, contudo, o tratamento matemático analítico não é trivial.

A contribuição mais significativa do capítulo se encontra na forma de apresentação assunto, cuja dificuldade foi reduzida em relação aos trabalhos originais de Micah Adler. A ênfase no caso de ataque através de trajetória única é uma forma de simplificar o problema, com a finalidade de melhorar o seu entendimento. Não se trata de uma visão restrita do estudo.

A proposta se mostra como uma importante alternativa para abordar o problema do rastreamento para a identificação de atacantes DoS. Abrem-se possibilidades de novos rumos para o uso da informação na direção da

identificação de atacantes.

Capítulo 7

Uso da Análise Complexa no Rastreamento Reverso

Uma proposta original para o rastreamento e identificação de atacantes por negação-de-serviço é o assunto tratado neste capítulo. O ponto de partida é um conjunto de dados coletados durante um ataque, juntamente com uma função que mapeia o ambiente de ataque no espaço de variáveis complexas. Aliando-se estes elementos a alguns importantes resultados da Teoria da Análise Complexa mostra-se como se pode determinar o número IP de um atacante. De acordo com esta proposta, que é de natureza teórica, se leva em conta o fato de que o ataque é desferido ao longo de uma única trajetória. Além de mostrar uma solução para este caso de trajetória única, pretende-se com esta proposta criar uma base, a partir da qual se possa desenvolver alguma solução de natureza mais geral, possível de ser aplicada a uma situação na qual um ataque seja desferido através de múltiplas trajetórias.

No campo do estudo da análise complexa de uma variável, o mais importante resultado é o conhecido **Teorema Integral de Cauchy**, conforme [60]. Este teorema constitui a origem de conceitos importantes, tanto teóricos, quanto práticos, dentre os quais um se destaca, a saber: o **numero de rotação**. O uso desse conceito, na abordagem do problema do rastreamento e da identificação de atacantes, contribui para a essência da inovação apresentada no presente Capítulo.

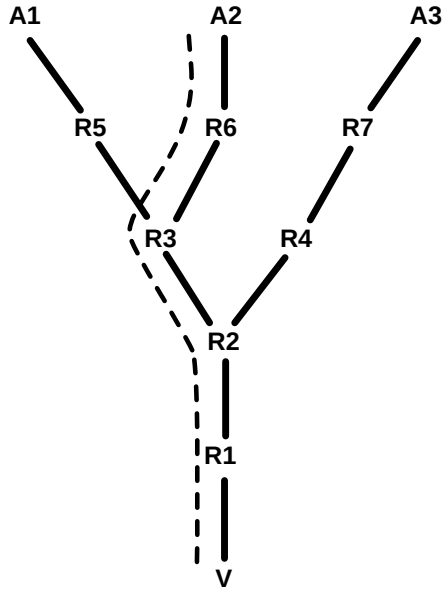

Figura 7.1: Topologia do Ambiente de Ataque DoS.

7.1 Considerações Iniciais

Na Figura 7.1, já apresentada no capítulo 4, pode-se observar o esquema do ambiente em que ocorre um ataque DoS, sob o ponto de vista da vítima. O ambiente de ataque é associado a um espaço virtual, que constitui uma abstração de todo um sistema de comunicações de âmbito mundial e que leva em conta apenas os equipamentos roteadores dos nós desta rede. Estes roteadores são as únicas referências endereçáveis deste espaço virtual.

Ao se falar em espaço virtual, a lembrança que de imediato vem à mente é a de um conjunto de roteadores por onde trafegam os pacotes da rede. O meio físico que interliga os roteadores não é e nem deve ser de importância para o usuário da rede, cujo interesse principal se concentra no funcionamento de suas próprias aplicações.

Com o intúito de desenvolver um tratamento com a formalidade matemática que é requerida neste caso, se torna necessário definir uma função injetiva, Φ, do espaço virtual no conjunto dos números complexos, $\mathbb{C}$. O conjunto dos pontos, denominado por A, que compõem a parte do espaço virtual

visualizado pela vítima, V, corresponde à coleção de números IP de uma rede implementada com o protocolo TCP/IP, no caso exemplificado, associados aos roteadores $R_1, \ldots, R_7$ da Figura 7.1. Este é o campo de definição da função Φ. A imagem da função é o conjunto U, definido como um subconjunto dos números complexos $\mathbb{C}$, de modo que se representa a função como sendo $\Phi : A \rightarrow U$.

A finalidade da função Φ, injetiva, é fazer com que a cada roteador R_k, de A, seja associado a um número complexo da forma $z_k = x_k + i.y_k$, em U. Os elementos que constituem as partes real, $\mathrm{Re}(z_k) = x_k$, e imaginária, $\mathrm{Im}(z_k) = y_k$, do número complexo z_k, correspondem à coordenadas cartesianas, obtidas por meio do uso de dispositivos capazes de fornecer tais coordenadas por meio de instrumentos que detectam o posicionamento geográfico global (ex. receptores GPS).

Por outro lado, uma vez que cada ponto no espaço virtual corresponde a um roteador que é representado por um número IP, a função injetiva $\Phi : A \rightarrow U$, na verdade, determina a associação (unívoca) a um par de coordenadas cartesianas. A fim de ser possível obter um sentido prático desta associação, é necessário representar a função injetiva Φ por meio de alguma expressão matemática. Na próxima seção é apresentada uma expressão para a função injetiva Φ, dentre outras que poderiam ser consideradas para este fim.

7.2 Definição da Função Φ

Para explorar os aspectos necessários à definição da função Φ, ilustrada na Figura 7.2, é utilizada uma notação apropriada para associar o número IP_k a um roteador R_k.

A expressão (7.1) mostra os quatro elementos componentes que representam os valores de um número IP, cada um dos quais pertence ao conjunto de classes residuais $\mathbb{Z}_{256} = \{0, 1, \ldots, 255\}$. Os componentes do quadrupleto

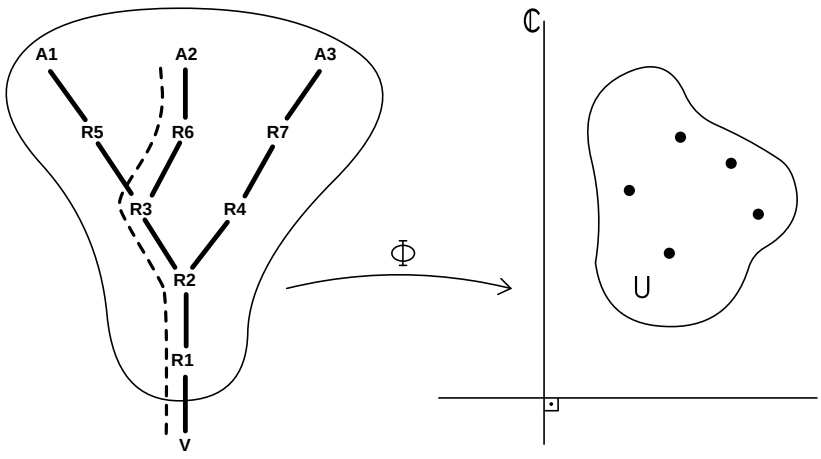

Figura 7.2: Função de Mapeamento Φ.

de valores que define a variável R_k são enumerados pelos índices de 0 a 3, que servem de recurso para formalizar a sua utilização em operações aritméticas, referentes à definição da função Φ.

$$R_k = ((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_k \tag{7.1}$$

Aplicando a função Φ ao roteador R_k, e sabendo que a imagem da função se encontra no campo complexo, obtém-se a expressão (7.2), a seguir:

$$\begin{aligned} \Phi(R_k) &= \Phi_x(R_k) + i.\Phi_y(R_k) \\ &= \Phi_x(((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_k) \\ &+ i.\Phi_y(((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_k) \\ &= x_k + i.y_k = z_k. \end{aligned} \tag{7.2}$$

A função Φ apresentada na expressão (7.2) deve ser injetiva, de modo que se possa mapear, univocamente, cada elemento do conjunto A, no espaço virtual, em elementos do conjunto U, no campo complexo. Um exemplo explícito para a função Φ será mostrado na próxima Subseção.

7.2.1 *Um Exemplo da Função* Φ

Sabe-se que a função Φ apresentada na expressão (7.2) tem a sua imagem no conjunto $U \subset \mathbb{C}$. Decorre desta apresentação as expressões para as duas funções componentes, real e imaginária, da função Φ, conforme mostrado a seguir:

$$x_k = \Phi_x(((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_k),$$

$$y_k = \Phi_y(((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_k).$$

O argumento em cada uma das expressões para x_k e y_k é o número IP do roteador R_k, cuja forma é o quadrupleto

$$(((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_k).$$

Os componentes do quadrupleto, identificados individualmente como $(\xi\xi\xi)_i$, sendo $i \in \{0, 1, 2, 3\}$, são números inteiros quaisquer do intervalo fechado $[0, 255]$. Isto significa, em outras palavras, que cada componente $(\xi\xi\xi)_i$ é um elemento do conjunto de algarismos do sistema de numeração de base 256.

Os componentes do número IP são justapostos de modo a formar o esquema de endereçamento do protocolo, de acordo com a hierarquia estabelecida para cinco classes distintas de endereços, enumeradas como **classe A**, **classe B**, **classe C**, **classe D**, **classe E**. Mais detalhes sobre esta hierarquia podem ser vistos em [16], p. 219-225.

Tendo em mente a idéia de que o quadrupleto que representa o número IP é um número inteiro do sistema de base 256, a conversão deste número para a base decimal pode ser univocamente efetuada por meio da expressão

$$(\xi\xi\xi)_3.256^3 + (\xi\xi\xi)_2.256^2 + (\xi\xi\xi)_1.256 + (\xi\xi\xi)_0.$$

Assim, para cada número IP de um roteador R_k, pode-se aproveitar esta característica de unicidade incorporada no procedimento de conversão para a base decimal, a partir da base 256, de modo que as funções componentes da função Φ sejam definidas como segue:

$$\Phi_x(R_k) = ((\xi\xi\xi)_3.256^3 + (\xi\xi\xi)_2.256^2)_k \tag{7.3}$$

$$\Phi_y(R_k) = ((\xi\xi\xi)_1.256 + (\xi\xi\xi)_0)_k \tag{7.4}$$

Visto que os pontos pertencentes ao conjunto imagem do ambiente de ataque, pela função Φ, ficam situados no âmbito de um sistema de coordenadas cartesianas em $\mathbb{C}$, o mesmo acontecerá com a imagem da vítima. Pode ser conveniente, para fins operacionais que, a função Φ possa ser definida de tal forma que o ponto imagem da vítima V corresponda à origem de um sistema de coordenadas cartesianas. Neste caso, considerando-se $V = R_0$, pode-se definir

$$R_0 = ((\xi\xi\xi)_3.(\xi\xi\xi)_2.(\xi\xi\xi)_1.(\xi\xi\xi)_0)_0 \tag{7.5}$$

de tal forma que as funções componentes da função Φ possam ser representadas, por exemplo, de acordo com as expressões a seguir:

$$\begin{aligned} \Phi_x(R_k) &= ((\xi\xi\xi)_3.256^3 + (\xi\xi\xi)_2.256^2)_k \\ &- ((\xi\xi\xi)_3.256^3 + (\xi\xi\xi)_2.256^2)_0 \end{aligned} \tag{7.6}$$

$$\begin{aligned} \Phi_y(R_k) &= ((\xi\xi\xi)_1.256 + (\xi\xi\xi)_0)_k \\ &- ((\xi\xi\xi)_1.256 + (\xi\xi\xi)_0)_0 \end{aligned} \tag{7.7}$$

Desta forma, pode-se dizer que a função injetiva $\Phi = \Phi_x + i.\Phi_y$, cujas componentes são mostradas nas expressões (7.6) e (7.7), estabelece um mapeamento possível, unívoco, entre o espaço virtual e o conjunto dos números complexos. O que permite que o problema de rastreamento e identificação de um atacante passa a poder ser tratado em um ambiente no qual se pode proceder a um desenvolvimento com rigor matemático. Comentários sobre aspectos do espaço complexo se constituem no assunto da próxima seção, devido à necessidade da preparação do ambiente para a apresentação da nova proposta.

7.3 Alguns Resultados da Análise Complexa

O assunto apresentado na Seção 7.2 caracteriza o fundamento que permite criar uma correspondência entre o problema de rastreamento e identificação de atacante, com o ambiente do espaço complexo. A fim de proceder a esta adaptação deve ser levado em conta que o mapeamento proporcionado pela função Φ é de natureza local. Isto significa que, dado um ponto do ambiente de ataque, existe uma *vizinhança* do mesmo na qual o mapeamento é válido. O conceito de *vizinhança*, (*neighborhood* em Língua Inglesa), pode ser encontrado em [38], p. 45-46. O fato é que, os roteadores mais próximos da vítima são aqueles cuja influência é mais significativa no que concerne ao volume de pacotes atacantes.

A função Φ leva os pontos do conjunto finito A do ambiente de ataque para um subconjunto U de $\mathbb{C}$, que satisfaz à relação $U \supset \Phi(A)$. Essa função pode ser construída de modo que o contorno de U, denotado como $\Gamma(U)$, seja uma *curva fechada*. Os conceitos precisos de *curva* e *curva fechada* podem ser vistos em [46], p. 15-21 e [50], p. 124-126. O exemplo contido na Subseção 7.2.1 confirma esse fato, o que permite concluir que nenhum dos pontos em A é levado ao infinito.

Além do mapeamento pela função Φ, a adaptação que se busca entre os espaços deve ser capaz de reproduzir, no novo ambiente, o aspecto referente ao movimento dos pacotes de um roteador para o outro. A representação deste trânsito de pacotes que é associada ao conceito matemático de **número de rotação**.

Apesar de ser básico no ramo de conhecimento da Matemática conhecido como **Topologia Algébrica**, este conceito aparece no campo de estudo das *funções holomorfas* de variáveis complexas, ver [29]. Entende-se por *função holomorfa em uma região* R o mesmo que *função analítica em uma região* R, isto é, uma função definida no conjunto dos números complexos e que é

diferenciável em todos os pontos desta região.

Voltando ao conceito de **número de rotação**, a sua apresentação formal se dá como conseqüência de dois resultados fundamentais na Análise complexa. O primeiro deles é o famoso **Teorema Integral de Cauchy**, vide [59], considerado fundamental no estudo das funções holomorfas, cujo enunciado é o seguinte:

Teorema 7.1. *Sendo $f : U \subset \mathbb{C} \to \mathbb{R}$ uma função holomorfa em uma região simplesmente conexa $R \subset U$ então, para qualquer caminho fechado $\gamma \subset R$, tem-se que*

$$\oint_{\gamma} f(\zeta)d\zeta = 0$$

.

A demonstração do teorema 7.1 não será aqui apresentada, pois foge ao objetivo deste trabalho. Mais detalhes sobre este assunto podem ser obtidos em [39], p. 86-125. Pode-se ver na definição 7.1 o significado da expressão *caminho fechado*, que aparece no enunciado do teorema 7.1 anterior, de acordo com [43].

Definição 7.1. *Um caminho γ é uma função contínua $\gamma : [a, b] \to C^0$, sendo $\gamma(a)$ o ponto inicial, $\gamma(b)$ o ponto final, e C^0 o espaço de funções contínuas. Caso $\gamma(a) = \gamma(b)$, então o caminho γ será fechado.*

A partir do Teorema Integral de Cauchy, conforme se vê em [59], pode-se construir uma expressão que permite calcular o valor de uma função holomorfa f em qualquer ponto interior a uma região R. A expressão conhecida pela denominação de **Fórmula Integral de Cauchy** é definida no teorema 7.2, com demonstração que pode ser encontrada em [24].

Teorema 7.2. *Sejam $f : U \subset \mathbb{C} \to \mathbb{R}$ uma função holomorfa em uma região simplesmente conexa $R \subset U$, o ponto $\omega_k \in R$ e o caminho fechado $\gamma \subset R$ em torno do ponto ω_k. Então tem-se que*

$$f(\omega_k) = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(\zeta)}{(\zeta - \omega_k)} d\zeta. \tag{7.8}$$

De acordo com a expressão no teorema 7.2, o valor $f(\omega_k)$ é obtido a partir do cálculo da integral de uma função ao longo de um caminho fechado, γ. O ponto ω_k se encontra no interior da região delimitada pelo caminho fechado e é envolvido pelo mesmo uma quantidade inteira de vezes, exatamente pela propriedade de o caminho ser fechado.

A integral de linha que aparece no lado direito da expressão (7.8) torna-se particularmente interessante, supondo-se que o caminho γ seja uma circunferência de raio unitário, com centro em ω_k, e a função $f(\zeta) \equiv 1$.

Visto que ζ é um ponto que se encontra sobre a circunferência γ, então é possível escrever a equação de γ como

$$\zeta - \omega_k = e^{it},$$

sendo $t \in [0, 2\pi]$. Substituindo a variável ζ pela variável t, na integral da expressão (7.8), quando $f(\zeta) \equiv 1$, segue-se o desenvolvimento abaixo:

$$\frac{1}{2\pi i} \oint_\gamma \frac{1}{(\zeta - \omega_k)} d\zeta = \frac{1}{2\pi i} \oint_0^{2\pi} e^{-it}(i.e^{it}dt) = 1.$$

O valor calculado para a integral

$$\frac{1}{2\pi i} \oint_\gamma \frac{1}{(\zeta - \omega_k)} d\zeta$$

é igual a um, considerando apenas uma volta dada em torno do ponto ω_k. Este desenvolvimento sugere um modo de calcular a quantidade de voltas que um caminho fechado faz em torno de um ponto, que se encontra formalizado na definição 7.2, a seguir.

Definição 7.2. *Sendo γ um caminho fechado em torno de um ponto ω_k, tal que $\omega_k \notin \gamma$, denomina-se* ***número de rotação com respeito ao ponto*** *ω_k, representando-se como $\eta(\gamma, \omega_k)$, à expressão*

$$\eta(\gamma, \omega_k) = \frac{1}{2\pi i} \oint_\gamma \frac{1}{\zeta - \omega_k} d\zeta. \tag{7.9}$$

Estes importantes resultados da análise complexa são utilizados na Seção 7.5, na proposta da solução para o problema do rastreamento e identificação de atacantes. Na próxima seção são considerados os aspectos probabilísticos envolvidos no problema em estudo.

7.4 Modelagem do Ambiente de Ataque

O modelo matemático adotado para o ambiente onde ocorre um ataque é representado como uma estrutura em árvore, tal como apresentado na Seção 7.1. De acordo como o modelo matemático os roteadores tomam os lugares dos vértices, ao mesmo tempo em que se faz a correspondência das linhas de comunicação com as arestas, na estrutura em árvore.

Os pacotes atacantes trafegam pela árvore desde os roteadores de origem até a vítima, como se saltassem de um roteador para outro. Este comportamento aparente permite concluir que a distância de um roteador até a vítima pode ser medida em "saltos". A formalização desta conclusão se encontra na definição 7.3.

Definição 7.3. *A distância d_k de um roteador R_k até o roteador R_0, que está diretamente associado à vítima, é igual à quantidade de saltos desde R_k até R_0. Considerando a representação da trajetória de ataque, de R_k até R_0 como*

$$R_k \rightarrow R_{k-1} \rightarrow \ldots \rightarrow R_1 \rightarrow R_0,$$

então a distância d entre R_k e R_0 é igual a k, isto é, a quantidade de arcos entre os roteadores.

No enunciado que se encontra na definição 7.3 observa-se que a variável k, utilizada para indexar o roteador R_k, é o principal elemento da expressão para o cálculo da distância do roteador até a vítima. Deste fato decorre a seguinte questão: o que se deve fazer para determinar o valor do índice k, de um roteador R_k?

Esta questão assume um aspecto grave quando se considera um ambiente como o da rede Internet, no qual não há qualquer centralização de controle. Neste caso, a vítima só poderá obter o valor de k se for possível receber dados adequados com esta finalidade, provenientes do ambiente de ataque. Os únicos veículos capazes de realizar o transporte destes dados são exatamente os pacotes que chegam até a vítima. Para tanto, é necessário que sejam introduzidas modificações nas regras de funcionamento do protocolo TCP/IP e que os pacotes atendam aos seguintes requisitos:

1. Cada pacote deve ter um campo para ser utilizado como um contador:
   Este é um campo numérico cujo conteúdo é incrementado ao longo da trajetória de ataque e que, ao chegar na vítima, o seu valor será igual à distância, em saltos, do roteador R_k até a vítima.

2. O campo contador deve ser iniciado com o valor igual a zero, ao passar pelo roteador R_k:
   Esta calibragem é necessária para que o valor do campo possa ter significado prático, no que concerne à representação da distância entre a vítima e o roteador R_k.

3. O valor do contador deve ser acrescido de uma unidade, em cada um dos sucessivos roteadores da trajetória:
   A adição de uma unidade ao campo contador existente no pacote, quando o mesmo chega a cada um dos roteadores, é uma maneira de manter atualizada a memória referente ao comprimento da trajetória até então percorrida.

Quando um pacote do ambiente chega no roteador R_0 da vítima o conteúdo do campo contador é o valor da distância desde o roteador R_k. Contudo, de acordo como o conjunto de requisitos apresentados acima, sabe-se que cada roteador do ambiente deverá ser, em algum momento, aquele no qual o campo contador de um pacote receberá o valor zero, ou o incremento

de uma unidade. Como não existe um controle central na rede para determinar, precisamente, esta propriedade a um roteador, uma alernativa para resolver este problema é definir uma forma de escolha ao acaso.

A maneira como funcionará a escolha aleatória do tipo de tarefa, que deve ser executada com cada pacote, exige que seja inserida uma alteração no conjunto de programas responsáveis pela implementação do protocolo TCP/IP. Em conseqüência desta alteração, cada pacote que chega a um roteador será submetido a um processamento adicional, além daquele estabelecido originalmente para o protocolo. Este processamento aumentará o tempo de funcionamento do programa para o tratamento de um pacote, em cada roteador da rede. Logo, o tempo total necessário para um pacote percorrer uma trajetória de ataque, que é a soma dos tempos de deslocamento entre os roteadores, com o tempo de tratamento em cada roteador, será maior do que aquele originalmente gasto, quando não havia processamento adicional nos roteadores.

Convém lembrar que, o processo de escolha ao acaso descrito anteriormene é o meio pelo qual se pode decidir se o campo contador de um pacote deve ser iniciado com o valor zero, ou se deve receber o acréscimo de uma unidade. Isto significa que, adotando-se este processo de escolha, todos os pacotes trafegando ao longo da rede deverão ser submetidos ao processamento adicional do protocolo TCP/IP, fato que contribui para os pacotes gastem mais tempo até atingir os seus destinos. Em outras palavras, ocorre uma degradação na eficiência com que a rede funciona.

O impacto causado por esta degradação no funcionamento da rede, decorrente do fato de que todos os pacotes trafegando ao longo da mesma são submetidos ao processamento adicional, pode ser contornado utilizando os recursos da **Teoria da Amostragem Estatística**. De acordo com esta teoria, ao invés de examinar o conjunto de todos os pacotes trafegando pelo ambiente de ataque, isto é a *população* de todos os pacotes, vide [32], p. 3, é possível obter os dados necessários para o rastreamento e a identificação de atacantes examinando-se apenas uma *amostra* de pacotes.

Segundo [61], uma amostra é um subconjunto de uma população que

pode ser extraído através da aplicação de um processo de seleção de elementos, seja de natureza aleatória ou fundamentado em algum outro critério. O propósito de uma amostra é prover dados para a investigação de propriedades da população de onde foi extraída. O processo de obtenção da amostra é denominado *amostragem*, e a quantidade de seus elementos se chama *tamanho da amostra*. Considerando-se que apenas uma amostra da população de pacotes deverá ser submetida ao processamento adicional em cada roteador da rede, o incremento do tempo de processamento será inferior àquele do caso em que toda a população fosse considerada.

Para a finalidade que se tem em mente, que é o rastreamento e a identificação de atacantes, apenas os pacotes da amostra serão examinados, dentre todos os que chegam até a vítima. Logo, existe a necessidade de se reconhecer se um determinado pacote que atinge a vítima se encontra, ou não, na amostra. Isto pode ser facilmente resolvido por meio da gravação de uma marca identificadora no pacote selecionado, durante o processo de amostragem.

Os aspectos descritos anteriormente, sobre a seleção aleatória de pacotes, se constituem em uma técnica utilizada para revelar informações internas de uma rede. Uma técnica com tais características é denominada **Marcação Probabilística de Pacotes**, vide [23]. Os dados coletados nos roteadores são armazenados no cabeçalho do protocolo IP e transportados até a vítima, que os utilizará para obter as informações desejadas. Na literatura especializada esta técnica é conhecida pela expressão da Língua Inglesa *Probabilistic Packet Marking*, abreviada como PPM.

Para o uso da técnica de marcação probabilística de pacotes é necessário que sejam formuladas hipóteses, acerca das condições em que ocorre o fenômeno sob estudo. No caso em questão, as características observadas no tráfego de pacotes pelo ambiente de ataque permitem que sejam adotas como válidas as condições a seguir:

1. Os roteadores são independentes uns dos outros, no que concerne ao

processo de marcação;

2. Cada pacote pode, ou não, ser marcado, de modo independente de qualquer outro;

3. A probabilidade p, de marcação de um pacote, é constante em todo o ambiente de ataque.

A independência entre os roteadores, objeto do primeiro ítem, estabelece que um roteador não interfere no comportamento de qualquer outro, que se encontra no ambiente de ataque. Isto significa que cada roteador tem a prerrogativa de marcar, ou não, qualquer pacote que receba. Já o segundo ítem estabelece que só existe uma de duas possibilidades distintas possíveis para cada pacote, no que concerne à marcação, sendo esta efetuada de modo independente entre os pacotes. Por fim, o fato de a probabilidade p de marcação de um pacote ser a mesma em todo o ambiente de ataque é uma característica que pode ser atribuída aos programas, que executam o processamento adicional em cada roteador.

A situação no ambiente de ataque, conforme se apresenta, atende às condições do que que se denomina um **Conjunto de Experimentos de Bernoulli**. De acordo com [25], p. 146, o que se costuma chamar Experimentos de Bernoulli são aqueles que possuem as seguintes propriedades:

- Os experimentos são independentes entre si;
- Um experimento somente pode se apresentar em um de dois resultados possíveis;
- A probabilidade de qualquer experimento é igual a um mesmo valor p.

Apesar da simplicidade de formulação, experimentos de Bernoulli são inspiradores de modelos probabilísticos de larga aplicação em diversos ramos do conhecimento, conforme pode ser verificado, por exemplo, em [25], p. 146-173, e [53], p. 145-167.

A próxima Subseção contém uma proposta para a um algoritmo destinado a implementar o processo de marcação de pacotes no ambiente de ataque.

7.4.1 A Marcação de Pacotes

A fim de que seja possível efetuar o procedimento de marcação de pacotes, cada roteador precisa ser munido de uma cópia do programa apropriado para esta finalidade. Uma proposta para tal algoritmo de marcação, inspirada em [51], p. 299, é descrita pelo procedimento representado no pseudocódigo $PS07-0100$, a seguir.

```
/* Pseudocódigo PS07 − 0100 */
para "cada pacote que chega ao roteador" faça
    se "pacote não marcado" então
        gerar número aleatório x ∈ [0, 1)
        se x < p então
            executar "marcar_pacote"
            contador ← 0
    senão
        contador ← contador + 1
```

Pode-se ver pela primeira instrução do pseudocódigo $PS07-0100$ que, qualquer pacote do ambiente de ataque é levado à consideração pelo roteador ao qual está chegando. A segunda instrução, cuja estrutura é do tipo desvio, indica que o campo destinado a receber a marcação deve ser examinado. Se o pacote já tiver recebido marcação em algum roteador anteriormente visitado, a próxima instrução a ser executada é a que estabelece o incremento do campo contador, isto é, $contador \leftarrow contador + 1$.

Por outro lado, caso o pacote ainda não tenha recebido marcação em algum roteador anterior, então a próxima instrução é *gerar número aleatório* $x \in [0, 1)$, a terceira de cima para baixo, cujo resultado que se obtém com o

seu funcionamento é um número aleatório, x, pertencente ao intervalo $[0, 1)$. Na próxima instrução, a quarta da seqüência, o valor de x é comparado com p, que é a probabilidade de um pacote ser marcado. No caso de o valor gerado para x ficar situado na região de aceitação, isto é, o intervalo onde x é não negativo e inferior ao valor de p, o procedimento "*marcar_pacote*" será executado e o campo "*contador*" receberá o valor zero. Depois dessas duas operações o pacote seguirá adiante na trajetória, devidamente marcado. Por outro lado, se o valor de x ficar fora da região de aceitação, o pacote também deverá seguir adiante, porém sem qualquer marcação.

Convém notar que, de acordo com a segunda instrução do código em $PS07 - 0100$, um pacote não poderá receber a marcação inicial mais do que uma vez. Depois da marcação inicial de um pacote, o seu campo "*contador*" será incrementado de uma unidade em cada um dos roteadores subseqüentes da trajetória. Deste modo, quando o pacote chegar na vítima o valor do campo "*contador*" representará a distância, em saltos, a que se encontra o roteador que efetuou a marcação inicial no pacote.

Considere-se que o total dos pacotes que chegam à vítima, marcados ou não, é igual a N. Desde que a probabilidade de um pacote ser marcado é igual a p, então a quantidade dos pacotes marcados que chegam à vítima é igual a $p.N$. Os pacotes marcados serão os únicos considerados no problema de rastreamento e identificação de atacantes. Esta seleção é um procedimento simples, devido ao modo de funcionamento do pseudocódigo $PS07-0100$, que separa explicitamente os pacotes marcados, dos que não recebem marcação.

Na próxima Subseção se tratará de um modelo probabilístico que descreve o processo de marcação inicial de um pacote. A partir deste modelo, se fará uma associação com a distância entre vítima e o roteador que realizou a primeira marcação no pacote.

7.4.2 Considerações Probabilísticas

A representação da trajetória de deslocamento de um pacote, desde o roteador no qual foi efetuada a sua marcação inicial, até o seu destino final, pode ser realizada por meio de uma cadeia de caracteres. Considerando a ocorrência de marcação inicial de um pacote em um roteador como um "Sucesso" (ou S) e todas as subseqüentes passagens por outros roteadores como "Fracasso" (ou F), a trajetória será representada por uma cadeia contendo um caracter S, sendo os demais caracteres todos iguais a F.

Assim, quando um pacote recebe a marcação inicial em um roteador que se encontra a uma distância de d saltos da vítima, a trajetória de ataque percorrida pode ser representada pela cadeia

$$\underbrace{SFF\ldots F}_{d}.$$

Lembrando da Subseção 7.4, que trata da modelagem do ambiente de ataque, sabe-se que os roteadores são independentes uns dos outros, para efeito de marcação de pacotes. A probabilidade p de que um pacote qualquer receba a marcação inicial é a mesama para todos os que trafegam pelo ambiente de ataque. Além disso, os pacotes são independentes no que concerne à sua marcação. Estes fatos caracterizam o ato de marcação de pacotes como o fenômeno probabilístico denominado *Experimento de Bernoulli*.

Considere-se que um certo pacote receba marcação inicial, com probabilidade p, em R_k que se encontra d saltos distante da vítima. Visto que a probabilidade do pacote não ser marcado em algum outro roteador é igual a $(1-p)$, a probabilidade de ele não ser marcado em todos os demais $(d-1)$ roteadores restantes da trajetória é igual a $(1-p)^{d-1}$. Logo, a probabilidade de que a vítima possa receber um pacote que recebeu marcação a uma distância d é dada pela seguinte expressão:

$$f(d) = p(1-p)^{d-1} \tag{7.10}$$

Uma rápida olhada na expressão (7.10) permite concluir que a função $f(d)$ é monótona decrescente. De fato, se as variáveis d_1 e d_2 representam

distâncias de roteadores do ambiente de ataque até a vítima, e $d_1 < d_2$, então

$$f(d_1) = p(1-p)^{d_1-1} > p(1-p)^{d_2-1} = f(d_2),$$

pois $(1-p) < 1$. Assim, quanto menor for o valor de d, maior será o valor de $f(d)$ e, portanto, a probabilidade de recebimento de um pacote com marcação. Em outras palavras, quanto mais próximo o roteador de ataque se encontra da vítima, maior será a probabilidade de que um pacote com marcação possa ser por ela recebido.

freqüências Os pacotes marcados que chegam até a vítima possuirão distintos valores armazendos no campo "*contador*". Organizando os pacotes em grupos cujo critério é o de que o valor no campo *contador* seja o mesmo, obtém-se o agrupamento dos pacotes que foram marcados a uma mesma distância da vítima. Assim, tomando como exemplo um grupo cujo valor do campo campo *contador* seja igual a d, sabe-se que todos aqueles pacotes foram marcados em um roteador genérico que se encontra d saltos distante da vítima.

A quantidade de pacotes reunida em cada grupo é uma medida da fração de todos os pacotes recebidos com marcação, que foi marcada em um roteador genérico. Este valor recebe a denominação *freqüência com que um roteador, que se encontra a uma distância d da vítima, efetuou a marcação de pacotes*, ou simplesmente *freqüência*. Tomando o conjunto dos valores destas freqüências é possível construir como os mesmos uma *tabela de freqüências de recebimento de pacotes marcados*, conforme mostrado a seguir.

Tabela de Freqüências de Recebimento de Pacotes Marcados

Distância	Freqüência
d_1	f_1
d_2	f_2
$\vdots$	$\vdots$
d_n	f_n

Este critério de agrupamento junta os pacotes que foram marcados à mesma distância d_k da vítima e o valor de f_k decorre de uma estimativa da freqüência

$f(d_k)$, calculada pela expressão (7.4).

A união dos resultados da análise complexa, com o carácter probabilístico da modelagem do ambiente de ataque são combinados na próxima seção, com o propósito de se justificar uma abordagem teórica que possa permitir o rastreamento e a identificação de atacantes.

7.5 Rastreamento e Identificação

A construção de uma função injetiva Φ, capaz de mapear o ambiente de ataque no espaço complexo, foi introduzida na Seção 7.2. Deste modo, a imagem de um roteador genérico R_k, identificado pelo seu número IP, será representada pelo número complexo $\omega_k = \Phi(R_k)$. Este mapeamento reflete o aspecto estático do fenômeno em estudo.

O fluxo de pacotes pelo ambiente de ataque trafegando do atacante em direção à vítima, representa o aspecto dinâmico envolvido na situação em estudo. Através do uso do instrumento apresentado na Subseção 7.4.2, a tabela de freqüências, é possível representar um forma de dinamismo que pode, em princípio, ser relacionado com a situação pesquisada. A tabela contém a associação da distância d_k na qual ocorreu marcação de pacotes, com a quantidade de pacotes marcados no roteador àquela distância, f_k, para $k \in \{1, \ldots, n\}$.

A próxima Subseção introduz detalhes de uma interpretação do aspecto dinâmico do problema, desta vez no âmbito do espaço complexo.

7.5.1 Visão no Espaço Complexo

A idéia central é a de que, o tráfego de pacotes passando por R_k será representado no ambiente do espaço complexo como sendo o escoamento de um flúido por sobre uma superfície plana. Contudo, para esta analogia ser completa é preciso que se possa representar, através da mesma, o significado

do mecanismo de marcação de pacotes.

Observando-se o pseudocódigo $PS07 - 0100$, claramente se vê que, de todos os pacotes chegando a um roteador genérico R_k, parte deles recebe marcação inicial ou o incremento no campo *contador*, enquanto a outra parte segue sem receber qualquer marcação. Este comportamento se repete ao longo da trajetória de ataque, de modo que a vítima recebe um conjunto de pacotes sem marcação e um outro conjunto com pacotes marcados e contendo variados valores do campo *contador*. Os pacotes que não recebem marcação se comportam como se passassem ao largo do roteador R_k. Por outro lado, aqueles submetidos à marcação se comportam como se "mergulhassem" no referido roteador.

Sabendo-se que a imagem do ambiente de ataque pela função Φ é uma região no espaço complexo, pode-se considerar que cada ponto ω_k, que é a imagem de cada roteador genérico R_k, se constitui em um sumidouro, por onde pode escoar parte do flúido se deslocando sobre a região. A quantidade de flúido que escoa por cada ponto ω_k representa o resultado do mecanismo de marcação de pacotes no roteador. Esta referida quantidade de flúido que escoa por um sumidouro, objeto da analogia do fluxo de pacotes que recebem marcação, é a base do método proposto para se identificar um atacante. A porção de flúido que percorre a superfície, até o ponto ω_0, imagem do roteador genérico R_0 ligado à vítima, sem escoar por algum sumidouro, corresponde ao conjunto dos pacotes que não recebem marcação. Os pacotes sem marcação não transportam dados relevantes para o rastreamento e a identificação de atacantes e, portanto, não têm qualquer valor para o tratamento do problema em estudo.

Depois de todas as considerações sobre a analogia que se está desenvolvendo entre o ambiente de ataque e o espaço complexo, convém refletir sobre a seguinte indagação: como se pode calcular a quantidade de flúido escoada através do sumidouro no ponto ω_k, que corresponde ao roteador genérico R_k?

De acordo com a analogia estabelecida, a quantidade de flúido escoada no ponto ω_k, imagem do roteador genérico R_k, pode ser medida de dois modos

distintos. Se olhado sob o ponto de vista do ambiente de ataque, deve-se tomar por base a quantidade de pacotes que chegam à vítima, cuja marcação inicial foi executada em R_k. Esta quantidade de pacotes marcados é denotada como sendo f_k, conforme visto na Seção 7.5.

A visão pelo lado do espaço complexo, por sua vez, permite utilizar propriedades inerentes às funções de variáveis complexas. Sendo ω_k um ponto do espaço complexo, imagem de um roteador genérico R_k, e ζ uma variável complexa, a função $\psi : \mathbb{C} \rightarrow \mathbb{C}$, definida no espaço complexo e de valores complexos, definida como

$$\psi(\zeta) = \frac{1}{(\zeta - \omega_k)},$$

é holomorfa em $\mathbb{C} - \{\omega_k\}$.

Conforme se pode ver na definição 7.2, a função ψ se encontra no integrando da expressão que define o número de rotação de um caminho γ em torno de um ponto ω_k. Além disso, o lado direito da expressão mostrada na definição 7.2, isto é,

$$\frac{1}{2\pi i} \oint_\gamma \frac{1}{\zeta - \omega_k} d\zeta,$$

possui uma importante propriedade. Apesar da sua aparente complexidade, segundo [46], p. 174, o seu valor é um número inteiro, que representa a quantidade de voltas completas do caminho γ em torno do ponto ω_k. Convém lembrar que a única restrição que se impõe é a de que o o ponto ω_k não pode pertencer ao caminho γ.

Tendo em mente a analogia entre fluxo de pacotes no ambiente de ataque e do fluxo de flúido no espaço complexo, pode-se propor uma nova definição da quantidade f_k, de pacotes marcados em um roteador genérido R_k. Sendo ω_k a imagem de R_k no espaço complexo, a quantidade de pacotes marcados em R_k é igual ao número de rotação de um caminho fechado γ, em torno de ω_k. A consolidação dos dois pontos de vista referentes ao modo de obter a quantidade de pacotes marcados no roteador R_k resulta na expressão a seguir:

$$f_k = \frac{1}{2\pi i} \oint_\gamma \frac{1}{\zeta - \omega_k} d\zeta. \tag{7.11}$$

A expressão (7.11) mostra a relação entre o ponto ω_k, imagem de R_k resultante da função de mapeamento Φ, e a quantidade de marcações de pacotes em R_k que chegou até a vítima. Na próxima Subseção se apresenta o desenvolvimento necessário para obter o valor do número IP_k do roteador R_k, onde os pacotes recebem a marcação, o que pode ser feito com o cálculo do valor inverso da função Φ, a partir da definição de um valor para f_k e de um caminho γ.

7.5.2 Determinação do Número IP

A fim de que se possa determinar o número IP_k, do roteador R_k, é preciso inicialmente encontrar o valor do número ω_k na expressão (7.11), que é a imagem de R_k no espaço complexo. O lado esquerdo da expressão (7.11), isto é, f_k, pode ser obtido por meio da coleta de dados realizada no conjunto de pacotes recebidos pela vítima, conforme descrito na Subseção 7.4.2. Quanto ao cálculo da integral que se encontra do lado direito da expressão, no entanto, é preciso fazer uma consideração simplificadora, com respeito ao caminho γ.

Deve ser lembrado que, a única observação sobre γ é a de que se trata de um caminho fechado, tal que $\omega_k \notin \gamma$. Não se perde em generalidade, portanto, fazer a suposição de que γ seja uma circunferência de centro em ω_k e raio unitário, pois o cálculo da integral leva em conta apenas a característica topológica de que o caminho seja fechado. No que concerne à quantidade de voltas da circunferência γ_k em torno do ponto genérico ω_k, a mesma é assumida como sendo igual a f_k, que é a quantidade de pacotes marcados no roteador genérico R_k.

Levando em conta as observações anteriores, a resolução da integral no

lado direito da expressão (7.11) se processa como segue:

$$\begin{aligned} f_k &= \frac{1}{2\pi i}\oint_{\gamma_k}\frac{1}{\zeta-\omega_k}d\zeta \\ &= \frac{1}{2\pi i}\oint_{\gamma_k}\frac{1}{\zeta-\omega_k}.\left(\frac{d(\zeta-\omega_k)}{d\zeta}\right)d\zeta \\ &= \frac{1}{2\pi i}\int_{\gamma_k}\frac{d}{d\zeta}(ln(\zeta-\omega_k))d\zeta \\ &= \frac{1}{2\pi i}(ln(\zeta-\omega_k))|_{\gamma_k} \end{aligned} \tag{7.12}$$

Os limites de integração considerados em (7.12) são números complexos que representam pontos, inicial e final, localizados sobre a circunferência γ_k. Apesar de o ponto inicial ser coincidente com o ponto final no plano complexo, os números que representam estes pontos são diferentes. Existem entre os mesmos a separação de uma quantidade inteira de voltas sobre a referida circunferência. Isto se deve ao fato de que o caminho sobre o qual se faz a integração é fechado. Estes limites de integração recebem a denominação de ζ_0 para o ponto de início, a partir do qual se contam as voltas em torno da circunferência γ_k, e ζ_{f_k} para o ponto final do caminho, no qual se completa a quantidade inteira de voltas sobre γ_k, respectivamente. Então, a expressão (7.12) pode ser escrita como sendo:

$$\begin{aligned} f_k &= \frac{1}{2\pi i}(ln(\zeta_{f_k}-\omega_k)-ln(\zeta_0-\omega_k)) \\ &= \frac{1}{2\pi i}[(ln|\zeta_{f_k}-\omega_k|+i.arg(\zeta_{f_k}-\omega_k)) \\ &- (ln|\zeta_0-\omega_k|+i.arg(\zeta_0-\omega_k))]. \end{aligned} \tag{7.13}$$

Lembrando que o caminho fechado γ_k em torno do ponto ω_k é uma circunferência de raio unitário, segue como conseqüência que

$$ln|\zeta_{f_k}-\omega_k| = ln|\zeta_0-\omega_k| = 0.$$

Logo, a expressão (7.13) pode ser simplificada e toma a forma seguinte:

$$f_k = \frac{1}{2\pi}[arg(\zeta_{f_k}-\omega_k)-arg(\zeta_0-\omega_k)]. \tag{7.14}$$

Desde que o cálculo da integral indicado na expressão (7.11) é efetuado ao longo de uma circunferência que não contém o ponto ω_k, não existe qualquer

restrição quanto às posições dos pontos inicial e final. Assim, pode-se tomar o ponto inicial ζ_0 como sendo um tal que $arg(\zeta_0 - \omega_k)$ seja igual a zero. Deste modo, a expressão (7.14) fica mais simplificada e toma a forma

$$arg(\zeta_{f_k} - \omega_k) = 2\pi f_k. \tag{7.15}$$

Considerando que o ponto representado pelo número complexo ζ_{f_k} pertence à circunferência γ_k, de centro no ponto representado pelo número complexo ω_k e de raio unitário , decorre que $(\zeta_{f_k} - \omega_k)$ é um número complexo cujo módulo é igual a um. Em conseqüência disto, pode-se escrever que

$$\zeta_{f_k} - \omega_k = exp(i.2\pi f_k). \tag{7.16}$$

Além disso, desde que ζ_{f_k} é o número complexo que representa o ponto final de um caminho que dá f_k voltas em torno da circunferência γ_k, o mesmo pode ser escrito na forma polar como sendo

$$\zeta_{f_k} = r_{f_k}.exp(i.(2\pi f_k + \theta_{f_k})). \tag{7.17}$$

Combinando as expressões (7.16) e (7.17), obtém-se

$$r_{f_k}.exp(i.(2\pi f_k + \theta_{f_k})) - \omega_k = exp(i.2\pi f_k),$$

de onde decorre a expressão para ω_k, que é o número complexo procurado:

$$\begin{aligned} \omega_k &= [r_{f_k}.exp(i.\theta_{f_k}) - 1].exp(i.2\pi f_k) \\ &= [r_{f_k}.exp(i.\theta_{f_k}) - 1]. \end{aligned} \tag{7.18}$$

Tomando-se a inversa Φ^{-1} da função de mapeamento, pode-se encontrar o valor do número IP do roteador R_k, por meio da expressão

$$\Phi^{-1}(\omega_k) = R_k.$$

Visto que o método é probabilístico, deste modo o provável atacante será identificado.

Comentários referentes a esta proposta de rastreamento e identificação de atacantes são o objeto da próxima seção.

7.6 Comentários Conclusivos

O ponto central da abordagem proposta neste Capítulo se baseia na analogia que se estabelece entre elementos de dois doínios distintos: um deles associado ao da topologia IP de uma rede TCP/IP e, o outro, associado ao domínio matemático dos números e funções complexas. Com efeito, o procedimento de marcação inicial de pacotes por um roteador, no ambiente de ataque, é relacionado à quantidade de voltas de um caminho fechado em torno de um ponto, no espaço complexo.

A originalidade da proposta se encontra no fato de serem utilizados, em conjunto, o conceito de **número de rotação** e a distribuição geométrica de probabilidade de marcação de pacotes que trafegam entre dois roteadores de uma rede, com a finalidade de se determinar o número IP do roteador que pode desempenhar a função de atacante. Esta idéia motiva o aprofundamento do uso de objetos e conceitos da Matemática, em especial oriundos da Análise Complexa, como argumentos na procura por soluções do problema de rastreamento e de identificação de atacantes em uma rede TCP/IP.

No que concerne à implementação de uma solução para o problema em estudo, tomando por base a proposta apresentada, convém levar em conta alguns aspectos fundamentais.

Em primeiro lugar, existe a necessidade de se definir a função Φ, de mapeamento entre o ambiente de ataque e o espaço complexo. O exemplo apresentado na Subseção 7.2.1 tem por objetivo definir a existência de uma tal função. Uma alternativa para definir uma função mais consistente precisa levar em consideração o conhecimento do ambiente de ataque, ao menos, daquele que é mais próximo da vítima. Este conhecimento deve incluir os números IP dos roteadores, além da distância topológica, em saltos, de cada roteador até a vítima.

O processo de amostragem de pacotes também precisa ser aperfeiçoado. De fato, para ser possível decidir de quais roteadores se originam pacotes

com o mesmo valor no campo "*contador*", o modelo proposto exige que seja incorporada uma adaptação nas unidades de dados do protocolo.

As observações anteriores, no entanto, fazem parte do elenco de possibilidades que surgem para novos estudos e a produção de trabalhos futuros, nesta linha de pesquisa. Outra importante linha de pesquisa pode ser considerada quando se configura o ambiente de ataque em uma rede na qual predomina a mobilidade. Trata-se de um problema de muita complexidade, pois os paradigmas de segurança são diferentes daqueles usualmente aplicados em redes geograficamente estáticas.

Por fim, convém lembrar que a atenção com a segurança nos protocolos para o disciplinamento do tráfego nas redes, em especial nas redes TCP/IP, é um assunto em permanente evolução. Um resumo da motivação histórica para o estudo da segurança pode ser visto no Capítulo 2. No que concerne ao ataque por negação-de-serviço, em particular, uma das primeiras propostas de contramedida se encontra no Capítulo 3 e é de natureza puramente computacional. A evolução do conhecimento sobre o assunto permitiu o surgimento de outras propostas alternativas, conforme se pode ver nos Capítulos 4, 5 e 6. Nestes três capítulos referidos podem-se ver abordagens para contramedidas, nas quais se alia o caráter computacional com aspectos de natureza matemática. Esta união se mostra como sendo a tendência que deverá predominar nas futuras propostas para contramedidas ao ataque por negação-de-serviço.

Capítulo 8

Conclusões e Trabalhos Futuros

O interesse pelos métodos destinados ao rastreamento reverso do número IP vem experimentando um acentuado crescimento, como forma de determinar as origens de ataque do tipo Negação-de-Serviço. Esta atitude tem fundamento no fato histórico ocorrido durante o mês de novembro de 1988.

Esta modalidade de ataque não é a única que se manifesta no âmbito das redes de computadores, em especial na Internet. Contudo, trata-se de uma ação predatória de extraordinário efeito destrutivo para a vítima, apesar da simplicidade envolvida na sua implementação.

Ressalte-se a importância de considerar o contexto histórico no âmbito do qual surgiu a necessidade de abordar o problema do rastreamento reverso. Ainda predominava o que se poderia denominar de um certo "romantismo" no uso da computação. O atual estágio de desenvolvimento dos recursos da Tecnologia da Informação e das Comunicações, por sua vez, não deixa margens para qualquer descaso no uso dos seus instrumentos. Essa potencialização do risco de ataques DoS e DDoS exige constante vigilância e empenho das pessoas e das organizações devotadas a estudo e desenvolvimento de soluções para problemas com a segurança de sistemas de computação.

8.1 Comentários e Conclusões

Ao longo do desenvolvimento do trabalho são apresentados diferentes cenários, concernentes ao estudo de contramedidas destinadas ao enfrentamento do problema causado pelos ataque dos tipos DoS e DDoS. A próxima subseção resume o assunto tratao em cada um dos capítulos anteriores

8.1.1 *Aspectos Históricos*

A apresentação da visão histórica que envolve o surgimento dos ataques DoS e DDoS é necessária para que se possa posicionar o problema em estudo. Sendo o enfoque deste trabalho a análise matemática de um problema real, o entendimento dos fatos que provocaram esta modalidade de ataque mostra como se deve proceder na aplicação da Matemática, visando encontrar a solução do referido problema.

Os ataques por negação de serviço, conhecidos como DoS e DDoS, cuja facilidade e simplicidade da sua execução se alia aos efeitos devastadores que podem provocar, suscitou um problema referente à busca de contramedidas para o mesmo. A contribuição do capítulo 2 se concentra, principalmente, no que concerne ao posicionamento histórico no qual se encontra situado o problema sob foco. Alí se apresentam aspectos dos eventos ocorridos em um período no qual a Ciência da Computação experimentou um significativo avanço, decorrente do salto qualitativo entre sistemas centralizados e o limiar do conhecimento do que se costuma denominar de sistemas distribuídos. E tudo o que foi exposto naquele capítulo permite formar um quadro de desafios presentes e futuros, no que concerne ao uso de redes de computadores, seja para os leigos, seja para os especialistas na área de segurança.

8.1.2 *Visão Determinística*

Nas seções do capítulo 3 foram apresentadas duas abordagens de natureza estritamente computacional, fundamentadas em aspectos puramente determinísticos. A primeira idéia que se tem é que ambas as abordagens não resistiriam a uma análise mais aprofundada, quando se faz apenas uma rápida exposição do seu funcionamento. Contudo, fizeram parte do esforço para o surgimento de propostas mais aperfeiçoadas, o que justifica a apresentação neste trabalho.

A primeira abordagem apresenta um método para marcação de pacotes que consiste na inserção de ndereços IP dos roteadores, como forma de identificar a trajetória de ataque. Trata-se e uma marcação determinística de pacotes, aparentemente de implementação difícil. No entanto, a análise matemática desta abordagem mostra que existem situações em que a mesma é exeqüível.

A outra abordagem apresentada foi a do rastreamento por contra-ataque, cuja análise foi limitada apenas a aspectos descritivos. A razão para esse procedimento é a inexistência de argumentos concretos, a partir dos quais se possa definir variáveis, e relações entre as mesmas, capazes de descrever o seu comportamento.

Particular interesse apresenta o Capítulo 4, cuja fonte de inspiração foi o trabalho conjunto de Dean, Franklin e Sttubfield, cujo título é *An Algebraic Approach to IP Traceback* e se encontra referido em [21]. A natureza matemática determinística mostra a utilização de métodos matemáticos tradicionais, como ferramentas úteis na marcação de pacotes, necessária à resolução do problema do rastreamento reverso. Naquele Capítulo pode-se ver, claramente, como o método de interpolação de Lagrange, alguns resultados do uso de estruturas algébricas, bem como a aritmética em conjuntos finitos podem auxiliar no estudo do rastreamento reverso. Publicado no ano de 2002, esse artigo tornou-se a principal fonte de motivação para o presente trabalho, inclusive através de valiosas opiniões

emitidas por um dos autores, Matt Franklin, quando consultado via Internet.

8.1.3 *Visão Probabilística*

No ano 2000 foi publicado um interessante artigo assinado por Savage, Wetherall Karlin e Anderson, que se tornou um marco no estudo probabilístico do problema do rastreamento reverso. O Capítulo 5 trata dos aspectos inerentes aos argumentos usados pelos autores, envolvendo intrincados problemas de contagem no processo de marcação de pacotes. Dentre os quais o famoso "Problema do Coletor de Cupons", nomenclatura em tradução literal. O artigo cujo conteúdo é tratado no capítulo apresenta uma proposta concreta para resolver a questão inerente à identificação de atacantes, sem modificações que promovam alterações na estrutura atual de um pacote que trafega pela rede. Por essa razão, o artigo recebe citações em todos os trabalhos que o sucederam, devido ao aspecto inovador para a solução do problema do rastreamento reverso do número IP.

A marcação probabilística de pacotes é associada com aspectos do dimensionamento da informação, no desenvolvimento do Capítulo 6. Fundamentado em um artigo de Micah Adler, intitulado *Tradeoffs in Probability Packet Marking for IP Traceback* e referido em [1] e em [44], trata das relações entre a quantidade de bits que deve ser utilizada para a representação de trajetórias de ataque. Naquele Capítulo se encontram demonstrações detalhadas dos fatos utilizados no artigo, de modo a permitir um perfeito entendimento da argumentação utilizada por aquele autor. A ênfase é dada apenas à situação considerada de uma única trajetória de ataque, para a qual todos os fatos são demonstrados.

Considerando a restrição de um ataque através de uma única trajetória, o protocolo descrito apresenta como característica a possibilidade de utilizar apenas um único bit para a finalidade de marcação. No que concerne à situação de múltiplas trajetórias de ataque, somente um é feito um

comentário resumido, visto ser um assunto vasto, que certamente poderia constituir, sozinho, toda uma tese.

8.1.4 *Uso da Análise Complexa*

No Capítulo 7 se apresenta uma contribuição original do autor, direcionada à solução do problema do rastreamento para a identificação de atacante. Trata-se do uso de um conhecido resultado da Teoria da Análise Complexa, decorrente do Teorema de Cauchy, que é a expressão para o cálculo do número de rotação de uma curva, em torno de um ponto do espaço complexo.

Para que seja possível utilizar a expressão para o cálculo do número de rotação, no entanto, é preciso que antes seja definida uma função bijetora entre o ambiente de ataque e um subconjunto do espaço complexo. Assim, a proposta do rastreamento para a identificação necessita que se defina uma função e, em seguida, seja utilizada uma expressão baseada no cálculo do número de rotação.

8.1.5 *Conclusões*

Todo o assunto que vai do Capítulo 2 até o Capítulo 7 trata de aspectos relevantes das contribuições mais significativas, referentes a contramedidas aos ataques DoS e DDoS. O resumo de todo o estudo anterior se encontra nos ítens a seguir:

- **A estrutura utilizada nos pacotes que trafegam pelas redes facilita a existência dos ataques dos tipos DoS e DDoS**.
  De fato, a proposta de criação do protocolo TCP/IP almejava a generalização do uso da rede mundial, de modo que todos pudessem

ser beneficiados com o uso da mesma. Não se levou em consideração a possibilidade de atitudes maliciosas por algum usuário da rede, de modo que a estrutura do cabeçalho de um pacote é apenas o suficiente para a realização do tráfego. A segurança não se traduziu de modo enfático no projeto do cabeçalho de pacote.

- **Uma proposta para o rastreamento reverso deve ser formulada levando em conta, conjuntamente, argumentos computacionais e matemáticos.**
  Apesar de essa ser uma conclusão óbvia, a sua presença é um modo de enfatizar um aspecto fundamental de ser atendido por qualquer futura proposta para abordar o problema do rastreamento reverso.

- **Os métodos matemáticos utilizados em propostas para abordar o rastreamento reverso do número IP devem ser de natureza probabilística.**
  Desde que as respostas procuradas envolvem a obtenção de informação sobre o ambiente de ataque, está clara a necessidade de ser focar o problema dentro de uma visão probabilística, na esteira de estudos mais detalhados da Teoria da Informação, e em especial na Teoria da Codificação.

8.2 Trabalhos Futuros

O estudo desenvolvido no presente trabalho aponta para direções que podem ser exploradas, na procura de novos resultados referentes ao problema do rastreamento reverso do número IP. Dentre as situações que podem ser relacionadas, destacam-se os problemas citados abaixo e que se encontram ainda em aberto:

- **No caso de trajetória única de ataque, para uma dada quantidade de bits, encontrar a expressão que estabelece a redução da lacuna entre os limites inferior e superior da quantidade ótima de pacotes, necessária para compor a amostra.**
  A determinação do tamanho da amostra de pacotes, que garanta representatividade de todos os roteadores do ambiente de ataque, tem por base a utilização de um conjunto de desigualdades conhecidas pela denominação de "limites de Chernoff". Detalhes sobre esse assunto podem ser obtidos em [36], p. 1-4, e em [55], p. 2-4.

- **No caso de múltiplas trajetórias de ataque, identificar as principais dificuldades existentes nos processos de marcação probabilística de pacotes e apresentar soluções.**
  O tratamento da situação em que se consideram múltiplas trajetórias de ataque necessita de ferramentas matemáticas apropriadas para tal. A criação e o refinamento dessas ferramentas é o caminho para a abordagem desse problema.

- **Descobrir as relações existentes entre as seguintes variáveis envolvidas no processo de rastreamento para identificação: quantidade de bits usadas para a marcação de pacotes, quantidade de trajetórias de ataque existentes e quantidade de pacotes necessária para a determinação de trajetórias.**
  Para a resolução deste problema é necessário desenvolver abordagens baseadas no uso de técnicas da Teoria da Informação e Teoria da Codificação.

Apesar de que os problemas enumerados acima se constituem em desafios significativos, esse fato não significa que os mesmos sejam os únicos. A percepção por novas situações certamente será aguçada, à proporção que os

referidos problemas supra forem sendo estudados e devidamente compreendidos.

Bibliografia

[1] Adler, Micah. "Tradeoffs in Probabilistic Packet Marking for IP Traceback". In *ACM Symposium Theory of Computing (STOC), pp. 19-21*, 2002.

[2] Ash, R. *Information Theory*. Interscience Plublishers, New York, 1967.

[3] Autor-Anônimo, . *Segurança Máxima*. Campus, Rio de Janeiro, 2000.

[4] Bachmann, P. *Analytische Zahlentheorie, Bd. 2: Die Analytische Zahlentheorie*. Teubner, Leipzig, 1894.

[5] Baran, Paul. *On Distributed Communications Networks*. Technical report, The Rand Corporation, 1962.

[6] Bastos, Gervásio Gurgel. *Notas de Álgebra*. Edições Livro Técnico, Fortaleza/CE, 2002.

[7] Birkhoff, Garret, MacLane, Saunders. *A Survey of Modern Algebra*. Macmillan Company, New York, 1965.

[8] Brillouin, L. *La Science et la Théorie de L'Information*. Masson, Paris, 1958.

[9] Burch, Hal, Cheswick, Bill. "Tracing Anonymous Packets to their Approximate Source". In *Proceedings of Usenix LISA ´00, pp. 313-321*, 2000.

[10] Burden, Richard, Faires, J.Douglas. *Análise Numérica*. Thomson, S. Paulo, 2003.

[11] Campello, Ruy Eduardo, Maculan, Nelson. *Algorítmos e Heurísticas*. Editora da Universidade Federal Fluminense, Niterói, 1994.

[12] CERT Advisory CA-1996-21, . "TCP SYN Flooding and IP Spoofing Attacks". http://www.cert.org/advisories/CA-1996-21.html, 2000. Access in 23/11/2005.

[13] CERT Advisory CA-1998-01, . "Smurf IP Denial-of-Service Attacks". http://www.cert.org/advisories/CA-1998-01.html, 2000. Access in 28/11/2005.

[14] CERT Carnegie Mellon Software Engineering Institute, . "Denial-of-Service Attacks". http://ww.cert.org/tech-tips/denial-of-service.html, 1999. Access in 14/12/2006.

[15] Cheswick, B., Burch, H., Branigan, S. "Mapping and Visualizing the Internet". In *Proceedings of USENIX Annual Technical Conference*, 2000.

[16] Comer, Douglas E. *Redes de Computadores e Internet*. Bookman, Porto Alegre, 2001.

[17] Corporation, RAND. "Objective Analysis, Effective Soluctions". http://www.rand.org/, 2006. Access in 07/12/2006.

[18] Corporation, RAND. "Paul Baran and the Origins of the Internet". http://www.rand.org/about/history/baran.html, 2006. Access in 07/12/2006.

[19] Coutinho, Severino Collier. *Números Inteiros e Criptografia RSA*. IMPA - SBM, Rio de Janeiro, 2000.

[20] DARPA, . "Transmission Control Protocol". http://www.ietf.org/rfc/rfc0793.txt?number=793, 1981. Access in 12/12/2006.

[21] Dean, Drew, Franklin, Matt, Sttublefield, Adam. "An Algebraic Approach to IP Traceback". *ACM Transactions on Information and System Security*, v. 5, n. 2, pp. 119–137, 2002.

[22] Doepner, Thomas W., Klein, Philip N., Koyfman, Andrew. "Using Router Stamping to Identify the Source of IP Packets". http://www.cs.brown.edu/ klein/publications/2000stampId.pdf, 2000. Access in 01/06/2007.

[23] Dong, Qunfeng, Banerjee, Suman, Adler, Micah, Hirata, Kazu. "Efficient Probabilistic Packet Marking". http://csr.bu.edu/icnp2005/Papers/33_qdong-eppm.pdf, 2005. Access in 08/01/2007.

[24] Douglas Arnold, . "Complex Analysis". http://www.matem.unam.mx/buendia/complex.pdf, 1997. Access in 29/05/2006.

[25] Feller, William. *An Introduction to Probability Theory and its Applications - Volume I; Third Edition*. John Wiley & Sons, New York, 1968.

[26] Godement, Roger. *Cours d´Algèbre*. Hermann, Paris, 1973.

[27] Govindan, R., Tangmunarunkit, H. *Heuristics for Internet Map Discovery*. Technical report, Computer Science Depto, University of Southern California, 1999.

[28] Guruswami, V., Sudan, M. "Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes". *IEEE Transactions on Information Theory*, v. 45, pp. 1757–1767, 1999.

[29] Hammick, Larry. "Winding Number". http://planetmath.org/?op=getobj&from=objects&id=3291, 2003. Access in 31/05/2006.

[30] Handley, M. "Internet Denial-of-Service Considerations". http://tools.ietf.org/html/rfc4732, 2006. Access in 28/05/2007.

[31] Hankerso, Darrel, Harris, Greg A., Jr., Peter D. Johnson. *Introduction to Information Theory and Data Compression*. CRC Press, New York, 1998.

[32] Hoel, Paul G., Jessen, Raymond J. *Basic Statistics for Business and Economics*. John Wiley & Sons, Santa Barbara, 1977.

[33] Howard, John D. "An Analysis of Security Incidents on the Internet 1989-1995". http://www.cert.org/research/JHThesis/Star.html, 1997. Access in 30/06/2005.

[34] Internet Architeture Board, . "A Brief History of the Internet Advisory / Activities / Architecture Board". http://www.iab.org/about/history.html, 1992. Access in 27/06/2005.

[35] Jacod, Jean, Protter, Philip. *Probability Essentials*. Springer, Berlin, 2000.

[36] John Canny, . "Chernoff Bounds". http://www.cs.berkeley.edu/ jfc/cs174/lecs/lec10/lec10.pd, 2006. Access in 07/03/2006.

[37] Kleinrock, Leonard. "Leonard Kleinrock's Home Page". http://www.lk.cs.ucla.edu/, 2005. Access in 25/06/2005.

[38] Kolmogorov, A.N., Fomin, S.V. *Introductory Real Analysis*. DOVER Publications, New York, 1970.

[39] Lang, Serge. *Complex Analysis*. Springer-Verlag, new York, 1993.

[40] Lopes, Raquel V., Sauvé, Jacques P., Nicolletti, Pedro S. *Melhores Práticas para Gerência de Redes de Computadores*. Campus, Rio de Janeiro, 2003.

[41] Luciana Salete Buriol, . "Roteamento do Tráfego na Internet: Algoritmos para Projeto e Operação de Redes com Protocolo OSPF". http://www.densis.fee.unicamp.br/ buriol/tese-buriol.pdf, 2003. Access in 30/05/2007.

[42] Malis, Andrew G. "The ARPANET 1822L Host Access Protocol". http://tools.ietf.org/html/rfc878, 1983. Access in 15/05/2007.

[43] Margherita Barile and Eric W. Weisstein, . "Path - MathWorld". http://mathworld.wolfram.com/Path.html, 2003. Access in 26/12/2006.

[44] Micah Adler, . "Tradeoffs in Probability Packet Marking for IP Traceback". http://www.cs.umass.edu/ micah/pubs/traceback.ps, 2002. Access in 17/09/2004.

[45] Olshevsky, V., Shokrollahi, M. A. "A Displacement Approach to Efficient Decoding of Algebraic-Geometric Codes". In *Proceedings of the 31st Annual ACM Symposium on Theory of Computation*, 1999.

[46] O'Neil, Barret. *Elementary Differential Geometry.* Academic Press, New York, 1969.

[47] Postel, J. "Character Generator Protocol". CERT Coordination Center - http://www.ietf.org/rfc/rfc0864.txt?number=864, 1983. Access in 01/07/2005.

[48] Press, William H., Flannery, Brain P., Teukolsky, Saul A., Vettering, William. *Numerical Recipes - The Art of Scientific Computing.* Cambridge University Press, New York, 1990.

[49] Reynolds, J. "The Helminthiasis of the Internet - RFC 1135". http://www.faqs.org/rfcs/rfc1135.html, 1989. Access in 30/03/2006.

[50] Rudin, Walter. *Principles of Mathematical Analysis - Second Edition.* McGRAW-HILL, New York, 1964.

[51] Savage, S., Wetherall, D., Karlin, A., T.Anderson, . "Pratical network Support for IP Traceback". In *Proceedings of ACM SIGCOMM 2000, pp. 295-306*, 2000.

[52] Scheinerman, Edward R. *Matemática Discreta - Uma Introdução.* Thomson, São Paulo, 2003.

[53] Soong, T. T. *Modelos Probabilísticos em Engenharia e Ciências.* Livros Técnicos e Científicos Editora S.A., Rio de Janeiro, 1986.

[54] Stallings, William. *Cryptography and Network Security - Principles and Practices.* Prentice Hall, Upper Sadlle River, second ed., 1999.

[55] Valentine Kabanets, . "Power of Randomness". http://www.cs.sfu.ca/ kabanets/cmpt881/lec/lec3.pdf, 2004. Access in 07/03/2006.

[56] Viana, Mateus Mosca. *Caracterização da Entropia e Aplicações.* Technical report, Depto. de Matemática, Universidade Federal do Ceará, 1981.

[57] Viana, Mateus Mosca, de Souza, José Neuman, Mota, João César Moura. "marcação probabilística de pacotes em um ambiente sob ataque de negação de serviço". In *Anais XXII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES - SBrT'05*, 2005.

[58] Vinton G. Cerf, . "The Internet Activities Board". http://www.rfc-archive.org/getrfc.php?rfc=1160, 1990. Access in 07/12/2004.

[59] Weisstein, Eric W. "Cauchy Integral Theorem". http://mathworld.wolfram.com/CauchyIntegralTheorem.html, 1999. Access in 26/05/2006.

[60] Weisstein, Eric W. "Complex Analysis". http://mathworld.wolfram.com/ComplexAnalysis.html, 1999. Access in 18/05/2006.

[61] Weisstein, Eric W. "Sample". http://mathworld.wolfram.com/Sample.html, 2004. Access in 05/01/2007.

Apêndice A

Experimento de Bernoulli

A.1 Introdução

Durante o estudo de fenômenos nos quais se trata com variáveis aleatórias discretas, a necessidade de construir modelos, com elevada freqüência, se depara com experimentos com as seguintes características:

- Cada experimento somente pode apresentar um de dois resultados possíveis, denominados *sucesso*, ou S, e *fracasso*, ou F.
- As probabilidades de S e F permanecem constantes em todos os experimentos.
- Os experimentos são independentes uns dos outros.

Um experimento que atenda a esses ítens supra descritos recebe a denominação de *Experimento de Bernoulli*, ou *Prova de Bernoulli*, vide as referências [25] e [53]. Costuma-se denominar p a probabilidade de sucesso e q a de fracasso, de modo que $p + q = 1$.

O espaço amostral para um experimento de Bernoulli é o conjunto $\{F, S\}$, que contém apenas dois elementos. Por outro lado, considerando n experimentos de Bernoulli simultâneos, o espaço amostral será o conjunto de agrupamentos com n elementos, cada um podendo assumir o valor F, ou S. Esse espaço amostral conterá 2^n elementos, cada um sendo do tipo $(x_1, x_2, \ldots, x_n)$.

Partindo do princípio de que, em um agrupamento com n experimentos

de Bernoulli existe independência entre os mesmos, e levando em conta que $Prob(S) = p$ e $Prob(F) = q$, então tem-se que

$$P\{(SSFSF \ldots FFS)\} = ppqpq \ldots qqp. \tag{A.1}$$

A.2 Distribuição Binomial

Considerando que a quantidade de experimentos de Bernoulli em um agrupamento é igual a n e a probabilidade de sucesso de cada um deles vale p, costuma-se estudar a variável aleatória discreta X, que representa o evento referente à *quantidade de sucessos ocorridos quando da realização dos experimentos*, ver [25]. Essa variável aleatória X é conhecida como uma *variável aleatória de natureza binomial*, em virtude do seu caráter dicotômico, e o seu comportamento é regulado pela *distribuição binomial de probabilidade*. A expressão (A.2) mostra a função de massa de probabilidade binomial, sendo p a probabilidade de sucesso de um experimento:

$$f(x) = P[X = x] = \binom{n}{x} p^x.(1-p)^{n-x}. \tag{A.2}$$

Associados à distribuição binomial existem parâmetros, que correspondem às seguintes medidas de tendência central e de dispersão, conforme se pode ver a seguir:

$$Media = \mu = n.p. \tag{A.3}$$

$$Variancia = \sigma^2 = n.p.(1-p). \tag{A.4}$$

$$Desvio \quad Padrao = \sigma = \sqrt{n.p.(1-p)}. \tag{A.5}$$

A expressão da função de distribuição de probabilidade binomial tem a forma mostrada a seguir:

$$F_X(x) = \sum_{k=0}^{m \leq x} P[X = x] = \sum_{k=0}^{m \leq x} \binom{n}{x} p^x.(1-p)^{n-x}. \tag{A.6}$$

A.3 Distribuição Geométrica

Considerando uma sucessão de experimentos de Bernoulli, um outro evento de interesse que costuma ser estudado é representado pela variável

aleatória discreta X, cujo valor indica *quantos experimentos devem ser realizados até que ocorra o primeiro sucesso*, ver referência em [53]. É importante notar que, diferente da situação anterior na qual existia uma quantidade determinada, n, de experimentos de Bernoulli, neste caso o valor de X pode variar desde zero até infinito.

Considerando o sucesso ocorrendo na k-ésima realização do experimento de Bernoulli, a função de massa de probabilidade de X será descrita pela expressão seguinte:

$$p_X(k) = P(\underbrace{FF\ldots F}_{k-1}S) = \underbrace{P(F)P(F)\ldots P(F)}_{k-1}P(S) = q^{k-1}.p, \qquad (A.7)$$

para valores de $k = 1, 2\ldots$, sem limite superior estabelecido.

A expressão (A.7) é conhecida como sendo a *função de massa de probabilidade geométrica*. Os parâmetros dessa função de massa são mostrados a seguir:

$$Media = \mu = \frac{1}{p}, \qquad (A.8)$$

$$Variancia = \sigma^2 = \frac{1-p}{p^2}. \qquad (A.9)$$

A função de distribuição de probabilidade geométrica, por seu turno é a seguinte:

$$F_X(x) = \sum_{k=1}^{m\leq x} p_X(k) = \sum_{k=0}^{m\leq x} q^{k-1}.p = 1 - q^m. \qquad (A.10)$$

Apêndice B

O Problema do Coletor de Cupons

B.1 Aspectos Teóricos

Considere-se uma população cujos elementos são de N diferentes tipos e de onde se deseja extrair uma amostra com repetição, que precisa conter r elementos distintos. Deseja-se determinar S_r, o tamanho da amostra. Assim, S_r é a variável aleatória que representa a quantidade de extrações necessárias de serem realizadas, até que seja incluído o r-ésimo sucesso, isto é, até existirem r elementos distintos na amostra. Além disso, sendo

$$X_r = S_{r+1} - S_r, \tag{B.1}$$

então $X_r - 1$ é a variável que representa a quantidade de extrações realizadas na população depois do fato de, na amostra, a quantidade de elementos distintos ser exatamente igual a r, vide [25].

Da definição da variável X_r decorre que

$$\begin{aligned} S_{r+1} &= S_r + X_r \\ &= S_{r-1} + X_{r-1} + X_r \\ &\vdots \\ &= S_1 + X_1 + X_2 + \ldots + X_{r-1} + X_r. \end{aligned} \tag{B.2}$$

Pela sua própria definição, sabe-se que S_1 é a quantidade de extrações para que se obtenha o primeiro sucesso. Mas esse primeiro sucesso ocorre

justamente quando se obtém o primeiro elemento da amostra, quando ainda não pode haver repetição. Por esse motivo, conclui-se que $S_1 = 1$. Desse modo, a expressão para S_r pode ser escrita como segue:

$$S_r = 1 + X_1 + X_2 + \cdots + X_{r-1}, \tag{B.3}$$

O objetivo do Problema do Coletor de Cupons se constitui na obtenção de um estimador para a variável aleatória S_r. A primeira atitude a ser tomada no sentido se obter esse estimador é a aplicação do operador esperança matemática em ambos os lados de (B.3). Levando em conta que esse é um operador linear, segue-se a expressão

$$E[S_r] = E[1 + X_1 + X_2 + \cdots + X_{r-1}] = 1 + \sum_{k=1}^{r-1} E[X_k]. \tag{B.4}$$

Conclui-se, da expressão (B.4), que o estimador da variável aleatória S_r depende apenas da esperança matemática da variável aleatória X_k, para os valores $k = 1, 2, \ldots, r-1$.

A obtenção da esperança matemática de X_k será levada a efeito por meio da variável aleatória discreta $X_k - 1$. Esta última representa a quantidade de fracassos precedendo o próximo sucesso em um experimento de Bernoulli, em uma população na qual $N - k$ elementos distintos ainda não foram selecionados. A partir dessa afirmação pode-se escrever a expressão da função de massa de probabilidade de $X_k - 1$ como segue:

$$Prob(X_k - 1 = \lambda) = q^{\lambda}.p. \tag{B.5}$$

Trata-se de uma função de massa geométrica, sendo λ a quantidade de fracassos antecedendo o primeiro sucesso. O parâmetro p é a probabilidade da ocorrência de um sucesso, enquanto o fracasso tem probabilidade de ocorrência igual a $q = 1 - p$. Logo, a expressão para a esperança matemática de $X_k - 1$ será a seguinte:

$$E[X_k - 1] = \sum_{\lambda=0}^{\infty} \lambda.q^{\lambda}.p. \tag{B.6}$$

Por outro lado, visto que na população, $N - k$ elementos distintos ainda não foram selecionados, tem-se que $p = (N - k)/N$ é a probabilidade da ocorrência de um sucesso. Segue de (B.6) que

$$E[X_k - 1] = q.p.\left(\sum_{\lambda=1}^{\infty} \lambda.q^{\lambda-1}\right) = q.p.\frac{d}{dq}\left(\frac{q}{1-q}\right), \tag{B.7}$$

cujo desenvolvimento permite concluir que $E(X_k - 1) = q/p$, ou ainda, $E(X_k) = 1 + q/p = 1/p$. Devido ao valor de p, essa última expressão pode, finalmente, ser escrita como:

$$E[X_k] = \left(\frac{N}{N-k}\right). \tag{B.8}$$

Finalmente, substituindo (B.8) em (B.4) obtém-se o resultado a seguir:

$$E[S_r] = 1 + \sum_{k=1}^{r-1}\left(\frac{N}{N-k}\right) = N.\sum_{k=0}^{r-1}\left(\frac{1}{N-k}\right). \tag{B.9}$$

Apesar de o raciocínio utilizado para se deduzir a expressão (B.8) ser baseado no fato de que a variável X_k se comporta de acordo com uma distribuição geométrica, essa premissa não é indispensável para encontrar o resultado, pois o problema em questão é de contagem. Desde que o cálculo de uma expressão do tipo (B.9) requer um certo esforço computacional, esse assunto é abordado na próxima seção.

B.2 Técnicas para Cálculos

De acordo com a expressão (B.9) o cálculo de $E[S_r]$ se concentra no somatório das parcelas $(1/(N-k))$, para $r = 0, 1, \ldots, (r-1)$. Observando apenas o somatório da referida expressão é trivial concluir que a igualdade abaixo é verdadeira:

$$\sum_{k=0}^{r-1}\left(\frac{1}{N-k}\right) = \sum_{k=0}^{r-1}\left(\frac{1}{N-((r-1)-k)}\right). \tag{B.10}$$

Como se pode ver, o somatório na direita na expressão (B.11) é o mesmo que está na esquerda, apenas com as parcelas em sentido contrário. Isso significa que a expressão para o valor esperado de S_r, isto é, $E[S_r]$, pode ser escrita como

$$E[S_r] = N.\sum_{k=0}^{r-1}\left(\frac{1}{N-((r-1)-k)}\right). \tag{B.11}$$

Através dessa nova forma de escrever a expressão para $E[S_r]$ pode-se formalizar uma interessante interpretação para o somatório. Basta considerar um sistema de eixos coordenados, no qual a variável k é representada por pontos no eixo horizontal e os valores $(1/(N-((r-1)-k)))$ são as ordenadas

corespondentes. Nessas condições, o somatório poderá ser interpretado como sendo uma soma de produtos de dois fatores.

Com efeito, cada um dos valores de k será a extremidade direita da base de um retângulo, definida como $[k-1, k]$ e de comprimento um. Por sua vez, a ordenada correspondente, $(1/(N-((r-1)-k)))$, é a altura desse mesmo retângulo. As somas das áreas dos retângulos representa exatamente o valor do somatório em (B.11) acima.

Decorre dessa interpretação que, a soma das áreas desses retângulos se torna uma aproximação da integral definida da função $f(x) = x^{-1}$ no intervalo fechado $[N-r+1, N]$. Conforme [10], segue-se a expressão abaixo:

$$E[S_r] \approx N \int_{N-r+1}^{N} x^{-1} dx = N.ln\left(\frac{N}{N-r+1}\right). \tag{B.12}$$

Uma conclusão imediata decorrente de (B.12) é que, no cálculo do valor esperado da variável S_r, a quantidade de extrações necessárias de serem realizadas até que seja incluído o r-ésimo sucesso, tem complexidade $O(N.logN)$. No caso particular em que se tem $r = N$, a expressão (B.11) toma a forma

$$E[S_N] = N. \sum_{k=0}^{N-1} \left(\frac{1}{N-((N-1)-k)}\right). \tag{B.13}$$

Levando em conta a interpretação de que os termos do somatório representam áreas de retângulos com base unitária e altura $(N-((N-1)-k))^{-1}$, então, conforme [10], tem-se

$$\int_1^N \frac{dx}{x+1} \leq \left(\sum_{k=0}^{N-1} \frac{1}{N-((N-1)-k)}\right) - 1 \leq \int_1^N \frac{dx}{x}. \tag{B.14}$$

Convém notar que o somatório considera um retângulo de área igual a um, cuja base é o intervalo $[0, 1]$ e que não está presente no cálculo das integrais. Decorre desse fato a necessidade de ser subtraído o valor um do somatório, para que a expressão (B.14) seja válida.

Depois do cálculo das integrais em (B.14) resulta

$$\ln(N+1) - \ln 2 \leq \left(\sum_{k=0}^{N-1} \frac{1}{N-((N-1)-k)}\right) - 1 \leq \ln N. \tag{B.15}$$

Em decorrência de (B.15), bem como de (B.10), resulta uma importante relação que limita a magnitude do valor esperado para a variável S_N, como

se pode ver a seguir:

$$E[S_N] = N.\left(\sum_{k=0}^{N-1} \frac{1}{N-k}\right) \leq N.(\ln N + 1). \tag{B.16}$$

Apêndice C

Conceitos de Álgebra Abstrata

O desenvolvimento de uma análise com fundamentação matemática, para estudar o problema do rastreamento reverso do número de IP, envolve a necessidade do uso de conceitos da Álgebra Abstrata. Seguem-se alguns enunciados importantes, não somente como suporte à tarefa de entendimento do assunto, como também fundamento ao desenvolvimento de modelos matemáticos para a abordagem do problema.

C.1 Estrutura Algébrica do Tipo Monóide

Seja $\mathcal{C}$ um conjunto no qual se pode definir uma operação binária "$\circ$" entre os seus elementos, que apresenta as seguintes propriedades:

1. *Fechamento* - Se a e $b \in \mathcal{C}$, então $a \circ b \in \mathcal{C}$.
2. *Associatividade* - Se a , b e $c \in \mathcal{C}$, então $(a \circ b) \circ c = a \circ (b \circ c)$.
3. *Identidade* - Existe um elemento $e \in \mathcal{C}$, denominado *identidade*, ou *elemento neutro*, tal que, para todo $a \in \mathcal{C}$, tem-se $a \circ e = e \circ a = a$.

Essas propriedades dão origem à seguinte

Definição C.1. *Sendo $\mathcal{C}$ um conjunto munido da operação $\circ$, que satisfaz às propriedades anteriores, então o par definido como $\mathcal{M} = \langle \mathcal{C}, \circ \rangle$ forma uma* ***estrutura algébrica de monóide****.*

C.2 Estrutura Algébrica do Tipo Grupo

Seja $\mathcal{C}$ um conjunto no qual se pode definir uma operação binária "$\circ$" entre os seus elementos, que apresenta as seguintes propriedades:

1. *Fechamento* - Se a e $b \in \mathcal{C}$, então $a \circ b \in \mathcal{C}$.
2. *Associatividade* - Se a , b e $c \in \mathcal{C}$, então $(a \circ b) \circ c = a \circ (b \circ c)$.
3. *Identidade* - Existe um elemento $e \in \mathcal{C}$, denominado *identidade*, ou *elemento neutro*, tal que, para todo $a \in \mathcal{C}$, tem-se $a \circ e = e \circ a = a$.
4. *Inverso* - Para cada elemento $a \in \mathcal{C}$ existe um outro elemento $a^{'} \in \mathcal{C}$, denominado *elemento inverso de* a, tal que $a \circ a^{'} = a^{'} \circ a = e$.

Essas propriedades dão origem à seguinte

Definição C.2. *Sendo $\mathcal{C}$ um conjunto munido da operação $\circ$, que satisfaz às operações anteriores, então o par definido como $\mathcal{G} = \langle \mathcal{C}, \circ \rangle$ forma uma* ***estrutura algébrica de grupo****.*

Convém observar que uma estrutura do tipo grupo pode ser vista como um monóide no qual cada elemento possui inverso. Pode ocorrer que a operação $\circ$ seja comutativa, isto é, dados a e $b \in \mathcal{C}$, tem-se sempre que $a \circ b = b \circ a$. Neste caso, diz-se que $\mathcal{G} = \langle \mathcal{C}, \circ \rangle$ é um *grupo comutativo*, ou um *grupo abeliano*.

C.3 Estrutura Algébrica do Tipo Anel

Considere-se um conjunto $\mathcal{G}$, sobre cujos elementos se definem e são fechadas as operações de adição, "+", e de multiplicação ".". O terno denominado $\mathcal{R} = \langle \mathcal{G}, +, . \rangle$ recebe a denominação de **anel**, se os seguintes axiomas são satisfeitos:

1. O par $\langle \mathcal{G}, + \rangle$ é um grupo abeliano.

2. A operação de multiplicação é associativa, isto é, sendo $a, b, c \in \mathcal{G}$, então $a(bc) = (ab)c$.

3. Sendo $a, b, c \in \mathcal{G}$, as leis distributivas valem tanto à esquerda, $a(b+c) = ab + ac$, quanto à direita, $(b + c)a = ba + ca$.

Em uma estrutura do tipo anel, $\mathcal{R}$, será sempre possível resolver equações aditivas, do tipo $x + a = b$. Com efeito, sendo $\mathcal{R}$ por definição um grupo abeliano com a operação de adição, para cada elemento $a \in \mathcal{R}$ existe um outro, denominado $(-a) \in \mathcal{R}$, tal que $a + (-a) = 0$. Logo, trivialmente pode-se verificar que a equação aditiva pode ser resolvida.

O conjunto $\mathcal{M}_{nxm}$ das matrizes retangulares de ordem nxm é um exemplo de anel.

C.3.1 Lei do Cancelamento

Um anel $\mathcal{R}$ pode ser fortalecido caso se inclua algumas propriedades na sua operação de multiplicação.

O primeiro destaque é para a chamada **lei do cancelamento**. Um anel está munido dessa lei quando, dados dois elementos quaisquer $a, b \in \mathcal{R}$, tais que $a, b \neq 0$, então $ab \neq 0$. De modo análogo, é possível enunciar essa lei dizendo que, se $a, b \in \mathcal{R}$ satisfazem à expressão $ab = 0$, então $a = 0$, ou $b = 0$. A conjunção "ou" inclui a possibilidade de ambos os valores serem iguais a zero. A afirmação de que em um anel $\mathcal{R}$ vale a lei do cancelamento equivalente a dizer que o anel não possui **divisores de zero**.

C.3.2 Domínio de Integridade

A fim de poder ser útil na solução de problemas reais, as estruturas algébricas precisam ser mais robustas, no que concerne às suas propriedades. Ao mesmo tempo em que restringe a abrangência da estrutura do tipo anel, a lei do cancelamento fornece meios para fortalecer a utilização dessa estrutura na aplicação a problemas reais.

Se em um anel $\mathcal{R}$ que não contém divisores de zero, acrescenta-se à operação de multiplicação as propriedades de possuir elemento identidade e

de ser comutativa, o anel torna-se-á uma estrutura mais robusta. A definição a seguir sintetiza essa idéia:

Definição C.3. *Um anel que não possui divisores de zero e cuja operação de multiplicação é comutativa, e munida de elemento identidade, recebe a denominação de* ***anel de integridade****, ou* ***domínio de integridade****.*

Um exemplo conhecido de domínio de integridade é o conjunto $\mathbb{Z}$, dos números inteiros.

C.4 Estrutura Algébrica do Tipo Corpo

A finalidade de conhecer os diversos tipos de estruturas algébricas decorre da necessidade de resolver problemas, que se apresentam na forma de equações matemáticas.

As equações de natureza aditiva, isto é, $x + a = b$, podem ser resolvidas no âmbito de estruturas algébricas do tipo conhecido como **grupo**. E isso se deve ao fato de que, em um grupo aditivo, todo elemento a possui um inverso aditivo, $(-a)$. Desde que todo anel é um grupo abeliano com a operação de adição, naturalmente tais equações são solúveis em um anel.

Contudo, devido à existência de uma outra operação aritmética, a multiplicação, no âmbito de um anel, pode surgir a necessidade de se resolver uma equação do tipo multiplicativo, isto é, $ax = b$, sendo $a \neq 0$. De modo análogo ao que ocorre na equação de natureza aditiva, torna-se necessário a existência de um inverso multiplicativo para o elemento a. Como se pode ver, as definições concernentes à estrutura do tipo anel não fazem qualquer referência a esse fato.

A incorporação ao anel da propriedade de que, cada elemento $a \neq 0$ possui inverso multiplicativo, implica em que o par $\langle \mathcal{R}, . \rangle$ torna-se um grupo abeliano multiplicativo. Segue-se uma nova estrutura algébrica conforme a definição a seguir:

Definição C.4. *Sendo $\mathcal{R}$ um conjunto munido das operações de adição e de multiplicação, o terno $\mathcal{K} = \langle \mathcal{R}, +, . \rangle$ formará uma* ***estrutura algébrica de corpo*** *se os pares $\langle \mathcal{R}, + \rangle$, e $\langle \mathcal{R}, . \rangle$ são ambos grupos abelianos.*

C.5 Classes Residuais

Considere-se $n \in \mathbb{Z}$ um número inteiro positivo. De acordo com o *Algoritmo de Euclides*, a divisão inteira de qualquer outro número $D \in \mathbb{Z}$, por n, terá como resto um elemento do conjunto $\{0, 1, 2, \ldots, (n-1)\}$. Dessa afirmação, segue a idéia de associar a cada número inteiro, D, o resto obtido da divisão de D por n. Decorre dessa associação que os números inteiros podem ser alocados em classes, conforme a definição a seguir:

Definição C.5. *Denomina-se* conjunto das classes resto módulo n *ao conjunto* $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{(n-1)}\}$, *cujos elementos representam todos os possíveis restos da divisão de um inteiro qualquer por n.*

Decorre da definição C.5 que, dado um número $n \in \mathbb{Z}$, uma classe $\overline{a} \in \mathbb{Z}_n$, originada por um inteiro $0 \leq a < n$, é definida como sendo $\overline{a} = \{a + k.n | k \in \mathbb{Z}\}$, vide [19]. Portanto, qualquer elemento b pertencente à classe $\overline{a}$ é tal que $b - a$ é múltiplo de n, ou seja, $b - a = k.n$, para algum $k \in \mathbb{Z}$.

Uma rápida inspeção na caracterização de uma classe $\overline{a} \in \mathbb{Z}_n$ permite concluir que a classe $\overline{0}$ é constituída pelos múltiplos de do número inteiro n. Além disso, pode-se definir uma operação de adição entre os elementos de $\mathbb{Z}_n$ como sendo $\overline{a} + \overline{b} = \overline{a + b}$, vide [6]. É trivial verificar que essa operação possui a propriedade associativa, herdada da adição entre números inteiros. Além disso, dada a classe $\overline{a}$, define-se a simétrica que lhe corresponde como sendo $-(\overline{a}) = (\overline{-a})$, de modo que $\overline{a} + (\overline{-a}) = (\overline{-a}) + \overline{a} = \overline{0}$. Logo, o par $\langle \mathbb{Z}_n, + \rangle$ apresenta uma estrutura algébrica do tipo grupo. Desde que a operação de adição é comutativa, tem-se que o par $\langle \mathbb{Z}_n, + \rangle$ é um grupo abeliano.

Tal qual a operação de adição em $\mathbb{Z}_n$, que foi herdada da adição no conjunto dos números inteiros, o mesmo ocorre com a operação de multiplicação. Com efeito, é tarefa trivial construir uma estrutura de anel com unidade no terno $\langle \mathbb{Z}_n, +, . \rangle$. Seguem-se alguns importantes resultados, de imediatos efeitos práticos.

Teorema C.1. *Todo domínio de integridade finito é um corpo.*

Demonstração. Sejam $0, 1, a_1, a_2, \ldots, a_n$, os elementos de um domínio de integridade finito, D. Esse domínio será um corpo se, dado um elemento

$a \in D$, $a \neq 0$, existe um outro elemento $b \in D$, tal que $a.b = 1$. Considerem-se, então, os produtos de a por cada um dos elementos de D, isto é, $a.1, a.a_1, a.a_2, \ldots, a.a_n$. Naturalmente, todos os produtos mostrados são distintos pois, caso $a.a_i = a.a_j$, para $i \neq j$, então $a_i = a_j$, pela lei do cancelamento, o que é absurdo. Logo, todos são distintos e, para algum i, deverá ocorrer que $a.a_i = 1$. Logo, D é um corpo. □

E em que condições um anel de classes residuais $\langle \mathbb{Z}_n, +, . \rangle$ pode ser anel de integridade? Basta que esse anel de classes residuais não possua divisores de zero. E isso significa que, dados $\overline{a}, \overline{b} \in \mathbb{Z}_n$, tais que $\overline{a} \neq 0$ e $\overline{b} \neq 0$, então $\overline{a}.\overline{b} \neq 0$. E esse fato ocorrerá desde que não existam dois números inteiros a e b, diferentes de 1 e de n, tal que $a.b = n$. Em outras palavras, n não deve possuir outros divisores que não ele próprio e a unidade, isto é, n deve ser um número primo. Segue, então, o

Corolário C.1. *Se $n \in \mathbb{Z}$ é primo, então $\mathbb{Z}_n$ é um corpo.*

Demonstração. Trivial. □

Apêndice D

Alguns Resultados Matemáticos

Neste apêndice são apresentados, de modo avulso, alguns resultados matemática de uso habitual em diversas classes de problemas, em especial naqueles tratados no presente trabalho. Tais resultados se prestam para utilização em algumas situações específicas, tendo explicação detalhada na seção correspondente.

D.1 Interpolação Polinomial

A observação de fenômenos, seja de que natureza for, é uma atividade que costuma dar origem a conjuntos de dados numéricos cuja apresentação, em geral, envolve pares de números da forma (x_i, y_i). A marcação desses pares de números como pontos em um sistema de coordenadas sugere a interpolação de uma curva entre os mesmos, como forma de melhor compreender o comportamento do fenômeno em estudo.

O desconhecimento da curva representativa do fenômeno que originou os dados induz o pesquisador a interpolar os dados através de um polinômio, devido à simplicidade dessa função. O teorema D.1 apresenta as condições em que um polinômio pode ser interpolado a um conjunto de pontos no plano cartesiano.

Teorema D.1. *Sejam* (x_i, y_i), $i = 0, 1, \ldots, n$, $(n+1)$ *pontos distintos, tal que* $x_i \neq x_j$ *se* $i \neq j$. *Então, existe um polinômio de grau* n, $P(x) = \sum_{k=0}^{n} a_k.x^k$

tal que $P(x_k) = y_k$.

Demonstração. Considere-se o polinômio definido pela expressão

$$P(x) = \sum_{k=0}^{n} y_k . L_{n,k}(x),$$

sendo

$$L_{n,k}(x) = \prod_{\substack{i=0 \\ i \neq k}} \frac{(x - x_i)}{(x_k - x_i)}.$$

É trivial constatar que

$$L_{n,k}(x_j) = \begin{cases} 0 & \text{se} \quad k \neq j \\ 1 & \text{se} \quad k = j \end{cases}$$

Logo conclui-se que $P(x_k) = y_k$. □

O teorema D.1 mostra tanto as condições em que um conjunto de pontos pode ser interpolado por um polinômio, quanto o modo de construir o polinômio. A técnica descrita é conhecida pela denoiminação de *Método de Interpolação de Lagrange.*

D.2 Medição de Complexidade

A complexidade que um algoritmo costuma ser avaliada pela quantidade de recursos que o mesmo demanda, durante o seu funcionamento e o recurso mais significativo costuma ser o tempo de processamento. A priori a velocidade do processador resolveria essa questão, se a mesma não fosse uma característica inerente ao próprio algoritmo. O fato é que a medida da complexidade de um algoritmo deve ser independente da máquina na qual o mesmo deverá funcionar.

O conceito de complexidade de um algoritmo é um problema cujo estudo se assentuou durante o Século XX. O conhecido *Critério de Edmonds* estabelece que um algoritmo pode ser considerado bom (ou eficiente) quando requer um número de passos cujo limite é uma função polinomial no tamanho do problema, ver [11].

O critério supra citado pode ser utilizado para caracterizar a complexidade

de um problema. Com efeito, se a classe de soluções para um determinado problema contém um algoritmo cujo tempo de execução possa ser definido por meio de uma função polinomial, essa será a complexidade do problema. A limitação do uso desse critério reside na dificuldade, maior ou menor, de se encontrar para o problema um algoritmo limitado por função polinomial.

A notação que designa a complexidade de um algoritmo surgiu no livro de Bachmann, ver [4], publicado no final do Século XIX, na Alemanha. A caracterização da complexidade se faz por meio de uma notação característica, ver [52], conforme descrito a seguir.

Definição D.1.

(O Grande) Sejam $f, g : \mathbb{N} \to \mathbb{R}$ funções reais definidas em $\mathbb{N}$. Diz-se que que $f(n)$ pertence à classe $O(g(n))$, $f(n) \in O(g(n))$, ou $f(n)$ é $O(g(n))$, se existe um número positivo M tal que, a menos de uma quantidade finita de exceções, tem-se

$$|f(n)| \leq M|g(n)|.$$

Definição D.2.

(Ω) Sejam $f, g : \mathbb{N} \to \mathbb{R}$ funções reais definidas em $\mathbb{N}$. Diz-se que que $f(n)$ pertence à classe $\Omega(g(n))$, $f(n) \in \Omega(g(n))$, ou $f(n)$ é $\Omega(g(n))$, se existe um número positivo N tal que, a menos de uma quantidade finita de exceções, tem-se

$$|f(n)| \geq N|g(n)|.$$

Definição D.3.

(Θ) Sejam $f, g : \mathbb{N} \to \mathbb{R}$ funções reais definidas em $\mathbb{N}$. Diz-se que que $f(n)$ pertence à classe $\Theta(g(n))$, $f(n) \in \Theta(g(n))$, ou $f(n)$ é $\Theta(g(n))$, se existem números positivos M e N tais que, a menos de uma quantidade finita de exceções, tem-se

$$N|g(n)| \leq |f(n)| \leq M|g(n)|.$$

Definição D.4.

(o Pequeno) *Sejam $f, g : \mathbb{N} \to \mathbb{R}$ funções reais definidas em $\mathbb{N}$. Diz-se que que $f(n)$ pertence à classe $o(g(n))$, $f(n) \in o(g(n))$, ou $f(n)$ é $o(g(n))$, se*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

Apêndice E

Considerações Teóricas da Visão Computacional Probabilística

E.1 Considerações Teóricas

O comportamento da fração em (5.8) depende da relação entre os elementos p e d. A fim de estudá-lo com mais detalhe, considere-se a função real $\xi : \mathbb{R}X\mathbb{R} \rightarrow \mathbb{R}$, dada pela expressão $\xi(x, y) = (ln(x)/y.(1 - y)^{x-1}$, para cada valor tomado para y, podem-se enunciar os resultados a seguir.

Lema E.1. *Sendo* $x \epsilon \mathbb{R} - \{0\}$ *e* $y \epsilon (0, 1)$*, então a função* $\xi(x, y) = (\ln x)/(y.(1 - y)^{x-1})$ *é monótona crescente.*

Demonstração. Considerando x_1, $x_2 \ \epsilon \mathbb{R} - \{0\}$, tal que $x_1 < x_2$, sabe-se que $\ln x_1 < \ln x_2$. Por outro lado, $(1-y)^{x_1-1} > (1-y)^{x_2-1}$, pois $(1-y) < 1$. Então, é fácil concluir que $\dfrac{\ln x_1}{(1-y)^{x_1-1}} < \dfrac{\ln x_2}{(1-y)^{x_2-1}}$, ou seja $\xi(x_1, y) < \xi(x_2, y)$. □

Lema E.2. *A função* $\xi(x, y) = (\ln x)/(y.(1-y)^{x-1})$ *tem a declividade positiva para todo* $x \epsilon \mathbb{R}$*, tal que* $x > 1$ *e* $y \epsilon (0, 1)$*.*

Demonstração. A primeira derivada de $\xi(x, y)$ é dada pela expressão

$$\frac{\partial \xi}{\partial x} = \frac{(1/x) - (\ln x).(\ln(1 - y))}{y.(1 - y)^{x-1}}, \tag{E.1}$$

cujo denominador $y.(1-y)^{x-1}$é sempre positivo. Resta determinar o sinal do numerador $(1/x) - (\ln x).(\ln(1-y))$. Porém desde que $\ln(1-y) < 0$, pois $y \epsilon (0,1)$, conclui-se que o numerador é positivo. Logo, segue o resultado proposto. □

Lema E.3. *Sendo* $d\epsilon\mathbb{R}$*, fixo, e* $y\epsilon(0,1)$*, então a função* $\xi(d,y) = (\ln d)/(y.(1-y)^{d-1})$ *atinge o mínimo quando* $y = 1/d$*.*

Demonstração. Considere-se a função auxiliar $f : (0,1) \rightarrow \mathbb{R}$, dada por $f(y) = y.(1-y)^{d-1}$, cuja derivada tem por expressão $f'(y) = (1-yd).(1-y)^{d-2}$. É fácil ver que essa derivada se anula em $y = 1/d$. Por outro lado, também se constata que, nesse ponto, a segunda derivada da função, cuja expressão é dada por $f''(y) = (-1).(1-yd)^{d-3}.[d.(1-y) + (d-2).(1-yd)]$, assume um valor negativo. Logo, a função auxiliar atinge um valor máximo em $y = 1/d$ e, em conseqüência, a função original $\xi(d,y)$ alcança um valor mínimo no mesmo ponto. □

Os lemas E.1 e E.2 mostram que não há valor global para a probabilidade p que resulte em uma quantidade mínima de pacotes a ser usado na reconstrução da trajetória de ataque. Por outro lado, o exemplo mostrado na tabela 1 permite constatar que, localmente podem ser identificadas condições que minimizam a quantidade de pacotes necessária ao trabalho de reconstrução da trajetória de ataque. Esse fato é conseqüência direta do lema E.3, através e uma interessante e simples relação entre as variáveis y e d. A primeira variável representa a probabilidade p de seleção de um pacote para marcação, enquanto a outra é a distância, em saltos, a que se encontra o roteador marcado.

A relação determinística mostrada no lema E.3 não se consegue obter na prática, em geral. Contudo, o comportamento conjunto entre p e d pode ser descrito de modo mais amplo, de acordo com o

Lema E.4. *Se* $p \in \Theta(1/d)$ *então* $E[Y] \leq O(d.log(d))$*.*

Demonstração. Desde que $p \in \Theta(1/d)$ decorre que existem números A e B, reais positivos, tal que

$$A|1/d| \leq |p| \leq B|1/d|.$$

Decorre da desigualdade anterior que

$$A|1/d| \leq |p| \quad \Rightarrow \quad |A|1/d| - 1| \leq ||p| - 1|$$

$$\Rightarrow \quad 1/|1-p| \leq 1/|A|1/d| - 1| = M.$$

Por outro lado, da expressão (5.8), que é repetida abaixo

$$E[Y] \leq \frac{\ln d}{p.(1-p)^{d-1}}, \tag{E.2}$$

pode-se escrever que

$$|E[Y]| \leq \left| \frac{\ln d}{p.(1-p)^{d-1}} \right| = \left| \frac{1}{(1-p)^{d-1}} \right| .|d.ln(d)| = M.|d.ln(d)|.$$

Logo, pode-se concluir que $E[Y] \in O(d.log(d))$. □

A conclusão que se extrai do lema E.2 diz respeito ao fato de que, se p pertence à $\Theta(1/d)$, então a quantidade de pacotes necessária para se ter a garantia da representatividade de todos os roteadores do ambiente de ataque pertence a $O((d.log(d)))$. De modo menos formal, se o valor de p não fica "muito distante"de $(1/d)$, então a quantidade de mínima de pacotes a ser recebida é de classe loglinear.