UNIVERSIDADE FEDERAL FLUMINENSE

FLÁVIO DE QUEIROZ GUIMARÃES

Modelagem de Ataque de Negação de Serviço nas Redes Centradas em Conteúdo

NITERÓI

2013

UNIVERSIDADE FEDERAL FLUMINENSE

FLÁVIO DE QUEIROZ GUIMARÃES

Modelagem de Ataque de Negação de Serviço nas Redes Centradas em Conteúdo

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Redes e Sistemas Distribuídos e Paralelos.

Orientador:
Prof. Antonio Augusto de Aragão Rocha

Co-orientador:
Prof. Célio Vinicius Neves de Albuquerque

NITERÓI

2013

FLÁVIO DE QUEIROZ GUIMARÃES

Modelagem de Ataque de Negação de Serviço nas Redes Centradas em Conteúdo

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Redes e Sistemas Distribuídos e Paralelos.

Aprovada em setembro de 2013.

BANCA EXAMINADORA

Prof. Antonio Augusto de Aragão Rocha
Orientador, UFF

Prof. Célio Vinícius Neves de Albuquerque
Coorientador, UFF

Prof. Pedro Braconnot Velloso, UFF

Prof. Ana Paula Couto da Silva, UFMG

Niterói
2013

À meu filho Jõao Pedro Diehl Guimarães, que este trabalho lhe sirva de inspiração futura.

Agradecimentos

À Deus por ter me guiado com energia, sabedoria e equilíbrio para que eu pudesse ter logrado êxito em mais uma meta pessoal.

À Marinha do Brasil, que me proporcionou condições para dedicação exclusiva à pesquisa, em especial ao Capitão-de-Fragata Vianna e ao Capitão-de-Corveta Salmon, que desde o início me incentivaram e acreditaram no meu vindouro sucesso e cumprimento desta nobre missão.

Aos professores membros da banca examinadora, por terem manifestado seus juízos de valor, contribuindo sobremaneira para o aperfeiçoamento deste trabalho.

Aos meu orientadores, professores Antonio Augusto (Guto) de A. Rocha e Célio Vinícius N. Albuquerque pela forma honesta, objetiva e profissional com que me conduziram durante todo o processo de pesquisa. Agradeço pelas demonstrações de apoio e inequívoca confiança a mim depositadas. Sou grato por terem compreendido minhas limitações, virtudes e anseios.

Ao grupo do Laboratório Midiacom, em especial aos amigos Diego Passos, Edelberto Silva, Joel dos Santos e Vitor Hugo pelo apoio e amizade. À adorável Sra. Mariester M. L. Outão, pela motivação e forma acolhedora com que pautou o espírito desse laboratório. De forma especial, sou grato ao amigo Igor Ribeiro, companheiro de bancos escolares, conferências e artigos. Obrigado por compartilhar seus conhecimentos. Sua ajuda foi fundamental para o êxito das metas a que me foram determinadas. Deixo a certeza que os laços de amizade firmados nesta instituição me deram suporte para manter meu caminho menos tortuoso. Agradeço a todos pelo convívio e ambiente agradável proporcionados neste período acadêmico.

À minha família, amada esposa Andrea e querido primogênito Jõao Pedro - os dois maiores bens que possuo - agradeço toda a inspiração que vocês me deram, a paciência, as palavras de carinho e estímulo que sempre me revitalizaram nos momentos difíceis desta singradura. Agradeço pela compreensão de minhas ausências e apoio incondicional.

Resumo

Os ataques distribuídos de negação de serviço permanecem um problema constante na Internet atual. As Redes Centradas em Conteúdo - RCC foram propostas como uma nova arquitetura para a Internet do Futuro que possui propriedades que minimizam tais ataques.

No entanto, um novo tipo de ataque de inundação de pacotes pode explorar os protocolo de solicitação e envio de conteúdos na rede. Este artigo propõe uma modelagem analítica dos ataques de inundação nas redes centradas em conteúdo, abordando as condições para ocorrência de tais ataques. Propõe-se também um modelo de otimização que permita maximizar o *throughput* do sistema.

Palavras-chave: Redes centradas em Conteúdo, RCC, negação de serviço, inundação, modelagem.

Abstract

Distributed Denial of Service is still a frequent problem in the current Internet. The Content Centric Networks have been proposed as a new architecture for the Future Internet that has properties that minimize current attacks.

However, a new type of flooding attack packets may exploit the content request and distribution protocols. This paper proposes an analytical modeling of flooding attacks in content centric networks, addressing the conditions for such attacks to occur. It also proposes an optimization model that maximizes the system throughput.

Keywords: Content Centric Networking, CCN, Denial-of-Service, flooding, modeling.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

CCN	:	Content Centric Networking;
DoS	:	Denial-of-Service;
DDoS	:	Distributed Denial-of-Service;
RTT	:	Round Trip Time;
TCP/IP	:	Transmission Control Protocol / Internet Protocol;
NDN	:	Named Data Networking
CS	:	Content Store
PIT	:	Pending Interest table
FIB	:	Forwarding Information Base
RFC	:	Request for Comment
ITU	:	International Telecommunication Union
NS3	:	Network Simulator 3

Sumário

Capítulo 1

Introdução

A Internet inicialmente foi concebida apenas por usuários confiáveis com conhecimento técnico e não existia a necessidade de se criar mecanismos para a proteção desses usuários, tampouco à infraestrutura da rede. Com a sua popularização, houve uma mudança no perfil dos usuários e consequentemente proliferaram as ameaças à segurança da rede como a disseminação de vírus, *spams* e os ataques distribuídos de negação de serviço (*Distributed Denial-of-Service* - DDoS). Um grande problema associado a este tráfego malicioso é o consumo da banda disponível por conteúdos indesejados. Apesar da utilização de *firewalls* prevenir a chegada deste tráfego não desejado aos clientes, há uma carência de mecanismos que possa proteger a infraestrutura da rede. Atualmente, a medida que os serviços essenciais se tornam cada vez mais dependentes da Internet, as consequências dessas ameaças são cada vez mais prejudiciais. Isto ocorre uma vez que a arquitetura da Internet atual não prevê nenhum mecanismo de proteção inerente à própria arquitetura da rede, que possa preservar tanto usuários legítimos como a própria infraestrutura da rede desses usuários maliciosos.

A premissa de não se poder alterar o núcleo da rede dificultou a larga implementação desses mecanismos, uma vez que o paradigma fim-a-fim defendia que os problemas de segurança deveriam ser tratados pela borda da rede através dos sistemas finais. No entanto, o crescimento do número de ataques DDoS ao longo dos anos evidenciou a necessidade de implementar mecanismos de segurança no núcleo da rede [5]. Assim, entre os pré-requisitos já identificados para a "Internet do Futuro" está a minimização dos ataques de negação de serviço [25]. Consequentemente, qualquer proposta de uma nova arquitetura deve limitar os efeitos dos ataques DDoS atuais, antecipar a possibilidade de desenvolvimento de novos ataques e incorporar defesas básicas na sua concepção. Este fato demonstra que há um consenso de que os aspectos de segurança devem ser levados

em conta desde o início do projeto da nova arquitetura da Internet.

A quebra da premissa de não se alterar o núcleo da rede, incentivou a pesquisa em novas propostas de arquiteturas *clean-slates* para a "Internet do Futuro" [38]. Além disso, a necessidade de acompanhar a mudança de perfil dos usuários ao longo dos anos motivou a mudança do paradigma orientado a localização (comunicações entre estações) para um novo paradigma orientado a conteúdo. Em tal processo de evolução, serviços, dados e aplicações são consumidos como conteúdo [1]. Neste contexto, Jacobson *et al.* propuseram as Redes Centradas em Conteúdo (*Content Centric Networking* - CCN), implementando o paradigma orientado a conteúdo, através da desassociação entre o conteúdo e a sua localização física. Assim, os usuários devem ser capazes de requisitar conteúdos pelo nome e cabe a própria rede localizar este conteúdo [19]. A arquitetura CCN é baseada no processo de requisição e resposta, na qual todos os roteadores, chamados de roteadores de conteúdo, funcionam como armazenadores de conteúdo e mantém estado de encaminhamento para cada requisição recebida. Além de propiciar uma disponibilidade e distribuição mais eficiente de conteúdo, a manutenção de estado nos roteadores permite que a CCN minimize a ação de grande parte dos atuais ataques de negação de serviço [**?**]. Dentre tais benefícios, o seu plano de controle de encaminhamento de pacotes proporciona a diminuição do volume do tráfego pela agregação de pacotes, há um balanceamento entre os fluxos de pacotes de requisição e resposta e a possibilidade de recuperação de conteúdos em quaisquer nós da rede.

1.1 Motivação

Qualquer proposta de alteração da arquitetura da Internet envolve o risco de introduzir novas oportunidades de ataque. Apesar da preocupação de se propor uma nova arquitetura mais resiliente às vulnerabilidades existentes na Internet atual, estudos anteriores [30] demonstram que usuários maliciosos podem explorar as características da arquitetura CCN para adaptar ataques tradicionais como os ataques distribuídos de negação de serviço . Um dos principais ataques é o de inundação de pacotes que tem como objetivo o esgotamento dos recursos da estrutura de dados dos roteadores responsável pela manutenção dos estados do plano de encaminhamento de pacotes. Tal estrutura ao manter estado de uma grande quantidade de requisições maliciosas, inibe o atendimento às requisições de usuários legítimos. Diferentemente dos ataques de inundação de pacotes na arquitetura TCP/IP, os principais alvos são os roteadores da rede e não propriamente servidores, uma vez que usuários maliciosos exploram a manutenção de estado dos roteadores de conteúdo.

1.2 Objetivos

Este trabalho tem como objetivo propor uma modelagem analítica de um roteador de conteúdo sob ataque de inundação de pacotes. Além disso, propõe-se uma análise da influência positiva (ou negativa) da definição do tempo máximo de permanência (*timeout*) dos estado nos roteadores na mitigação dos ataques de inundação. Com isso, pretende-se revelar a existência de um *trade-off* para este valor definido pelo roteador e busca-se avaliar a fragilidade da proposta CCN aos ataques de inundação.

Para alcançar este objetivo

1.3 Contribuições

Como contribuições deste trabalho pode-se destacar:

i) Uma modelagem analítica dos fluxos de um roteador de conteúdo sob ataque de inundação, onde a abstração definida pelo modelo consiste em um sistema de filas $M/G/c/c$, com limitação da taxa de serviço. O modelo permite uma melhor compreensão do desempenho sob ataque DDoS da estrutura de dados responsável pela manutenção de estado. Além disso, a modelagem contribui para o entendimento de como detectar o ataque de inundação através da observação do comportamento estatístico do tráfego;

ii) Um modelo de otimização para o estabelecimento do tempo máximo de permanência dos estados nos roteadores (*timeout* ótimo). A formulação permite maximizar a *throughput* útil do sistema através da obtenção do valor ótimo para o *timeout* dos roteadores de conteúdo; e

iii) Comparação dos resultados numéricos entre o modelo analítico e o modelo de otimização através de simulações do fluxo de requisições legítimas e maliciosas em um roteador de conteúdo.

1.4 Organização

O trabalho está organizado em um total de sete capítulos. Após este capítulo introdutório, são apresentados no Capítulo 2 a fundamentação teórica sobre os conceitos fundamentais

da CCN e questões de segurança envolvendo suas fragilidades. No Capítulo 3 são abordadas as características dos ataques de negação de serviço na CCN. O Capítulo 4 propõe uma modelagem analítica de um roteador de conteúdo sob ataque de inundação de pacotes, seguido da sua avaliação experimental abordada no Capítulo 5. A modelagem de otimização do tempo máximo de permanência dos estados é exposta no Capítulo 6. Por fim, conclui-se o trabalho com a exposição das considerações finais e trabalhos futuros no Capítulo 7.

Capítulo 2

Fundamentação Teórica

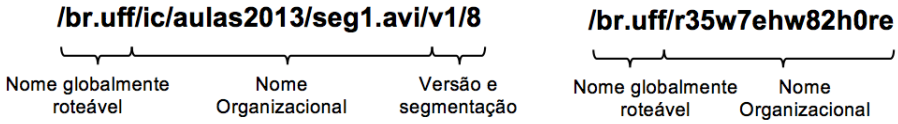
A arquitetura CCN desassocia os conteúdos de sua localização física e possibilita que usuários consumidores requisitem os conteúdos disponibilizados por usuários publicadores através da nomeação explícita dos conteúdos, sem se preocupar com o local de armazenamento dos mesmos. Desta forma, a CCN utiliza o conteúdo como objeto elementar da rede, onde a própria infraestrutura da rede, por sua vez, é responsável por encontrar e devolver o conteúdo requisitado pelos consumidores. Diferentemente da Internet atual, a CCN mantém o conteúdo ("o quê") como o seu papel central, ao invés de "onde"o conteúdo está localizado. Os princípios arquitetônicos da CCN são implementados através do projeto *Named-Data Networking* - NDN [42] no qual se encarrega de pesquisar os desafios técnicos que devem ser abordados para validar a CCN como uma arquitetura da "Internet do Futuro"através de *testbeds* e simulações. Para um melhor entendimento da arquitetura CCN, faz-se necessário destacar os princípios fundamentais da arquitetura CCN, conhecer as estruturas de dados internas de um roteador de conteúdo e compreender o processo de recuperação de conteúdo.

2.1 Princípios Fundamentais da Arquitetura CCN

A principal distinção da CCN para as redes TCP/IP é o fato de que cada fragmento de de conteúdo (*chunk)* da CCN tem um nome atribuído e os pacotes de requisição e resposta são encaminhados pelos nomes ao invés de endereços IP. Além disso, a CCN possui alguns princípios fundamentais arquitetônicos: modelo de comunicação baseado no receptor, esquema próprio de nomeação de conteúdo, arquitetura baseada em rede de *caches* mecanismos de segurança inerentes a rede.

- **Modelo de comunicação baseado no receptor:** Na comunicação baseada no processo de requisição e resposta, os receptores (usuários consumidores) são responsáveis por manifestar seu interesse ao conteúdo desejado. Um consumidor envia um pacote de requisição de conteúdo à rede, na qual será respondido no máximo com um único pacote de resposta com o conteúdo desejado. Assim, o consumidor é responsável por enviar uma nova requisição, caso não receba o conteúdo requisitado. Desta forma, o consumidor torna-se responsável por retransmitir uma requisição mal sucedida. Este modelo contribui para um balanceamento de fluxos entre os pacotes de requisição e resposta, diminuindo o volume de tráfego na rede.

- **Nomeação de Conteúdos:** Como na CCN os conteúdos são independentes da sua localização física, eles são considerados como dados com nomes arbitrários definidos pelos usuários publicadores. Para isso, os nomes devem seguir uma estrutura hierárquica semelhante a URLs. Os nomes dos conteúdos são formados por um conjunto de componentes separados entre si pelo caractere "/", representando uma hierarquia [19]. Os nomes hierárquicos, também chamados de prefixos, são opacos à rede. Isto significa que os roteadores de conteúdo não têm conhecimento da semântica desses nomes e apenas sua estrutura hierárquica é relevante. Por exemplo, um fragmento de conteúdo publicado pelo Instituto de Computação da Universidade Federal Fluminense para o vídeo da primeira aula de segurança da informação poderia ser requisitado pelo identificador: `/uff.br/ic/aulas2013/seg1.avi/v1/8`. Desta forma a requisição é encaminhada de acordo com o nome globalmente roteável `/uff.br`, conforme representado pela Figura 2.1(a).



(a) Exemplo de nome hierárquico legítimo (b) Exemplo de nome hierárquico malicioso

Figura 2.1: (a) Exemplo de nome hierárquico legítimo e (b) malicioso

Grandes conteúdos podem ser divididos em fragmentos menores (*chunks*), onde neste caso, é o oitavo fragmento do conteúdo. Dessa forma, contanto que os nomes sigam tal estrutura, os publicadores de conteúdo são livres para adotar qualquer padrão de nomeação que atenda melhor as suas necessidades. Estas propriedades também permitem que os consumidores requisitem um nome de um conteúdo inexistente cujo publicador seja capaz de gerar o conteúdo de desejo dinamicamente. Por

outro lado, possibilita que consumidores maliciosos manifestem interesse a um conteúdo inexistente, ao atribuir um nome aleatório qualquer, conforme representado pela Figura 2.1(b).

- **Tipos de Pacotes de Requisição e Resposta da CCN:** Toda a comunicação na CCN é baseada no processo de requisição e resposta de conteúdo, onde são utilizados apenas dois tipos de pacotes: Pacotes de Interesses e Pacotes de Dados. Os consumidores solicitam um conteúdo à rede ao enviar um Pacote de Interesse que transporta o nome do conteúdo desejado, no qual é utilizado pelos roteadores para estabelecer o encaminhamento dos pacotes. Um determinado Pacote de Interesse pode ser "satisfeito" por quaisquer roteadores da rede, por outros consumidores ou pelo publicador original através da emissão do respectivo Pacote de Dados no qual transporta o conteúdo requisitado, conforme representado pela Figura 2.2.

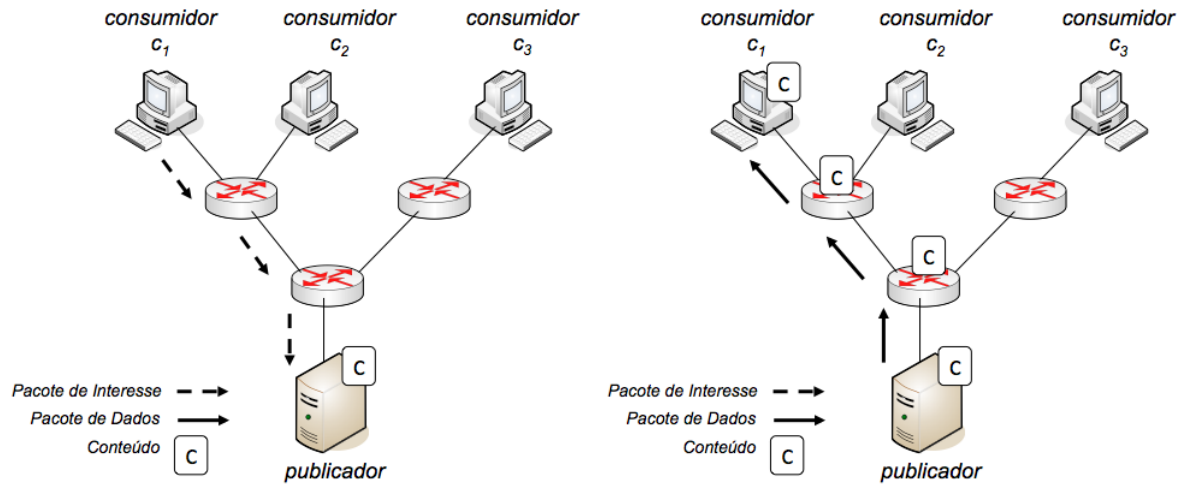


Figura 2.2: Exemplo de encaminhamento de Pacote de Interesse e transmissão de Pacote de Dados. (a) Um consumidor c_1 emite à rede um Pacote de Interesse para um conteúdo C qualquer. Como não há tal conteúdo disponível em *cache*, o Pacote de Interesse é encaminhado salto a salto até o publicador fonte de conteúdo. (b) O publicador responde ao Pacote de Interesse transmitindo o respectivo Pacote de Dados. Neste caso, o Pacote de Dados com o conteúdo C é replicado no núcleo da rede.

Por questões de segurança, todos os Pacotes de Dados são assinados digitalmente pelo publicador de conteúdo de forma a certificar a ligação entre o conteúdo e seu nome. Para que essa assinatura possa ser verificada, tais pacotes também contêm informações como o algoritmo de criptografia utilizado e um localizador para a recuperação da chave pública do publicador. Tal fato possibilita a verificação da assinatura pelos consumidores e possivelmente pelos roteadores da rede.

- **Arquitetura baseada em rede de *caches*:** Como os roteadores da CCN possuem a funcionalidade de armazenar conteúdos, caracteriza-se a CCN como uma grande rede de *caches*. Assim, em requisições posteriores o mesmo conteúdo desejado pode ser recuperado do *cache* mais próximo, reduzindo o tempo de resposta e o consumo de largura de banda no núcleo da rede, conforme ilustrado pela Figura 2.3.

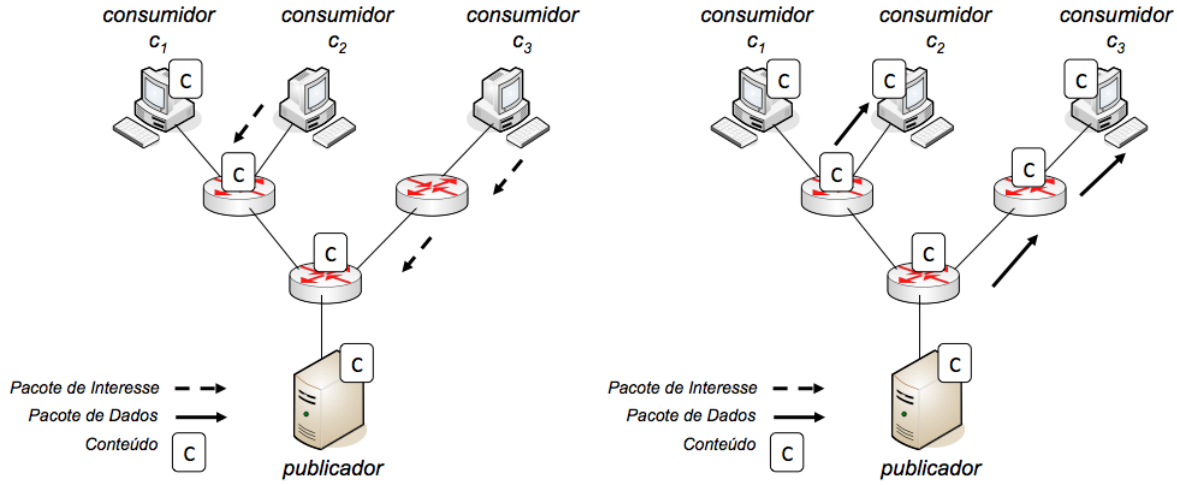


Figura 2.3: Exemplo de recuperação de conteúdo através dos *caches* da rede. Consumidores c_2 e c_3 emitem à rede um Pacote de Interesse para um conteúdo C qualquer. Como há cópia do Pacote de Dados com o conteúdo C nas *caches*, os roteadores respondem diretamente aos consumidores.

2.2 Roteadores de Conteúdo

O projeto dos roteadores de conteúdo é facilmente implementável quando comparados com os roteadores atuais e estudos anteriores indicam que há um maior nível de eficiência na distribuição de conteúdo quando comparados com a atual rede [4]. Apesar da ideia de implementação de *caching* nos roteadores não ser nova, na CCN tal funcionalidade permite que os roteadores sejam uma fonte independente de conteúdo. Os roteadores de conteúdo além de manterem estruturas para o *caching* de conteúdo, possui outras estruturas internas responsáveis pela manutenção de estado de encaminhamento de pacotes e roteamento.

2.2.1 Estruturas Internas de um Roteador de Conteúdo

Cada nó da arquitetura CCN mantém três estruturas de dados distintas para operações de encaminhamento de pacotes: um Armazenador de Conteúdo (*Content Store* - CS), uma Tabela de interesses pendentes (*Pending Interest Table* - PIT) e uma base de informações de encaminhamento (*Forwarding Information Base* - FIB), conforme representado pela Figura 2.4.

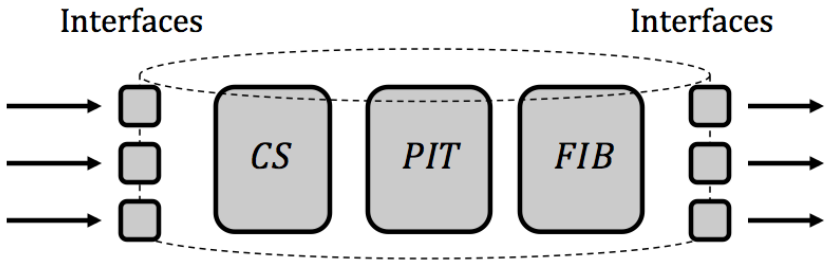


Figura 2.4: Representação das estruturas internas de um roteador de conteúdo.

2.2.2 Armazenador de Conteúdos

O CS provê a funcionalidade do aumento da eficiência da recuperação do conteúdo pelos consumidores através da disponibilidade de conteúdo em *cache* nos roteadores. Para isso, o CS mantém dois componentes principais: um armazenador de Pacotes de Dados e uma tabela de índices com os nomes dos conteúdos contidos em seu *cache*. Tal tabela se mantém atualizada e possibilita verificar o nome do Pacote de Interesse com o nome dos conteúdos armazenados nos Pacotes de Dados através da correspondência pelo maior prefixo. A atualização da tabela indexada depende do período de expiração e política de substituição de *cache* adotada. O primeiro componente do roteador a ser acessado ao receber um Pacote de Interesses é o CS. Após o recebimento de tal pacote são executadas as operações: a correspondência pelo maior prefixo do nome do conteúdo existente na tabela indexada e a atualização da tabela indexada em caso de expiração do Pacote de Dados em *cache*. Esta última operação depende diretamente da política de substituição adotada como LRU, LFU ou *random*.

2.2.3 Tabela de Interesses Pendentes

A PIT pode ser entendida de maneira simplificada como uma tabela *hash* indexada por nomes de conteúdo. Cada uma de suas entradas armazena uma ou múltiplas interfaces físicas de chegada por onde os Pacotes de Interesses para um mesmo conteúdo foram

recebidos e uma ou múltiplas interfaces de saída, indicando que o Pacote de Interesse foi encaminhado por vários caminhos definidos pela FIB. Além de manter as interfaces de entrada e saída, a PIT registra os *nonces* de cada Pacote de Interesse. Assim, se um mesmo Pacote de Interesse for recebido mais de uma vez pelo mesmo roteador, há a comparação dos *nonces* e o Pacote de Interesse repetido é descartado. Isto evita a formação de *loops* pelos pacotes.

Ao receber um Pacote de Dados, o roteador de conteúdo utiliza o nome do conteúdo para consultar a PIT através da correspondência de maior prefixo para obter a lista de interfaces por onde os Pacotes de Interesses para este conteúdo foram recebidos. O Pacote de Dados é então transmitido por todas as interfaces registradas nesta lista. A partir deste processo, conclui-se que os conteúdos requisitados retornam aos consumidores seguindo o caminho inverso daquele criado pelo seu respectivo Pacote de Interesse. A manutenção de estado dos interesses pendentes da PIT permite a agregação de Pacotes de Interesse, na qual contribui para a redução o consumo de largura de banda no núcleo da rede. Uma vez que os Pacotes de Dados sempre retornam pelo caminho inverso do seu respectivo Pacote de Interesse, os roteadores de conteúdo não precisam encaminhar mais de um Pacote de Interesse para o mesmo conteúdo.

Desta forma, a PIT mantém o estado dos interesses pendentes, ainda “não satisfeitos"pelo roteador recebedor dos respectivos Pacotes de Interesse. Cada interesse pendente possui um tempo de permanência (*lifetime*) associado à sua entrada na PIT, na qual é removida após a expiração do *timeout* defindo pelo roteador. Logo, uma entrada da PIT pode ser removida de duas maneiras: ao receber um Pacote de Dados de forma a“satisfazer"o interesse pendente, onde o tempo de permanência da entrada depende do RTT ou após a expiração do *timeout* estabelecido previamente.

2.2.4 Base de Informações de Encaminhamento

A FIB de um roteador de conteúdo é semelhante a de um roteador IP. Geralmente uma FIB IP associa um prefixo de rede específico a uma única interface de saída. Esta interface de saída faz parte do caminho de melhor custo calculado pelo protocolo de roteamento. Por outro lado, a FIB CCN mantém uma lista com várias interfaces de saída dos nomes globalmente roteáveis, permitindo que um pacote de interesse seja encaminhado através de múltiplos caminhos. Caso um Pacote de Interesse for recebido por um nó da rede e o conteúdo requisitado não estiver em seu CS e também não existir uma entrada correspondente na PIT ou na FIB, este interesse será descartado.

2.3 Processo de Encaminhamento e Recuperação de Conteúdos

um roteador de conteúdo realiza diferentes processos para o encaminhamento de Pacotes de Interesses e recebimento de Pacotes de Dados.

Ao receber um Pacote de Interesse por uma interface i qualquer um roteador R segue as seguintes operações:

- **Verificação no CS:**

  1) Extrai o nome do conteúdo do Pacote de Interesse e realiza uma busca (*lookup* pelo maior prefixo em seu CS.

  2) Caso haja uma correspondência o roteador transmite o Pacote de Dados armazenado no CS para para a(s) interface(s) de chegada do Pacote de Interesse.

- **Verificação na PIT:**

  3) Caso não haja o conteúdo em *cache*, o roteador verifica se já existe uma entrada em sua PIT para o conteúdo.

  4) Caso exista, o roteador verifica se o *nonce* do interesse recebido está contido na lista de *nonces* armazenada na entrada da PIT. Em caso afirmativo, o interesse recebido é uma cópia duplicada e é descartado. Caso contrário, a sua interface de entrada i e seu *nonce* são armazenados nesta entrada da PIT e em seguida o interesse é descartado.

- **Verificação na FIB:**

  5) Caso não haja entrada correspondente na PIT, o roteador faz uma busca de maior prefixo em sua FIB, tentando encontrar interfaces de saída para encaminhar o interesse. Se nenhuma interface de saída for encontrada para o conteúdo requisitado pelo interesse, então este é descartado. Caso contrário, é criada uma entrada na PIT contendo a interface de chegada e o *nonce* do interesse, conforme representado pela Figura 2.5.

Ao receber um Pacote de Dados por uma interface i qualquer um roteador R segue as seguintes operações:

- **Verificação na PIT:**

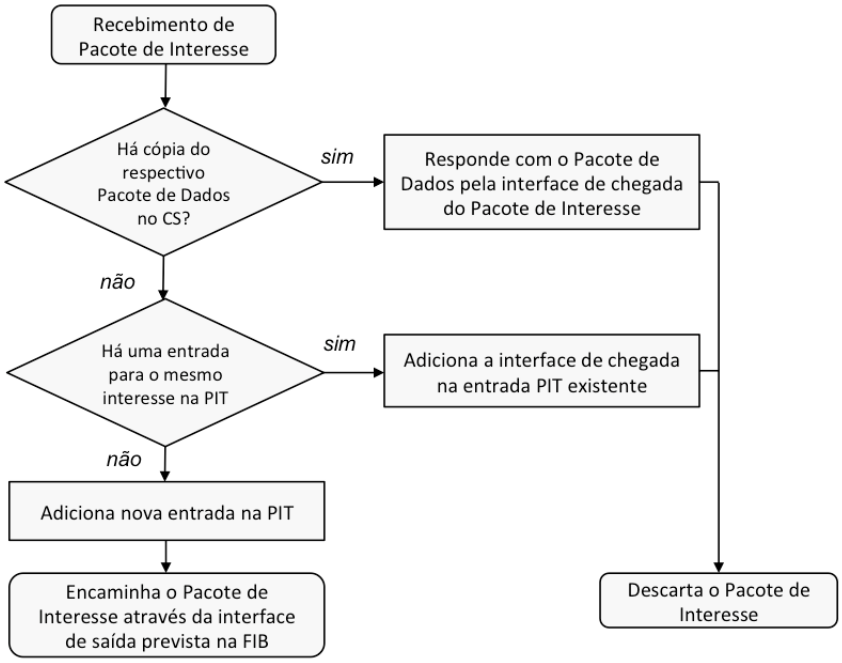


Figura 2.5: Fluxograma do processo de recebimento de um Pacote de Interesse

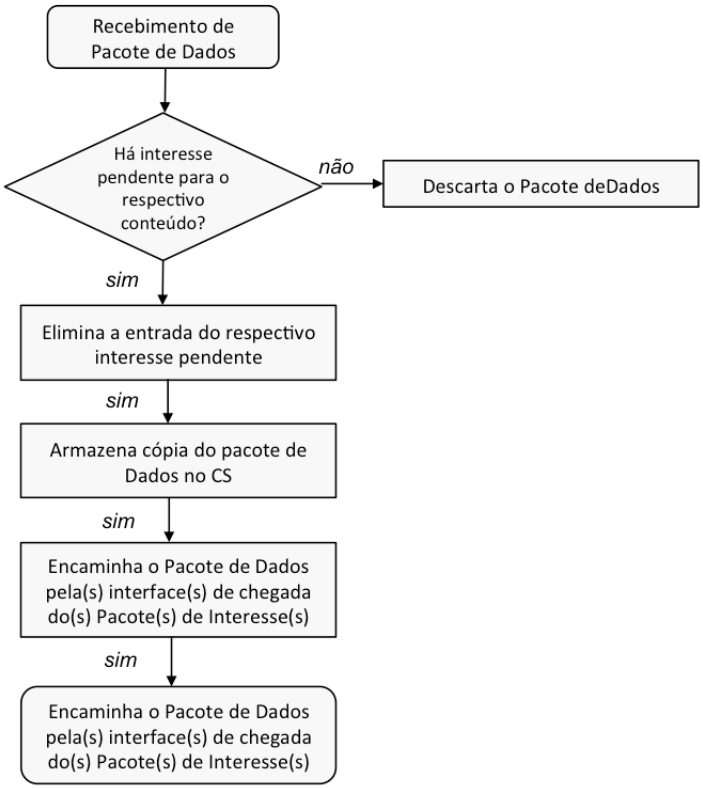


Figura 2.6: Fluxograma do processo de recebimento de um Pacote de Dados

1) Extrai o nome do conteúdo e verifica se existe alguma entrada na PIT para o mesmo. Caso não exista, significa que a entrada para o interesse pendente foi expirada e o Pacote de Dados é descartado.

2) Caso exista, a entrada na PIT é removida e o Pacote de Dados é armazenado no CS do roteador e em seguida é encaminhado por todas as interfaces contidas na entrada da PIT, conforme representado pela Figura 2.6.

2.3.1 Resumo dos Principais Eventos Participantes na Mudança de Estado em um Roteador de Conteúdo

Destacam-se como principais eventos que influenciam na alteração de estado da PIT de um roteador de conteúdo:

i) *Chegada de um Pacote de Interesse*: Evento gerado com o processamento de um Pacote de Interesse na PIT após a confirmação de não haver o conteúdo de interesse em *cache* através da verificação no CS;

ii) *Bloqueio de Pacote de Interesse*: Evento gerado pelo esgotamento de recursos da PIT, obrigando o descarte do Pacote de Interesse;

iii) *Satisfação de Interesse pendente*: Evento gerado através da chegada do respectivo Pacote de Dados “satisfazendo"o interesse pendente; e

iv) *Expiração de Interesse pendente*: Evento gerado após término do tempo máximo de permanência de um interesse pendente na PIT (*timeout*, conforme representado pela Figura 2.7.

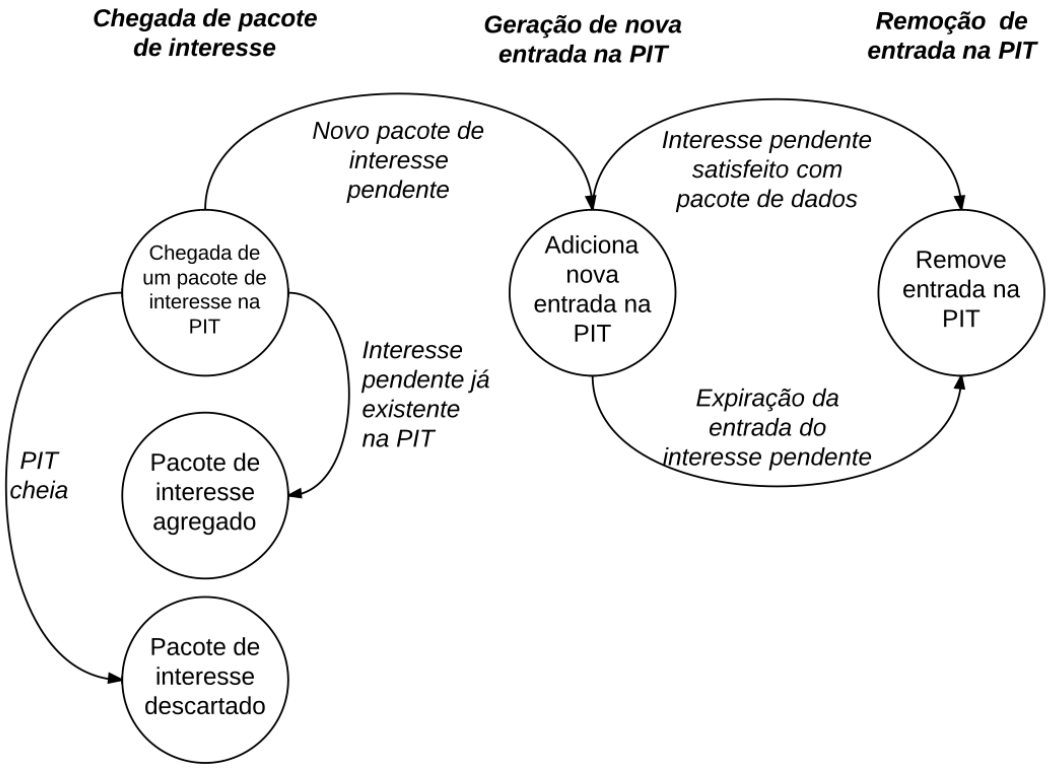


Figura 2.7: Eventos que influenciam a mudança de estado da PIT.

Capítulo 3

Ataques de Negação de Serviço na CCN

De acordo com o exposto no capítulo anterior a CCN possui propriedades que contribuem para minimizar os ataques de negação de serviço quando comparados com a rede atual. Tais propriedades como o balanceamento de fluxo entre Pacotes de Interesse e de Dados, a agregação de Pacotes de Interesse e a recuperação de conteúdos nos *caches* diminuem o volume de tráfego no núcleo da rede. O próprio paradigma orientado a conteúdo contribui para a mitigação de ataques de negação de serviço, uma vez que os pacotes não transportam informações de origem e destino, dificultando o direcionamento à alvos específicos. Assim, ataques tradicionais na Internet atual como ataque por reflexões, esgotamento de largura de banda e "buraco negro"podem ser mitigados pela arquitetura CCN [**?**]. Apesar disso, pode-se criar variações efetivas de tais ataques e usar maliciosamente as propriedades da CCN para reproduzi-los. Usuários mal comportados podem negar os serviços oferecidos pela arquitetura CCN restringindo seus benefícios, através envenenamento de *caches*, ao disseminar conteúdo corrompido na rede e explorar a manutenção de estado na PIT dos roteadores, ao inundar a rede com Pacotes de Interesses maliciosos e impedir o atendimento de interesses pendentes legítimos.

3.1 Principais Definições e Objetivos dos Ataques de Negação de Serviço

Pode-se entender que o conceito de serviço na CCN se estende ao aumento da disponibilidade de conteúdo e diminuição do tempo de recuperação (RTT) dos mesmos, quando comparados a arquitetura atual da Internet. Para um melhor entendimento, aborda-se os conceitos de disponibilidade, serviço e os objetivos dos ataques de negação de serviço.

i) *Disponibilidade*: A disponibilidade está entre os principais serviços de segurança de redes de computadores [33]. A recomendação X.800 da *International Telecommunication Union*- ITU, *Security architecture for Open Systems Interconections* - OSI, define disponibilidade como "uma propriedade de estar acessível e utilizável mediante requisição de uma entidade autorizada"[37]. A disponibilidade pode ser definida de uma forma menos abrangente como "a capacidade de uso de uma informação ou um recurso desejado [6]. Em uma descrição mais formal, de acordo com o RFC 2828 - *Internet Security Glossary*, a disponibilidade é definida como sendo "a propriedade de um sistema ou de um recurso do sistema ser acessível e utilizável sob demanda por uma entidade autorizada do sistema, de acordo com especificações de desempenho"[32]. Assim, pode-se determinar que um sistema se torna disponível caso ofereça seus serviços de acordo com a demanda de projeto sempre que solicitado por usuários legítimos. Neste contexto a CCN torna acessível a seus usuários todas a propriedades arquitetônicas desenvolvidas em sua arquitetura.

ii) *Serviço*: Um serviço pode ser caracterizado como uma determinada função de um nó ou infraestrutura da rede que visa atender a uma demanda específica[22]. Pode ser o uso de um buscador de páginas, a compra de produtos ou uma troca de mensagens entre dois nós da rede. Assim, a manutenção de estado nos roteadores pode ser caracterizada como um serviço aos seus usuários.

iii) *Ataques de Negação de Serviço*: Os ataques que visam bloquear a disponibilidade dos sistemas ou serviços de um nó componente de uma rede de computadores são geralmente tratados como ataques de negação de serviço (*Denial-of-Service* - DoS). Uma definição apresentada por [14] assume que o ataque DoS é a indisponibilidade de um serviço específico autorizado a usuários legítimos por um período de tempo que excede o tempo de espera de processamento pretendido. De acordo com o RFC 4732 [15] o ataque DoS "é um ataque no qual uma ou mais máquinas-alvo tentam impedir a vítima de fazer um trabalho útil". Assim, o objetivo dos ataques DoS é interromper os serviços providos pela vítima aos usuários legítimos, mesmo que temporariamente, tornando-os indisponíveis. A vítima deixa de oferecer o seu serviço aos clientes legítimos enquanto tenta tratar o tráfego gerado pelo ataque [23].

Na CCN além do ataques de envenenamento de *caches*, usuários maliciosos podem explorar a manutenção de estado dos roteadores através dos ataques de inundação de pacotes de Interesses.

3.2 Robustez da CCN à Ataques de Negação de Serviço

A arquitetura da CCN possui algumas propriedades importantes que contribuem para a robustez em relação aos ataques de negação de serviço.

Na CCN existe uma relação direta entre os Pacotes de Interesses e seus respectivos Pacote de Dados, uma vez que ambos possuem o mesmo nome, no qual é o nome do conteúdo desejado. Esta relação proporciona um balanceamento de fluxos, permitindo que um Pacote de Interesse recupere apenas um único Pacote de Dados. Tal propriedade contribui para dificultar os ataques de negação de serviço, uma vez que a geração de pacotes maliciosos somente pode ser estabelecida pela emissão de Pacotes de Interesses.

Outra propriedade que caracteriza a arquitetura CCN é o encaminhamento dos Pacote de Dados exatamente pelo mesmo caminho percorrido pelo seu respectivo Pacote de Interesse, ou seja, o encaminhado se dá pelo caminho inverso. Tal propriedade geralmente é utilizada pelas propostas de mitigação de ataques de negação de serviço.

Já pela propriedade da agregação de pacotes de interesse, caso um roteador receba múltiplos Pacotes de Interesses para o mesmo conteúdo, ele encaminhará para o próximo salto apenas um único Pacote de Interesse, mantendo o registro das interfaces de chegada de tais interesses na PIT. Este mecanismo, contribui para minimizar o volume de tráfego da rede e consequentemente obriga aos usuários maliciosos a gerarem tráfego de ataque com diferentes nomes de conteúdos de forma a inibir o mecanismo de agregação de Pacotes de Interesse.

Como na CCN todos os nós da rede possuem um CS, quaisquer nós intermediários somente encaminharão os Pacotes de Interesses até a fonte de conteúdo (publicador), caso não exista a cópia do conteúdo desejado nos seus CS's. Isso possibilita a diminuição do volume de tráfego até a fonte de conteúdo.

A possibilidade de detecção e eliminação de *loops* na rede permite que os roteadores explorem a redundância topológica, encaminhando os pacotes por múltiplos caminhos, contribuindo para a redução de ataques de negação de serviço, uma vez que uma forma de reação ao ataque é a tentativa de encaminhamento por caminhos alternativos. Isso aumenta a probabilidade de encaminhamento de pacotes por um caminho que não tenha sido afetado pelo ataque.

Devido a essas características, grande parte dos ataques tradicionais de negação de serviço [24], como ataques por reflexão, esgotamento de largura de banda e buraco negro

são mitigados. Porém novas vulnerabilidades foram exploradas pelos usuários maliciosos de forma a adaptar os ataques de negação de serviço à arquitetura da CCN.

3.2.0.1 Ameaças à CCN

Apesar da aparente falta de eficácia ou de redução do impacto dos ataques de DoS, algumas variações dos ataques atuais podem ser bastante eficaz contra a CCN. Para isso, o usuário malicioso deve buscar explorar as características fundamentais que distinguem os roteadores da Internet atual dos roteadores de conteúdo: a manutenção do estado dos interesses pendentes (entradas da PIT) necessárias para realizar o encaminhamento de conteúdo, a agregação de pacotes e o uso de *caches* de conteúdo.

A PIT suporta um um número limitado de entradas e existem duas formas de se remover uma entrada da PIT, quando um Pacote de Dados "satisfaz"o interesse pendente ou pela expiração do (*lifetime*) da entrada. Com isso, caso a PIT esteja completamente cheia, os novos interesses recebidos pelo roteador de conteúdo serão descartados, uma vez que a CCN implementa a política de substituição *Tail Drop*. O problema da escalabilidade da PIT foi levado em consideração por [29] e em [11]. Em [39] são analisados a manutenção do estado na PIT, identificando a exaustão da memória com a transmissão excessiva de Pacotes de Interesses. A fragilidade do esgotamento dos recursos da PIT pode ser explorada por usuários maliciosos, através da emissão de uma quantidade considerável de Pacotes de Interesses, inibindo o atendimento de interesses pendentes de usuários legítimos. Este ataque é conhecido como Ataque de Inundação de Pacotes de Interesses, conforme representado na Figura 3.4.

3.3 Ataques de Inundação de Pacotes de Interesse

Os Pacotes de Interesse da CCN são encaminhados através da rede de acordo com os prefixos dos conteúdos, consumindo os recursos da PIT dos roteadores, conforme representado pela Figura 3.1. Porém, a PIT pode sofrer o chamado “efeito *Slashdot*" [11], onde a demanda para atendimento de interesses pendentes aumenta para um nível mais elevado que o habitual. Isso torna os Pacotes de Interesse um potencial meio para adaptação dos ataques de negação de serviço por inundação na CCN.

Como roteadores de conteúdo mantém o estado de encaminhamento na PIT para cada Pacote de Interesse encaminhado, ou seja, para cada uma de suas entradas, ao receber uma quantidade excessiva de pacotes maliciosos pode ocorrer esgotamento dos recursos

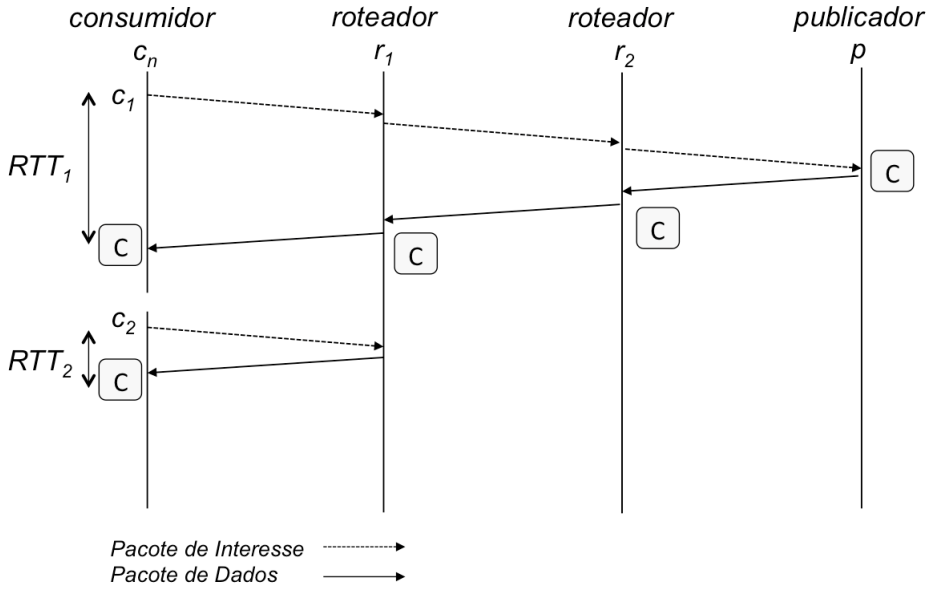


Figura 3.1: Abstração do uso legítimo do protocolo de encaminhamento de pacotes

do roteador, fazendo com que o ele seja incapaz de criar novas entradas ao bloquear o recebimento de Pacotes de Interesses legítimos, conforme representado pela Figura 3.2.

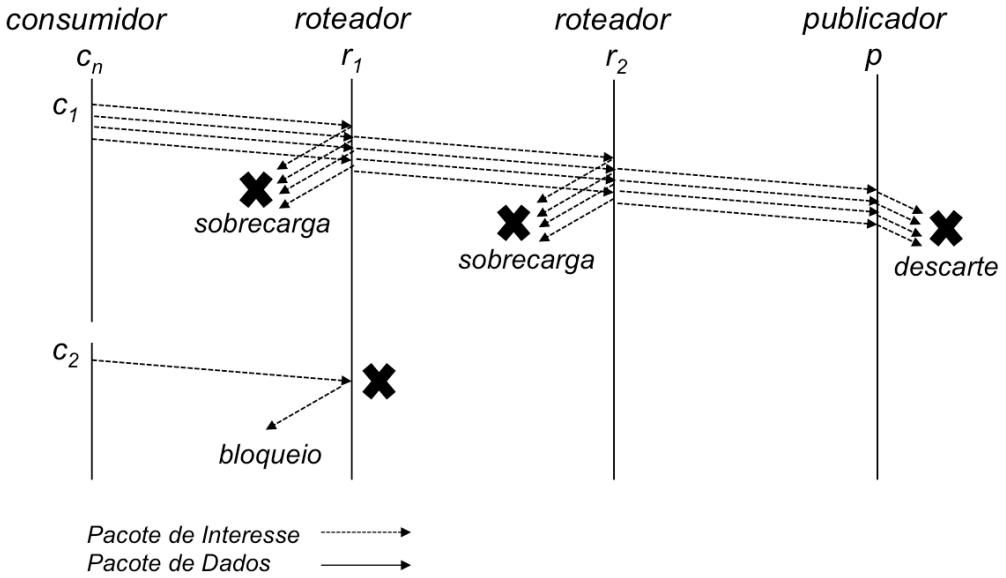


Figura 3.2: Abstração do ataque de inundação de Pacotes de Interesses

3.3.1 Composição do Tráfego Malicioso

Conforme observado em [13], os ataques de negação de serviço por inundação de Pacotes de Interesses podem ser divididos em três categorias, dependendo do tipo de conteúdo requisitado no ataque:

i) *Conteúdos Existentes*: aqueles que foram publicados e estão disponíveis na rede para serem requisitados pelos usuários, como por exemplo o quarto fragmento de conteúdo multimídia `/music.com/playlist/audio1.mp3/4`;

ii) *Conteúdos Gerados dinamicamente*: aqueles gerados apenas quando requisitados através de um Pacotes de Interesse, como por exemplo um *Dynamic* DHTML *web site* `/server.com/pages/mypage.dhtml`; e

iii) *Conteúdos Inexistentes*: aqueles cujos Pacotes de Interesse nunca serão atendidos, ou seja, as entradas dos interesses pendentes na PIT nunca serão "satisfeitas". Um exemplo de geração de conteúdo com nome aleatório como `/domain.com/q2xzk9r/5` para ataque de inundação é representado pela Figura 3.3;

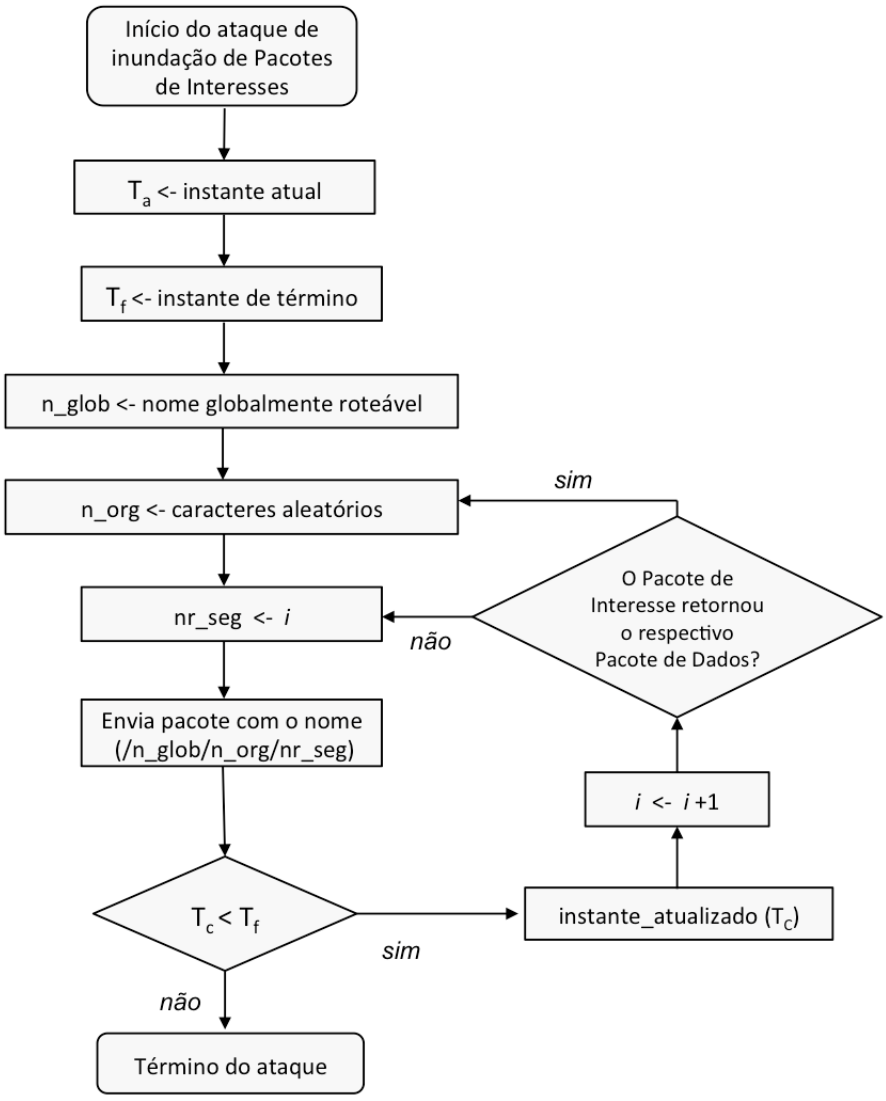


Figura 3.3: Exemplo de geração de conteúdo aleatório.

O tráfego malicioso com Pacotes de Interesses para conteúdos existentes tem efetividade limitada e são mais frequentemente utilizados para atacar a infraestrutura da rede e não as fontes de conteúdo. Devido a implementação de *caches* de conteúdo nos roteadores da rede, os interesses para um conteúdo existente somente atingirão o publicador em um primeiro momento. Nas próximas requisições, os interesses serão atendidos pelas *caches*. O tempo de permanência das entradas dos interesses pendentes para tais conteúdos dependem do RTT de recuperação do pacote de Dados. Tal tráfego deve ser composto por diferentes conteúdos existentes de forma a inibir a agregação de Pacotes de Interesses na PIT. Além disso, os usuários maliciosos devem conhecer previamente o nome de todos os conteúdos publicados pela fonte de conteúdo.

Já o trafego malicioso com Pacotes de Interesses para conteúdos gerados dinamicamente são mais adequados quando o objetivo do usuário malicioso é causar a inoperabilidade de um publicador específico. Uma vez que os conteúdos são gerados dinamicamente, estes não são armazenados em *cache* e os interesses para tais conteúdos sempre são encaminhados até o seu publicador. Se a geração de tais conteúdos for computacionalmente cara, tanto em memória quanto em processamento, o publicador pode ficar inoperante, dependendo do volume do tráfego malicioso. Por outro lado, o impacto deste ataque nos roteadores depende da sua proximidade em relação ao publicador. Intuitivamente, os roteadores mais próximos tendem a manter uma quantidade maior de interesses pendentes maliciosos em sua PIT, devido a concentração do tráfego a ser encaminhado ao publicador específico.

Os ataques com Pacotes de Interesses para conteúdos inexistentes poderão ser mais eficientes pois não podem ser “satisfeitos"pelas *caches* da rede e são necessariamente encaminhados até o publicador. Uma vez que os conteúdos requisitados são inexistentes, podem ser gerados em grandes volumes e suas entradas permanecerão na PIT até a expiração por *timeout*. Como os conteúdos requisitados não existem, a lista de nomes de conteúdo disponíveis para requisição é virtualmente infinita. Dessa forma, gerar muitos interesses para conteúdos diferentes é mais fácil neste ataque do que nos outros dois tipos, conforme representado pela Figura 3.3.

3.3.2 Taxonomia dos Ataques de Inundação de Pacotes de Interesses

Diferentemente dos ataques de inundação tradicionais da arquitetura da Internet atual [24], o objetivo principal dos ataques de inundação na CCN são os roteadores da rede.

Ao sobrecarregar a PIT dos roteadores com interesses pendentes maliciosos, os usuários consumidores e publicadores têm seus Pacotes de Interesses inibidos pela exaustão dos recursos da PIT dos roteadores da rede. Consequentemente, haverá descarte dos pacotes legítimos, uma vez que não há entradas disponíveis na PIT e a política de descarte adotada por padrão é a *tail drop* [39].

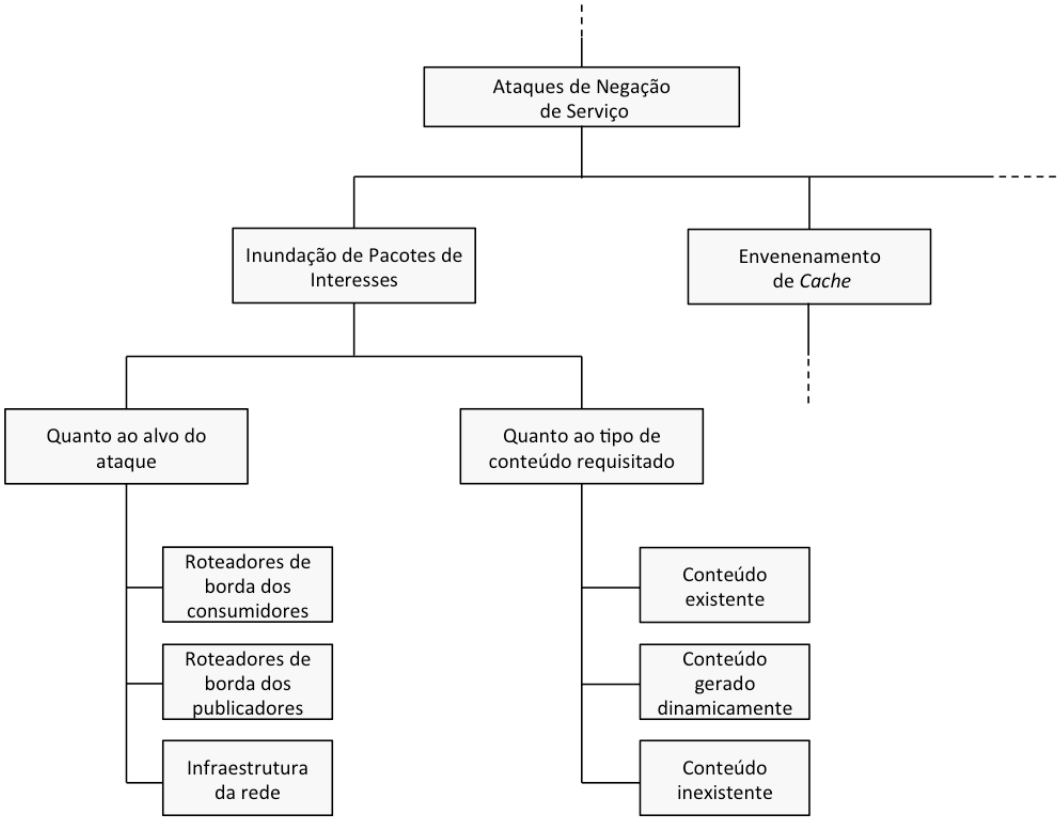


Figura 3.4: Taxonomia dos ataques de negação de serviço na CCN

Os pacotes trafegados na CCN não transportam informações de origem e destino em seus cabeçalhos. Assim, da mesma forma que a rede é orientada ao conteúdo, os ataques também precisam ser. Ao invés de escolher o endereço de destino do alvo, o usuário malicioso necessita decidir quais conteúdos requisitar e para qual publicador direcionar o tráfego de ataque de forma a alcançar seu objetivo. Desta forma, todo o tráfego de ataque tem como destino final um publicador.

Uma variação dos ataques de inundação é o esgotamento da PIT do roteador de borda dos usuários consumidores, conforme representado pela Figura 3.5.

Neste ataque, o usuário malicioso deve compartilhar o mesmo roteador dos usuários legítimos. O objetivo é a inundação da PIT do seu roteador de borda de forma a inibir o atendimento dos Pacotes de Interesses dos consumidores compartilhados, ao impedir

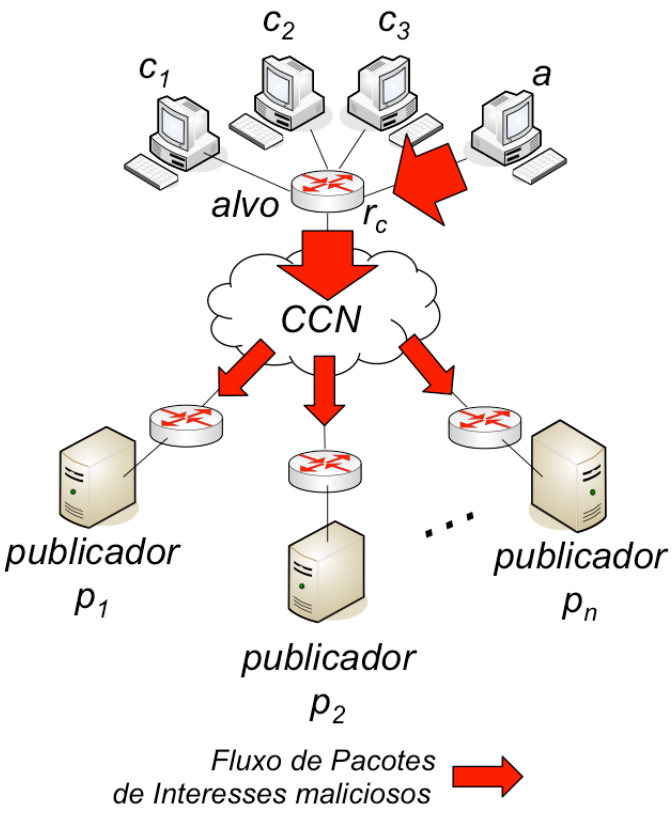


Figura 3.5: Representação de ataque de inundação ao consumidor de conteúdo.

o encaminhamento dos pacotes à rede. Assim, não há necessidade de se estabelecer um publicador específico para direcionamento do tráfego de ataque, podendo ser encaminhado para um ou mais diferentes publicadores. Como a intensidade do ataque é limitada a poucas máquinas sob domínio do usuário malicioso, a eficiência deste ataque depende da geração de um grande volume de pacotes maliciosos. Tal dependência é evidenciada pela relação entre o tamanho da PIT, a capacidade do enlace entre o roteador e o atacante do valor da sua taxa máxima de transmissão de pacotes.

Da mesma forma, pode-se atacar aos roteadores de borda dos publicadores, conforme ilustrado pela Figura 3.6. Ao assumir que um atacante controla uma *botnet* com transmissão síncrona, o volume do tráfego malicioso pode ser distribuído entre os usuários controlados direcionando todo o tráfego de ataque para um publicador específico. Intuitivamente o maior volume do tráfego de ataque é concentrado no roteador de borda do publicador. O objetivo do ataque é inibir quaisquer consumidor de recuperar um determinado conteúdo do publicador ligado ao roteador de borda sob ataque. Ao mesmo tempo o publicador inibido, recebe todo o volume do tráfego de ataque. Caso o tráfego de ataque seja formado por Pacotes de Interesses para conteúdos inexistentes, a PIT do publicador será inundada. Caso o tráfego de ataque seja composto por Pacotes de Interesses para

conteúdos existentes haverá inundação somente se a taxa de resposta com os Pacotes de Dados for menor que a taxa de inundação.

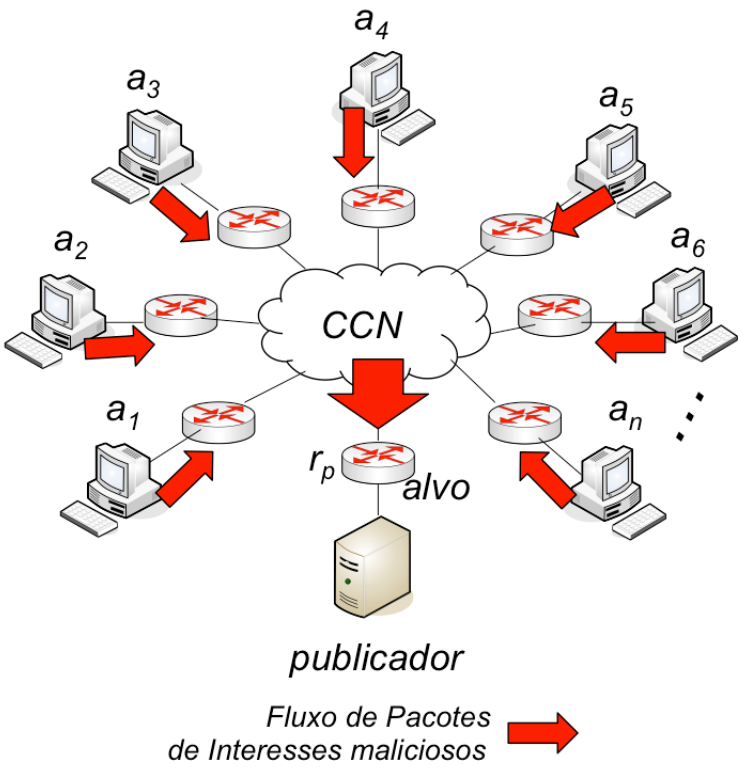


Figura 3.6: Representação de ataque de inundação ao publicador de conteúdo

Outra variação dos ataques de inundação tem como alvo os roteadores da infraestrutura da rede. Neste caso, o objetivo dos usuários maliciosos é inundar as PITs dos roteadores do núcleo da rede em uma determinada região. Ao assumir que um atacante controla pelo menos duas hordas de *botnets* com transmissão síncrona, o volume dos tráfegos maliciosos podem ser distribuídos entre os usuários controlados direcionando todos os tráfegos de ataque para uma área específica, conforme representado pela Figura 3.7. Assim ambas *botnets* enviam Pacotes de Interesses maliciosos entre si de forma coordenada. Com isso o volume do tráfego das bordas permanece pequeno, enquanto o volume do tráfego no núcleo da rede concentra um volume maior de tráfego. Tal ataque é dependente da topologia da rede e necessita de um posicionamento estratégico dos nós controlados pelos usuários maliciosos. Uma variação deste ataque é manter uma *botnet* consumidora e outra publicadora.

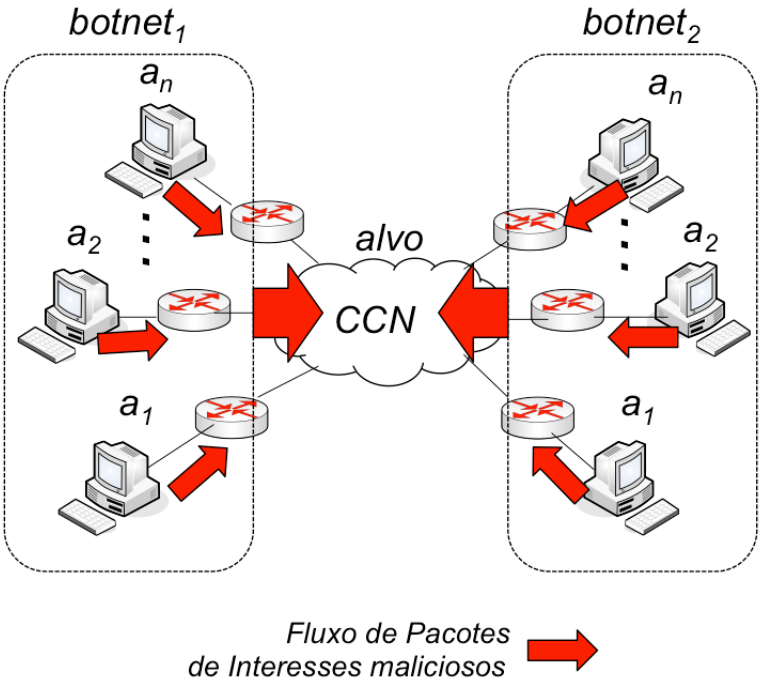


Figura 3.7: Exemplo de figura

3.3.3 Propostas de Mitigação aos Ataques de Inundação na CCN

A falta de informações de origem e a ausência de assinatura nos Pacotes de Interesse dificulta o rastreamento da origem dos ataques de inundação de interesses. Assim, qualquer usuário pode gerar um fluxo de Pacotes de Interesse e manter seu anonimato. Para contornar este problema, seria possível adotar uma solução onde os consumidores fossem obrigados a assinar os pacotes de interesse por ele gerados. Dessa forma, em um ataque de inundação seria possível descobrir qual usuário os originou e tomar as devidas contramedidas. Porém, esta solução causaria sérios problemas à privacidade dos usuários e não seria completamente efetiva, já que adversários operam *botnets* para realizar os ataques. Para mitigar os ataques de negação de serviço por inundação de interesses sem interferir na privacidade dos usuários, propõe-se contramedidas baseadas em estatísticas nos roteadores.

Inicialmente, foram sugeridas contramedidas intuitivas em [13],como o uso de estatísticas fornecidas pela monitoração de estado nos roteadores, mantendo o controle dos interesses insatisfeitos (expirados e descartados) e de métricas como o número de interesses pendentes por interface de saída, por interface de entrada ou por nomes. Com o número de interesses pendentes por interface de saída, pela propriedade de balanceamento de fluxo, um roteador pode detectar quando um roteador do salto anterior está enviando muitos interesses que não podem ser todos satisfeitos, Já pelo número de interesses pen-

dentes por interface por nomes, quando um determinado prefixo está sob um ataque, os roteadores pelo caminho podem detectar o número incomum de interesses insatisfeitos em para esse prefixo em suas PIT's. Assim, os roteadores podem limitar o número total de interesses pendentes para este prefixo e restringindo o número de interesses transmitidos pelas interfaces de entrada que enviaram muitos interesses insatisfeitos para esse prefixo. Os principais artifícios utilizados pelas abordagens de mitigação propostas na literatura são o índice de satisfação de interesses e o mecanismo de *push-back*, variando apenas a metodologia de implementação e como os artifícios são chamados.

O índice de satisfação de interesses é calculado através da proporção entre os pacotes de interesses pendentes encaminhados e os respectivos pacotes de dados retornados de um determinado roteador. Assim, a métrica serve para detectar um estado anormal no roteador. Como exemplo, considere $T(i)$ o tempo médio de resposta necessário para recuperação dos dados de modo a satisfazer o respectivo interesse pendente anteriormente encaminhado através da interface $I(i)$ e $R(i)$ a taxa média de resposta para os pacotes de interesses encaminhados. Como os Pacotes de Dados são enviados pelo caminho inverso do seu respectivo Pacote de Interesse, caso um roteador encaminhe $n(i)$ Pacotes de Interesses através de $I(i)$, então espera-se que o roteador recupere uma quantidade de pacotes de dados maior que o produto $n(i) \cdot R(i)$ dentro do tempo médio de resposta $T(i)$ segundos. Assim, se o índice de satisfação de interesses pendentes diminui fica abaixo de um determinado *threshold* definido, então o roteador classifica como estado anormal, passível de um ataque de negação de serviço.

Já o mecanismo de *Push-Back*, conforme proposto em [17] e [18], permite que os roteadores isolem a origem do ataque, limitando a a taxa de encaminhamento de interesses para o prefixo em ataque e propagam uma mensagem de alerta de ataque pelas interfaces por onde os interesses para tal prefixo foram recebidos. Com isso, possibilita que os demais roteadores dos saltos anteriores pelo caminho, tambeem reduzam a taxa de transferência da interface de chegada dos interesses maliciosos. O objetivo é limitar o tráfego de ataque por todo o caminho até a sua fonte ou pelo menos até o local onde seja detectável. Uma característica importante dessa contramedida é que ela pode ser implementada sem alterações na infraestrutura atual da CCN.

Capítulo 4

Modelagem Analítica de Roteador de Conteúdo sob Ataque de Inundação

A modelagem analítica possibilita avaliar a vulnerabilidade dos recursos do sistema sob ataque. Além disso, colabora para o entendimento de como detectar o ataque de inundação através da observação do comportamento estatístico do tráfego. Ela também contribui para o desenvolvimento de metodologias e algoritmos que possam futuramente detectar e defender a CCN contra tais ataques. O sucesso dos ataques de inundação possui uma relação direta entre a demanda de Pacotes de Interesse, a capacidade da PIT e o tempo de permanência dos interesses pendentes na PIT. Para uma melhor compreensão da modelagem do roteador CCN sob ataque, propõe-se primeiramente um modelo dos fluxos existentes entre as estruturas internas do roteador. Em seguida, propõe-se uma abstração da PIT modelada por sistema de múltiplos servidores. Enfim, modela-se a PIT do roteador sob ataque de inundação de Pacotes de Interesse.

4.1 Modelagem dos Fluxos Existentes em um Roteador de Conteúdo

Suponha que um consumidor C envie requisições à rede para um conteúdo gerado dinamicamente a partir de um determinado publicador P. Assuma que P possua apenas um único servidor de conteúdo na rede. Assim, garante-se que todo volume de tráfego será direcionado ao seu roteador de borda. Considere $R_{(\cdot)}$ a denominação de um roteador qualquer da rede. Para C recuperar o conteúdo diretamente de P, deve transmitir Pacotes de Interesse que serão encaminhados de acordo com a FIB dos roteadores por w saltos através do caminho $C = \{R_0, R_1, ..., R_{x-1}, R_x, R_{x+1}, ..., R_w\}$, onde R_0 é o roteador

de borda de C e R_w o roteador de borda de P.

4.1.1 Recebimento de Pacotes de Interesse

Considere que um roteador R_x tenha n interfaces e receba Pacotes de Interesse por uma interface i, onde p_{CS}^{hit} é a fração dos Pacotes de Interesses "satisfeitos" pelos Pacotes de Dados armazenados no CS. Assuma a taxa total $X_{(\cdot)}^{(\cdot)}$ como o somatório das taxas de um determinado fluxo para uma interface i qualquer. Dada a taxa de chegada de Pacotes de Interesse no CS do roteador Λ_{CS}^{inInt}, os Pacotes de Dados serão diretamente respondidos pela interface i com taxa $\Lambda_{CS}^{outDat} = p_{CS}^{hit} \cdot \Lambda_{CS}^{inInt}$. Com isso os Pacotes de Dados seguem o caminho inverso dos respectivos Pacotes de Interesse, proporcionando um balanceamento de fluxo. Caso não possua o conteúdo em *cache*, os Pacotes de Interesse serão encaminhados para a PIT com taxa $\Lambda_{CS}^{outInt} = (1 - p_{CS}^{hit}) \cdot \Lambda_{CS}^{inInt}$, conforme representado pela Figura 4.3. Considerando que o CS consegue processar todos os pacotes que chegam, deduz-se que $\Lambda_{CS}^{inInt} = \Lambda_{CS}^{outDat} + \Lambda_{CS}^{outInt}$.

Símbolo	Definição
p_{CS}^{hit}	Fração dos Pacotes de Interesses "satisfeitos'.
Λ_{CS}^{inInt}	Taxa de chegada de Pacotes de Interesse.
Λ_{CS}^{outDat}	Taxa de resposta de Pacotes de Dados.
Λ_{CS}^{outInt}	Taxa de encaminhamento de interesses para a PIT.

Tabela 4.1: Definição de métricas do CS para recebimento de Pacotes de Interesses.

Dado Λ_{CS}^{outInt}, caso ocorra esgotamento dos recursos da tabela, apenas uma fração p_{PIT} de Pacotes de Interesses será processada com taxa média $\Lambda_{PIT}^{inInt} = (1 - p_{CS}^{hit}) \cdot \Lambda_{CS}^{inInt} \cdot p_{PIT}$. A fração de pacotes não processados $(1 - p_{PIT})$ será bloqueada com taxa média $\Phi_{PIT}^{dropInt} = (1 - p_{CS}^{hit}) \cdot \Lambda_{CS}^{inInt} \cdot (1 - p_{PIT})$.

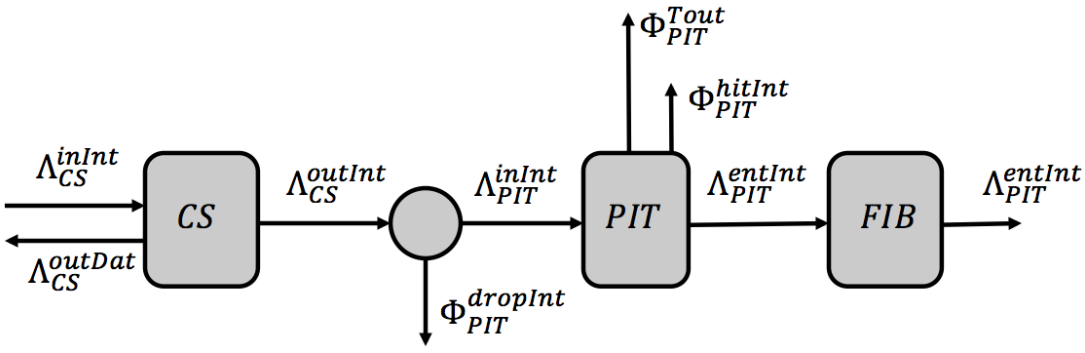


Figura 4.1: Processamento de Pacotes de Interesse no CS e na PIT.

Considere p_{PIT}^{hitInt} a fração de Pacotes de Interesses para a qual uma requisição para o

mesmo conteúdo já tenha sido encaminhada. Neste caso, não serão criadas novas entradas, sendo apenas adicionadas as interfaces de entrada nos interesses pendentes já estabelecidos, permitindo a agregação de pacotes. Consequentemente, os pacotes serão agregados com taxa média $\Phi_{PIT}^{hitInt} = p_{PIT}^{hitInt} \cdot \Lambda_{PIT}^{inInt}$. Caso não existam entradas para os conteúdos desejados na PIT e seja possível processar os pacotes, serão criadas novas entradas na tabela com taxa média $\Lambda_{PIT}^{entInt} = (1 - p_{PIT}^{hitInt}) \cdot \Lambda_{PIT}^{inInt}$. Em seguida os Pacotes de Interesses são encaminhados para a FIB, assumindo que todos os pacotes sejam encaminhados para o próximo salto. Considere p_{PIT}^{Tout} a fração dos interesses pendentes na PIT que serão descartados após a expiração dos seus *timeout*. A taxa média de descarte de interesses pendentes por *timeout* será $\Phi_{PIT}^{Tout} = p_{PIT}^{Tout} \cdot \Lambda_{PIT}^{entInt}$, conforme representado pela Figura 4.3.

Símbolo	**Definição**
p_{PIT}	Fração de Pacotes de Interesse processada pela PIT
p_{PIT}^{hitInt}	Fração de Pacotes de Interesses agregados
p_{PIT}^{Tout}	Fração dos interesses pendentes descartados por *timeout*
Λ_{CS}^{outInt}	Taxa de encaminhamento de interesses
Λ_{PIT}^{inInt}	Taxa média de processamento de interesses
Λ_{PIT}^{entInt}	Taxa média de geração de novos interesses pendentes
$\Phi_{PIT}^{dropInt}$	Taxa média de bloqueio de Pacotes de Interesse
Φ_{PIT}^{hitInt}	Taxa média de agregação de interesses pendentes

Tabela 4.2: Definição de métricas da PIT para recebimento de Pacotes de Interesse.

4.1.2 Recebimento de Pacotes de Dados

Assuma Λ_{PIT}^{inDat} como a taxa média de chegada de Pacotes de Dados por uma interface i qualquer. Os Pacotes de Dados no qual seus respectivos interesses pendentes foram expirados são descartados com taxa média $\Phi_{PIT}^{dropDat} = \Lambda_{PIT}^{inDat} \cdot p_{PIT}^{Tout}$. Os interesses pendentes que permaneceram na PIT serão "satisfeitos" pelos Pacotes de Dados, ou seja, terão as entradas removidas, com taxa média de satisfação de interesses pendentes $\Lambda_{PIT}^{satInt} = \Lambda_{PIT}^{inDat} \cdot (1 - p_{PIT}^{Tout})$. O tempo de permanência de um interesse pendente na PIT é definido pelo $min(RTT, T_{out})$, onde RTT é o tempo médio entre a criação de uma entrada e a chegada do respectivo Pacote de Dados e T_{out} o tempo máximo de permanência. Posteriormente, o roteador armazena uma cópia dos Pacotes de Dados no CS e os encaminham aos nós dos saltos anteriores relativa às interfaces i pelas quais o interesse foi recebido, conforme representado pela Figura 4.2. Os Pacotes de Dados são armazenados no CS de acordo com a política de substituição de *cache* como LRU -*Least Recent Used* ou LFU - *Least Frequently Used*.

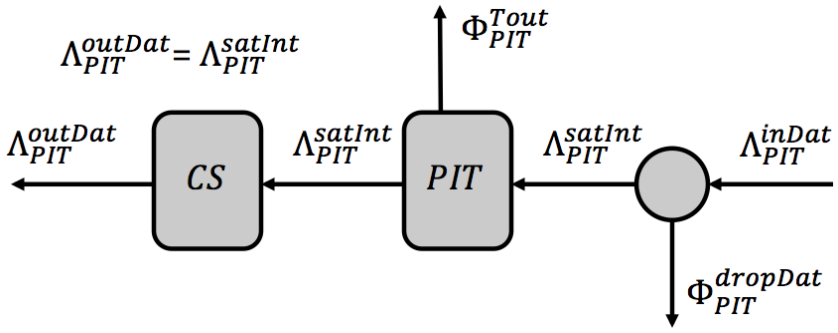


Figura 4.2: Processamento de Pacotes de Dados no CS e na PIT.

Símbolo	Definição
Λ_{PIT}^{inDat}	Taxa média de chegada de Pacotes de Dados.
$\Phi_{PIT}^{dropDat}$	Taxa média de descarte de Pacote de Dados.
Λ_{PIT}^{satInt}	Taxa de satisfação de interesses pendentes.

Tabela 4.3: Definição de métricas da PIT para recebimento de Pacotes de Dados.

O monitoramento dos fluxos nos roteadores pode contribuir para a mitigação de ataques de negação de serviço. Uma das métricas sugeridas por [**?**] para a detecção dos ataques de inundação é o uso de estatísticas dos roteadores. Neste sentido, o índice de satisfação de interesses por interface $I_{sat}^{i} = \Lambda_{PIT_i}^{satInt}/\Lambda_{PIT_i}^{entInt}$ apresenta uma relação entre a geração e remoção de entradas na PIT. Ao estabelecer um limiar para I_{sat}^{i} pode-se caracterizar um roteador sob ataque de inundação [2].

4.2 Abstração e Modelagem da PIT com Múltiplos Servidores e Tempo de Serviço Limitado

A PIT é a estrutura de dados responsável pela manutenção do estado do roteador e será um alvo direto durante um ataque de inundação de Pacotes de Interesse. Dada uma distribuição de probabilidade para as taxas de chegada e tempo de serviço (tempo de permanência na PIT) das requisições de conteúdo, modela-se a utilização da PIT. Consequentemente, deduz-se o desempenho médio global do sistema em função de métricas-chaves. Esta aproximação é semelhante à análise de sistemas de fluxo de filas [31].

Assume-se que exista um período de tempo em que a distribuição das requisições de conteúdos esteja aproximadamente em equilíbrio, ou seja, no estado estacionário. Na CCN um fluxo é identificado pela transmissão de Pacotes de Interesse para um mesmo publicador e um *lifetime* médio baseado no *RTT* médio ou *timeout*. Os fluxos são identificados

de forma *on-the-fly* através da análise dos pacotes pelos roteadores [28].

4.2.1 Sistema de Perda de Erlang $M/G/c/c$

O sistema de fila $M/G/c/c$ [21] é um dos mais importantes e populares modelos para análise de sistemas de servidores caracterizados por padrões aleatórios de chegada e tempo de serviço, considerando um número limitado de recursos e sem fila de espera. Conhecido também como sistema de perda, foi introduzido pelo matemático A. K. Erlang (1878-1929) para serviços de telefonia [12]. Pela notação de Kendall [20] $M/G/c/c$ significa que o processo de chegada do cliente é por Poisson ou *memoryless* (M), os tempos de serviço seguem uma distribuição geral (G), existem c servidores idênticos e a capacidade total do sistema é limitada a c, conforme representado pela Figura .Vários autores também utilizam notações alternativas quando se referem ao sistema de perda de Erlang como: $M/G/n/n$, $M/G/m/m$, $M/G/s/s$ ou $M/G/k/s$, onde k é igual a s.

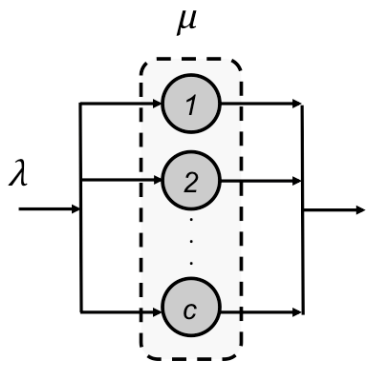


Figura 4.3: Representação do sistema $M/G/c/c$.

A popularidade do sistema de perdas de Erlang se deve à simplicidade da distribuição de probabilidades no estado estacionário do número de servidores ocupados. Este fato, facilita a estimação da utilização dos recursos e da proporção de clientes que são perdidos pelo sistema no longo prazo. Esta métrica de desempenho é uma importante medida da qualidade do serviço, em muitos contextos práticos. Desta forma, um resultado fundamental proposto para os problemas de engenharia de tráfego telefônico foi a função de perda de Erlang ou fórmula Erlang-B, conforme representada pela Equação 4.1 :

$$P_b(\rho, c) = \frac{\dfrac{\rho^c}{c!}}{\displaystyle\sum_{k=0}^{c} \frac{\rho^k}{k}} \tag{4.1}$$

onde $P_b(\rho, c)$ é a probabilidade de ocorrer o bloqueio de clientes no sistema em função da carga oferecida ao sistema $\rho = \lambda \cdot 1/\mu$ definida pela razão da taxa de chegada λ pela taxa de serviço μ e a capacidade c do sistema.

Apesar da fórmula Erlang-B ser utilizada inicialmente para selecionar o número apropriado de troncos (servidores) necessários para assegurar uma pequena percentagem de chamadas perdidas (clientes), sua utilização ainda é proposta em diversas abordagens atuais [7] [10] [16] [36].

4.2.2 Modelagem da PIT a partir de um sistema $M/G/c/c$

Considere um roteador de conteúdo R_x com n interfaces. Cada interface i recebe um determinado fluxo F_i de Pacotes de Interesses com taxa de Λ_i. Assim, a taxa total de chegada de Pacotes de Interesses no roteador é dada por $\Lambda = \sum_{i=1}^{n} \Lambda_i$.

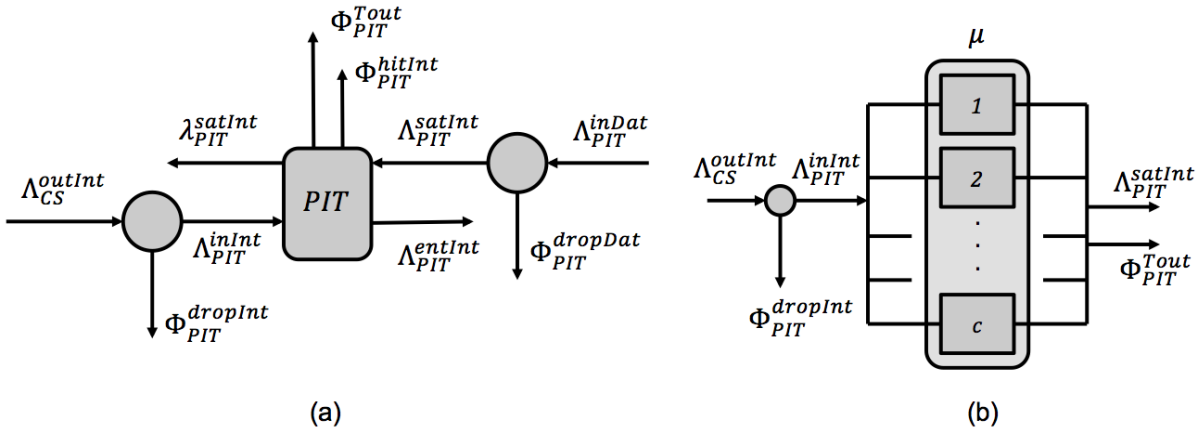


Figura 4.4: (a) Abstração da PIT e (b) Modelagem pelo sistema $M/G/c/c$.

Abstraindo a PIT deste roteador, propõe-se a sua modelagem através do sistema de perda de Erlang $M/G/c/c$ com limitação do tempo de serviço [35], conforme a representado pela Figura 4.4. Assim, caracteriza-se o tempo entre chegadas de Pacotes de Interesse na PIT de acordo com uma distribuição de Poisson M com taxa média $\lambda = \sum_{i=1}^{n} \Lambda_{CS}^{outInt} i$. A taxa de serviço μ segue uma distribuição geral $G = G' \oplus D$, onde "$\oplus$" denota o compartilhamento síncrono das distribuições, G' uma distribuição geral para o RTT médio e D uma distribuição determinística para a expiração do *timeout*. O sistema possui múltiplos c servidores, com capacidade máxima de c clientes, uma vez que não há espaço para fila de espera de clientes. Caso todos os c servidores estejam ocupados, o próximo cliente recém chegado será rejeitado. Analogamente, cada servidor representa uma entrada na PIT e os clientes representam os Pacotes de Interesse que são encaminhados para a PIT.

Para o sistema, denota-se por p_K a probabilidade no estado estacionário de existir k entradas na PIT, onde $k = 0, 1, 2, ..., c$. A aplicação da técnica de variável complementar abordada por [34] resulta na equação de balanceamento de fluxo:

$$\lambda p_k = (k+1)\mu p_{k+1} \quad , onde \quad k = 0, 1, 2, ..., c-1 \tag{4.2}$$

O lado esquerdo da Equação (4.2) representa a mudança de um estado k para o estado $k+1$, enquanto que o lado direito da equação representa um estado $k+1$ para um estado k.

4.3 Modelagem da PIT sob Ataque Distribuído de Inundação de Pacotes de Interesse

Similarmente como abordado para a modelagem de inundação de pacotes SYN TCP/IP em [8], propõe-se a modelagem da PIT sob ataque de inundação estabelecendo um modelo matemático e métricas de desempenho. Considere um ataque ao roteador de borda R_p de um publicador de conteúdo P com um único servidor disponível na rede. Assuma o roteador sob ataque e considere a modelagem da PIT de R_p a partir do sistema de perda de Erlang $M/G/c/c$.

4.3.1 Modelo de Rede e de Tráfego

Na CCN, o tráfego oferecido à rede se dá através da emissão de Pacotes de Interesse. Um Pacote de Interesse é essencialmente uma requisição gerada por um nó CCN para reservar um conjunto fixo de recursos na PIT salto a salto ao longo do processo de encaminhamento até encontrar um conteúdo. Assim, garante o uso exclusivo do fluxo de informações associado ao interesse pendente mantido na PIT. O tráfego oferecido à rede pode ser descrito por um processo de chegada de Pacotes de Interesse, o qual pode ser obtida a taxa de chegada dos pacotes no roteador e uma distribuição do tempo médio de permanência dos interesses pendentes na PIT. Como a PIT possui recursos limitados, alguns Pacotes de Interesse podem ser bloqueados por esta limitação.

4.3.1.1 Considerações sobre a Rede e Modelo do Tráfego

O modelo refere-se ao ataque de inundação de pacotes de Interesses ao roteador de borda do publicador. Para isso, assume-se que o publicador possui apenas um único servidor

na rede de forma que todas as requisições se concentrem em um único roteador de borda. Considera-se neste modelo as seguintes premissas:

i) Ao abstrair o roteador sob ataque, o modelo não considera a topologia da rede. Considera-se apenas o volume de tráfego associado às interfaces de chegada;

ii) A chegada de Pacotes de Interesses no roteador ocorre de acordo com um processo de Poisson. Justifica-se esta premissa uma vez que o modelo clássico de Erlang [21] [9] que serve como suporte teórico para o modelo analítico apresentado neste trabalho considera as chegadas de clientes no sistema a partir de um regime poissoniano;

iii) Supõe-se que o tempo de permanência (*lifetime*) dos interesses pendentes na PIT do roteador sejam independentes de acordo com uma variável aleatória Υ distribuída exponencialmente com taxa média μ. Todos os interesses pendentes possuem o mesmo tempo máximo de permanência na PIT fixado pelo roteador a partir de um valor de *timeout*;

iv) Ao chegar um Pacote de Interesse uma interface i qualquer, após a verificação da não existência do respectivo Pacote de Dados no CS, caso haja recursos disponíveis na PIT, é gerada uma entrada de interesse pendente e imediatamente inicia a contagem do seu tempo de permanência. Caso contrário, os Pacotes de Interesses serão bloqueados (descartados) e não há a retransmissão dos referidos pacotes por parte do consumidor;

v) Considera-se todas as probabilidades de bloqueio como probabilidades estacionárias. Ou seja considera-se que a rede esteja em estado permanente ou de equilíbrio;

vi) Não são consideradas filas nos roteadores e nem atrasos de processamento no roteador como tempo de verificação no CS e na PIT. Assume-se também que o valor da capacidade dos enlaces do roteador sob ataque são proporcionais as taxas definidas, ou seja, não há perda de pacotes;

vii) Apesar da PIT ser uma tabela *hash*, considera-se sua capacidade c em termos de unidade de entrada e não em termos de consumo de memória. Caso não haja agregação ou bloqueio de pacotes, cada Pacote de Interesse demanda uma unidade de entrada de interesse pendente na PIT; e

viii) O roteador possui conhecimento da proporcionalidade entre os tráfegos legítimos e maliciosos. Assume-se que o roteador estime tal proporção utilizando métricas

estatísticas como o índice de satisfação de interesses pendentes na PIT, dado pela razão da quantidade de interesses pendentes satisfeitos pelo número total de interesses pendentes.

A taxa de chegada Pacotes de Interesse por uma interface i em um roteador λ_i é definida como $\lambda_i = \lim_{t\to\infty} n_i/t$, onde n_i é o número de chegadas de pacotes no intervalo $[0, t]$. A taxa média de permanência na PIT é dada por $\mu = 1/\tau$, onde τ é o tempo médio de permanência na PIT. A carga oferecida ao sistema a é definida como $a = \lambda\tau$. Já a intensidade de tráfego é uma medida da carga oferecida ao sistema ρ é definida como a razão entre o tempo médio de permanência de um interesse pendente na PIT pelo tempo médio entre chegadas de Pacotes de Interesse. Outra forma de considerar *rho* é pelo produto da taxa de chegada pelo tempo médio de permanência dos interesses pendentes na PIT $\rho = \lambda/\mu$. A intensidade do tráfego é expressa em Erlangs, embora seja adimensional.

4.3.1.2 Modelagem

O tráfego total legítimo é composto de conteúdos dinâmicos com taxa média λ_l e o tráfego total malicioso é composto por Pacotes de Interesse para conteúdos inexistentes com taxa média λ_m. De forma a não expor as características do tráfego de ataque para identificação por mecanismos de segurança, considere que o atacante gera um tráfego com uma distribuição idêntica ao tráfego legítimo. Assuma que não há limitação do volume do tráfego em função da capacidade dos enlaces de cada interface. Como ambos os tráfegos são gerados por um processo de Poisson, considera-se a taxa total de encaminhamento de Pacotes de Interesse para a PIT, a soma das taxas por todas as n interfaces dada por $\lambda = \lambda_l + \lambda_m$ [31]. Apesar de haver variações na intensidade do tráfego, por simplificação, considera-se o tráfego legítimo constante.

O tempo de permanência dos interesses pendentes legítimos t_l segue uma distribuição geral G caracterizada pelo RTT médio. O tempo de permanência das requisições maliciosas t_m é caracterizado pelo T_{out}. O *timeout* segue uma distribuição determinística D com um valor constante, iniciado no instante da geração da entrada do interesse pendente. Caso não haja entrada disponível, os Pacotes de Interesses serão bloqueados e não haverá retransmissão de pacotes por parte dos consumidores.

Considere μ_l e $G_l(t)$ como, respectivamente, a taxa média de tempo de permanência e a função distribuição de probabilidade (*fdp*) do tempo de permanência dos interesses

Símbolo	Definição
l	Referente ao tráfego legítimo
m	Referente ao tráfego malicioso
$\lambda_{(\cdot)}$	taxa média de chegada de Pacotes de Interesses.
n	Número de interfaces do roteador.
$t_{(\cdot)}$	Tempo de permanência de interesses pendentes na PIT
μ	Taxa média de permanência na PIT.
RTT	Tempo de permanência na PIT de interesse pendente legítimo.
T_{out}	Tempo máximo de permanência na PIT.
$G(t)$	Função Distribuição de Probabilidade.
$q_{(\cdot)}$	Proporção da quantidade de interesses pendentes na PIT.
ρ	carga oferecida ao sistema.
$P_b\,(\rho, c)$	Probabilidade de bloqueio.

Tabela 4.4: Definição de métricas da PIT para recebimento de Pacotes de Dados.

pendentes legítimos t_l, conforme representado pela Equação (4.3). Assuma $G_l(t) = \mu_l e^{-t\mu_l}$ como uma distribuição exponencial para qualquer intervalo de tempo t, onde $t < T_{out}$ ou $G_l(t) = 0$ caso $t \geq T_{out}$ somada com a função delta de Dirac $\delta(t)$. A função delta de Dirac é ponderada pela probabilidade de um interesse pendente legítimo expirar p_l:

$$G_l(t) = \begin{Bmatrix} \mu_l e^{-t\mu_l} & t < T_{out} \\ 0 & t = T_{out} \end{Bmatrix} + \delta(t - T_{out}^{+})p_l, \quad p_l = \int_{T_{out}}^{\infty} \mu_l e^{-t\mu_l} dt = e^{-T_{out}\mu_l} \tag{4.3}$$

Considere $E(G_l(t)) = t_l$ o valor esperado do tempo médio de serviço para os interesses pendentes legítimos, onde:

$$t_l \equiv \int_0^{\infty} tG_l(t)dt = \int_{T_{out}}^{\infty} te^{-\mu_l t} dt = \frac{1 - e^{-T_{out}\mu_l}}{\mu_l} \tag{4.4}$$

Dado o tempo médio de serviço de interesses pendentes legítimos t_l e o tempo de serviço de interesses maliciosos $t_m = T_{out}$, calcula-se o tempo médio de serviço geral do sistema.

Suponha que durante um intervalo de tempo Δt a PIT receba $\lambda \cdot \Delta t$ Pacotes de Interesse. Porém, somente uma quantidade q de interesses pendentes serão aceitos, conforme abordado na Subseção 4.4.2. Esta proporção de pacotes é dada por $q = q_l + q_{l'} + q_m$, onde q_l é a quantidade de interesses legítimos que geram novas entradas, $q_{l'}$ são os interesses legítimos agregados e q_m é a quantidade de interesses maliciosos na PIT. Como $q_{l'}$ não gera novas entradas, considera-se apenas $q = q_l + q_m$. Assumindo o processo de chegada de Poisson, espera-se que q_l e q_m sejam formados pelas proporções representadas por:

$$q_l = \frac{q \cdot \lambda_l}{\lambda} \quad e \quad q_m = \frac{q \cdot \lambda_m}{\lambda} \tag{4.5}$$

Desta forma, o tempo médio de permanência geral de interesses pendentes no sistema $\bar{t}$ durante um intervalo de tempo Δt é igual a soma ponderada dos tempos de permanência legítimos e maliciosos de acordo com a proporção de interesses pendentes gerados no intervalo de tempo Δt, conforme representado pela Expressão (4.6):

$$\bar{t} = t_l \frac{q_l}{q} + t_m \frac{q_m}{q} = t_l \frac{\lambda_l}{\lambda} + t_m \frac{\lambda_m}{\lambda} = \frac{t_l \lambda_l + t_m \lambda_m}{\lambda} = \frac{t_l \lambda_l + t_m \lambda_m}{\lambda_l + \lambda_m} \tag{4.6}$$

Logo, a taxa média geral de permanência é dada por $\mu \equiv 1/\bar{t}$, conforme representado pela Equação (4.7):

$$\mu \equiv \frac{1}{\bar{t}} = \frac{\lambda_l + \lambda_m}{t_l \lambda_l + t_m \lambda_m} = \frac{\lambda_l + \lambda_m}{\left(\dfrac{1 - e^{-T_{out}\mu_l}}{\mu_l}\right) \lambda_l + T_{out} \lambda_m} \tag{4.7}$$

Consequentemente, a carga geral do sistema $\rho = \lambda/\mu$, é dada pela Equação (4.8):

$$\begin{aligned} \rho &= \lambda \cdot \frac{1}{\mu} \\ &= (\lambda_l + \lambda_m) \cdot \frac{\left(\dfrac{1 - e^{-T_{out}\mu_l}}{\mu_l}\right) \lambda_l + T_{out} \lambda_m}{\lambda_l + \lambda_m} \\ &= \left(\frac{1 - e^{-T_{out}\mu_l}}{\mu_l}\right) \lambda_l + T_{out} \lambda_m \end{aligned} \tag{4.8}$$

Estabelecida a carga geral ρ oferecida ao sistema, é possível determinar a probabilidade de bloqueio $P_b(\rho, c)$ [21] em função da carga ρ e da quantidade total c de entradas da PIT. Trata-se da probabilidade de um Pacote de Interesse ser bloqueado e descartado caso não haja entrada disponível na PIT. $P_b(\rho, c)$ é denominada função de perda de Erlang ou Erlang-B, conforme representado pela Equação (4.9):

$$P_b(\rho, c) = \frac{\dfrac{\rho^c}{c!}}{\displaystyle\sum_{k=0}^{c} \frac{\rho^k}{k}} \tag{4.9}$$

Quando ρ e c são muito grandes o cálculo da Equação (4.9) pode ter um alto custo computacional. Porém, a função Erlang-B também pode ser expressada de forma recursiva:

$$P_b(\rho, c) = \frac{\rho P_b(\rho, k-1)}{k + \rho P_b(\rho, k-1)} \qquad para \quad k = 1, 2, ..., c \tag{4.10}$$

Capítulo 5

Avaliação Experimental

5.1 Avaliação Experimental do Modelo

Nesta subseção, valida-se o modelo de ataque mostrando a influência da proporção do tráfego de ataque em relação a probabilidade de bloqueio de pacotes e analisa-se a utilização da PIT pelo tráfego malicioso. Da mesma forma, busca-se mostrar que não é somente o bloqueio de pacotes que impede o serviço do sistema, mas também uma definição inadequada do valor do tempo máximo de permanência na PIT.

5.1.1 Simulador Utilizado

Através do Simulador *Network Simulator* 3 - NS3 [27], utilizou-se o módulo $ndnSIM$ [3] no qual proporciona a simulação das operações básicas da CCN ao implementar as estruturas internas nos nós da rede e a pilha de protocolos CCN. A escolha do NS3 e $ndnSIM$ foi motivada pela ampla utilização nas atuais pesquisas sobre CCN, conforme observado em: [40], [43], [41], [2] dentre outros. Para informações mais detalhadas do módulo $ndnSIM$ recomenda-se [3] e [26] onde estão detalhadas suas funcionalidades básicas, protocolos e modelos. Utilizou-se a versão 3.17 do NS3 e versão 0.2.8 do módulo $ndnSIM$.

5.1.2 Modelo de Simulação

Simula-se um ataque distribuído de inundação ao roteador de borda R_w de um publicador P com um único servidor em toda a rede, conforme ilustrado pela Figura **??**. Em todas as simulações, o modelo de simulação é composto por dois nós, sendo um publicador e seu roteador de borda. No roteador são instalados na pilha CCN duas aplicações geradoras de

tráfego (legítimo e malicioso). A geradora de tráfego malicioso simula o tráfego associado proveniente de uma *botnet* com transmissão síncrona, com Pacotes de Interesses para conteúdos inexistentes. A geradora de tráfego legítimo simula um tráfego concorrente de Pacotes de Interesses para conteúdos diferentes gerados dinamicamente pelo publicador. A intensidade do tráfego malicioso é dada a partir da proporção entre o tráfego malicioso e legítimo na forma $\lambda_m(\lambda_l)$.

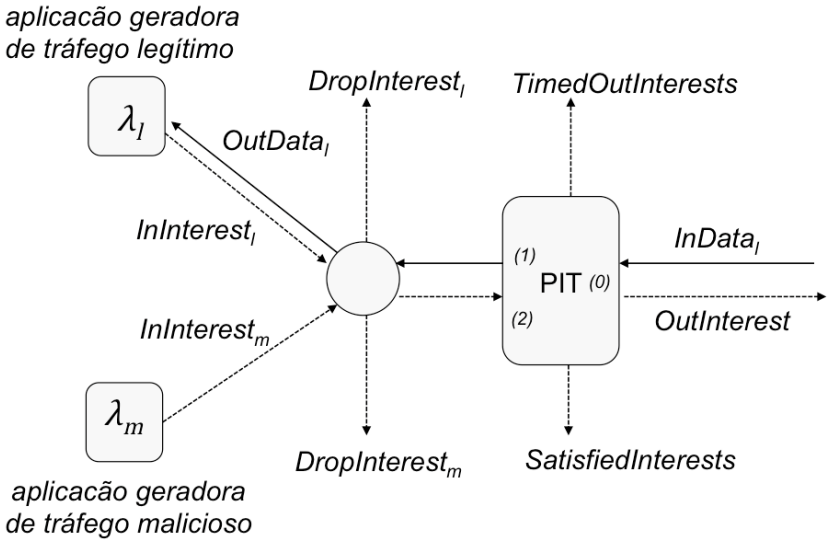


Figura 5.1: Modelo de Simulação aplicado ao nó 1 (roteador) da simulação no módulo ndnSIM.

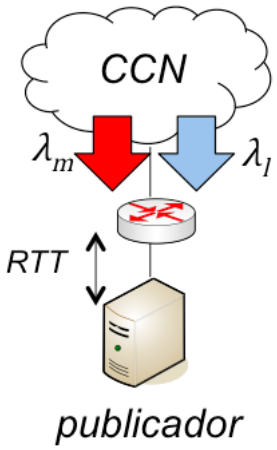


Figura 5.2: Representação da simulação.

Conforme apresentado pela Tabela 6.1 em todos os cenários, considera-se ambos os tráfegos, legítimo e malicioso, gerados de acordo com um processo de Poisson com taxas λ_l e λ_m, onde $\lambda_l + \lambda_m = 1000 pacotes/s$. O tempo de permanência dos interesses pendentes legítimos na PIT (RTT) é estabelecido de acordo com uma variável aleatória com distribuição exponencial e média de $\tau = 0,1s$. De forma a enfatizar as relações entre o tráfego

gerado e a probabilidade de bloqueio, admite-se uma PIT do roteador com capacidade para $c = 100$ interesses pendentes. Considera-se que o período de amostragem de pacotes $t = 1000s$ seja significativamente suficiente para assegurar que os efeitos da quantização sobre os tempos de amostragem sejam desconsiderados. Assume-se o caso mais extremo onde não há perda de pacotes devido à capacidade do enlace.

Métrica	**Valor**
Tráfego	Poisson
$\lambda_l + \lambda_m$	1000 pacotes/s
$\lambda_m(\lambda_l)$	Proporcão entre valor do tráfego malicioso e legítimo.
RTT	Exponencial com média $\tau = 0,1s$
c	100 interesses pendentes
t_{simul}	$1000s$

Tabela 5.1: Definição de métricas principais da simulação.

5.1.3 Comparação dos Resultados Numéricos da Probabilidade de Bloqueio entre Modelo e Simulação

Para avaliar o impacto do tráfego maliciosos na PIT, foram realizadas simulações para diferentes valores de λ_l e λ_m (sempre mantendo a proporção total).

A probabilidade de bloqueio na simulação $P_b(t)$ para o estado estacionário pode ser medida através de um estimador natural baseado nas observações do sistema sobre um intervalo $[0, t]$ qualquer, pela forma:

$$P_b\left(\rho, c\right) \equiv P_b(t) = \frac{B(t)}{L(t) + M(t)} \tag{5.1}$$

onde $B(t)$ e $(L(t)+M(t))$ são respectivamente, a quantidade de Pacotes de Interesses bloqueados e a quantidade total de de Pacotes de Interesses encaminhados à PIT, legítimos $L(t)$ e maliciosos $M(t)$. Os resultados obtidos através do modelo $(P_b(\rho, c))$ e simulação $(P_b(t))$ da fração dos Pacotes de Interesse descartados pela limitação de espaço na PIT, para um $T_{out} = 0.2$ e $T_{out} = 0.5$ são mostrados através dos gráficos das Figuras 5.3 e 5.4 respectivamente. Em ambos os casos, tanto na simulação quanto no modelo analítico, percebe-se que à medida que aumenta a intensidade do tráfego malicioso, aumenta também a probabilidade do Pacote de Interesse não ser processado pela PIT. Esta fato deve-se ao incremento da quantidade de interesses pendentes maliciosos na PIT em relação ao tráfego legítimo concorrente. Observa-se ainda que os resultados para um tempo máximo de permanência $T_{out} = 0.5s$ são mais elevados quando comparados com os re-

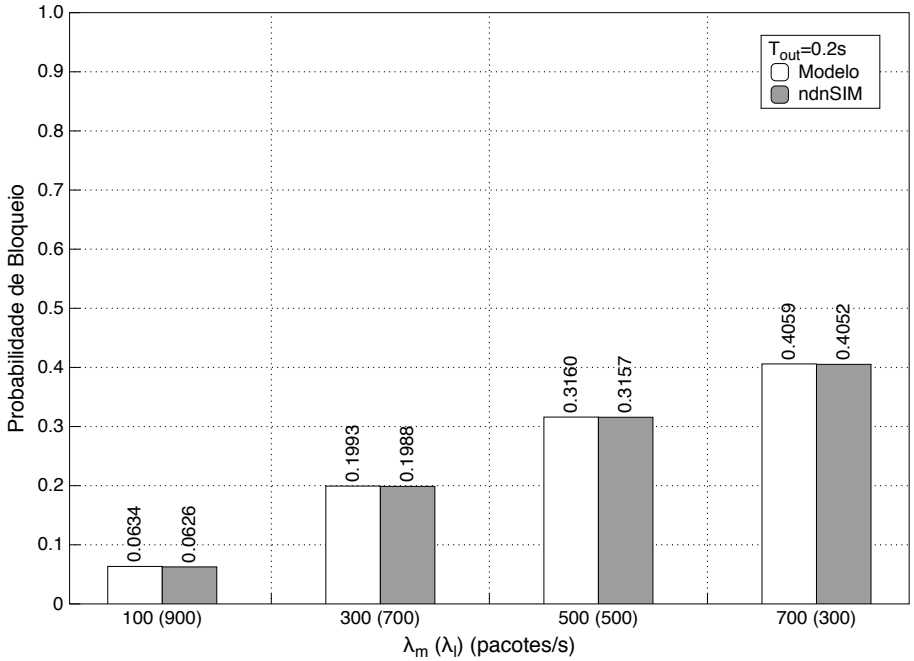


Figura 5.3: Comparação dos resultados numéricos para valores da probabilidade de bloqueio entre o modelo e simulação para um valor do tempo máximo de permanência na PIT, T_{out} igual a $0.2s$.

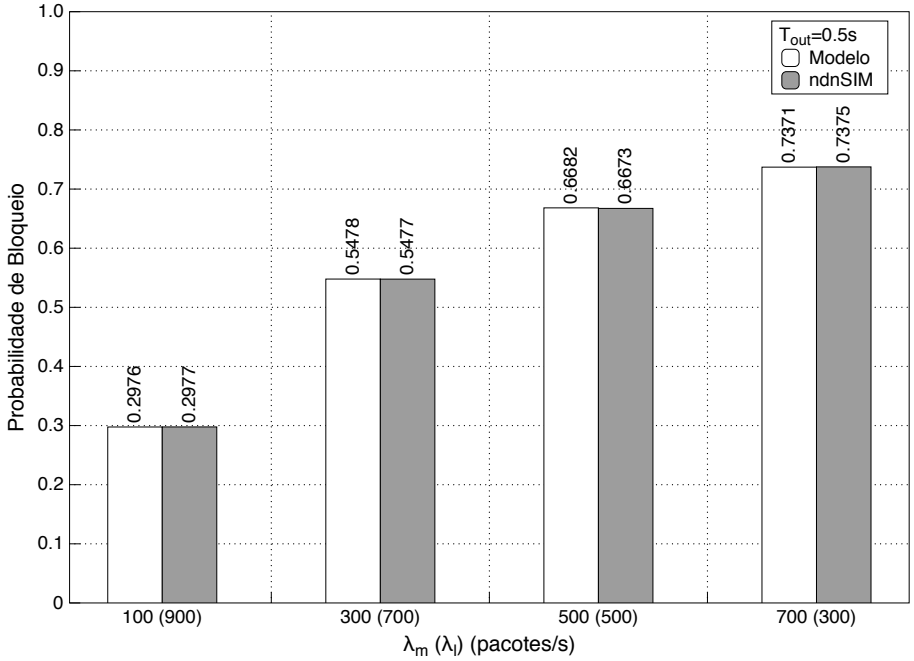


Figura 5.4: Comparação dos resultados numéricos para valores da probabilidade de bloqueio entre o modelo ($P_b(\rho, c)$) e simulação ($P_b(t)$) para um valor do tempo máximo de permanência na PIT, T_{out} igual a $0.5s$.

sultados para $T_{out} = 0.2s$. Isto indica intuitivamente que o valor definido para o *timeout* dos interesses pendentes na PIT pode influenciar positivamente (ou negativamente) na mitigação de ataque de inundação na CCN.

5.1.4 Análise da Relação entre o Tempo Máximo de Permanência e a Quantidade de Interesses Pendentes satisfeitos na PIT

Na subseção anterior 5.1.3, além de apresentar a influência da proporção do tráfego malicioso para o bloqueio da PIT, evidencia-se também que o valor definido na simulação para o tempo máximo de permanência dos interesses pendentes ($T_{out} = 0.2s$ e $T_{out} = 0.5s$) pode fortalecer a intensidade do tráfego malicioso λ_m.

Intuitivamente, percebe-se que ao aumentar o valor do *timeout* aumenta o tempo de permanência dos interesses pendentes maliciosos, contribuindo para o sucesso do ataque de inundação uma vez que diminui o processamento de Pacotes de Interesses legítimos na PIT. A partir desta análise, busca-se através da simulação ilustrar a quantidade de total de interesses pendentes "satisfeitos"ao término de cada simulação para diversos valores de *timeouts* em função da intensidade do tráfego de ataque. Para tal, considera-se o *timeout*-base como o valor do RTT médio $T_{out} = 0.1s$ e a partir deste valor define-se mais quatro valores, sendo duas ordens de grandeza acima e duas abaixo ($T_{out} = [0.001s; 0.01s; 0.1s; 1.0s; 10s]$). Da mesma forma, define-se diferentes proporções de λ_l e λ_m. Nota-se que a partir do gráfico da Figura 5.5, para valores de T_{out} extremamente

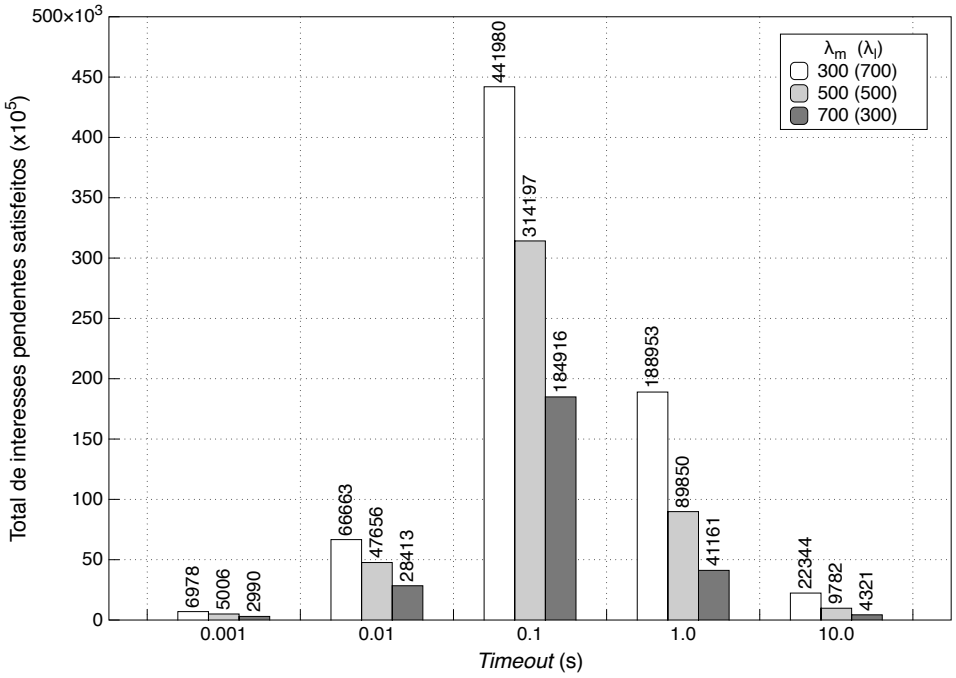


Figura 5.5: *Trade-off* entre a quantidade de Pacotes de Interesses legítimos atendidos e o valor do *timeout*.

baixos, a quantidade de interesses pendentes legítimos satisfeitos é inibida. Neste caso a PIT é subutilizada, pois está excluindo as entradas tão rapidamente que ela nunca terá a chance de manter interesses pendentes próximo da sua capacidade, como representado

pelo gráfico (a) da Figura 5.6. Deste modo, a quantidade de entradas legítimas expiradas é alta, pois os interesses pendentes possuem pouco tempo para serem satisfeitos antes que a que suas entradas permaneçam até expirar com o valor de T_{out}, caracterizado pelo fato de que o $RTT < T_{out}$. Para valores de *timeouts* muito elevados, há o efeito contrário.

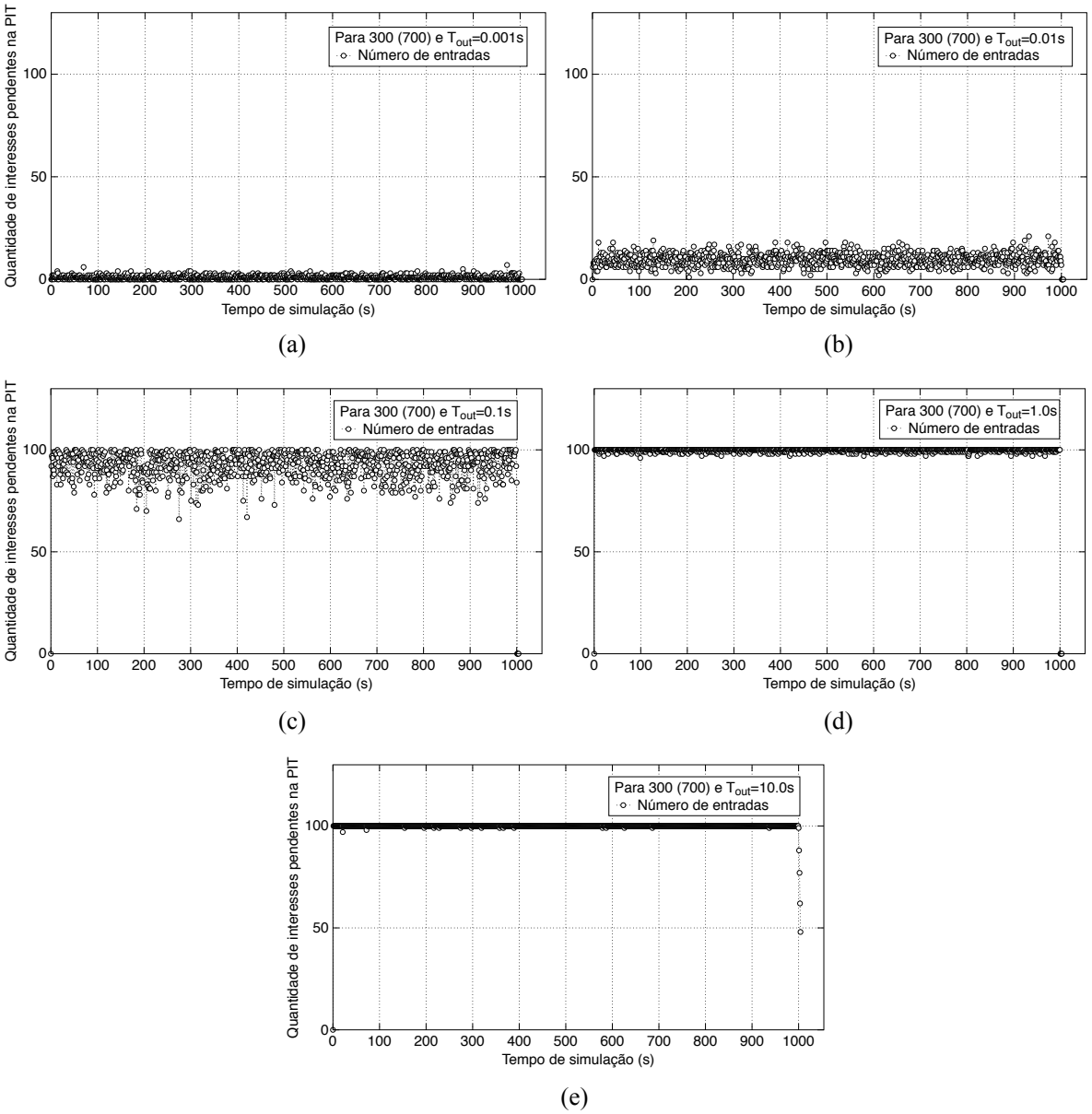


Figura 5.6: Quantidade de interesses pendentes na PIT a cada $0.1s$ para uma proporção de tráfego 300(700) e para diferentes *timeouts*: (a) $0.001s$, (b) $0.01s$, (c) $0.1s$, (d) $1.0s$ e (e) $10s$.

Isso ocorre porque os interesses pendentes maliciosos possuem muito tempo para serem satisfeitos e assim podem bloquear a chegada de interesses legítimos. Assim, como o tempo de permanência dos interesses pendentes é maior, a PIT enche mais facilmente e aumenta

a quantidade de Pacotes de Interesses legítimos descartados durante o encaminhamento para a PIT. Tal fato, mantém a PIT operando constantemente no limiar de sua capacidade, como mostrado no gráfico (e) da Figura 5.6.

Observa-se que para um valor de $T_{out} = 0.1s$ há a maior quantidade de interesses pendentes satisfeitos. Intuitivamente, um valor de T_{out} o mais próximo possível do RTT médio minimiza a expiração de interesses pendentes legítimos. Porém, a definição do valor do *timeout* pode ser otimizada. Este valor ótimo de T_{out} é determinado quando a soma dos interesses expirados e descartados é mínima, onde depende diretamente das taxas de tráfego legítimos e maliciosos e da capacidade da PIT.

Capítulo 6

Modelagem de Otimização do Tempo Máximo de Permanênciana PIT

O desempenho da PIT pode ser influenciado diretamente pela definição do tempo máximo de permanência T_{out} dos seus interesses pendentes. A definição deste valor de *timeout* é fundamental para estabelecer o comportamento da PIT do roteador sob ataque.

6.1 Função de Otimização

Intuitivamente, um valor de T_{out} bem definido pode contribuir para a mitigação de ataques de inundação através da diminuição do tempo de permanência de interesses pendentes maliciosos na PIT. Por outro lado, um valor de T_{out} impropriamente dimensionado pode contribuir para o sucesso do ataque de inundação. Para T_{out} muito baixos, pode ocorrer a expiração de entradas de interesses pendentes legítimos na PIT, uma vez que $RTT > T_{out}$. Para T_{out} muito altos, aumenta o tempo de permanência na PIT de entradas para interesses pendentes maliciosos, contribuindo para a sobrecarga da tabela e bloqueio dos Pacotes de Interesses legítimos que chegam na PIT.

Assim, busca-se estabelecer um valor ótimo para T_{out} de modo a maximizar a *throughput* de satisfação dos interesses pendentes legítimos na PIT. Isto possibilita contribuir para a mitigação dos ataques de inundação na CCN, ao tornar o *timeout* um mecanismo de defesa em um primeiro nível.

Considerando um roteador qualquer da rede, este valor ótimo de T_{out} pode ser diferente para cada entrada da PIT do roteador, uma vez que depende diretamente do valor do RTT para recuperação de dados. Como o RTT para cada publicador é diferente, os interesses pendentes da PIT para cada roteador podem ter *timeouts* diferentes. No caso de ataque

ao roteador de borda do publicador, a diferença entre os $RTTs$ para cada entrada podem ser bem próximos podendo estabelecer um RTT médio.

Considerando diferentes Pacotes de Interesses legítimos para conteúdos gerados dinamicamente, ou seja, que não são recuperados em *cache*, pode-se enumerar as condições fundamentais para que um interesse pendente legítimo na PIT seja satisfeito:

i) *Sem bloqueio*: O respectivo Pacote de Interesse não pode ser bloqueado pela PIT; e

ii) *Sem expiração*: O interesse pendente legítimo deve ser satisfeito antes de atingir o tempo máximo de permanência na PIT, ou seja, $RTT < T_{out}$.

Métrica	**Valor**
$f(t)$	Função de *throughput* de satisfação dos interesses pendentes legítimos.
$f'(t)$	Primeira derivada de $f(t)$.
$f''(t)$	Segunda derivada de $f(t)$.
$P_l(t)$	fda do tempo de permanência dos interesses legítimos.
$(1 - e^{-t\mu_l})$	fda da probabilidade de interesse legítimo ser satisfeito em $t < T_{out}$
$(1 - P_b)$	Probabilidade de pacote de Interesse não ser bloqueado na PIT.

Tabela 6.1: Definição de métricas principais da simulação.

Assim, seja $f(t)$ a função de *throughput* de satisfação dos interesses pendentes legítimos, no qual são encaminhados para a PIT de acordo com uma determinada taxa de chegada λ_l pelo processo de Poisson. Assuma $P_l(t)$ como a função de distribuição acumulada (fda) do tempo de permanência dos interesses pendentes legítimos na PIT como o produto da probabilidade de um Pacote de Interesse não ser bloqueado $(1-P_b)$ com a fda da probabilidade de um interesse pendente legítimo ser satisfeito em um tempo $t < T_{out}$ na forma $(1 - e^{-t\mu_l})$:

$$P_l\left(t\right) = (1 - P_b) \cdot \left(1 - e^{-t\mu_l}\right) \tag{6.1}$$

Dados λ_l e $P_l(t)$, espera-se maximizar a função de *throughput* $f(t)$ definida como:

$$max \quad f(t) = \lambda_l \cdot P_l\left(t\right) \tag{6.2}$$

$$s.t. \quad T_{out} > 0$$

Teorema 4.1 *$f(t)$ é uma função côncava e, portanto, possui um valor ótimo global que pode ser determinado.*

Prova: Seja $f(t)$ uma função contínua, demonstrando que ela é duas vezes derivável e com um ponto crítico t_x, ao determinar a segunda derivada $f''(t) < 0$, conclui-se que possui um único valor máximo relativo, no qual pode ser estimado como um valor ótimo global.

Como λ_l é uma constante em relação a função $f(t)$, pode-se desconsiderá-la no cálculo das derivadas. Assim, calcula-se $p_l'(t)$ e $p_l''(t)$, respectivamente, como a primeira e segunda derivada de $P_l(t)$. Da mesma forma, desconsidera-se $(1 - P_b)$ por ser uma constante em relação a $p_l(t)$. Com isso, deriva-se:

$$\begin{aligned} p_l'(t) &= \left(1 - e^{-t\mu_l}\right)' \\ &= -e^{-t\mu_l} \cdot (-\mu_l) \\ &= \mu_l e^{-t\mu_l} \end{aligned} \tag{6.3}$$

$$\begin{aligned} p_l''(t) &= \left(\mu_l e^{-t\mu_l}\right)' \\ &= \left(\mu_l e^{-t\mu_l}\right) \cdot (-\mu_l) \\ &= -\mu_l^2 e^{-t\mu_l} \end{aligned} \tag{6.4}$$

Como $p_l^{''}(t) < 0$ implica em $f(t)'' < 0$, para $\forall\ t\ \varepsilon\ \mathbb{R}$, $f(t)$ é caracterizada como uma função côncava com um único valor ótimo global estimado. A partir dos cálculos, pode-se buscar maximizar $f(t)$ para $t = T_{out}$, dado que $Tout > 0$. ■

6.1.1 Comparação dos Resultados Numéricos entre o Modelo de Otimização e a Simulação

Para esta comparação fora utilizadas as mesmas condições e modelo de simulação conforme apresentado anteriormente na Subseção 5.1.2 através do módulo $ndnSIM$ do NS3, como mostrado na tabela 6.1.1.

Métrica	**Valor**
Tráfego	Poisson
$\lambda_l + \lambda_m$	1000 pacotes/s
$\lambda_m(\lambda_l)$	Proporcão entre valor do tráfego malicioso e legítimo.
RTT	Exponencial com média $\tau = 0,1s$
c	100 interesses pendentes
t_{simul}	$1000s$

Tabela 6.2: Definição de métricas principais da simulação.

A *throughput* ótima de satisfação de interesses pendentes legítimos é calculada ao final de cada simulação em função da variação dos valores de *timeout*. Com isso, considera-se a simulação com o *timeout* ótimo, aquela que ao ser definido T_{out} e ao se fixar uma taxa λ_l, obtém a maior quantidade de interesses pendentes satisfeitos definida como $S_{max}(t)$. A *throughput* ótima é dada por:

$$max \quad f(t) = \frac{S_{max}(t)}{T} \tag{6.5}$$

onde T é o tempo total da simulação. Outra forma se dá através do valor da probabilidade de um Pacote de Interesse legítimo ser satisfeito, ou seja, a Probabilidade de satisfação $P_s(t)$, na forma:

$$P_l(t) \equiv P_s(t) = \frac{S(t)}{L(t)} \tag{6.6}$$

onde $S(t)$ e $L(t)$ são respectivamente, a quantidade total de interesses legítimos satisfeitos e a quantidade total de Pacotes de Interesses legítimos encaminhados para a PIT. Assim, a simulação com maior valor de $P_s(t)$ é aquela cujo *timeout* possui o valor ótimo.

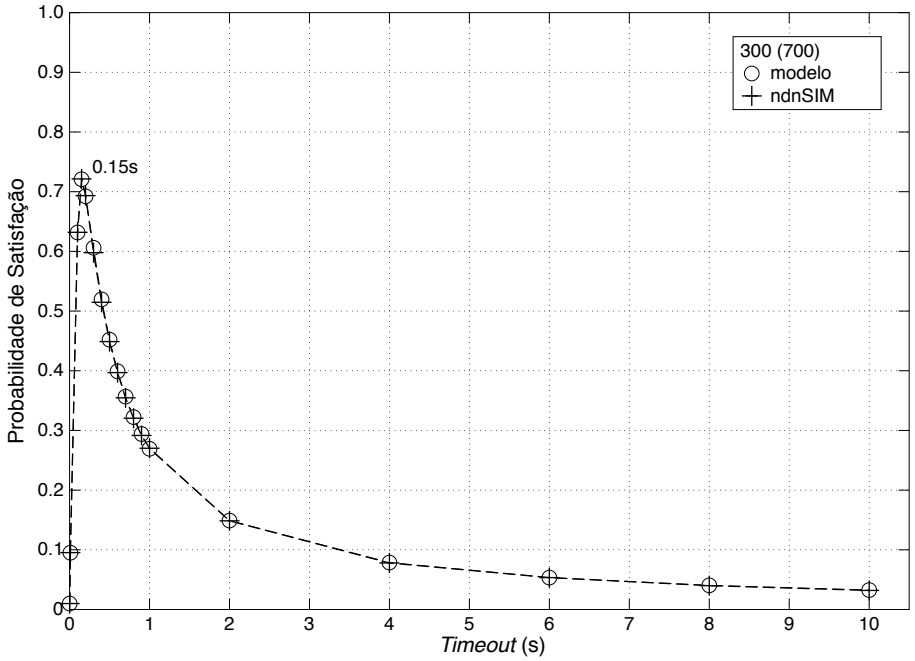


Figura 6.1: Comparação do modelo de otimização e simulação da taxa de interesses pendentes atendidos em função da Probabilidade de Satisfação e do valor do tempo máximo de permanência na PIT.

Através do gráfico da Figura 6.1 mostra-se a comparação dos resultados numéricos entre o modelo de otimização e a simulação para a probabilidade de satisfação de interesses pendentes legítimos em função da variação do valor de *timeout*. Percebe-se que para as condições de tráfego impostas ao roteador, um valor ótimo a ser definido se encontra

$T_{out} = 0,15s$. À medida que se define valores de *timeouts* menores que o valor ótimo, probabilidade de satisfação dos interesses pendentes legítimos decresce linearmente. Já para valores de T_{out} acima do valor ótimo, o valor da *throughput* decresce exponencialmente. A variação da curva próxima ao valor ótimo pode ser observada a partir da Figura 6.2

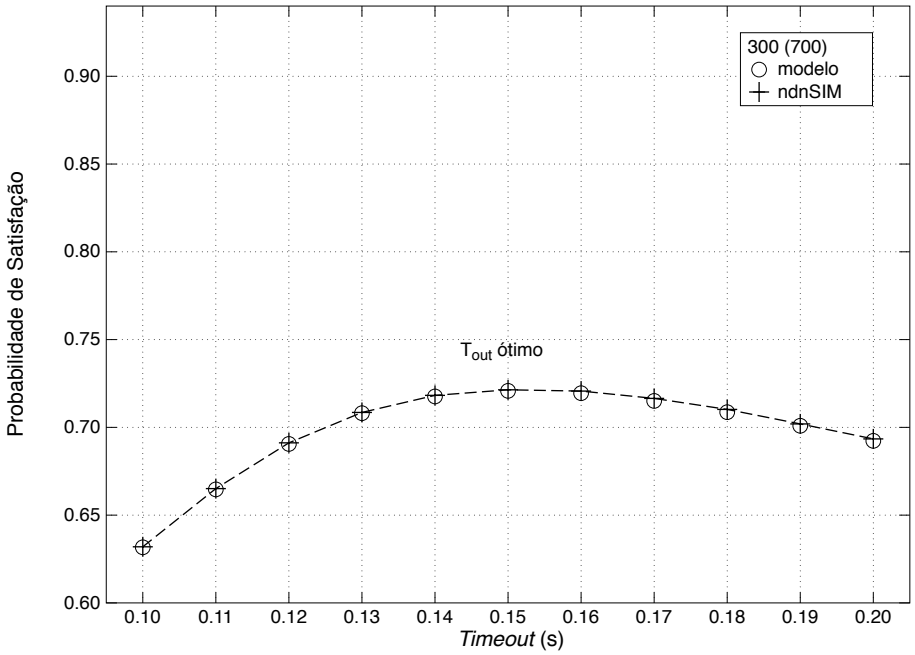


Figura 6.2: Valor da probabilidade de satisfação em função dos *timeouts* nas proximidades do valor ótimo .

No gráfico da Figura 6.3 pode-se comparar os resultados numéricos da *throughput* de satisfação em interesses pendentes por segundo entre o modelo e simulador. Pode-se analisar a diferença entre a *throughput* relacionada com o *timeout* ótimo $T_{out} = 0.15s$ e a relacionada ao RTT médio $T_{out} = 0.1s$. Percebe-se que ao definir um valor de *timeout* intuitivamente a partir do RTT médio tem-se uma perda de cerca de 9% na *throughput* de satisfação dos interesses pendentes legítimos, conforme o gráfico da Figura 6.4.

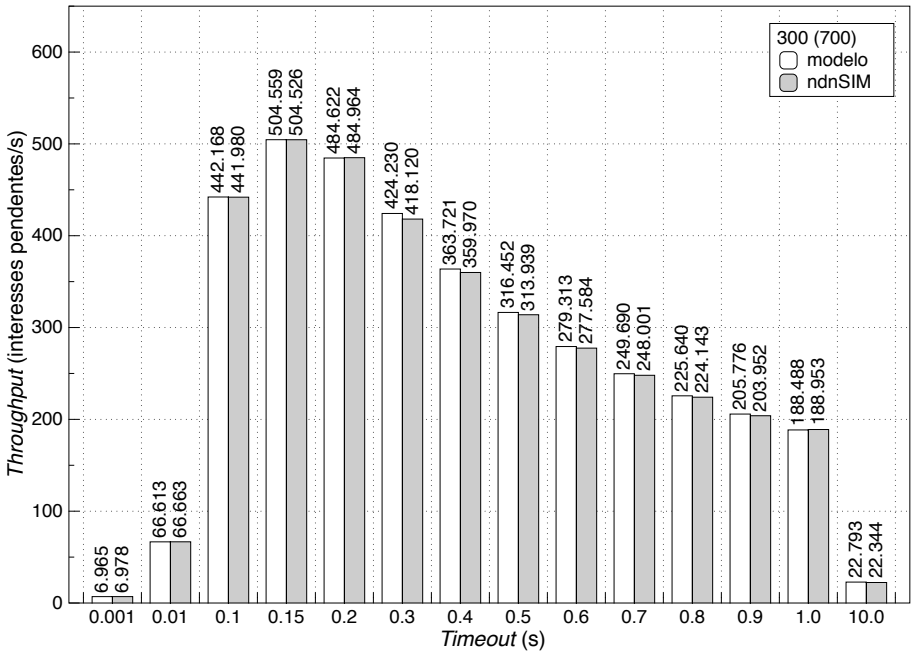


Figura 6.3: Valor da *throughput* em função dos *timeouts* nas proximidades do valor ótimo .

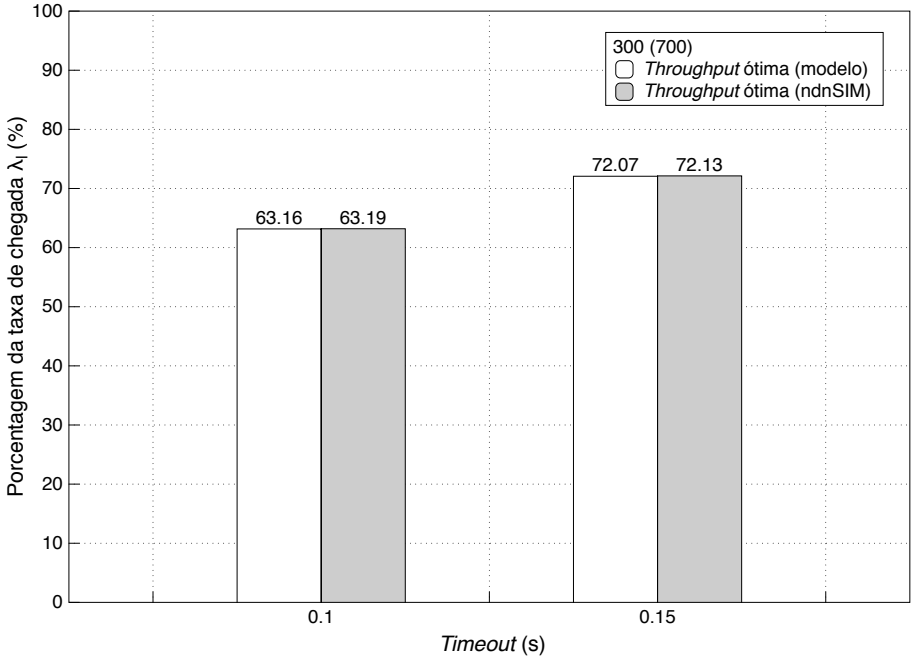


Figura 6.4: Diferença entre os valores da *throughput* ótima e a definida com *timeout* em função do RTT médio.

Capítulo 7

Considerações Finais e Trabalhos Futuros

7.1 Conclusão

Neste trabalho, propõe-se como principal contribuição a apresentação de um modelo analítico de roteador de conteúdo da CCN sob ataque de negação de serviço através de um sistema $M/G/c/c$, um modelo de otimização do valor do tempo máximo de permanência de interesses pendentes na PIT para mitigação de ataques de inundação e suas avaliações através de simulações.

A modelagem matemática do roteador CCN sob ataque de inundação contribui para o entendimento do *trade-off* entre a capacidade da PIT, a intensidade do tráfego maliciosos e a probabilidade de bloqueio. O modelo de otimização do tempo de permanência mostra que o valor a ser definido para o *timeout* pode contribuir para a mitigação de ataques de inundação na CCN. Com isso, a definição deste *timeout* pode ser considerada como um primeiro nível de proteção contra ataques DoS. Através das simulações, confirma-se a intuição de que um *timeout* bem definido pode ser positivo, porém um valor mal determinado pode ter um efeito negativo.

Tais contribuições podem ser aplicadas em mecanismos de mitigação contra ataques de negação de serviço. Como trabalhos futuros, pretende-se estabelecer valores de *timeouts* ótimos dinâmicos de acordo com a carga da rede, caracterizado por *lifetimes* adaptativos. Assim, espera-se implementar nos roteadores CCN um gerenciamento inteligente dos tempos máximos de permanência de interesses pendentes de acordo com a variação da carga do tráfego e da ocupação da PIT.

7.2 Discusão

Este trabalho destaca algumas questões de pesquisas futuras a serem discutidas e elucidadas em função da manutenção de estado da PIT:

i) *Custo computacional RTT médio versus timeout ótimo*: apesar do estabelecimento de um valor de *timeout* ótimo aumentar a *throughput* dos interesses pendentes legítimos, faz-se necessário uma melhor avaliação em termos de custo computacional ao incrementar o estado dos roteadores.

ii) *Custo computacional para timeouts adaptativos*: Apesar da definição do valor de *timeout* ótimo contribuir para a mitigação dos ataques de inundação, estabelecer um *timeout* adaptativo diferente para cada entrada na PIT pode gerar um alto custo computacional. Uma vez que a PIT é varrida frequentemente para a verificação das entradas, ao se estabelecer um valor adaptativo, haverá uma variação na frequência de varredura da PIT contribuindo para o aumento do consumo da memória.

Referências

[1] From content distribution networks to content networks -Ť issues and challenges. *Computer Communications 29*, 5 (2006), 551 – 562.

[2] Afanasyev, A.; Mahadevan, P.; Moiseenko, I.; Uzun, E.; Zhang, L. Interest flooding attack and countermeasures in Named Data Networking. In *Proceedings of International Federation for Information Processing Networking, IFIP 2013* (2013).

[3] Afanasyev, A.; Moiseenko, I.; Zhang, L. ndnSIM: NDN simulator for NS-3. Relatório Técnico NDN-0005, 2012.

[4] Arianfar, S.; Nikander, P.; Ott, J. On content-centric router design and implications. In *Proceedings of the Re-Architecting the Internet Workshop* (2010), ReARCH '10, pp. 5:1–5:6.

[5] Bellovin, S. M.; Clark, D. D.; Perrig, A.; Song, D. A clean-slate design for the next-generation secure internet. *Relatório Técnico - Report for NSF Global Environment for Network Innovations (GENI) Workshop* (2005).

[6] Bishop, M. *Computer Security: Art and Science*. Addison Wesley Publishing Company Incorporated, 2003.

[7] Bonald, T.; Roberts, J. W. Internet and the erlang formula. *SIGCOMM Comput. Commun. Rev. 42*, 1 (2012), 23–30.

[8] Boteanu, D.; Fernandez, J. M. A comprehensive study of queue management as a DoS counter-measure. *International Journal of Information Security IJIS, Springer-Verlag* (2013), 1–36.

[9] Chen, T. Network traffic modeling. *The Handbook of Computer Networks Wiley* (2007).

[10] Chromy, E.; Misuth, T.; Weber, A. Application of formulae in next generatin networks. *International Journal of Computer Network and Information Security(IJCNIS) 4*, 1 (2012), 59–66.

[11] Chung, Y. Distributed denial of service is a scalability problem. *ACM SIGCOMM Computer Communication Review 42*, 1 (2012), 69–71.

[12] Erlang, A. K. The theory of probabilities and telephone conversations. *Nyt Tidsskrift for Matematik 20*, B (1909), 33–39.

[13] Gasti, P.; Tsudik, G.; Uzun, E.; Zhang, L. DoS & DDoS in Named-Data Networking. *Proceedings of International Conference on Computer Communications and Networks (ICCCN 2013)* (2013).

[14] Gligor, V. A note on denial-of-service in operating systems. *Software Engineering, IEEE Transactions on SE-10*, 3 (1984), 320–324.

[15] Handley; Rescorla. Rfc 4732 - internet denial-of-service considerations, 2006.

[16] Huo, D. Generalized erlang-b formula for mobile and wireless radio channels. In *Global Telecommunications Conference, 1995. Conference record. Communication Theory Mini-Conference, GLOBECOM '95., IEEE* (1995), pp. 38–41.

[17] Ioannidis, J.; Bellovin, S. M. Pushback: Router-Based Defense Against DDoS Attacks, 2001.

[18] Ioannidis, J.; Bellovin, S. M. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *Network and Distributed System Security Symposium - NDSS* (2002).

[19] Jacobson, V.; Smetters, D. K.; Thornton, J. D.; Plass, M. F. Networking Named Content. *International Conference on emerging Networking Experiments and Technologies, CoNEXT'09* (2009).

[20] Kendall, D. G. Some problems in the theory of queues. *Journal of the Royal Statistical Society. Series B (Methodological), Wiley for the Royal Statistical Society 13*, 2 (1951), 151–185.

[21] Kharoufeh, J. The M/G/s/s queue. *Wiley Encyclopedia of Operations Research and Management Science, John Wiley & Sons, New York, NY.* (2011).

[22] Laufer, R. P.; Moraes, I. M.; Velloso, P. B.; Bicudo, M. D. D.; Campista, M. E. M.; Cunha, D. O.; Costa, L. H. M. K.; Duarte, O. C. M. B. Negação de Serviço: Ataques e Contramedidas. In *Minicurso - Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg* (2005), pp. 1–63.

[23] Mirkovic, J.; Dietrich, S.; Dittrich, D.; Reiher, P. *Internet Denial of Service: Attack and Defense Mechanisms.* Prentice Hall PTR, 2004.

[24] Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review 34*, 2 (Apr. 2004), 39–53.

[25] Moreira, M.; Fernandes, N.; Costa, L.; Duarte, O. Internet do futuro: Um novo horizonte. In *Minicurso - Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC* (2009), pp. 1–59.

[26] ndnSIM. ndnSIM web site. http://www.ndnsim.net/, 2013.

[27] NS-3. NS-3 web site. http://www.nsnam.org/, 2013.

[28] Oueslati, S.; Roberts, J.; Sbihi, N. Flow-aware traffic control for a content-centric network. In *INFOCOM, 2012 Proceedings IEEE* (2012), pp. 2417–2425.

[29] Park, C., K. T. C. Y. Scalability problem for interest diffusion in content-centric network. *In Proceedings of the 14th Conference on Next Generation Communication Software (NCS)* (2010), 36–39.

[30] Ribeiro, I. C. G.; Guimarães, F. Q.; Kazienko, J.; Rocha, A. A. A.; Velloso, P. B.; Moraes, I. M.; De Albuquerque, C. V. Segurança em Redes Centradas em Conteúdo: vulnerabilidades, ataques e contramedidas. *Minicurso Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, SBSeg* (2012), 101–150.

[31] Ross, S. M. *Simulation*, 5 ed. Academic Press, 2013.

[32] Shirey, R. RFC 2828 - Internet Security Glossary. 2000.

[33] Stallings, W. *Cryptography and Network Security: Principles and Practice*, 4rd ed. Prentice Hall, 2006.

[34] Takahashi, Y.; Kino, I. The supplementary variable technique and product form solutions. *Communications of Operations Research Society of Japan 43*, 10 (1998), 562–567.

[35] Takahashi, Y.; Shikata, Y.; Okada, K.; Komatsu, N. Multi-server loss system with t-limited service for traffic control in information networks. In *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on* (2007), pp. 491–496.

[36] Tan, Y.; Lu, Y.; Xia, C. H. Provisioning for large scale loss network systems with applications in cloud computing. *SIGMETRICS Perform. Eval. Rev. 40*, 3 (2012), 83–85.

[37] Telegraph, I.; Committee, T. C. *CCITT Recommendation X.800: Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications : Security Architecture for Open Systems Interconnection for CCITT Applications*. International Telecommunication Union, 1991.

[38] Trossen, D.; Sarela, M.; Sollins, K. Arguments for an information-centric internetworking architecture. *ACM SIGCOMM Computer Communications Review 40*, 2 (2010), 26–33.

[39] Wählisch, M.; Schmidt, T. C.; Vahlenkamp, M. Bulk of interest: performance measurement of content-centric routing. In *Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication* (2012), SIGCOMM '12, pp. 99–100.

[40] Wang, L.; Afanasyev, A.; Kuntz, R.; Vuyyuru, R.; Wakikawa, R.; Zhang, L. Rapid traffic information dissemination using named data. In *Proceedings of the 1st ACM workshop on Emerging Name-Oriented Mobile Networking Design - Architecture, Algorithms, and Applications (NoM 12)* (2012), pp. 7–12.

[41] Yi, C.; Afanasyev, A.; Moiseenko, I.; Wang, L.; Zhang, B.; Zhang, L. A case for stateful forwarding plane. *Computer Communications 36*, 7 (2013), 779–791.

[42] Zhang, L.; Estrin, D.; Burke, J.; Jacobson, V.; Thornton, J.; Smetters, D.; Zhang, B.; Tsudik, G.; Claffy, K.; Krioukov, D.; Massey, D.; Papadopoulos, C.; Abdelzaher, T.; Wang, L.; Crowley, P.; Yeh, E. Named Data Networking (NDN) Project.

[43] Zhu, Z.; Bian, C.; Afanasyev, A.; Jacobson, V.; Zhang, L. Chronos: Serverless multi-user chat over ndn. Technical Report NDN-0008, NDN, 2012.