Nem Tanto, Nem Tão Pouco: Existe um *Timeout* Ótimo para PIT CCN na Mitigação de Ataques DoS

Flávio de Q. Guimarães*, **Igor C. G. Ribeiro***,
Antonio A. de A. Rocha, Célio V. N. de Albuquerque*

Instituto de Computação (IC)
Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

{flavio,iribeiro,arocha,celio}@ic.uff.br

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.*

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.*

1. Introdução

O crescimento do número de ataques distribuídos de negação de serviço (*Distributed Denial of Service* - DDoS) ao longo dos anos evidenciou a necessidade de implementação de mecanismos de segurança no núcleo da rede. A quebra da premissa de não se alterar o núcleo da rede incentivou novas propostas de arquiteturas *clean-slate* para a Internet do Futuro [Trossen et al. 2010]. Neste contexto, [Jacobson et al. 2009] propuseram as Redes Centradas em Conteúdo (*Content Centric Networks* - CCN), na qual todos os roteadores da rede mantêm estado de encaminhamento dos pacotes. Além de visar a distribuição mais eficiente de conteúdo, a manutenção de estado nos roteadores permite que a CCN seja resistente a grande parte dos atuais ataques de negação de serviço. O plano de controle de encaminhamento de pacotes da CCN proporciona a diminuição do volume do

*Laboratório MídiaCom

 ©2013 SBC — Soc. Bras. de Computação

tráfego pela agregação de pacotes, o balanceamento do fluxo entre pacotes e a recuperação de dados em quaisquer nós da rede.

Apesar da preocupação de se definir uma arquitetura mais resiliente às vulnerabilidades de ataque existentes na Internet atual (por exemplo, os ataques distribuídos de negação de serviço), estudos têm demonstrado que usuários maliciosos podem explorar características da arquitetura para adaptar alguns desses ataques [Ribeiro et al. 2012]. Um dos principais ataques é o de inundação de pacotes que visa o esgotamento dos recursos dos roteadores, impedindo o atendimento a usuários legítimos. Este artigo avalia exatamente a fragilidade da proposta CCN a um ataque específico, o de inundação da estrutura de dados que mantém o estado nos roteadores.

A eficácia dos ataques de inundação de pacotes na CCN possui uma relação direta entre o volume dos tráfegos de ataque e legítimo, do tempo de recuperação dos conteúdos desejados (*Round Trip Time* - RTT), da capacidade da estrutura de dados que possibilita manter o estado nos roteadores e do tempo de permanência dos estados nesta estrutura. Este trabalho apresenta uma análise de como a definição do tempo máximo de permanência (*timeout*) dos estados nos roteadores pode influenciar positivamente (ou negativamente) a mitigação dos ataques de inundação, revelando a existência de um *trade-off* para esse valor definido pelo roteador.

Portanto, as contribuições dete artigo são: (i) uma modelagem analítica dos fluxos de um roteador da CCN sob ataque de inundação. A abstração definida pelo modelo consiste em um sistema de filas $M/G/c/c$, com limitação da taxa de serviço; (ii) um modelo de otimização para determinar o *timeout* ótimo, a ser definido nos roteadores, para o tempo de manutenção de estados dos pedidos recebidos. A formulação permite maximizar o *throughput* útil do sistema através da obtenção do valor ótimo para o *timeout* dos roteadores; e, (iii) validação do modelo analítico e do modelo de otimização através de simulações do fluxo de dados legítimo e malicioso em um roteador CCN.

O restante deste artigo está organizado da seguinte forma: na Seção 2 são brevemente descritas as características básicas da arquitetura CCN. Os ataques de inundação de pacotes e suas variações são abordados na Seção 3. Na Seção 4 é apresentada uma modelagem analítica de um roteador CCN sob ataque de inundação de forma análoga a um sistema de filas e uma análise através de simulações. Na Seção 5 propõe-se uma modelagem de otimização do tempo máximo de manutenção de estado nos roteadores CCN. Por fim, na Seção 6 são apresentadas as considerações finais e trabalhos futuros.

2. Visão Geral da CCN e Trabalhos Relacionados

O processo de recuperação de conteúdo na CCN é baseado na requisição e resposta entre usuários consumidores e publicadores de conteúdo. Os consumidores solicitam os conteúdos à rede enviando Pacotes de Interesse que transportam os nomes dos conteúdos utilizados pelos roteadores para estabelecer o encaminhamento dos pacotes. Ao invés de tratar o conteúdo pela sua localização, como na arquitetura TCP/IP, a CCN se refere ao conteúdo diretamente pelo nome (prefixo), transformando-o em uma entidade de primeira classe, através da nomeação explicita dos conteúdos ao invés de locais físicos. Por exemplo, o oitavo fragmento do conteúdo publicado pelo Instituto de Computação da Universidade Federal Fluminense para a primeira aula de segurança da informação poderia ter o nome: `/uff.br/ic/aulas2013/seg1/8`. Desta forma, grandes conteúdos

 ©2013 SBC — Soc. Bras. de Computação

podem ser divididos em fragmentos menores (*chunks*).

A CCN propõe que todos os nós da rede estabeleçam armazenamento dos conteúdos. Um determinado Pacote de Interesse pode ser "satisfeito" por quaisquer roteadores da rede, por outros consumidores ou pelo publicador original através da emissão do Pacote de Dados com o conteúdo desejado. Os Pacotes de Interesse e de Dados são os únicos tipos de pacotes pertencentes ao processo de requisição e transmissão de conteúdos. Porém, somente os Pacotes de Dados são assinados pelos publicadores, possibilitando a verificação da assinatura pelos consumidores e possivelmente pelos roteadores da rede.

Cada nó da arquitetura CCN possui três estruturas de dados básicas: o Armazenador de Conteúdo, a Tabela de Interesses Pendentes e a Base de Encaminhamento de Dados. Cada estrutura desempenha uma função no processo de encaminhamento de pacotes na CCN. O Armazenador de Conteúdo (*Content Store* - CS) mantém o *cache* temporário de dados recebidos e permite replicar o conteúdo no núcleo da rede. A Tabela de Interesses Pendentes (*Pending Interest Table* - PIT) mantém o estado dos interesses pendentes, ainda "não satisfeitos" pelo roteador. Cada entrada na PIT contém uma ou múltiplas interfaces físicas de entrada, indicando que o mesmo conteúdo foi solicitado por vários consumidores diferentes e uma ou múltiplas interfaces de saída, indicando que um Pacote de Interesse foi transmitido por vários caminhos diferentes. Cada interesse pendente possui um tempo de vida (*lifetime*) associado à sua entrada na PIT, a qual é removida após expiração do *timeout* T_{out} estabelecido. A Base de Informações de Encaminhamento (*Forwarding Information Base* - FIB) é uma tabela de encaminhamento que mantém os prefixos e suas correspondentes interfaces de saída. Através da política utilizada, a FIB possibilita o encaminhamento dos pacotes salto a salto e estabelece o caminho do consumidor até a fonte de conteúdo.

Dos trabalhos relacionados, destaca-se um modelo de roteador de conteúdo genérico proposto por [Perino e Varvello 2011] com seus três componentes principais (CS, PIT e FIB) com foco na avaliação de desempenho do roteador. Para cada componente, são analisados os requisitos de armazenamento e restrições de latência em relação ao processo de chegada de Pacotes de Interesses e de Dados. Em [You et al. 2012], é proposta uma modelagem da PIT para avaliação dos tamanhos das tabelas e seus custos atuais. É apresentada uma equação para a geração do número de entradas na PIT em função da taxa de acerto de *cache* e distribuição de popularidade do tráfego. Porém, não é considerado o tempo máximo de permanência de uma entrada na PIT até sua expiração (T_{out}).

3. Os Ataques de Inundação de Pacotes de Interesse na CCN

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. Porém, a PIT pode sofrer o chamado "efeito *Slashdot*" [Chung 2012], 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.

Diferentemente dos ataques de inundação tradicionais da arquitetura da Internet atual [Mirkovic e Reiher 2004], o objetivo principal dos ataques de inundação na CCN

 ©2013 SBC — Soc. Bras. de Computação

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*.

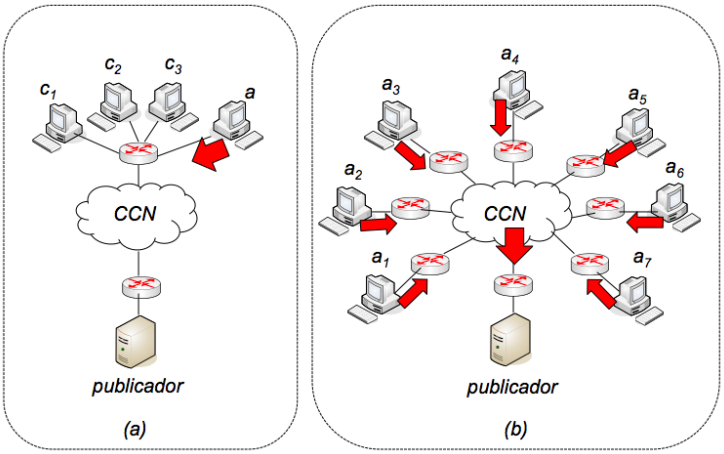

Figura 1. (a) Ataque de inundação ao roteador de borda dos consumidores e (b) Ataque de inundação ao roteador de borda do publicador.

Uma variação dos ataques de inundação é o esgotamento da PIT do roteador de borda dos usuários consumidores ou publicadores, conforme representado pela Figura 1. Nos ataques aos roteadores de borda dos consumidores, o atacante deve compartilhar o mesmo roteador dos usuários maliciosos. Com isso, a eficiência do ataque depende da geração de um grande volume de pacotes maliciosos pelo atacante. Nos ataques aos roteadores de borda dos publicadores, assumindo que um atacante controla uma *botnet* com transmissão síncrona, o volume do tráfego malicioso pode ser distribuído entre os usuários controlados. Intuitivamente o maior volume do tráfego de ataque é concentrado no roteador de borda do publicador.

O tráfego de ataque pode ser composto por Pacotes de Interesses para conteúdos existentes, dinâmicos ou inexistentes. O fluxo de ataque para requisições de conteúdos existentes intuitivamente é o menos eficaz, uma vez que os *caches* no núcleo da rede e a agregação de pacotes contribuem para diminuição do volume do tráfego de ataque até o publicador de conteúdo. Os conteúdos dinâmicos são gerados apenas quando requisitados através de Pacotes de Interesse e são recuperados diretamente dos publicadores de conteúdo. O ataque com Pacotes de Interesse para conteúdos dinâmicos é intuitivamente inviável, uma vez que requer um conhecimento prévio de um grande volume de conteúdos a serem publicados. A forma mais eficaz de geração de tráfego de ataque é através de Pacotes de Interesses para diferentes conteúdos inexistentes. Como tais pacotes nunca serão satisfeitos ou agregados, podem ser gerados em grandes volumes e permanecerão na PIT até a expiração por *timeout*.

4. Modelagem Analítica de um Roteador de Conteúdo sob Ataque de Inundação de Pacotes de Interesse

A modelagem analítica possibilita avaliar a vulnerabilidade dos recursos do sistema sob ataque. Além disso, contribui para o entendimento de como detectar o ataque de

 ©2013 SBC — Soc. Bras. de Computação

inundação através da observação do comportamento estatístico do tráfego. 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.

4.1. Modelagem dos Fluxos Existentes em um Roteador de Conteúdo

Suponha que um consumidor C envie requisições à rede para conteúdo de determinado publicador P. Assuma que P possua apenas um único servidor de conteúdo na rede. 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 $W = \{R_0, R_1, ..., R_{x-1}, R_x, R_{x+1}, ..., R_w\}$, onde R_0 é o roteador de borda de C e R_w o roteador de borda de P.

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 que serão "satisfeitos" pelos Pacotes de Dados armazenados no CS. 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 2. Considerando que o CS consegue processar todos os pacotes que chegam, deduz-se que $\Lambda_{CS}^{inInt} = \Lambda_{CS}^{outDat} + \Lambda_{CS}^{outInt}$.

Considere Λ_{CS}^{outInt} a taxa média de encaminhamento de Pacotes de Interesse para PIT. 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 descartada com taxa média $\Phi_{PIT}^{dropInt} = (1 - p_{CS}^{hit}) \cdot \Lambda_{CS}^{inInt} \cdot (1 - p_{PIT})$.

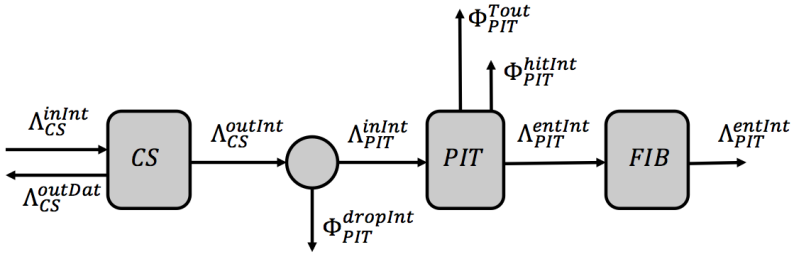

Figura 2. Processamento de Pacotes de Interesse no CS e na PIT.

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 descartados 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

 ©2013 SBC — Soc. Bras. de Computação

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. 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 2.

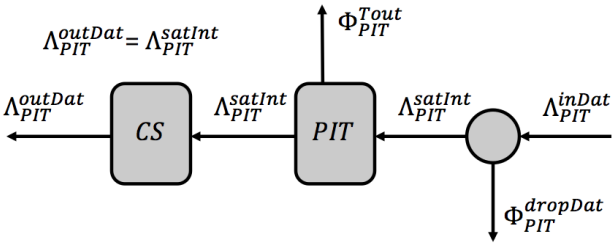

Figura 3. Processamento de Pacotes de Dados no CS e na PIT.

Assuma Λ_{PIT}^{inDat} como a taxa média de chegada de Pacotes de Dados por uma interface i qualquer. Os Pacotes de Dados cujos respectivos interesses pendentes foram expirados serão 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 com taxa média de remoção de entradas $\Lambda_{PIT}^{satInt} = \Lambda_{PIT}^{inDat} \cdot (1 - p_{PIT}^{Tout})$. 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 pelas interfaces por onde o interesse foi recebido, conforme representado pela Figura 3. 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*.

O monitoramento dos fluxos nos roteadores pode contribuir para a mitigação de ataques de negação de serviço. Uma das métricas sugeridas por [Gasti et al. 2012] para a detecção dos ataques de inundação é o uso de estatísticas dos roteadores. Neste sentido, o índice de satisfação de interesses por interface $I_i^{sat} = \Lambda_{PIT_i}^{satInt} / \Lambda_{PIT_i}^{entInt}$ apresenta uma relação entre a geração e remoção de entradas na PIT. Ao estabelecer um limiar para I_i^{sat} pode-se caracterizar um roteador sob ataque de inundação [Afanasyev et al. 2013].

4.2. Abstração e Modelagem da PIT por Sistema com Múltiplos Servidores com Limitação do Tempo de serviço

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 [Ross 2013].

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 para um mesmo publicador e um *lifetime* médio baseado no RTT médio ou *timeout*. Os fluxos são identificados de

 ©2013 SBC — Soc. Bras. de Computação

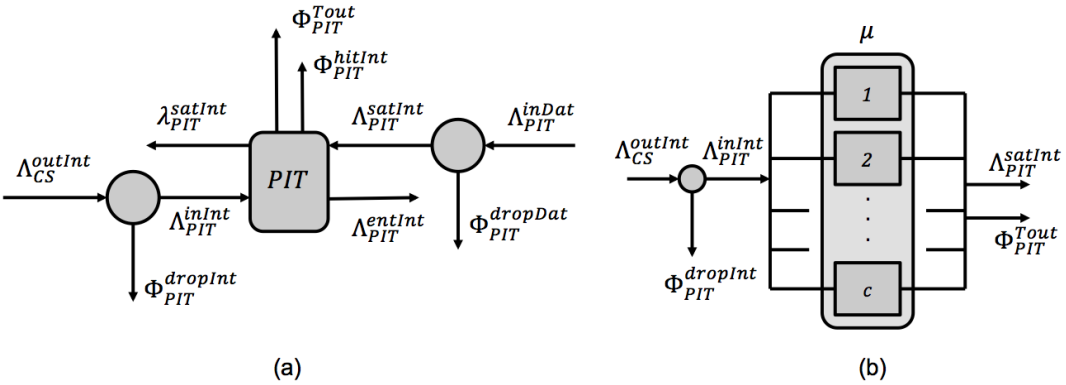

Figura 4. (a) Abstração da PIT e (b) Modelagem pelo sistema M/G/c/c.

forma *on-the-fly* através da análise dos pacotes pelos roteadores. 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 $\Lambda = \sum_{i=1}^{n} \Lambda_i$.

Abstraindo a PIT deste roteador, propõe-se a sua modelagem através do sistema de perda de Erlang $M/G/c/c$ [Kharoufeh 2011] com limitação do tempo de serviço, conforme a representado pela Figura 4. Pela notação de Kendall [Kendall 1951] 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 [Takahashi e Kino 1998] resulta na equação de balanceamento de fluxo:

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

O lado esquerdo da Equação (1) 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 [Boteanu e Fernandez 2013], 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 $M/G/c/c$.

 ©2013 SBC — Soc. Bras. de Computação

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 $\lambda = \lambda_l + \lambda_m$ [Ross 2013]. 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 pendentes legítimos t_l, conforme representado pela Equação (2). 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:

$$G_l(t) = \begin{Bmatrix} \mu_l e^{-t\mu_l} & t < T_{out} \\ 0 & t = T_{out} \end{Bmatrix} + \delta(t - T_{out}^{+})p_l, \quad p_l = \int_{T_{out}}^{\infty} \mu_l e^{-t\mu_l} dt = e^{-T_{out}\mu_l} \tag{2}$$

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

$$t_l \equiv \int_0^{\infty} tG_l(t)dt = \int_{T_{out}}^{\infty} te^{-\mu_l t} dt = \frac{1 - e^{-T_{out}\mu_l}}{\mu_l} \tag{3}$$

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 4.1. 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:

$$q_l = \frac{q \cdot \lambda_l}{\lambda} \quad e \quad q_m = \frac{q \cdot \lambda_m}{\lambda} \tag{4}$$

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

 ©2013 SBC — Soc. Bras. de Computação

legítimos e maliciosos de acordo com a proporção de interesses pendentes gerados no intervalo de tempo Δt, conforme representado pela Equação (5):

$$\bar{t} = t_l \frac{q_l}{q} + t_m \frac{q_m}{q} = t_l \frac{\lambda_l}{\lambda} + t_m \frac{\lambda_m}{\lambda} = \frac{t_l \lambda_l + t_m \lambda_m}{\lambda} = \frac{t_l \lambda_l + t_m \lambda_m}{\lambda_l + \lambda_m} \tag{5}$$

Logo, a taxa média geral de permanência é dada por $\mu \equiv 1/\bar{t}$, conforme representado pela Equação (6):

$$\mu \equiv \frac{1}{\bar{t}} = \frac{\lambda_l + \lambda_m}{t_l \lambda_l + t_m \lambda_m} = \frac{\lambda_l + \lambda_m}{\left(\frac{1 - e^{-T_{out}\mu_l}}{\mu_l}\right) \lambda_l + T_{out} \lambda_m} \tag{6}$$

Consequentemente, a carga geral do sistema $\rho = \lambda/\mu$, é dada pela Equação (7):

$$\begin{aligned} \rho &= \lambda \cdot \frac{1}{\mu} = (\lambda_l + \lambda_m) \frac{\left(\frac{1 - e^{-T_{out}\mu_l}}{\mu_l}\right) \lambda_l + T_{out} \lambda_m}{\lambda_l + \lambda_m} \\ &= \left(\frac{1 - e^{-T_{out}\mu_l}}{\mu_l}\right) \lambda l + T_{out} \lambda_m \end{aligned} \tag{7}$$

Estabelecida a carga geral ρ oferecida ao sistema, é possível determinar a probabilidade de bloqueio $P_b(\rho, c)$ [Kharoufeh 2011] 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 (8):

$$P_b(\rho, c) = \frac{\frac{\rho^c}{c!}}{\sum_{k=0}^{c} \frac{\rho^k}{k}} \tag{8}$$

Quando ρ e c são muito grandes o cálculo da Equação (8) pode ter um alto custo computacional. Porém, a função Erlang-B também pode ser expressada de forma recursiva:

$$P_b(\rho, c) = \frac{\rho P_b(\rho, k-1)}{k + \rho P_b(\rho, k-1)} \qquad para \;\; k = 1, 2, ..., c \tag{9}$$

4.4. Simulação de Roteador CCN sob Ataque de Inundação de Pacotes de Interesse

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.

 ©2013 SBC — Soc. Bras. de Computação

4.4.1. Modelo de Simulação

Através do simulador *Network Simulator* - NS3, utiliza-se o módulo ndnSIM [Afanasyev et al. 2012] para simular 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 1(b) da Seção 3. Em todas as simulações, o modelo de simulação é composto por dois geradores de tráfego (legítimo e malicioso), um roteador de conteúdo e um servidor publicador. O gerador de tráfego malicioso simula os fluxos provenientes da *botnet* com Pacotes de Interesses para diferentes conteúdos inexistentes, enquanto o gerador de tráfego legítimo simula um tráfego concorrente de Pacotes de Interesses para diferentes conteúdos existentes.

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 $\lambda_l + \lambda_m = 1.000\ pacotes/s$, alterando apenas a proporção entre os tráfegos denotada por $\lambda_m(\lambda_l)$. O tempo de permanência dos interesses pendentes legítimos na PIT é estabelecido de acordo com uma variável aleatória com distribuição exponencial e média de $0,1s$. A PIT do roteador admite uma capacidade para 100 interesses pendentes. Considera-se que o período de amostragem de pacotes $t = 1.000s$ seja significativamente suficiente para assegurar que os efeitos da quantização sobre os tempos de amostragem sejam desconsiderados.

4.4.2. Verificação do Modelo de Probabilidade de Bloqueio e Análise da Utilização da PIT

Para avaliar o impacto do tráfego maliciosos na PIT foram realizadas simulações para diferentes valores de $\lambda_m(\lambda_l)$. A Figura 5(a) mostra os resultados obtidos pelo modelo para $P_b(\rho, c)$ e pela simulação, da fração dos pacotes descartados por falta de espaço na PIT para *timeout* igual a $0,2s$ e $0,5s$. Tanto na simulação quanto no modelo analítico, percebe-se que à medida que aumenta a intensidade do tráfego malicioso, aumenta a probabilidade do pedido não ser "aceito" na PIT. Tal fato ocorre devido ao incremento da quantidade de interesses pendentes maliciosos na PIT em relação ao tráfego legítimo concorrente.

A Figura 5(b) mostra o total de interesses pendentes armazenados na PIT ao final de cada simulação em função da variação da intensidade do tráfego malicioso para *timeout* igual a $0,2s$ e $0,5s$. Percebe-se que, conforme aumenta-se a intensidade do tráfego malicioso, diminui-se a quantidade total de interesses pendentes armazenados na PIT. Isso ocorre pelo fato de que o pedido malicioso permanece na PIT por mais tempo do que o pedido legítimo. Nota-se também que a proporção de interesses pendentes armazenados da PIT por pacotes do tráfego malicioso aumenta com o incremento de λ_m.

4.4.3. Análise da Relação entre o Tempo Máximo de Permanência e a Quantidade de Entradas Atendidas na PIT

A Figura 6 mostra os resultados do total de pedidos atendidos obtidos através de simulação para diversos valores de *timeout*, onde $T_{out} = [0,001; 0,01; 0,1; 1; 10]$, e diferentes proporções de λ_l e λ_m. Pela figura, nota-se que, para valores de T_{out} muito baixos, a quantidade de interesses pendentes legítimos atendidos é inibida. Neste caso, a PIT está

 ©2013 SBC — Soc. Bras. de Computação

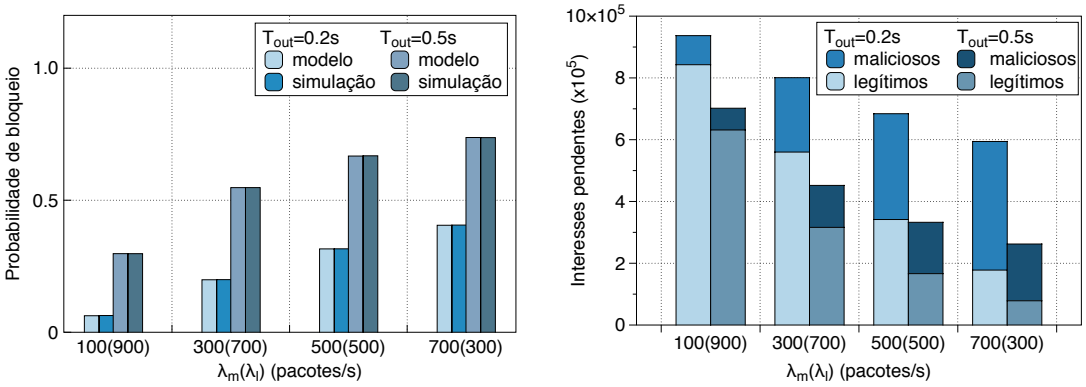

Figura 5. (a) Probabilidade de bloqueio x intensidade do tráfego malicioso e (b) Total de interesses pendentes legítimos e maliciosos armazenados na PIT.

excluindo as entradas tão rapidamente que ela nunca terá a chance de manter interesses pendentes próximo da sua capacidade. Por outro lado, 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 T_{out}, caracterizando que o $RTT < T_{out}$. Para valores de *timeouts* muito elevados, há o efeito contrário. 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.

O valor ótimo de T_{out} é determinado quando a soma dos interesses expirados e descartados é mínima. Este valor depende diretamente das taxas de tráfego legítimos e maliciosos e da capacidade da PIT.

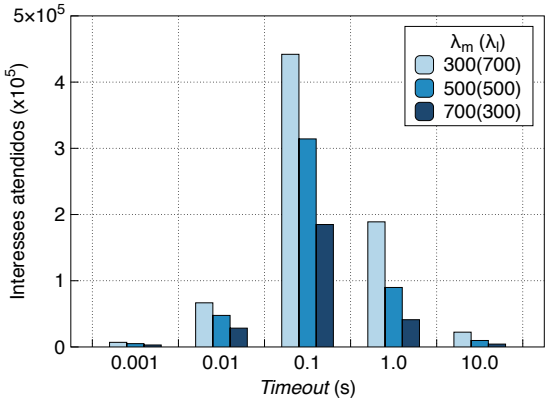

Figura 6. *Trade-off* entre a quantidade de Pacotes de Interesses legítimos atendidos e o valor do *timeout*.

5. Modelagem de Otimização do Tempo Máximo de Permanência na 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.

 ©2013 SBC — Soc. Bras. de Computação

5.1. 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 contribuição para a mitigação dos ataques de inundação na CCN. Isto torna 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.

Seja $f(t)$ a função de *throughput* dos Pacotes de Interesses legítimos 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 com a fda da probabilidade de um interesse pendente legítimo ser atendido em um tempo $t < T_{out}$:

$$P_l\left(t\right) = \left(1 - P_b\right) \cdot \left(1 - e^{-t\mu_l}\right) \tag{10}$$

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

$$max \;\; f(t) = \lambda_l \cdot P_l\left(t\right) \tag{11}$$

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

Teorema 5.1 *$f(t)$ 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:

$$\begin{aligned} p_l'(t) &= \left(1 - e^{-t\mu_l}\right)' \\ &= -e^{-t\mu_l} \cdot (-\mu_l) \\ &= \mu_l e^{-t\mu_l} \end{aligned} \tag{12}$$

 ©2013 SBC — Soc. Bras. de Computação

$$\begin{aligned} p_l''(t) &= \left(\mu_l e^{-t\mu_l}\right)' \\ &= \left(\mu_l e^{-t\mu_l}\right) \cdot (-\mu_l) \\ &= -\mu_l^2 e^{-t\mu_l} \end{aligned} \tag{13}$$

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 $Tout > 0$. ■

5.2. Comparação entre o Modelo de Otimização e a Simulação

A Figura 7 mostra a comparação dos resultados numéricos entre o modelo de otimização e a simulação para o *throughput* de interesses pendentes legítimos atendidos para um tráfego 700 (300) em função da variação do valor de *timeout*. Percebe-se que para as condições de tráfego impostas ao roteador, o valor ótimo a ser definido é $T_{out} = 0,15s$. A medida que se define valores de *timeouts* menores que o valor ótimo, menor é a taxa de atendimento aos interesses pendentes legítimos. Da mesma forma, para valores de T_{out} acima do valor ótimo, menor é o *throughput*.

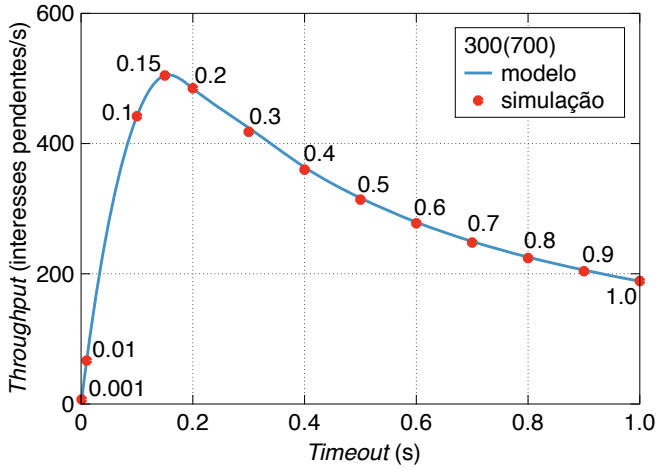

Figura 7. Comparação do modelo de otimização e simulação da taxa de interesses pendentes atendidos em função do valor do tempo máximo de permanência na PIT.

6. Considerações Finais

Neste artigo, 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.

 ©2013 SBC — Soc. Bras. de Computação

Referências

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

Afanasyev, A., Moiseenko, I. e Zhang, L. (2012). ndnSIM: NDN simulator for NS-3. Relatório Técnico NDN-0005.

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

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

Gasti, P., Tsudik, G., Uzun, E. e Zhang, L. (2012). DoS & DDoS in Named-Data Networking. http://arxiv.org/abs/1208.0952.

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

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

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

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

Perino, D. e Varvello, M. (2011). A reality check for Content Centric Networking. Em *Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking*, ICN '11, páginas 44–49.

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

Ross, S. M. (2013). *Simulation*. Academic Press, 5a. edição.

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

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

You, W., Mathieu, B., Truong, P., Peltier, J. e Simon, G. (2012). Realistic storage of pending requests in Content-Centric Network routers. Em *International Conference on Communications in China, ICCC*, páginas 120–125.

 ©2013 SBC — Soc. Bras. de Computação