Um Modelo de Rede Centrada na Informação Resiliente a Ataques de Negação de Serviços por Inundação de Interesses

Nilton Flávio S. Seixas[1], **Adriana Viriato Ribeiro**[1], **Leobino N. Sampaio**[1]

[1]Programa de Pós-graduação em Ciência da Computação (PGCOMP)
Instituto de Matemática – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

nfsseixas@dcc.ufba.br, adrianavr@dcc.ufba.br, leobino@ufba.br

Abstract. *In denial of services attacks by IFA (Interest Flooding Attack) the routers of caching network become unable to forward or receive legitimate packets, due to an exhaustion of memory reserved to PIT, occupied by an excessive number of false interests. In this work, it is proposed a model of Information Centric Network that sugests a cooperation between providers of content and routers to provide resilience to the practice of IFA. The cooperation facilitates the discrimination of illegitimate packets, making the model reaching more efficiency in the processes of detection and mitigation. Obtained results throught the simulation of caching network on the backbone of Internet2 demonstrated the effectiveness of proposed model.*

Resumo. *Em ataques de negação de serviço do tipo IFA (Interest Flooding Attack), os roteadores de uma rede de cache ficam inaptos para encaminhar ou receber pacotes legítimos, devido a uma exaustão da memória reservada para a tabela de pacotes de interesses pendentes, ocupada por um excessivo número de interesses falsos. Nesse trabalho, é proposto um modelo de Rede Centrada na Informação que sugere a cooperação entre provedores de conteúdos e roteadores para prover resiliência à prática de IFA. A cooperação facilita a discriminação dos pacotes ilegítimos, fazendo com que o modelo alcance maior eficiência e eficácia nos processos de detecção e mitigação. Resultados obtidos através da simulação de uma rede de cache no backbone da Internet2 evidenciaram a efetividade do modelo proposto.*

1. Introdução

Redes NDN (sigla da expressão em inglês, *Named Data Networks*) [Jacobson et al. 2009] tratam-se de uma das arquiteturas de Redes Centradas na Informação (*Information Centric networks* – ICN) [Xylomenos et al. 2014] que possui, como princípio fundamental, o uso de conteúdos nomeados na comunicação entre produtores e consumidores. O esquema de nomeação de conteúdo adotado em NDNs segue uma organização hierárquica, que é explorada pelos métodos de roteamento e encaminhamento implementados nos roteadores responsáveis pelo gerenciamento dos caches de tais redes [Ioannou and Weber 2016].

Para que seja possível a adoção de um plano de encaminhamento fortemente baseado em nomes de conteúdos, implementações de NDNs fazem uso de pacotes de interesse e de dados. Pacotes de interesse possuem informações sobre quais conteúdos são

requisitados pelos consumidores, enquanto os pacotes de dados transmitem os conteúdos disponibilizados pelos produtores. Os equipamentos de rede utilizam três estruturas de dados para processar e armazenar esses tipos de pacotes: a PIT (*Pending Interest Table*) armazena o nome dos pacotes de interesse que ainda não foram resolvidos e as interfaces que os requisitaram; a FIB (*Forwarding Interest Base*) é utilizada no armazenamento da lista de prefixos dos conteúdos para as interfaces de encaminhamento; e a CS (*Content Store*) realiza o armazenamento temporário de conteúdos disponibilizados na rede. PIT, FIB e CS são estruturas de dados mantidas através de recursos de memória e processamento finitos [Carofiglio et al. 2015, Wang and Hengkui 2015]. Como consequência, tais estruturas são passíveis de serem exploradas em ataques de negação de serviço (do inglês, *Denial of service* – DoS) [AbdAllah et al. 2015].

O IFA (sigla para a expressão em inglês, *Interest Flooding Attack*) é um dos métodos de ataque de DoS em NDNs que tem sido foco de investigação das recentes pesquisas sobre ICN [Mai et al. 2016, AbdAllah et al. 2015]. O método consiste no envio de um excessivo número de pacotes contendo interesses falsos aos roteadores, de forma que os recursos de memória reservados para a PIT sejam esgotados. Este tipo de ataque torna-se viável, dado que interesses não-resolvidos permanecem em memória até alcançar o tempo de expiração. Ao atingir a capacidade total da sua PIT, os roteadores ficam inaptos a processar interesses legítimos, caracterizando, assim, um DoS.

Soluções de detecção e mitigação de DoS com as características do IFA têm sido fortemente investigadas pela comunidade de redes [Mai et al. 2016, Nguyen et al. 2015, Wang et al. 2014, Wang et al. 2013, Compagno et al. 2013, Gasti et al. 2013]. Inicialmente, as soluções de mitigação propostas faziam a mitigação dos efeitos do IFA sem fazer a distinção entre pacotes legítimos e ilegítimos [Compagno et al. 2013, Wang et al. 2014]. Assim, o processo de mitigação implicava em perdas de desempenho da rede para os usuários não maliciosos. Esse problema motivou a criação de métodos mais sofisticados no sentido de tentar mitigar os efeitos do IFA a partir de uma melhor identificação e tratamento de pacotes ilegítimos [Wang et al. 2013, Nguyen et al. 2015]. Atualmente, essa é uma das questões em aberto na área e que ainda carece de investigação. As propostas atuais sugerem que o gerenciamento de pacotes legítimos e ilegítimos seja realizado apenas pelos nós da NDN, o que acarreta numa maior sobrecarga de trabalho no núcleo da rede.

Em contrapartida ao uso dos nós da rede, os provedores de conteúdo possuem um forte potencial para auxiliar no processo de diferenciação entre pacotes legítimos e ilegítimos. Além de possuir mais recursos computacionais, já fazem o gerenciamento dos seus conteúdos localmente, permitindo que o problema seja resolvido de forma distribuída. Por tais motivos, este trabalho apresenta um modelo de NDN em que provedores de conteúdo e nós da rede trabalham de forma cooperativa no processo de detecção e mitigação de IFA. Resultados experimentais obtidos através de simulações do *backbone* da Internet2[1] comprovam a efetividade do modelo. Além do modelo, este trabalho apresenta as seguintes contribuições: i) uma técnica para rápida detecção de DoS em redes de caches; ii) um mecanismo de mitigação de DoS em redes NDN que não sobrecarrega os nós da rede.

[1] www.internet2.edu

Este artigo está organizado da seguinte forma. A Seção 2 discute brevemente os fundamentos e principais características de ataques de negação de serviços do tipo IFA(por interesses falsos) em redes de cache. A Seção 3 apresenta o modelo proposto neste trabalho, detalhando seus elementos e principais características. A Seção 4 descreve o ambiente de avaliação construído para a realização dos experimentos e, a Seção 5, os principais resultados obtidos. Por fim, a Seção 6 apresenta as conclusões do trabalho.

2. Detecção e mitigação de IFA em redes de cache

Em ataques de DoS do tipo IFA, os roteadores ficam inaptos para encaminhar ou receber pacotes de interesses devido à uma exaustão da memória reservada para a PIT [Mai et al. 2016, AbdAllah et al. 2015]. Três abordagens costumam ser empregadas para atingir este objetivo [Gasti et al. 2013]: (i) **uso de conteúdo estático**, que tem o propósito de degradar a eficiência da rede para os consumidores a partir do foco do ataque nos produtores e roteadores que estão associados a conteúdos específicos; (ii) **uso de conteúdo dinâmico**, em que o atacante e seus *zombies* inundam o produtor com pacotes de interesse sobre conteúdos que serão criados dinamicamente pelo produtor; e, por fim, (iii) **uso de interesses falsos**, através do qual, o atacante inunda a PIT do roteador alvo com pacotes de interesse sobre conteúdos inexistentes, ou seja, interesses que jamais serão satisfeitos.

A fim de lidar com tais abordagens, algumas estratégias de mitigação de IFA se baseiam na filtragem ou descarte de pacotes de interesse, assim que os ataques são detectados. Em [Compagno et al. 2013], cada roteador possui uma relação de entrada de pacotes de interesse por saída de pacotes de dados por interface. Quando o valor dessa relação ultrapassa seu limiar, os interesses vão sendo rejeitados. Mensagens de controle são enviadas por essas interfaces cujo limiar foi transposto, para que os roteadores enviem menos pacotes, possibilitando a redução do fluxo de entrada no roteador originário da mensagem. Esse processo se repete até que chegue nos roteadores de borda, impedindo que pacotes maliciosos adentrem a rede. Em [Wang et al. 2014], o ataque é detectado após a taxa de ocupação ou taxa de interesses expirados da PIT ultrapassarem determinados limiares. Então, mensagens de controle percorrem as interfaces de chegada do prefixo apontado como malicioso, até chegarem nos roteadores de borda. Lá, os interesses com o dado prefixo são descartados até que a taxa de recebimento obedeça ao limiar preestabelecido.

Uma característica comum a tais estratégias de mitigação é que não existe distinção entre os pacotes legítimos e ilegítimos no descarte de interesses. Consequentemente, há uma queda de desempenho da rede como um todo durante o processo de mitigação, sobretudo para os usuários não maliciosos.

3. Modelo Proposto

O modelo de NDN proposto neste trabalho baseia-se na colaboração entre produtores e nós da rede para detectar rapidamente o IFA e mitigar seus efeitos sem prejudicar os usuários não maliciosos. A Figura 1 apresenta uma descrição resumida dos principais elementos e suas interações.

A figura mostra que os nós da NDN são responsáveis pela detecção de comportamentos suspeitos. Para confirmar a possível ocorrência de um IFA (1), os nós enviam

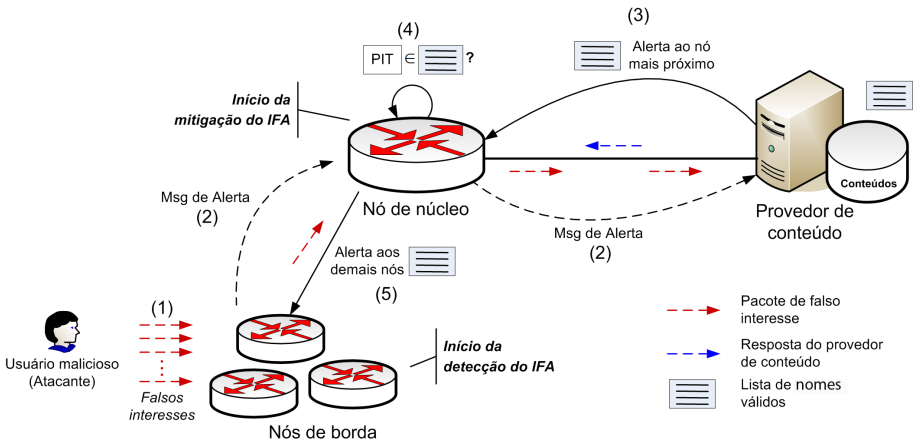

Figura 1. Modelo de NDN proposto em que o nó da rede trabalha de forma colaborativa com os produtores de conteúdo no processo de detecção e mitigação de IFA.

mensagens de alerta aos produtores quando o número de pedidos dos consumidores ultrapassa um determinado limiar (2). Os produtores, que já são responsáveis pelo gerenciamento dos seus conteúdos, enviam aos nós do núcleo uma lista de nomes de dados sob a sua responsabilidade, sempre que uma mensagem de alerta é recebida (3). Ao receber a lista de nomes resolvíveis dos produtores, um nó é capaz de comparar os pedidos da sua PIT e os interesses resolvíveis enviados pelos produtores (4). Em caso de existir inconsistências, o mesmo inicia o processo de mitigação, que consiste em: (i) apagar os interesses falsos de sua PIT; (ii) encaminhar alertas a outros nós envolvidos na comunicação; e (iii) bloquear demais pedidos que estão fora da lista de nomes resolvíveis. Esse mesmo processo de mitigação é propagado para os demais nós da NDN a partir do recebimento da lista de nomes válidos (5). É preciso destacar que a lista de nomes resolvíveis é mantida em memória. Após um determinado período de tempo sem receber interesses falsos ela é removida.

As próximas subseções detalham o papel desses elementos, suas implementações e como as interações ocorrem entre os mesmos, tendo em vista a detecção e mitigação de IFA.

3.1. Estrutura da informação da NDN

A estrutura da informação do modelo proposto se baseia em dois tipos de pacotes: de dados e de interesse. Ambos os tipos tem em sua composição o nome do conteúdo, sendo que o pacote de dados possui também o conteúdo propriamente dito.

Os nomes dos conteúdos estão organizados de forma hierárquica e seguem a seguinte estrutura: prefixo/sufixo. Cada produtor é responsável por um conjunto de dados de um determinado prefixo, cabendo a ele responder aos interesses referentes aos conteúdos armazenados ou que podem ser produzidos sob tal prefixo.

O prefixo identifica o grupo pelo qual o conteúdo pertence. O sufixo destaca unicamente o conteúdo no grupo. Por exemplo, o prefixo "*youtube/*" agrupa todos os vídeos armazenados no produtor que é responsável por ele. O prefixo "youtube/dvdstones" agrupa os conteúdos referentes ao subgrupo "*dvdstones*". A concatenação do prefixo "*youtube/dvdstones*" com o sufixo "parte1" compõe um nome de conteúdo e o identifica

especificamente como membro do subgrupo "*youtube/dvdstones*"

3.2. Produtor de conteúdo

O produtor de conteúdo é o responsável pelo gerenciamento local dos conteúdos disponibilizados na NDN. Seu papel é manter atualizada a lista dos nomes válidos para que os nós da rede possam fazer o processo de mitigação.

Neste trabalho, parte-se da premissa que os produtores participam da NDN conforme um modelo de confiança que garante o envio das listas de nomes resolvíveis sempre que uma mensagem de alerta é recebida. Portanto, assume-se que os produtores não apresentam comportamento malicioso, assim como, não formam algum tipo de conluio com outros produtores no intuito de viabilizar um IFA. Este problema está fora do escopo deste trabalho. Uma discussão mais aprofundada sobre a necessidade de modelos de confiança para prevenir ataques em conluio em cenários de ICN pode ser encontrado em [Salah and Strufe 2016].

3.3. Roteador NDN

Os roteadores desempenham o papel de monitores da rede de forma que o início de um possível IFA possa ser detectado. No modelo proposto, os nós enviam, aos produtores, mensagens de alarme em caso de ocorrência de anomalias no tráfego resultante de um prefixo específico. Além disso, monitoram o comportamento dos produtores. Essa monitoração visa garantir o cumprimento dos protocolos pré-estabelecidos no modelo. Produtores que não seguem o protocolo são descredenciados e todos os prefixos são automaticamente removidos da FIB em questão.

Um roteador NDN possui na sua estrutura os elementos básicos de toda NDN, a saber: PIT, FIB e CS. Complementar a esses elementos, o modelo propõe que cada roteador possua também as seguintes infraestruturas: A tabela de alarmes pendentes (PAT – *Pending Alarm Table*), lista de descartes e o Filtro. Essas estruturas são utilizadas no gerenciamento das mensagens de alarme e na manipulação das listas de nomes válidos enviadas pelos produtores.

A Figura 2 apresenta uma descrição do comportamento das estruturas no roteador NDN. Ao receber um alarme, a PAT o encaminha usando informações da FIB ou descarta caso tenha encaminhado um alarme de mesmo prefixo em um curto intervalo de tempo. Ao receber a resposta ao alarme, é feito o processamento junto com a PIT, que consiste na identificação e descarte dos interesses falsos e no encaminhamento da resposta de alarme para os outros nós da rede que foram percorridos por esses interesses. A CS é utilizada para armazenar conteúdo e resolver pacotes de interesse. Caso o roteador esteja em estado de alerta, o filtro é acionado para identificar se os interesses são resolvíveis, caso não sejam, são descartados.

3.4. Fases do processo de detecção e mitigação

O processo de detecção e mitigação de IFA realizado nos roteadores é composto por três etapas: (i) determinação de limiares, (ii) detecção de anomalias, e (iii) mitigação do IFA.

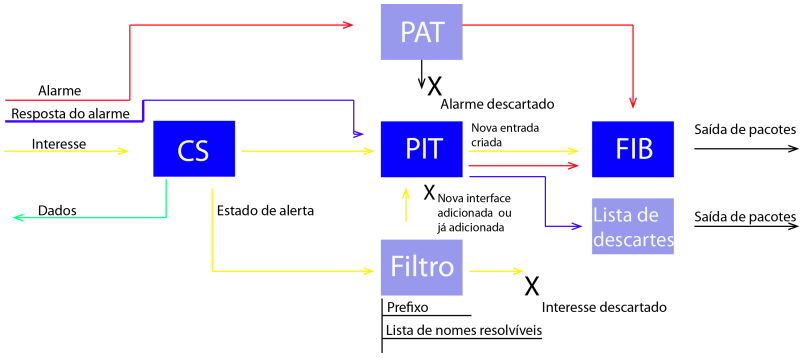

Figura 2. Estrutura de um roteador NDN do modelo proposto.

3.4.1. Determinação de limiares

A determinação de limiares visa estabelecer um limite de entradas para cada prefixo de conteúdos gerenciados pelos produtores. Os roteadores definem os limiares de detecção para cada prefixo armazenado em suas respectivas FIBs. Deste modo, os valores variam para cada roteador e são atualizados dinamicamente, visto que os dispositivos de encaminhamento podem agregar fluxos diferentes e cada prefixo possui um fluxo de tráfego que pode ser diferente dos demais. Seja $P = \{p_1, p_2, \cdots, p_n\}$ a lista de prefixos da NDN, $R = \{r_1, r_2, \cdots, r_m\}$ o conjunto dos roteadores e α_{p_n} a quantidade de pedidos na PIT para o prefixo p_n. l_{p_r} é definido como o limiar l do prefixo p no roteador r. Se, após o envio de um alerta, por conta da ultrapassagem do limiar (ou seja, $\alpha_{p_n} > l_{p_r}$), o IFA for confirmado, o valor de l_{p_r} permanece o mesmo. Caso contrário, trata-se de um falso positivo, então $l_{p_r} \leftarrow \alpha_{p_n}$, estabelecendo assim um novo limiar l_{p_r}. Dado que o padrão dos fluxos da rede pode mudar, cada roteador redefine os limiares de cada prefixo reiniciando a fase de determinação de limiares.

3.4.2. Detecção de anomalias

Após a determinação dos limiares, é realizada a detecção de anomalias, que busca identificar os padrões de requisições que estão fora da normalidade esperada comparando o número de requisições com o limiar estabelecido. Quando o número de requisições excede o limiar, uma mensagem de alerta é enviada ao produtor de conteúdos responsável pelo prefixo.

Após o envio da mensagem de alarme, a PAT é atualizada. A PAT é uma tabela que armazena referências de alarmes recebidos pelo roteador. Cada entrada é composta por prefixo, interface de chegada e o Tempo do Último Encaminhamento (LFT – *Last Forwarding Time*). O roteador que recebe a mensagem de alarme adiciona a interface de chegada do referido prefixo e verifica o LFT. Caso não seja obtida resposta do produtor em um determinado intervalo de tempo, a mensagem de alerta é encaminhada novamente. Esse intervalo entre encaminhamentos é necessário para não inundar a rede. Conforme já mencionado, ao receber uma mensagem de alarme, os produtores enviam uma lista com os nomes de dados que ele é capaz de resolver.

3.4.3. Mitigação

Finalizadas a determinação de limiares e a detecção de anomalias, é feito o processo de mitigação, descrito no Algoritmo 1. A lista enviada pelo produtor é utilizada para identificar a legitimidade dos interesses. O interesse que não constar na lista terá sua interface armazenada em uma lista de descarte e será removido da PIT. As mensagens de resposta percorrem o caminho reverso ao ataque, esse procedimento é essencial para a propagação da mitigação. Após o envio da mensagem de resposta pelo produtor, o roteador entra em estado de alerta, filtrando todos os pacotes que não possam ser resolvidos.

Algorithm 1 Algoritmo de Mitigação

```
1:  procedure MONITORAMENTO
2:  Ao receber um pacote de interesse:
3:      Identifique o prefixo
4:      Atualize a tabela de monitoramento
5:      se Se ocupação estiver acima do limiar então
6:          Mitigação(prefixo)
7:      fim se
8:  procedure MITIGAÇÃO(Prefixo)
9:  Enviar mensagem de alarme para o produtor do prefixo
10: Ao receber uma mensagem de resposta:
11: Para cada entrada na PIT:
12:     se a entrada conter o prefixo então
13:         se a entrada não constar na lista de nomes resolvíveis então
14:             Adicione as interfaces de chegada na lista de descarte
15:             Remova a entrada
16:         fim se
17:     fim se
18: Enviar mensagem de resposta pelas interfaces da lista de descarte
19: Estado de alerta ← true
```

O roteador que receber um interesse não-resolvível durante seu estado de alerta responde com uma mensagem de resposta de alarme pela interface de chegada do pacote. A chegada de um interesse falso em um dispositivo que já ativou a mitigação pode ocorrer quando a resposta a alarmes ainda não alcançou todos os caminhos do ataque. Após enviar mensagens de resposta de alarmes por todas as interfaces maliciosas e estas chegarem aos roteadores de borda, não haverá possibilidade de chegada de interesses falsos, dado que roteadores de borda impedem que os interesses maliciosos adentrem a rede.

Após um tempo determinado sem filtrar pacotes maliciosos, os roteadores saem do estado de alerta. Uma vez que as mensagens resposta de alarme já chegaram a todos os roteadores de borda, que são fontes do ataque, não é mais necessário que as entidades de encaminhamento que estavam no caminho do DoS continuem a filtrar interesses, permitindo, assim, uma redução do uso de recursos computacionais.

Em contrapartida, caso seja constatado que a lista de descarte está vazia, entende-se que todos os pacotes com o prefixo alarmado são resolvíveis. Nesse caso, o incidente é tratado como um falso positivo e, consequentemente, o processo de mitigação não é

disparado. É razoável tal interpretação posto que, se há um ataque em progresso, o dispositivo mais próximo do produtor armazenará e identificará pelo menos um interesse falso, iniciando o processo de mitigação.

É importante salientar que o processo de mitigação ocorre também nos roteadores que não detectaram o ataque ou que estejam em caminhos diferentes do trilhado por uma mensagem de alarme. Isso ocorre pois a mensagens de resposta percorrem caminhos reversos aos fluxos de ataque. Ao receber uma mensagem de resposta, o roteador verifica se contém pacotes maliciosos, podendo assim, disparar a mitigação independente de ter detectado o ataque. Isso propicia um abreviamento dos efeitos da negação de serviço na rede por facilitar a propagação da mitigação.

4. Simulação

Esta seção descreve os cenários, parâmetros, fatores e métricas utilizados no simulador OMNeT++ para avaliação do modelo proposto neste artigo.

4.1. Definição do sistema

O sistema é caracterizado por uma rede NDN formada pelo conjunto C = [0,1,...,n] de consumidores, A = [0,1,...,m] de usuários maliciosos, P = [0,1,...,n] de produtores e R = [0,1,...,j] de roteadores, sendo $r_{borda} \subset$ R e e $r_{bb} \subset$ R, os conjuntos de roteadores de borda e do backbone, respectivamente. Cada roteador possui uma CS e uma PIT. O tamanho da CS e da PIT dos roteadores do *backbone* e de borda são definidos por CS_{bb} e PIT_{bb} e CS_{borda} e PIT_{borda}. Seja D = [0,1,...,n] o conjunto de dados do sistema, cada produtor está associado a um conjunto $D_p \subset$ D, que agrupa dados com um mesmo prefixo. Os consumidores fazem requisições de conteúdos que pertencem a esse conjunto, enquanto os adversários fazem requisições que representam interesses falsos compostos por um prefixo verdadeiro e um sufixo falso, de modo que o interesse chegue a um produtor, porém não possa ser resolvido.

A Figura 3 apresenta a topologia da rede Internet2 utilizada nos experimentos. Foram simulados 13 roteadores no *backbone* (vértices em vermelho), 26 roteadores de borda (vértices em azul) e 8 produtores de conteúdo. Os enlaces de conexão são de 100Gbps entre roteadores e 100 Mbps entre roteador e usuário.

4.2. Cenários, fatores, parâmetros e métricas

O fator avaliado foi a mitigação numa rede que sofre ataques de negação de serviço por inundação de pacotes de interesse. Desse modo, dois cenários associados a esse fator foram analisados: cenário com mitigação e sem mitigação. A avaliação foi realizada de acordo com as seguintes métricas:

- Taxa de ocupação da PIT: avalia o impacto do fluxo malicioso no consumo de memória da PIT. É calculada de acordo com a Equação 1, onde PIT_{req} representa as requisições que estão armazenadas na PIT em um dado instante de tempo t e PIT_{cap} a capacidade da PIT. Essa métrica pode ser medida como uma média geral da ocupação da PIT por cada roteador ou em função do tempo, para verificar o comportamento da taxa de ocupação antes, durante e após o ataque.

$$OcPIT = 100 \times \frac{PIT_{req}}{PIT_{cap}} \quad (1)$$

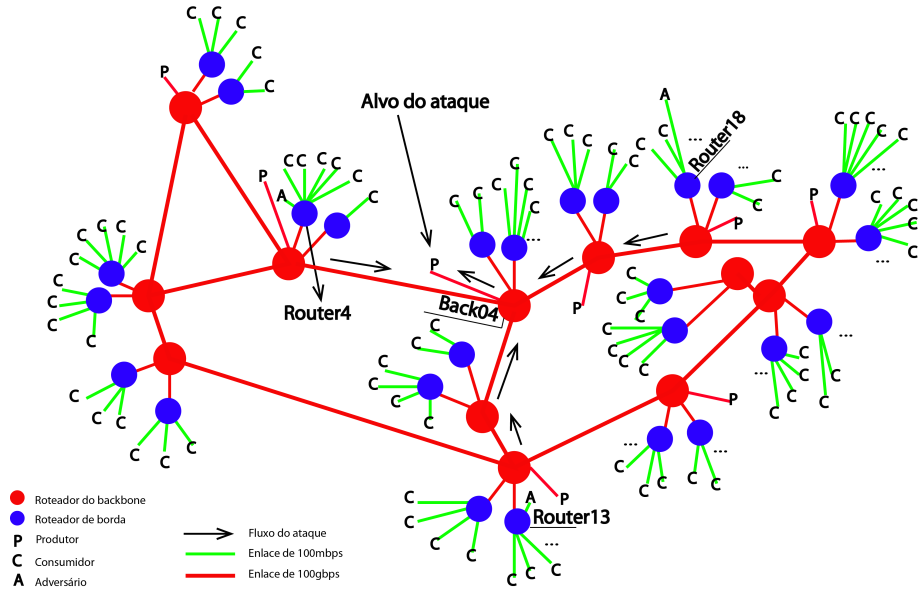

Figura 3. Topologia adaptada do backbone da rede IP da Internet2.

- Taxa de descarte de interesses: essa métrica visa medir o desempenho da rede quanto a satisfação de interesses e pode ser observada na Equação 2, onde I_{desc} refere-se a quantidade de interesses descartados pelo roteador e I_{rec} à quantidade de interesses recebidos. Quanto maior a taxa de descarte, menor é a quantidade de interesses que são resolvidos, indicando portanto, queda no desempenho da rede.

$$DescRot = 100 \times \frac{I_{desc}}{I_{rec}} \tag{2}$$

Os parâmetros utilizados na simulação são definidos na Tabela 1. A rede é composta por 180 nós, sendo 8 produtores, 130 consumidores, 3 adversários, 26 roteadores de borda e 13 do *backbone*. Os 40.000 conteúdos disponíveis foram distribuídos uniformemente entre os produtores e são requisitados a uma taxa de 0-40 pacotes por segundo (pps). Durante o ataque, os adversários solicitam conteúdos falsos a uma taxa de 300-700 pps.

A estimativa do tamanho da PIT foi feita considerando as seguintes premissas: (i) cada consumidor envia rajadas de interesses em intervalos de 0.5s; (ii) - o tempo de resolução de interesses varia de 0.1s a 0.3s e (iii) - A taxa de envio varia de 0 a 20 pacotes por intervalo. Sendo assim, estimou-se o número de entradas suportadas pela PIT em um intervalo de 0.5s, de acordo com a Equação 3. Na qual Router_{maxCap} é a quantidade máxima de nós conectados em um roteador e Taxa_{max} é a taxa máxima de interesses enviados em um intervalo de 0.5s por um consumidor. O resultado desse cálculo é 300. Sendo esta, portanto, a capacidade de armazenamento de entradas da PIT em um roteador de borda. Neste cenário, cada roteador de núcleo agrega dois roteadores de borda, o que acarreta em uma estimativa de 600 entradas. No entanto, foi constatado que 600 entradas era mais do que o suficiente e a fim de economizar memória, a capacidade foi reduzida para 500 entradas neste experimento.

$$PIT_{size} = Router_{maxCap} \times Taxa_{max} \tag{3}$$

Para modelar a taxa de envio de pacotes falsos, foi considerada a capacidade dos roteadores de borda com 300 entradas e o tempo de expiração de 1s. Sendo assim, a taxa mínima do ataque foi de 300 interesses falsos por segundo. Já para garantir a substituição dos interesses existentes por novos interesses falsos, variou-se de 300 a 700 interesses. Com tais valores foi possível assegurar o estouro da PIT e o seu repreenchimento com interesses falsos. Nos experimentos, foram enviados no máximo, 520 mil interesses legítimos (Taxa máxima * Intervalos * nº de consumidores).

Tabela 1. Parâmetros da Simulação

Parâmetro	**Valor**
Quantidade de consumidores	130
Quantidade de adversários	3
Quantidade de roteadores	26 (borda), 13 (*backbone*)
Quantidade de conteúdos disponíveis	40000
Política de descarte de cache	LFU
CSr_{bb}, CSr_{borda}	100
$PITr_{bb}$	500
$PITr_{borda}$	300
Taxa de envio de interesses por consumidores	0 - 40 pps
Taxa de envio de interesses falsos por adversários	300 a 700 pps
Duração da simulação	100s.
Intervalo do ataque	41s - 71s

5. Avaliação dos resultados

Esta seção apresenta a avaliação dos resultados obtidos referente à taxa de ocupação da PIT dos roteadores de borda e de núcleo, assim como o percentual de descarte dos pacotes de interesses.

5.1. Avaliação das taxas de ocupação da PIT

A Figura 4 apresenta a evolução da taxa média de ocupação da PIT dos roteadores de borda "Router4", "Router13" e "Router18". As médias foram calculadas em intervalos de tempo com duração de 1s. Por exemplo, o instante $t = 1$, corresponde à média de valores registrados na PIT no intervalo de 0 a $1s$.

Os roteadores possuem fluxos de tráfego diferentes. Na esquerda estão os resultados obtidos sem o processo de mitigação e na direita com a mitigação. Para fins de comparação, os testes foram executados com os mesmos parâmetros. Como é possível observar, nos testes sem o processo de mitigação, durante o IFA, o percentual de ocupação sobe rapidamente a partir do segundo 41 da simulação, ocupando aproximadamente 90% da memória em todos os roteadores. Já nos resultados apresentados com o processo de mitigação, o mesmo ataque foi reproduzido e, no entanto, a taxa de ocupação não foi afetada, demonstrando a efetividade do processo de mitigação do modelo proposto.

É preciso destacar que os roteadores de borda estão conectados diretamente aos usuários maliciosos. Portanto, agregam um menor fluxo quando comparado com roteadores de núcleo e, assim, são mais sensíveis às variações de tráfego. Deste modo, a anomalia no padrão de consumo da PIT por conta da IFA fica mais evidente.

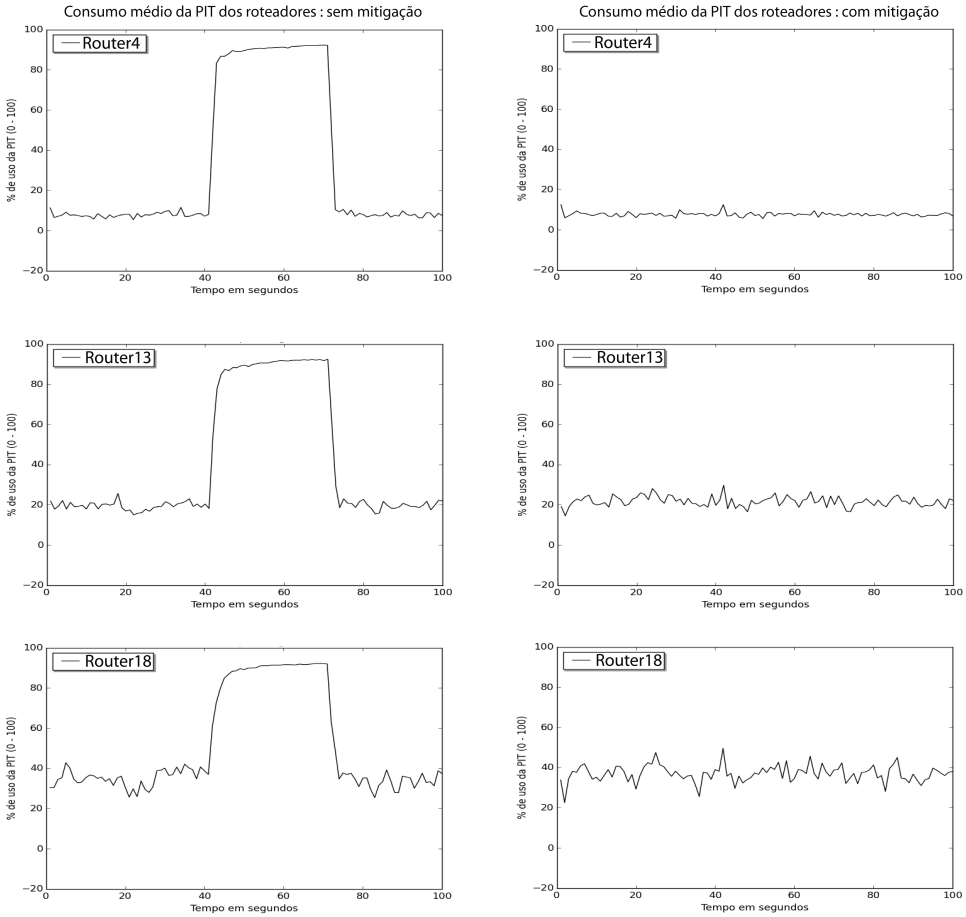

Figura 4. Evolução da taxa de ocupação da PIT dos roteadores de borda com e sem o processo de mitigação.

A Figura 5 apresenta os resultados obtidos na avaliação do roteador de núcleo "Back04" com (a) e sem (b) mitigação. Diferentemente dos de borda, esse roteador está conectado diretamente com o produtor, alvo do IFA. No instante $t = 40$, o processo de determinação de limiares é finalizado e cada roteador fixa os picos como limiares de detecção por prefixo. No instante $t = 41s$, o IFA é iniciado. É possível observar um processo semelhante aos roteadores de borda, exceto que a PIT tem um consumo maior por se tratar de um roteador que agrega tráfego de outros pontos da rede.

Algumas observações precisam ser feitas relacionadas ao experimento. Durante o intervalo do ataque, que é de $t = 41s$ à $t = 71s$, ocorre a saturação da PIT nos roteadores afetados pelo IFA, provocando o descarte de interesses. Entretanto, os valores médios dos intervalos não atingem 100%. Isso é devido ao tempo de expiração dos interesses, que é de $1s$, o que traduz expiração de pacotes em todos os intervalos, exceto pelo intervalo de $t = 0s$ à $t = 1s$. Os valores assumidos em um intervalo de ataque, por exemplo, podem ser 100%, 90%,100% e 88%, resultando em uma média de 94.5%. Ao fim do ataque, os pacotes falsos são expirados e a taxa de ocupação da PIT vai sendo reduzida, dando espaço para a entrada de interesses legítimos. Posteriormente o fluxo volta a sua regularidade.

Diferentemente dos consumidores e usuários maliciosos, os roteadores não enca-

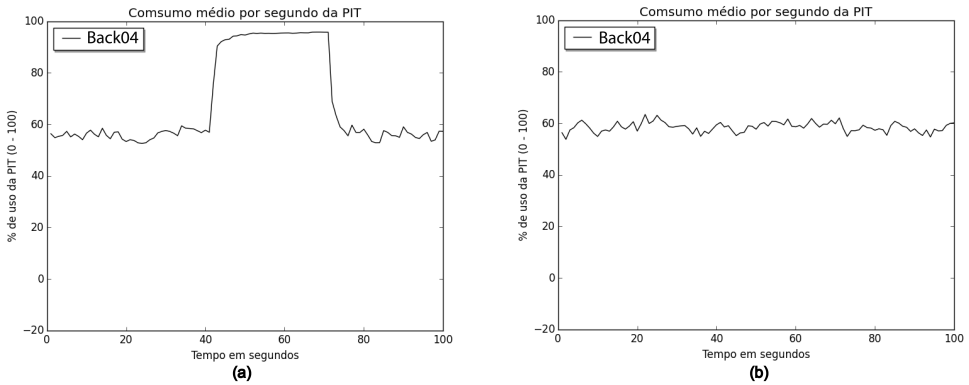

Figura 5. Taxa de ocupação média do roteador de núcleo "Back04". Em (a), sem mitigação. Em (b), com mitigação.

minham as mensagens em rajadas. Assim que a mensagem é processada, ela é encaminhada ou descartada. Nesse contexto, assim que o interesse é adicionado na PIT e constatado a transposição do limiar do seu prefixo, o alarme é enviado em direção ao produtor. A conexão entre roteadores e de roteador com produtor é de 100gbps, enquanto a conexão de roteadores com usuários legítimos/maliciosos é de 100mbps. Essa configuração torna a resposta ao IFA, neste cenário, rápida o bastante para impedir o crescimento da taxa de ocupação média da PIT, como os resultados demonstraram. Após mitigado o ataque, os roteadores de borda filtram os pacotes de interesse, impedindo que os não-resolvíveis adentrem a rede, fazendo com que o tráfego se mantenha regular.

5.2. Avaliação das taxas de descartes

A Figura 6 (a) apresenta a taxa média total de ocupação da PIT dos roteadores de borda e núcleo, com e sem o processo de mitigação do modelo proposto. A Figura 6 (b) apresenta as respectivas taxas de descartes de pacotes de interesses. O percentual com mitigação do "Router4" dos gráficos da Figura 6 (a) é inferior ao percentual sem mitigação. Isso ocorre porque o percentual com mitigação representa o fluxo legítimo recebido por aquele roteador, já que a mitigação descarta a entrada de interesses maliciosos. No entanto, o mesmo não ocorre quando o mecanismo de mitigação é desativado, permitindo a entrada do tráfego malicioso e, consequentemente, aumentando a média total do roteador.

A taxa média total nos roteadores tende a ser maior sem a mitigação devido ao aumento do fluxo provocado pelo ataque. Quanto maior for o fluxo agregado pelo roteador, maior será sua taxa média referente a mitigação. Por exemplo, "Back04" é um roteador de núcleo que agrega regularmente um alto tráfego de pacotes e, por essa razão, recebe o fluxo de ataque oriundo de outros roteadores, aumentando sua taxa média referente a mitigação, e assim reduzindo a variação percentual entre os cenários com e sem mitigação.

Na Figura 6 (b) o percentual de descartes de interesses nos roteadores é calculado através da Equação 2. O percentual com mitigação implica no descarte de pacotes ilegítimos, majoritariamente. Enquanto no cenário sem mitigação, representa o descarte causado pela saturação da PIT. Já a variação do fluxo tem uma importante relevância na taxa de descartes com e sem mitigação. Quando o fluxo malicioso é muito maior do que o legítimo, o roteador tende a descartar mais pacotes pelo processo de mitigação do que

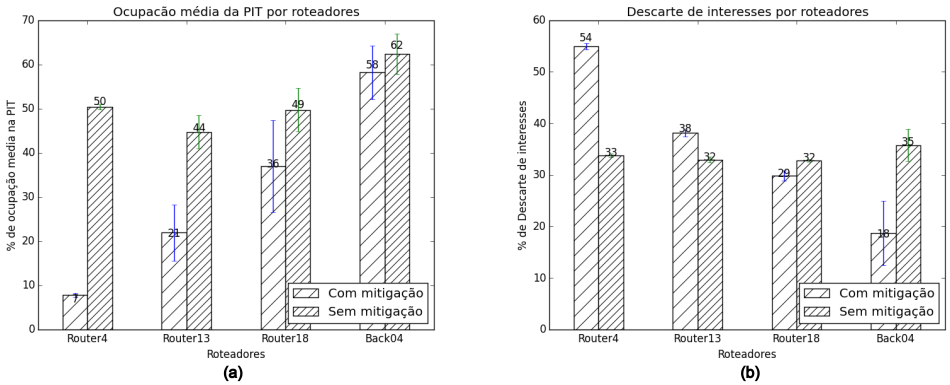

Figura 6. a) Média geral dos valores percentuais assumidos pela PIT dos roteadores. b) Taxa percentual de descartes de interesses por roteadores

por saturação da PIT. Quando o tráfego legítimo é equiparável ao ilegítimo, haverá mais pacotes a serem processados pelo roteador e , por conta disso, terá um aumento na taxa de descarte causado pela insuficiência de memória da PIT do roteador.

Os resultados apresentados para "Router4" e "Router13" demonstram que a taxa com mitigação é maior que a taxa sem mitigação. Nesses roteadores, o fluxo ilegítimo foi maior do que o legítimo. Portanto, o descarte pela mitigação é maior do que por saturação. Já os roteadores "Router18" e "Back04", que agregam um maior fluxo na rede, tendem a descartar mais pacotes por saturação do que por mitigação. Por essa razão, as taxas sem mitigação são maiores.

Na Figura 6 (b), o percentual com mitigação no roteador "Back04" é menor em comparação aos outros roteadores. Isso ocorre devido a PIT dos roteadores de núcleo serem maiores do que a PIT dos roteadores de borda. Sendo assim, apresenta percentuais relativamente menores. Uma outra implicação dessa característica é que os roteadores de borda atuam como gargalos do ataque, descartando uma grande quantidade do tráfego malicioso que recebe, reduzindo assim os efeitos do IFA nos roteadores de núcleo.

6. Conclusão e Trabalhos Futuros

De acordo com os resultados apresentados na Seção 5, o modelo proposto se mostra eficaz na mitigação de ataques de IFA por interesses falsos. Isso acontece devido a sua capacidade de mitigar o ataque sem descartar interesses legítimos preservando o desempenho da rede, a propagação da mitigação pelos roteadores e o descarte de novos interesses maliciosos. Para trabalhos futuros, será realizada a simulação em redes com maior número de nós, sobretudo roteadores, para prover a validação da escalabilidade do modelo. Além disso, o modelo deverá comportar uma proposta de modelo de confiança de produtores para que a rede possa mitigar o ataque, mesmo com a inclusão de produtores em conluio com atacantes.

7. Agradecimentos

Os autores agradecem o apoio da FAPESB e CAPES.

Referências

AbdAllah, E. G., Hassanein, H. S., and Zulkernine, M. (2015). A survey of security attacks in information-centric networking. *IEEE Communications Surveys Tutorials*, 17(3):1441–1454.

Carofiglio, G., Gallo, M., Muscariello, L., and Perino, D. (2015). Pending interest table sizing in named data networking. In *Proceedings of the 2Nd ACM Conference on Information-Centric Networking*, ACM-ICN '15, pages 49–58, New York, NY, USA. ACM.

Compagno, A., Conti, M., Gasti, P., and Tsudik, G. (2013). Poseidon: Mitigating interest flooding ddos attacks in named data networking. In *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*, pages 630–638. IEEE.

Gasti, P., Tsudik, G., Uzun, E., and Zhang, L. (2013). Dos and ddos in named data networking. In *Computer Communications and Networks (ICCCN), 2013 22nd International Conference on*, pages 1–7. IEEE.

Ioannou, A. and Weber, S. (2016). A survey of caching policies and forwarding mechanisms in information-centric networking. *IEEE Communications Surveys Tutorials*, PP(99):1–1.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM.

Mai, H. L., Nguyen, N. T., Doyen, G., Ploix, A., and Cogranne, R. (2016). *On the Readiness of NDN for a Secure Deployment: The Case of Pending Interest Table*, pages 98–110. Springer International Publishing, Cham.

Nguyen, T., Cogranne, R., and Doyen, G. (2015). An optimal statistical test for robust detection against interest flooding attacks in ccn. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 252–260.

Salah, H. and Strufe, T. (2016). Evaluating and mitigating a collusive version of the interest flooding attack in ndn. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 938–945.

Wang, K. and Hengkui, W. (2015). Tcam-pc: Space-efficient tcam-based packet classification with packet-forwarding-rate constraints. In *2015 12th IEEE International Conference on Electronic Measurement Instruments (ICEMI)*, volume 01, pages 260–264.

Wang, K., Zhou, H., Qin, Y., Chen, J., and Zhang, H. (2013). Decoupling malicious interests from pending interest table to mitigate interest flooding attacks. In *2013 IEEE Globecom Workshops (GC Wkshps)*, pages 963–968.

Wang, K., Zhou, H., Qin, Y., and Zhang, H. (2014). Cooperative-filter: countering interest flooding attacks in named data networking. *Soft Computing*, 18(9):1803–1813.

Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K. V., and Polyzos, G. C. (2014). A survey of information-centric networking research. *Communications Surveys & Tutorials, IEEE*, 16(2):1024–1049.