Uma Análise do Impacto do Ataque de Poluição de *Cache* em Redes Orientadas a Conteúdo Sem-Fio

Elise G. Cieza[1], **Igor M. Moraes**[1], **Pedro B. Velloso**[2]

[1]Instituto de Computação – Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

[2]POLI/COPPE – Universidade Federal do Rio de Janeiro (UFRJ)
Rio de Janeiro, RJ – Brasil

elisecieza@id.uff.br, igor@ic.uff.br, velloso@poli.ufrj.br

Abstract. *Wireless Information Centric Networks (ICN) based on the Data-Centric Network architecture (NDN) often employ proactive caching. Thus, a node can store a content even if there is no pending interest for it. The objective is to take advantage of the broadcast nature of the wireless medium to increase the content availability. Proactive caching, however, can enhance cache pollution attacks. This paper therefore evaluates the impact of these attacks on NDN wireless networks through simulations. We compare the network performance with and without proactive caching in standard operation and under attack. The performance metrics are: delivery rate, delay, the content retrieval time, malicious occupation of caches, the cache hit rate, and the number of hops traversed by contents. The proactive cache enhances the pollution attack, on the other hand it improved the network efficiency.*

Resumo. *Nas Redes Orientadas a Conteúdo Sem-fio baseadas na arquitetura* Data-Centric Network *(NDN) pode ser empregada uma política de* cache *proativo. Assim, um nó pode armazenar um conteúdo mesmo que não tenha um interesse pendente para esse conteúdo. O objetivo é aproveitar a natureza de difusão do meio sem-fio para aumentar a disponibilidade dos conteúdos. Um problema dessa abordagem, entretanto, é que a política de* cache *proativo pode potencializar ataques de poluição de* cache*. Este trabalho, portanto, avalia o impacto desses ataques em redes NDN sem-fio através de simulações. Compara-se o desempenho da rede considerando o uso da políticas de* cache *proativo e não proativo, com e sem mobilidade, em condições normais de operação e sob ataque. O desempenho é avaliado em relação à taxa de entrega, atraso, à ocupação maliciosa do* cache *dos nós, taxa de* hit *no* cache *e número médio de saltos atravessados pelos conteúdos. O* cache *proativo potencializou o ataque de poluição dos* caches*, em contrapartida melhorou a eficiência da rede.*

1. Introdução

O uso de dispositivos móveis cresce em todo o mundo e é previsto que até 2015 a quantidade de dispositivos móveis irá superar a quantidade de estações fixas [Venkataramani et al. 2012]. Entretanto, a arquitetura TCP/IP não previu suporte nativo à mobilidade. A comunicação é orientada à localização dos nós o que torna desafiador lidar com mudanças geográficas dos nós e mudanças da topologia

da rede. Algumas alternativas foram propostas para lidar com a questão da mobilidade, como, por exemplo, o IP Móvel. Entretanto, estas funcionam como remendos e os resultados não são satisfatórios. Há preocupações com segurança e qualidade de serviço [Wu et al. 2005]. Portanto, neste contexto surge uma oportunidade para projetar e desenvolver uma nova arquitetura voltada para dispositivos móveis, aplicações móveis, dentre outros [Venkataramani et al. 2012].

As redes orientadas a conteúdo (ROCs) móveis representam uma proposta interessante, tendo em vista os desafios de mobilidade, pois a comunicação é orientada a conteúdo. Este novo paradigma de comunicação desagrega a localização do processo de obtenção de conteúdo. Quando um nó se move a requisição não é necessariamente perdida [Tyson et al. 2012]. Basta que o consumidor reenvie o pedido não atendido, sem perder conexão. Foram realizados experimentos em cenários com alta mobilidade nestas redes e os resultados mostraram que foi possível lidar com até 97% das requisições [Wang et al. 2010]. As ROCs são redes de *caches* e qualquer nó pode armazenar conteúdo. Sendo assim, quanto maior a demanda de um conteúdo maior será a disponibilidade do mesmo na rede, visto que será armazenado pelos *caches* da rede. Isto evita que seja necessário ir sempre até a fonte do conteúdo. Este pode ser obtido do *cache* mais próximo, o que pode ser vantajoso para a mobilidade. Além disso, é importante observar que muitas das aplicações atuais da Internet são voltadas para obtenção de conteúdos. Os usuários têm interesse em obter o conteúdo independentemente de ter conhecimento de quem o fornece, fazendo uso de redes de sucesso como BitTorrent [Brito et al. 2012].

Existem diversas propostas de arquiteturas de ROCs, este estudo irá se basear na *Named Data Networking* (NDN) [Jacobson et al. 2012]. Esta arquitetura foi escolhida por ser uma abordagem bastante referenciada na literatura. Nesta arquitetura, a obtenção de conteúdo é realizada por meio do envio de pacotes de interesse na rede que contêm o nome do conteúdo desejado. Em resposta aos pacotes de interesse são enviados pacotes de dados, contendo o conteúdo. Uma política proativa de armazenamento em *cache* foi proposta com objetivo de melhorar o suporte à mobilidade [Rao et al. 2013]. Basicamente, esta política consiste em armazenar em *cache* todo conteúdo recebido, diferente do funcionamento padrão da NDN. A política não proativa apenas armazena conteúdos cujas requisições foram recebidas. Ou seja, enquanto a política de *cache* não proativo trabalha em função das requisições de conteúdo, a política de *cache* proativo trabalha em função dos pacotes de dado que estão trafegando na rede. Portanto, é independente do recebimento direto das requisições, apresentando resultados com menor atraso e maior taxa de entrega.

Contudo, surgem novos desafios para estas redes, como é o caso da segurança [Brito et al. 2013]. O ataque de poluição de *cache* se aproveita do fato de que todos os nós armazenam conteúdo em uma ROC. Este ataque tem como objetivo inserir conteúdos irrelevantes nos *caches*, ocupando espaço que deveria estar disponível para conteúdos legítimos. Poucos são os trabalhos de poluição de *cache* em comparação aos estudos de ataques de negação de serviço. Alguns propõem soluções para mitigar o ataque, como [Gasti et al. 2012], [Ribeiro et al. 2014], [Park et al. 2012]; e poucos realizaram uma análise experimental [Ghali et al. 2014] e [Conti et al. 2013]. Porém, não foram encontrados trabalhos que analisem ataques de poluição em redes sem-fio móveis, como é o caso deste trabalho. Apesar da importância de estudos de segurança em redes

móveis, tendo em vista que a mobilidade é cada vez mais presente a cada dia. Além disso, segurança em redes móveis sempre foi um desafio devido à vulnerabilidade da comunicação em redes sem-fio [Djenouri et al. 2005].

Considerando esse contexto e os desafios mencionados, este trabalho tem como objetivo analisar o ataque de poluição de *cache* em conluio na eficiência da rede NDN sem-fio, em função das políticas de armazenamento em *cache*. Foram realizados experimentos por meio de simulações no ndnSim [Afanasyev et al. 2012]. Tanto para cenários com mobilidade quanto para cenários sem mobilidade, com topologia em grade. Os resultados abrangem os cenários com mobilidade, sem mobilidade, com atacante, sem atacante, com política proativa e com política não proativa. Além disso, mais de uma variação de atacante foi implementada. A primeira variação consiste em aumentar a quantidade de atacantes na rede e manter a mesma taxa de requisição para todos. Já na segunda, a taxa de requisição aumenta enquanto a quantidade de atacantes permanece a mesma. Verificou-se nos cenários com mobilidade que o uso do *cache* proativo aumentou a taxa de entrega de conteúdos legítimos, resultou em menor número de saltos atravessados para obter o conteúdo e menor tempo de recuperação. Mesmo os cenários com atacantes, estes resultados positivos foram observados. Já com relação à ocupação maliciosa e ao *hit rate*, notou-se que o *cache* proativo favoreceu os atacantes.

O trabalho está organizado como descrito a seguir. Na Seção 2 são descritos alguns elementos importantes da arquitetura NDN e o modelo do atacante. Na Seção 3 são abordados alguns trabalhos relacionados. Na Seção 4 será descrita a simulação realizada, os cenários avaliados e os parâmetros utilizados. A Seção 5 apresenta os resultados, considerando as seguintes métricas: taxa de entrega, atraso, ocupação maliciosa, *hit rate* e número médio de saltos. A Seção 6 conclui o artigo e discute trabalhos futuros.

2. Fundamentos Teóricos

2.1. Visão Geral da NDN

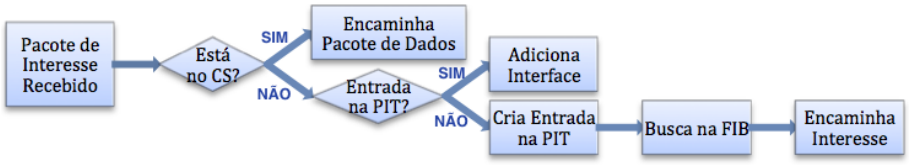
Na NDN existem apenas dois tipos de pacotes, um para a solicitação e outro para recuperação de conteúdos. São estes: pacotes de interesse (*interest packets*) e pacotes de dados (*data packets*). Um conteúdo é encontrado quando o campo *Nome do Conteúdo*, extraído do pacote de interesse, é encontrado por uma busca de maior prefixo no *cache* do nó que recebeu aquele pacote de interesse. Os nomes dos conteúdos adotam o esquema de nomeação hierárquica e possuem semântica [Jacobson et al. 2012].

Um nó NDN possui três componentes principais: (i) FIB (*Forwarding Information Base*), (ii) CS (*Content Store*) e (iii) PIT (*Pending Interest Table*). Estas estruturas de dados são responsáveis pelo recebimento e encaminhamento dos pacotes de dados e interesses.

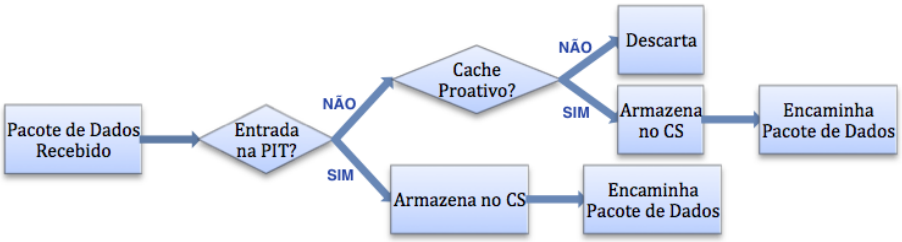
A FIB é a tabela responsável pelo encaminhamento de pacotes e é semelhante à tabela de roteamento de um roteador IP para redes cabeadas. Em redes sem-fio a FIB possui apenas uma entrada, uma vez que os nós comumente possuem apenas uma interface de rede. Assim, todos os pacotes são recebidos e encaminhados pela mesma interface. Essa, inclusive, é uma restrição que tem que ser alterada das regras de encaminhamento da NDN padrão para que essa arquitetura possa ser empregada em redes sem-fio. A PIT é a tabela de interesses pendentes cuja função é guardar os prefixos dos conteúdos requisitados e ainda não atendidos por um nó. Nas redes cabeadas a PIT é utilizada para

retornar o conteúdo pelo caminho das requisições, para isto as interfaces pelas quais os pedidos foram recebidos são registradas nesta tabela. Esta tabela é indexada por nome dos conteúdos, ou seja, pelos prefixos. O CS é o armazenador de conteúdos. Esta estrutura possui uma tabela indexada por nomes de conteúdos que é verificada quando um pacote de interesse é recebido. Define-se ainda que um consumidor é o nó origem de um pacote de interesse e o produtor o nó que primeiramente disponibiliza e mantém de forma persistente um conteúdo em seu *cache*.

Na Figura 1 pode-se observar como são processados os pacotes de dados e de interesse em um nó NDN. Quando um pacotes de dados é recebido é verificado se existe uma entrada na PIT correspondente ao dado recebido. Em caso positivo, o dado é inserido no *cache* e é encaminhado. Em caso negativo irá depender da política de armazenamento. Caso o nó implemente o *cache* proativo então os dados serão inseridos no *cache*, mesmo não possuindo entrada na PIT e serão encaminhados. Caso contrário, o pacote de dados é descartado, o que estabelece a política de *cache* não proativo.



(a) Recepção de Interesse



(b) Recepção de Dado

Figura 1. Processo de envio e recebimento dos pacotes de Interesse e de Dados na NDN.

2.2. Modelo do Atacante

Os ataques de poluição de *cache* têm como objetivo reduzir a taxa de entrega e aumentar o atraso de conteúdos legítimos. Para tanto, nós maliciosos disseminam conteúdos que são apenas do seu interesse na rede. Assim, é consumido espaço em *cache* que poderia ser utilizado para armazenar conteúdos de interesse de nós legítimos.

Assume-se que existe um consumidor malicioso e um produtor malicioso que agem em conluio para poluir os *caches* dos nós [Nassarela e Moraes 2015]. Tanto o produtor malicioso quanto o consumidor malicioso operam como um nó qualquer da rede. Ou seja, encaminham e recebem pacotes da mesma forma que um nó legítimo, ver Figura 1. O conteúdo dos nós maliciosos possui as mesmas propriedades do conteúdo legítimo, exceto pelo fato de que o conteúdo malicioso apenas interessa aos atacantes. Este conteúdo ocupa o mesmo espaço que um conteúdo legítimo em *cache*. Os consumidores atacantes requisitam, no mínimo, duas vezes mais interesses por segundo. Os interesses dos atacantes sempre serão satisfeitos porque existe um produtor atacante que produz o conteúdo

requisitado, sendo portanto, um ataque de poluição em conluio. O conteúdo enviado em resposta ao consumidor atacante será disseminado na rede de acordo com o funcionamento das redes orientadas a conteúdo, disputando *cache* com os conteúdos legítimos.

3. Trabalhos Relacionados

O ataque de poluição é uma preocupação na NDN tendo em vista que todos os nós da rede devem armazenar conteúdos em *cache* [Ribeiro et al. 2012]. Ao contaminar os *caches* a propriedade de disponibilidade de conteúdos é comprometida Na NDN, é possível poluir o *cache* de duas formas [Gasti et al. 2012]. Na primeira, um nó malicioso pode responder um pacote de interesse legítimo com um conteúdo corrompido, diferente do conteúdo original disponibilizado pelo produtor. Na segunda, consumidores e produtores podem agir em conluio para fazer com que um conteúdo que não seja de interesse de nós legítimos seja armazenado em *cache*.

Para verificar se uma assinatura é válida é necessário conhecer a chave pública do assinante e verificar a autenticidade dessa chave. Portanto, existem dois grandes desafios para implementar essa medida padrão: a sobrecarga de verificação de assinatura e o gerenciamento de confiança [Gasti et al. 2012, Ribeiro et al. 2014]. É muito custoso verificar a assinatura do conteúdo a cada salto e por isso, na prática, a assinatura só é verificada no consumidor. Sendo assim, caso o conteúdo esteja poluído ele será encaminhado por toda a rede até o usuário, levando à propagação do mesmo pela rede. Ribeiro *et al.* propõem que a verificação seja realizada por alguns nós do caminho de forma probabilística. Sendo assim, existe a chance de que caso o conteúdo esteja poluído ele seja descartado antes de chegar ao consumidor [Ribeiro et al. 2014]. Park *et al.* propõem um mecanismo de detecção contra ataques de poluição baseado na aleatoridade de requisições de um conteúdo. Cada nó armazena dados estatísticos em uma matriz e caso atinja um limite é indício de que está ocorrendo um ataque na rede [Park et al. 2012]. Ghali *et al.* analisam por meio de simulações uma proposta de mitigar ataques de poluição por meio de ranqueamento de conteúdos, podendo um conteúdo ser classificado como bom ou ruim. Este ranqueamento é realizado de acordo com os dados estatísticos coletados pelos nós da rede [Ghali et al. 2014].

Poucos trabalhos, no entanto, avaliam o ataque de poluição em conluio. Nassarela e Moraes avaliam esse ataque na NDN considerando uma rede cabeada. O ataque implementado consiste em ocupar os *caches* com conteúdos maliciosos o que resultou no aumento do atraso em até 23,5 vezes em redes cabeadas. O ataque em conluio é difícil de ser detectado, pois para a NDN as requisições são legítimas e os conteúdos são válidos. Uma vez que o produtor gera conteúdos com assinaturas válidas nenhuma contramedida de verificação de assinatura evitará que os conteúdos poluídos sejam disseminados pela rede [Nassarela e Moraes 2015]. Este trabalho, por sua vez, avalia o ataque de poluição de *cache* em conluio com objetivo de disseminar conteúdos inválidos pela rede sem-fio com e sem mobilidade. Não foram encontrados trabalhos que realizem análise em redes sem-fio, apesar do crescimento do uso de dispositivos móveis[1]. Uma nova arquitetura deve considerar este fato. São analisados cenários com e sem uso de *cache* proativo. Ao passo que o *cache* proativo pode aumentar a disponibilidade de conteúdos, aumenta-se também a probabilidade de disseminação de conteúdos inválidos pelos *caches* da rede.

[1]Só em 2014 o tráfego global de dados móveis cresceu 69% (*Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019.*)

4. Simulação

As simulações foram realizadas utilizando o módulo ndnSim versão 0.4.3 do NS-3 [Afanasyev et al. 2012]. Para obter suporte à comunicação em redes sem-fio foram utilizadas: a implementação da camada 2 de transmissão veículo a veículo por uma interface NDN e a implementação da estratégia de encaminhamento NDN para comunicações veiculares [Wang et al. 2012]. Considera-se o padrão IEEE 802.11a, com taxa de transmissão de 24Mbps e os modelos de propagação: *Constant Speed Propagation Delay Model*, *Three Log Distance Propagation Loss Model* e *Nakagami Propagation Loss Model*.

Foram simulados quatro cenários: (i) Com mobilidade, (ii) Sem mobilidade, (iii) Com mobilidade e poluidores e (iv) Sem mobilidade e poluidores.

Os nós estão dispostos em uma grade 7 x 7 em uma área de 800 m x 600 m. A ideia é reproduzir o cenário de um estacionamento de um shopping horizontal. Para os cenários sem mobilidade os nós permanecem na mesma posição até o final da simulação. Para os cenários com mobilidade foi utilizado o modelo *Vehicular2dMobilityModel* que permite ao nó sortear uma direção para seguir, contanto que não seja igual a direção atual [Prates e Moraes 2014]. No caso deste trabalho, a cada 100 m o nó sorteia uma nova direção.

As simulações foram realizadas tanto para a política de *cache* proativo quanto para a política de *cache* não proativo, explicadas na Seção 2.1. Os nós implementam a política de substituição de *cache Least Recently Used* (LRU) que tem maior custo benefício em relação a outras políticas, é mais simples de implementar e tem bom desempenho [Brito et al. 2013]. Foram realizadas 20 rodadas para cada experimento. A definição dos nós que serão consumidores e produtores a cada rodada, sejam estes legítimos ou maliciosos, é aleatória. A rede contém o total de 49 nós. Para os cenários sem atacante 10% da rede é composta de consumidores legítimos, enquanto os demais nós são roteadores e existe um produtor do conteúdo requisitado pelos consumidores legítimos. Para os cenários com atacante a mesma porcentagem é mantida para os consumidores legítimos, enquanto os consumidores atacantes representam no mínimo 6% da rede e existe um produtor do conteúdo requisitado pelos atacantes, configurando assim um ataque de poluição de *cache* em conluio. Foram realizadas duas variações de atacantes. Na primeira, a quantidade de atacantes varia de 6% até 26%, para observar o ataque quando há menos atacantes do que nós legítimos e quando há mais atacantes do que legítimos. A taxa de requisição maliciosa é 2 vezes maior do que a taxa de envio dos consumidores legítimos, a qual é fixa. Na segunda, a quantidade de atacantes é fixada para 6% da rede e a taxa varia de 2 vezes até 7 vezes maior do que a taxa dos consumidores legítimos, taxas muito altas são facilmente detectadas como tráfego malicioso.

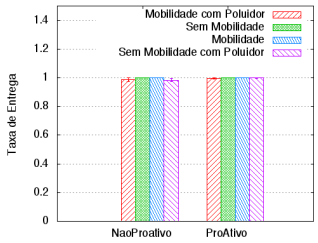
Os consumidores legítimos requisitam o mesmo conteúdo que é composto de *n chunks*, onde *n* é a quantidade máxima de *chunks* que podem ser armazenados em um *cache*. Um *chunk* tem o tamanho de 500 *bytes* e um *cache* tem 2 Mb de capacidade de armazenamento. Quando um consumidor legítimo já requisitou os *n chunks*, antes da simulação terminar, ele volta a pedir novamente a partir do *chunk* 1, tendo portanto melhor proveito do *cache*. Por outro lado, os consumidores maliciosos solicitam *chunks* sequencialmente de um conteúdo de tamanho indeterminado que só existe no produtor malicioso. Nos cenários com *cache* proativo os conteúdos maliciosos serão armazenados por qualquer nó que receba o pacote de dados. Já para o *cache* não proativo os conteúdos

maliciosos serão armazenados apenas pelos nós com entrada na PIT para pedidos maliciosos.

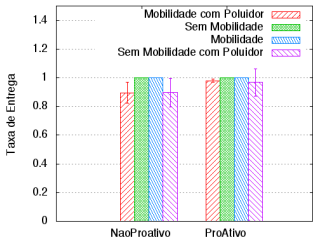
5. Resultados

Para avaliar o efeito do ataque de poluição na rede em relação ao uso ou não do *cache* proativo são avaliadas as seguintes métricas: taxa de entrega, atraso, ocupação maliciosa do *cache*, *hit rate* e *hop count*. Para os pontos dos gráficos obtidos, são calculados intervalos de confiança representados por barras verticais para um nível de confiabilidade de 95%.

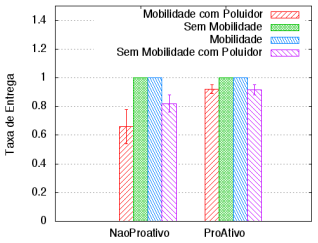
Nos gráficos da Figura 2 são comparados os cenários com 6% de atacantes com taxa 2 vezes maior, 7 vezes maior e 26% de atacantes. Tanto o aumento de atacantes na rede quanto o aumento da taxa dos atacantes causa impacto na taxa de entrega, comparando com o cenário visto na Figura 2(a). Entretanto, para a política de *cache* proativo o impacto é menor. A alta disseminação de conteúdos pelos *caches* permite que os conteúdos sejam recuperados em um tempo menor em comparação ao *cache* não proativo. Fazendo com que a taxa de entrega seja maior para a política proativa.



(a) Taxa de Entrega para 6% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.



(b) Taxa de Entrega para 26% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.



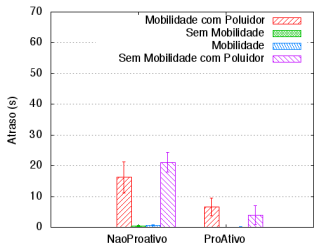
(c) Taxa de Entrega para 6% de atacantes e taxa 7 vezes maior do que taxa do consumidor legítimo.

Figura 2. Comparação da taxa de entrega entre os quatro cenários.

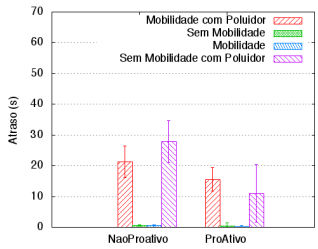
Os gráficos da Figura 3 avaliam o atraso que aumenta ao acrescer o número de atacantes na rede e ao aumentar a taxa dos atacantes. Os cenários sem atacantes têm um atraso quase nulo. Portanto ao comparar estes cenários pode-se afirmar que os atacantes aumentam o atraso, afetando o desempenho da rede.

Na Figura 4 são apresentados os gráficos para o *hit rate*. Na Figura 4(b) observa-se algo diferente do que foi visto nos gráficos anteriores. O *cache* proativo teve desempenho inferior. O fato de haver mais atacantes na rede permite que estes distribuam o conteúdo pelos *caches* da rede. Isto tem como consequência, em comparação com a política não proativa, um *hit rate* menor para o proativo quando há mais atacantes e um *hit rate* maior para o proativo quando a taxa de requisição maliciosa é maior.

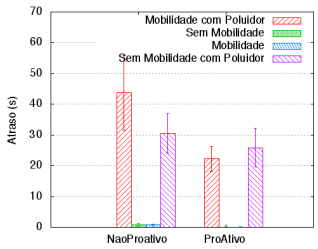
A Figura 5 complementa o resultado observado nas Figuras 3 e 2. Apesar do desempenho ter sido afetado, o consumidor ainda é atendido, porém a um custo maior de saltos. Além disso, o aumento da taxa de requisição do atacante teve um impacto maior no desempenho de forma geral, em comparação com o aumento de aplicações maliciosas na rede. Aumenta-se o atraso, reduz-se o *hit rate* e reduz-se a taxa de entrega. Porém o



(a) Atraso para 6% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.

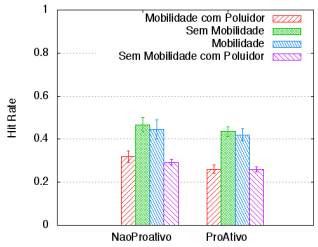


(b) Atraso para 26% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.

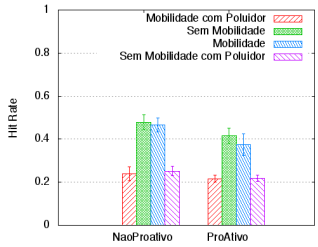


(c) Atraso para 6% de atacantes e taxa 7 vezes maior do que taxa do consumidor legítimo.

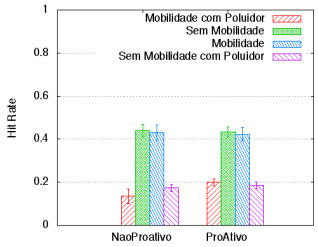
Figura 3. Comparação do atraso entre os quatro cenários.



(a) *Hit Rate* para 6% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.



(b) *Hit Rate* para 26% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.



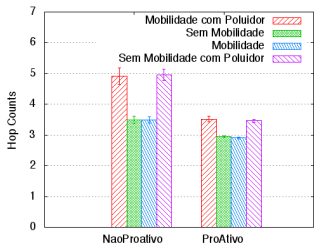
(c) *Hit Rate* para 6% de atacantes e taxa 7 vezes maior do que taxa do consumidor legítimo.

Figura 4. Comparação do *hit rate* entre os quatro cenários.

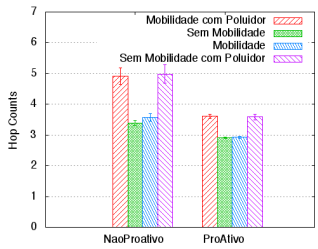
hop count é maior na Figura 4(b), sugerindo que a distribuição dos conteúdos maliciosos na rede foi bem sucedida ao ter mais atacantes na rede. Nos cenários sem atacante o posicionamento aleatório dos nós na grade pode ter impacto significativo nos resultados, como ocorre nas Figuras 4 e 5.

A partir deste ponto serão apresentados os resultados para as variações de atacantes. Primeiro serão analisados os gráficos para a variação da quantidade de atacantes. Depois para a variação com aumento da taxa de interesses maliciosos.

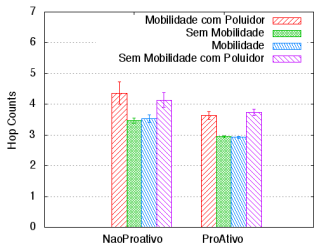
Na Figura 6, os dois gráficos apresentam taxa de entrega próxima ou superior a 90%, o que é um resultado favorável para a NDN. Apesar da taxa de entrega ser inferior no cenário com mobilidade esta ainda é superior a 90%. Comparando as curvas de mobilidade para os gráficos das Figuras 6(a) e 6(b), pode-se ver que para a política proativa a taxa de entrega foi superior à taxa observada para a política não proativa. Isto corrobora a ideia de que a distribuição de conteúdos por meio do *cache* proativo melhora o serviço da rede. Na Figura 6(a) a curva do cenário sem mobilidade fica acima da curva do cenário com mobilidade. Isto pode ser explicado pela natureza da política não proativa, uma vez que o armazenamento do conteúdo em *cache* depende da existência de uma entrada na PIT. Portanto, tendo em vista que nos cenários com mobilidade a probabilidade de reenviar os interesses e perder alguns pacotes de dados é maior, é compreensível que a curva do cenário sem mobilidade esteja a cima da curva do cenário com mobilidade. Já o *cache* proativo resolve em boa parte este problema, ao aumentar a distribuição de conteúdos por



(a) *Hop count* para 6% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.



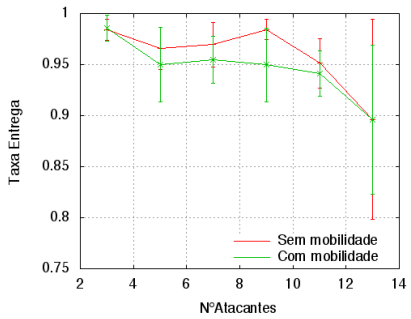
(b) *Hop count* para 26% de atacantes e taxa 2 vezes maior do que taxa do consumidor legítimo.



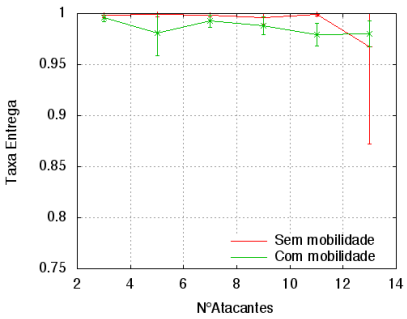
(c) *Hop count* para 6% de atacantes e taxa 7 vezes maior do que taxa do consumidor legítimo.

Figura 5. Comparação do *hop count* entre os quatro cenários.

toda a rede.



(a) Entrega Não Proativo.

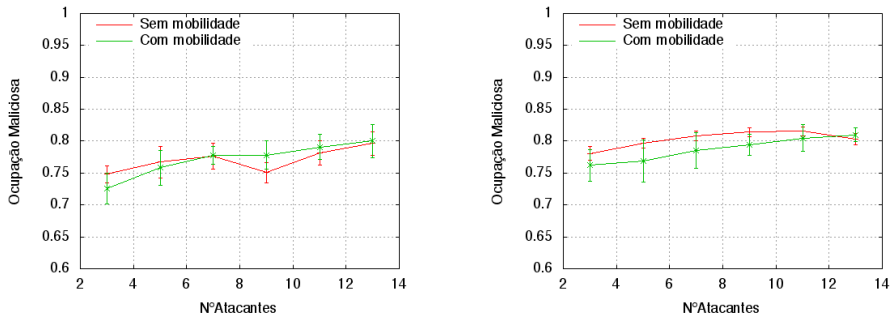


(b) Entrega Proativo.

Figura 6. Taxa de entrega para variação de quantidade de atacantes com taxa de envio 2 vezes maior do que taxa do consumidor legítimo.

Com relação à ocupação maliciosa, na Figura 7 pode-se notar que para ambas políticas de *cache* os resultados foram próximos de 80%. Para a política de *cache* proativo, a ocupação maliciosa é menor quando há mobilidade, mas aumenta com o número de nós maliciosos, pois a disseminação do conteúdo malicioso foi favorecida por esta política. A curva para o cenário sem mobilidade da Figura 7(b) cresce com o aumento de atacantes, com exceção do último ponto que pode ser justificado pela aleatoridade do posicionamento dos nós. Na Figura 7(a) as curvas também crescem à medida que a quantidade de nós maliciosos aumenta na rede, porque aumentam também as requisições e a quantidade de entradas na PIT com pedidos maliciosos. Como o posicionamento dos atacantes na rede é aleatório, há maior espalhamento desses pedidos quando existe mobilidade, o que fica claro no gráfico da Figura 7(a). A curva do cenário com mobilidade fica acima da curva do cenário sem mobilidade quando o número de atacantes na rede é maior do que 7.

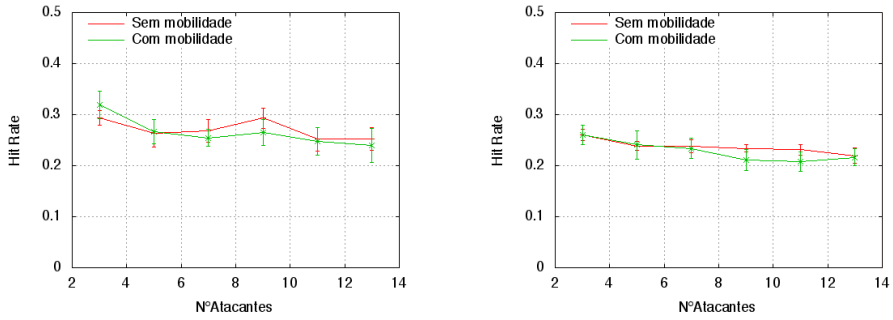
Quanto maior a ocupação maliciosa menor será o *hit rate*, uma vez que será mais difícil encontrar um conteúdo legítimo. O *hit rate* na Figura 8 comprova essa ideia. Na Figura 8(b) o *hit rate* é menor para a política proativa. Assim como visto na Figura 7(b). Portanto, o *cache* proativo prejudica os consumidores legítimos neste sentido, ao melhorar a distribuição dos conteúdos maliciosos aumentando a ocupação e diminuindo o *hit rate*.



(a) Ocupação Maliciosa Não Proativo. (b) Ocupação Maliciosa Proativo.

Figura 7. Ocupação maliciosa para variação de quantidade de atacantes com taxa de envio 2 vezes maior do que taxa do consumidor legítimo.

Entretanto, foi observado que a política proativa sofre menos com relação ao desempenho. Nas Figuras 5 e 3, pode-se ver que a quantidade de saltos atravessados para obter conteúdo é menor e consequentemente o atraso também.



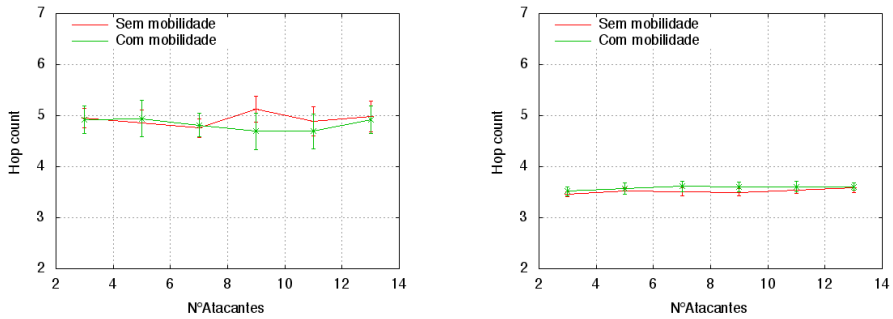
(a) *Hit Rate* Não Proativo. (b) *Hit Rate* Proativo.

Figura 8. *Hit Rate* para variação de quantidade de atacantes com taxa de envio 2 vezes maior do que taxa do consumidor legítimo.

Na Figura 9 é possível observar que em relação ao número de saltos atravessados pelos pacotes de dados a política de *cache* proativo é melhor do que a política de *cache* não proativo. O *hop count* é menor com o *cache* proativo. Apesar da quantidade de atacantes aumentar na rede o *hop count* não sofre alteração significante na Figura 9(b). Este fato corrobora os dados analisados com relação ao atraso, que é maior para a política de *cache* não proativo. É necessário buscar o conteúdo a mais saltos com a política não proativa, enquanto para a política proativa é possível recuperar conteúdo de um vizinho mais próximo. Como visto na Figura 5, o *hop count* é similar apesar das variações de quantidade de atacantes e da taxa de requisição. Entretanto, nos três gráficos observa-se que o *hop count* para o *cache* proativo é sempre menor.

Os próximos resultados detalham o impacto da variação da taxa de requisição maliciosa. Esta feta mais o desempenho da rede do que a variação do número de atacantes. Define-se que 6% da rede é composta por atacantes consumidores e a taxa de envio de interesses maliciosos varia de 2 vezes maior até 7 vezes maior em relação à taxa de requisições legítimas.

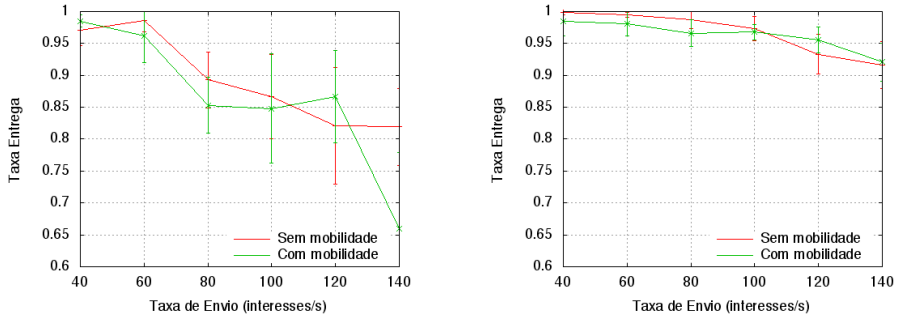
Para esta variação de atacante, pode-se observar na Figura 10 como a variação de



(a) *Hop Count* Não Proativo. (b) *Hop Count* Proativo.

Figura 9. *Hop Count* médio para variação de quantidade de atacantes com taxa de envio 2 vezes maior do que taxa do consumidor legítimo.

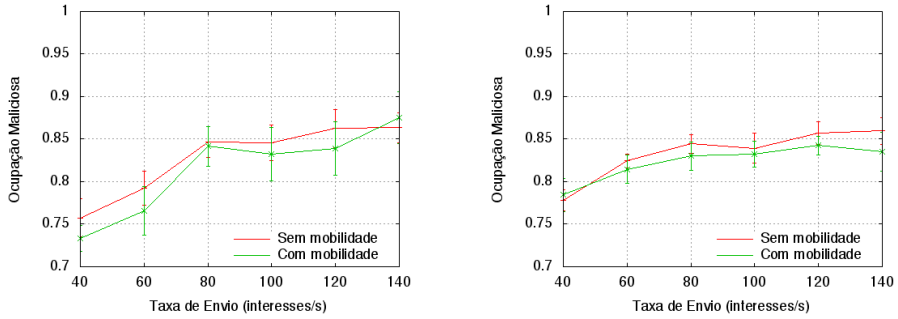
taxa de requisição de conteúdo malicioso impacta na taxa de entrega. Apesar da quantidade de atacantes consumidores ser apenas de 6%. A política de *cache* proativo até certo ponto mantém uma taxa de entrega próxima de 100%, como visto na Figura 10(b). Porém, quando a taxa é 5 vezes maior nota-se que a curva começa a cair. Já para a Figura 10(a), pode-se ver que com a política de *cache* não proativo a taxa de entrega cai rapidamente à medida que a taxa de envio de interesses maliciosos aumenta. Esta chega a quase 60% para o cenário com mobilidade e 80% para o cenário sem mobilidade. Enquanto para o *cache* proativo tanto para o cenário com mobilidade quanto o cenário sem mobilidade a taxa de entrega é de aproximadamente 92%. O *cache* proativo aumenta a disponibilidade de todos conteúdos na rede. Este otimiza o uso do *cache*, visto que num tempo menor é possível ter uma rede operando com o máximo possível de recursos utilizados.



(a) Entrega Não Proativo. (b) Entrega Proativo.

Figura 10. Taxa de entrega para variação da taxa de envio de interesses maliciosos, rede com 6% de atacantes consumidores.

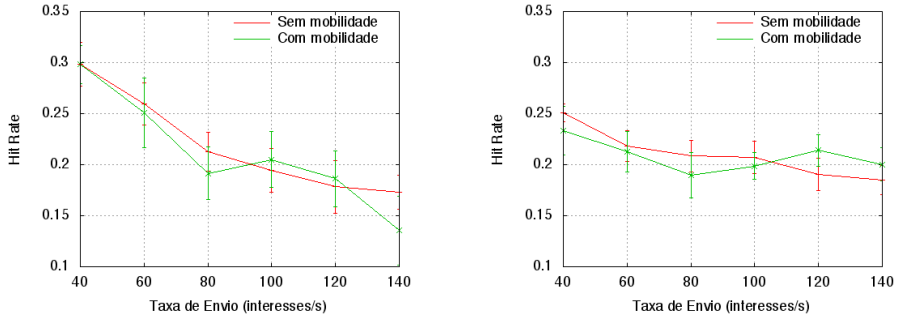
A Figura 11 apresenta um comportamento semelhante ao que foi visto na Figura 7. Na Figura 11(b) é possível observar que a ocupação de *cache* maliciosa cresce junto com a taxa. Além disso, a curva do cenário com mobilidade se mantém abaixo da curva do cenário sem mobilidade. Assim como na Figura 7(b), porém, com uma ocupação média maior. Já na Figura 11(a)à medida que a taxa aumenta os valores de ocupação ao final da curva são superiores ou próximos aos da política proativa. Isto ocorre devido à alta injeção de pacotes de interesses maliciosos. Esta variação de ataque foi mais eficiente do que aumentar a quantidade de atacantes na rede.



(a) Ocupação Maliciosa Não Proativo. (b) Ocupação Maliciosa Proativo.

Figura 11. Ocupação maliciosa para variação da taxa de envio de interesses maliciosos, rede com 6% de atacantes consumidores.

Os gráficos da Figura 12 mostram que o *hit rate* diminui à medida que a taxa de interesses maliciosos aumenta. Relacionando com os gráficos de ocupação maliciosa da Figura 11, pode-se notar um espelhamento do comportamento, como esperado. Uma vez que a ocupação maliciosa aumenta torna-se mais difícil encontrar um conteúdo legítimo. Portanto, há mais *cache miss*, diminuindo assim o *hit rate*.



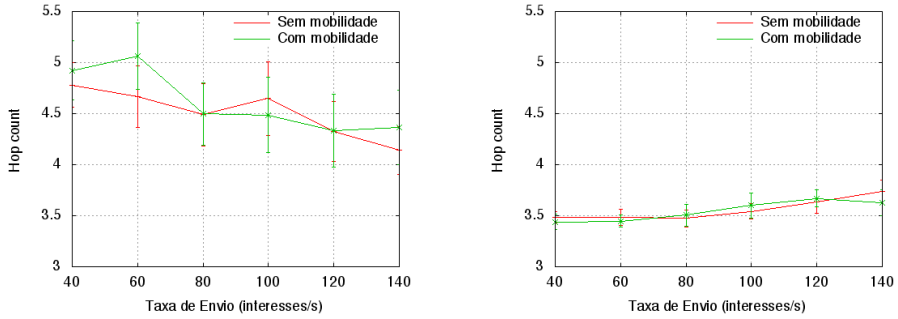
(a) *Hit Rate* Não Proativo. (b) *Hit Rate* Proativo.

Figura 12. *Hit Rate* para variação da taxa de envio de interesses maliciosos, rede com 6% de atacantes consumidores.

Na Figura 13 o *hop count* para a política de *cache* não proativo é superior ao *hop count* no *cache* proativo. Isto coincide com o atraso observado no gráfico da Figura 3(c). Para a política de *cache* proativo o *hop count* mostra que a recuperação de conteúdo está sendo realizada de vizinhos próximos. Isso porque o *cache* proativo aumenta a disponibilidade do conteúdo, ainda que a rede esteja sob condições anormais. Portanto, com relação à eficiência da rede pode-se dizer que a política proativa tem um resultado favorável para os nós legítimos. Estes continuam obtendo o conteúdo com um atraso maior do que num cenário sem ataque, mas bem menor do que em um cenário com ataque e *cache* não proativo.

6. Conclusão

Este trabalho tem como objetivo analisar o impacto do ataque de poluição de *cache* na eficiência de uma rede NDN sem-fio e sobre a política de *cache* proativo que consiste em armazenar o conteúdo ainda que ele não tenha sido requisitado por um nó. Este



(a) *Hop Count* Não Proativo. (b) *Hop Count* Proativo.

Figura 13. *Hop Count* médio para variação da taxa de envio de interesses maliciosos, rede com 6% de atacantes consumidores.

comportamento proativo portanto potencializa o ataque de poluição de *cache*, uma vez que todo conteúdo malicioso recebido será armazenado, independentemente de estar na PIT.

Por meio dos experimentos foi verificado que o *cache* proativo aumentou a ocupação maliciosa e, com isso, reduziu o *hit rate*. Por outro lado, os benefícios da adoção do *cache* proativo se mostraram superiores do que as desvantagens, ainda que esta rede esteja sob ataque. Com o aumento da disponibilidade de conteúdos, o número de saltos atravessados pelos conteúdos recuperados e, consequentemente, o tempo de recuperação são menores com *cache* proativo. Em cenários com atacantes, observa-se que o atraso aumentou. Porém, esse aumento foi menor na política de *cache* proativo. Mesmo com *caches* da rede próximos de 85% de ocupação maliciosa pode-se observar que a taxa de entrega permaneceu acima de 90% para *cache* proativo e acima de 65% para *cache* não proativo. Como trabalhos futuros pretende-se investigar outros cenários, explorar outros parâmetros de simulação. Como por exemplo: variar o tamanho do *cache*, implementar o consumidor *Zipf–Mandelbrot* e utilizar um modelo de mobilidade de registros reais.

Referências

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

Brito, G. M., Velloso, P. B. e Moraes, I. M. (2012). Redes orientadas a conteúdo: Um novo paradigma para a Internet. Em *Minicurso do Simpósio Brasileiro de Redes de Computadores (SBRC)*, páginas 211–264.

Brito, G. M., Velloso, P. B. e Moraes, I. M. (2013). *Information Centric Networks: A New Paradigm for the Internet*. Wiley-ISTE, 1a. edição.

Conti, M., Gasti, P. e Teoli, M. (2013). A lightweight mechanism for detection of cache pollution attacks in Named Data Networking. Em *Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 57 Issue 16*, páginas 3178–3191.

Djenouri, D., Khelladi, L. e Badache, N. (2005). A Survey of Security Issues in Mobile Ad Hoc Networks. *IEEE communications Surveys and Tutorials*, páginas 2–28.

Gasti, P., Tsudik, G., Uzun, E. e Zhang, L. (2012). DoS & DDoS in named-data networking.

Ghali, C., Tsudik, G. e Uzun, E. (2014). Needle in a Haystack: Mitigating Content Poisoning in Named-Data Networking. Em *NDSS Workshop on Security of Emerging Networking Technologies (SENT)*.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M., Briggs, N. e Braynard, R. (2012). Networking named content. *Communications of the ACM*, 55(1):117–124.

Nassarela, A. L. e Moraes, I. M. (2015). Uma Avaliação do Ataque de Negação de Serviço em Conluio Consumidor-Produtor em Redes Orientadas a Conteúdo. Em *Anais do 33o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – SBRC*.

Park, H., Widjaja, I. e Lee, H. (2012). Detection of cache pollution attacks using randomness checks. Em *Communications (ICC), IEEE International Conference*, páginas 1096–1100.

Prates, A. A. e Moraes, I. M. (2014). GeoZone: Um Framework Eficiente de Difusão de Interesses em Redes Veiculares Orientadas a Conteúdo. Em *Anais do 32o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – SBRC*.

Rao, Y., Zhou, H., Gao, D., Luo, H. e Liu, Y. (2013). Proactive Caching for Enhancing User-Side Mobility Support in Named Data Networking. *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, páginas 37–42.

Ribeiro, I. C. G., Alburquerque, C. V. N., Rocha, A. A. e Queiroz, F. (2014). On the Possibility of Mitigating Content Pollution in Content-Centric Networking. Em *IEEE LCN*.

Ribeiro, I. C. G., Guimarães, F. Q., Kazienko, J. F., de A. Rocha, A. A., Velloso, P. B., Moraes, I. M. e Albuquerque, C. V. N. (2012). Segurança em redes centradas em conteúdo: Vulnerabilidades, ataques e contramedidas. Em *Minicurso do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, páginas 101–150.

Tyson, G., Cuevas, R., Mauthe, A., Sastry, N. e Rimac, I. (2012). A Survey of Mobility in Information-Centric Networks : Challenges and Research Directions. *Proceedings of the 1st ACM workshop on Emerging Name-Oriented Mobile Networking Design - Architecture, Algorithms, and Applications*, páginas 1–6.

Venkataramani, A., Raychaudhuri, D. e Nagaraja, K. (2012). MobilityFirst: A Robust and Trustworthy Mobility- Centric Architecture for the Future Internet. *ACM SIGMOBILE Mobile Computing and Communications Review*, páginas 2–13.

Wang, J., Wakikawa, R. e Zhang, L. (2010). Dmnd: Collecting data from mobiles using named data. Em *IEEE Vehicular Networking Conference (VNC)*, páginas 49–56.

Wang, L., Afanasyev, A., Kuntz, R., Vuyyuru, R., Wakikawa, R. e Zhang, L. (2012). Rapid Traffic Information Dissemination Using Named Data. *ACM NoM Wkshp.*, páginas 7–12.

Wu, T., Huang, C. e Chao, H. (2005). A survey of Mobile IP in cellular and Mobile Ad-Hoc Network environments. *Ad Hoc Networks, Elsevier, Volume 3, Issue 3*, páginas 351–370.

