Sobre a Influência dos Nós Egoístas no Descarregamento de Tráfego com Redes Oportunistas

Claiton Luiz Soares[1,2], **Igor Monteiro Moraes**[1]

[1]Laboratório MídiaCom, PGC-TCC
Instituto de Computação - Universidade Federal Fluminense
Niterói, Rio de Janeiro, Brasil

[2]Instituto Federal do Triângulo Mineiro -IFTM
Paracatu, Minas Gerais, Brasil

{csoares,igor}@ic.uff.br

Abstract. *The cellular infrastructure is overloaded because of the increasing number of mobile devices and applications. A solution to tackle this problem is to offload the network traffic by using an alternative network as a secondary communication channel. Several studies in the literature propose to employ opportunistic networks as this secondary channel. To be effective, however, opportunistic communication relies that nodes cooperate each other in order to forward messages and to confirm to the infrastructure the successful reception of messages sent by other nodes. In this paper, we evaluate the impact of selfish nodes on the performance of the traffic offloading with opportunistic networks. Selfish are those nodes that do not forward messages to other nodes or do not send acknowledgments to the infrastructure or combine both behaviors. Results show the offloading efficiency decreases from 70% to up to 18% if selfish nodes are in the network.*

Resumo. *A infraestrutura celular está sobrecarregada com o crescente número de dispositivos e aplicações móveis. Uma solução para este problema é descarregar parte do tráfego da rede utilizando outra rede como canal de comunicação secundário. Muitos trabalhos na literatura propõem o uso de redes oportunistas como este canal secundário. Para se ter sucesso na comunicação oportunista, entretanto, os nós precisam cooperar uns com os outros para encaminhar mensagens e confirmar para a infraestrutura o recebimento das mensagens encaminhadas por outros nós. Neste artigo, avalia-se a influência dos nós egoístas no descarregamento de tráfego com redes oportunistas. Nós egoístas são aqueles que não encaminham mensagens para outros nós ou não enviam reconhecimentos positivos para infraestrutura ou que combinam ambos os comportamentos. Resultados mostram que a eficiência do descarregamento é reduzida de 70% para até 18% com a presença de nós egoístas na rede.*

1. Introdução

A crescente proliferação de dispositivos móveis juntamente com o rápido desenvolvimento de tecnologias de comunicação móvel está provocando um aumento nas solicitações de conteúdo da rede celular. Consequentemente, a crescente demanda de tráfego faz com que a infraestrutura de rede celular se aproxime do seu limite. Embora

as novas tecnologias de comunicação ofereçam mais largura de banda para os usuários, prevê-se que até mesmo redes celulares 4G não vão ser capazes de lidar com a enorme demanda de tráfego de dados dos usuários nos próximos anos [Li et al. 2014].

Uma possível solução para este problema é utilizar uma técnica conhecida como descarregamento de tráfego (*traffic offloading*) [Rebecchi et al. 2015, Han et al. 2010]. O objetivo dessa técnica não é substituir a rede móvel de dados, que seria o canal principal de comunicação, mas empregar um canal secundário de comunicação, no caso uma rede oportunista, para reduzir o volume de dados transportado na rede celular. Neste contexto, muitos usuários estão interessados em um mesmo conteúdo, premissa que é válida para muitos conteúdos disponíveis na Internet. Se esses conteúdos são recuperados usando somente o canal primário, várias cópias desse mesmo conteúdo, uma para cada usuário interessado, são encaminhadas pela infraestrutura de rede. Isso gera desperdício de recursos e pode reduzir a qualidade de experiência do usuário. Com as redes oportunistas, os nós não precisam recuperar exclusivamente um conteúdo da sua fonte. Ele pode ser recuperado também de outro nó da rede que anteriormente tenha solicitado esse mesmo conteúdo. A comunicação entre os nós é feita de forma *ad hoc* através de outras interfaces sem-fio cada vez mais comuns nos dispositivos móveis, como Wifi e *Bluetooth*. A ideia é se beneficiar da mobilidade dos nós utilizando uma rede secundária em troca de uma maior tolerância ao atraso que pode ser experimentada pelos usuários. Para incentivar a participação nas redes oportunistas, as operadoras podem oferecer descontos de preços para os assinantes de telefonia móvel em troca dos seus recursos de bateria e armazenamento para descarregar o tráfego [Zhuo et al. 2011].

A ideia das redes oportunistas é permitir que dois nós consigam se comunicar mesmo que nunca exista um caminho fim-a-fim entre eles. Para tanto, essas redes empregam, em geral, a arquitetura DTN (*Delay Tolerant Networking*) [Oliveira et al. 2007]. As DTNs encaminham as mensagens segundo o paradigma armazena-carrega-e-encaminha (*store-carry-and-forward*). Assim, se não existe um caminho fim-a-fim entre uma fonte e um destino num determinado momento, os nós podem armazenar e transportar os dados até encontrar futuramente outros nós. Quando o nó entra no raio de alcance de outro nó e tem uma oportunidade de encaminhamento, chamada de contato, todos os nós encontrados podem ser candidatos a receberem cópias das mensagens carregadas. Portanto, as redes oportunistas dependem da mobilidade e cooperação dos nós para proverem pelo menos caminhos esporádicos para que a informação possa ser devidamente entregue ao destino [Chaintreau et al. 2006].

Uma proposta que utiliza as redes oportunistas como um canal secundário para auxiliar a infraestrutura no descarregamento de tráfego é o *framework Push-and-Track* (PnT) [Whitbeck et al. 2011] . Com o PnT, a infraestrutura envia cópias da mensagem de interesse para um subconjunto de nós através do canal primário, ou seja, a rede celular 3G ou 4G. Em seguida, os nós que receberam uma dessas cópias começam a encaminhar a mensagem para outros nós através do canal secundário (Wi-Fi ou Bluetooth) à medida que entram em contato com esses nós. Ao receber a mensagem de forma oportunista, os nós enviam para a infraestrutura uma mensagem de reconhecimento positivo (ACK) e também passam a encaminhar a mensagem para outros nós. Essa realimentação permite que a infraestrutura mantenha o controle dos nós que receberam a mensagem e avalie a oportunidade de reenviar novas cópias da mensagem. Se a infraestrutura percebe que o en-

caminhamento da mensagem através da comunicação oportunista não irá atingir todos os interessados dentro de um intervalo de tempo predefinido, ela envia cópias da mensagem usando o canal primário para todos os interessados que ainda não receberam a mensagem. Esse mecanismo faz com que o *Push-and-Track* garanta a entrega das mensagens mesmo usando uma rede oportunista para descarregamento de tráfego.

O *Push-and-Track*, porém, assume que todos os nós têm interesse em encaminhar a mensagem para outros nós e confirmam para a infraestrutura as mensagens recebidas de outros nós. Na prática, tal fato pode não ser verdade em função de falhas de funcionamento dos nós ou comportamentos egoístas para prejudicar o desempenho da rede ou simplesmente para economizar recursos. Esse comportamento egoísta prejudicará a disseminação da mensagem entre os nós e pode provocar reenvios desnecessários da mensagem, uma vez que é através das mensagens de reconhecimento que a infraestrutura tem o controle de quantos e quais nós receberam a mensagem. Neste artigo, propõe-se avaliar a influência dos nós egoístas, que não encaminham mensagens para outros nós ou não enviam reconhecimentos positivos para infraestrutura ou que combinam ambos os comportamentos, no desempenho do PnT. Avaliam-se diferentes cenários por simulação, variando-se o número de nós egoístas e a função de disseminação das mensagens. Considera-se um modelo real de mobilidade e mede-se a carga de tráfego enviada pela rede oportunista e pela infraestrutura. Nota-se que o aumento dos nós egoístas reduz a eficiência do descarregamento de tráfego com o PnT de 70% para 54% quando 20% dos nós tem o comportamento egoísta combinado. Se 60% dos nós são egoístas, a eficiência é reduzida para 18%.

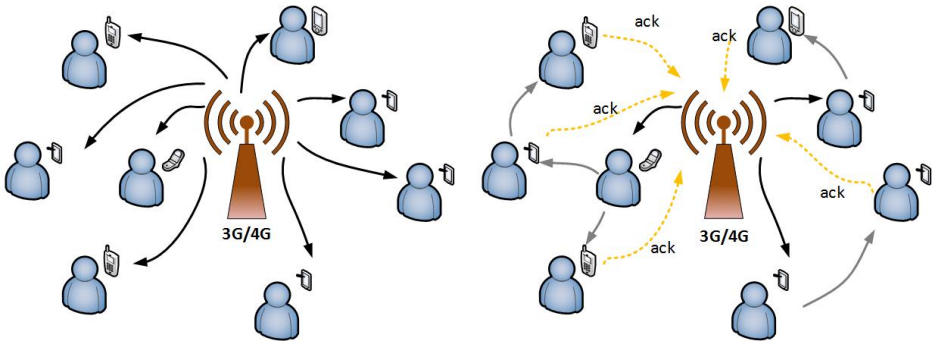
O restante do artigo está organizado da seguinte forma. A Seção 2 aborda a questão do descarregamento de tráfego com redes oportunistas e detalha o funcionamento do *Push-and-Track*, que é o mecanismo usado na avaliação deste artigo. A Seção 3 define os modelos de ataques empregados na avaliação neste artigo. A Seção 4 define os parâmetros de configuração e os cenários de avaliação utilizados nas simulações. A Seção 5 analisa e discute os resultados. A Seção 6 apresenta os trabalhos relacionados à presença de nós egoístas em redes oportunistas e ao descarregamento de tráfego. Por fim, a Seção 7 discute as conclusões e as direções futuras deste trabalho.

2. Descarregamento de Tráfego

A premissa de funcionamento dos mecanismos de descarregamento de tráfego é que vários usuários estão interessados no mesmo conteúdo. Uma situação em que essa premissa é válida é quando torcedores querem receber o mapa de assentos na chegada ao estádio ou na saída quando querem saber a localização das estações de metrô, pontos de táxi e ônibus para voltarem para suas casas. A ideia, portanto, é que parte deste tráfego composto por cópias do mesmo conteúdo seja entregue através de um canal secundário, diminuindo assim a carga de tráfego do canal primário da infraestrutura. Nesse contexto, diversos trabalhos de pesquisa estão sendo realizados usando redes oportunistas como canal secundário para descarregar parte do tráfego das redes 4G [Rebecchi et al. 2015].

Uma das propostas é o *framework Push-and-Track* (PnT) [Whitbeck et al. 2011, Whitbeck et al. 2012], cuja principal característica é garantir a entrega de todas as mensagens mesmo usando uma rede oportunista para aliviar a carga da infraestrutura de rede celular. A Figura 1 compara os modos de operação nos quais somente a infraestrutura en-

trega as mensagens e com o *Push-and-Track* funcionando. Na Figura 1(a), a infraestrutura envia uma cópia da mensagem através da rede celular para cada um dos nós interessados no mesmo conteúdo. Logo, a carga da rede está relacionada com o número de nós interessados nesse conteúdo. Na Figura, 1(b), com o PnT, a infraestrutura envia apenas três cópias inicialmente para alguns nós da rede e espera a disseminação da mensagem através da comunicação oportunista. Cada nó ao receber a mensagem através do canal secundário envia um reconhecimento positivo (ACK) para a infraestrutura confirmando o recebimento correto da mensagem. Assim, alivia-se a carga da infraestrutura, pois algumas cópias da mensagem podem ser entregues através da comunicação oportunista.



(a) Infraestrutura pura. (b) *Push-and-Track.*

Figura 1. Modos de Operação: infraestrutura pura e PnT.

O PnT possui um claro compromisso de desempenho. Quanto mais cópias iniciais enviadas, menor a redução da carga da infraestrutura, porém, menor o tempo de entrega das mensagens. Por outro lado, quanto menos cópias iniciais, menor a carga da infraestrutura e, provavelmente, maior o tempo de entrega das mensagens. Os pontos-chave do PnT, portanto, são (*i*) decidir quantas cópias iniciais devem ser injetadas, (ii) para quem devem ser enviadas essas cópias e (iii) se novas cópias devem ser injetadas ao longo do tempo. Para isso, o PnT implementa um sistema de controle com base nos ACKs recebidos pela infraestrutura de rede. Para decidir se novas cópias devem ser injetadas, o sistema de controle do PnT utiliza informações da função objetivo e da taxa de infecção. Define-se que a função objetivo é uma métrica predefinida que deve ser atendida no processo de divulgação da mensagem através da comunicação oportunista. A taxa de infecção, por sua vez, é dada pelo número de nós que receberam a mensagem, calculado através do número de ACKs recebidos pela infraestrutura. Em intervalos de tempos curtos, compara-se a função objetivo com a taxa de infecção. Caso a taxa de infecção seja menor do que a função objetivo, a infraestrutura envia mais cópias da mensagem pelo canal primário para outros nós que ainda não receberam o conteúdo para acelerar a disseminação. Para tomar a decisão para quem enviar cópias, pode-se utilizar estratégias aleatórias, baseadas no tempo de permanência, localização e conectividade [Whitbeck et al. 2011, Whitbeck et al. 2012]. Whitbeck *et al.* concluem que escolher aleatoriamente nós para envio de novas cópias pela infraestrutura é uma estratégia simples e eficiente.

Para garantir que todos os nós receberão uma cópia da mensagem desejada dentro de um intervalo máximo de tempo, o PnT define uma zona de pânico. No instante inicial da zona de pânico, a infraestrutura envia através do canal primário cópias da mensagem

para todos os nós interessados que ainda não confirmaram o recebimento da mensagem. A fatia tempo da zona de pânico é calculada pela diferença entre o tempo necessário para a infraestrutura enviar uma cópia da mensagem para todos os nós interessados através do canal primário e o tempo máximo predefinido para entregar a mensagem a todos os nós. Portanto, entrar na zona de pânico tem um efeito negativo, pois a eficiência do descarregamento diminui, principalmente se a infraestrutura tiver que enviar um número muito grande de cópias neste período. Isso resulta em um aumento significativo da carga de tráfego por mensagem.

Whitbeck *et al.* definem diferentes funções objetivo e analisam o desempenho da rede utilizando essas funções. Definem, por exemplo, funções com taxas de envio de mensagens mais lentas (*Slow Start*) e funções com taxas mais rápidas (*Fast Start*). Os resultados apresentados mostraram uma alta eficiência do descarregamento com o PnT. Porém, foram obtidos em um cenário perfeito, no qual todos os nós cooperam com a comunicação oportunista e enviam mensagens de reconhecimento positivo para a infraestrutura. Na prática, os nós podem apresentar comportamento egoísta não enviando mensagens de reconhecimento e não encaminhando mensagens para outros nós. Neste trabalho, é analisada a influência destes comportamentos no desempenho do descarregamento de tráfego com o PnT.

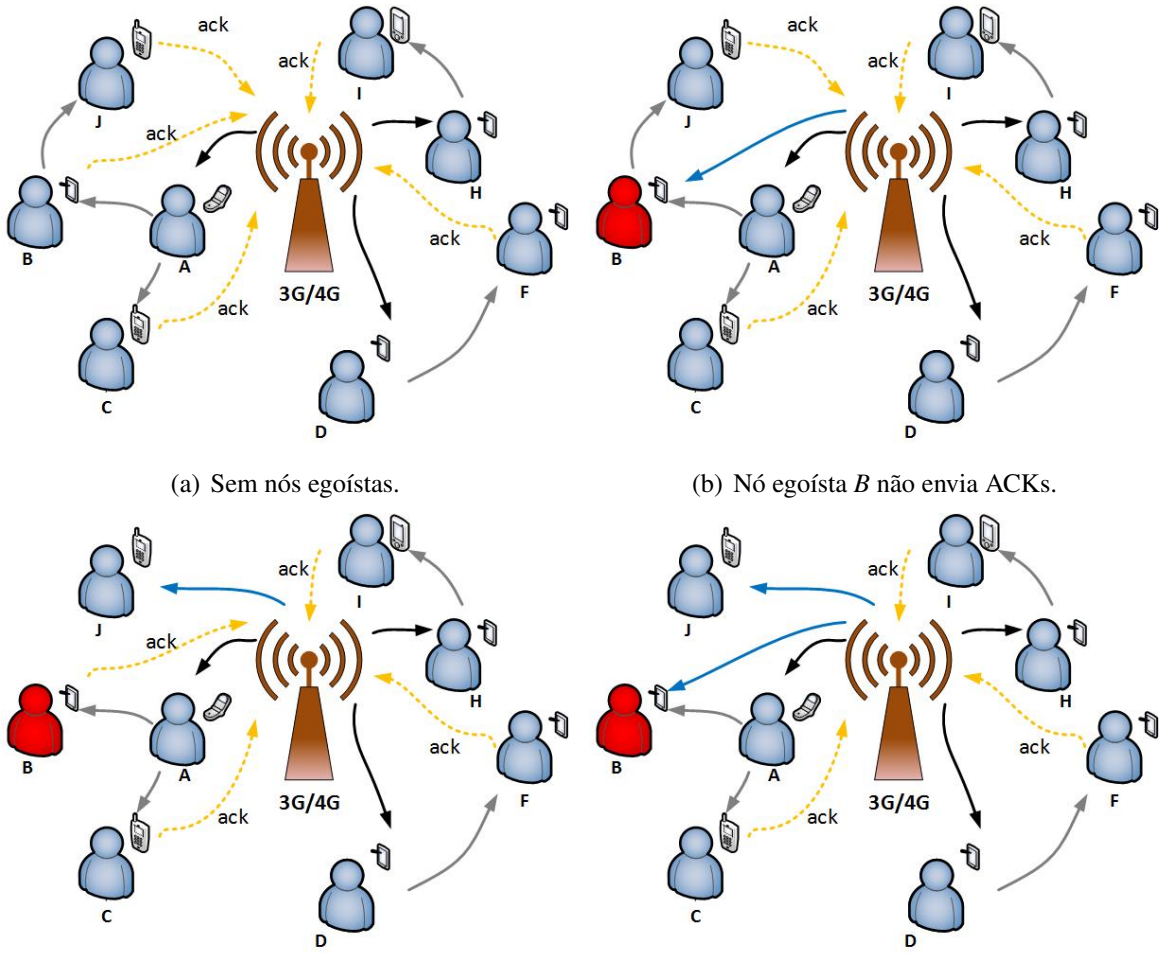
3. Modelos de Ataque

Neste trabalho, são considerados três possíveis comportamentos de nós egoístas, chamados de ataques, por simplificação:

- Ataque de não confirmação: nós egoístas recebem as mensagens através da rede oportunista, mas não enviam ACKs para a infraestrutura;
- Ataque de não encaminhamento: nós egoístas recebem as mensagens da infraestrutura ou da rede oportunista, mas não encaminham as mensagens para outros nós;
- Ataque combinado: nós egoístas recebem as mensagens da infraestrutura ou da rede oportunista, mas não encaminham as mensagens para outros nós e não enviam ACKs para a infraestrutura.

No ataque de não confirmação, como os nós não encaminham ACKs, a infraestrutura não terá controle dos nós que receberam as mensagens através da comunicação oportunista. Na Figura 2(b), o nó *B* apresenta comportamento egoísta. *B* recebe a mensagem através do contato oportunista com o nó *A*, porém não envia um ACK para a infraestrutura. Este comportamento prejudica o sistema de controle da infraestrutura no cálculo da taxa de infecção, ou seja, a infraestrutura não terá a informação correta de quantos e quais nós receberam a mensagem. Logo, a infraestrutura poderá reinjetar mais cópias desnecessárias para atingir a função objetivo ou reenviar a mensagem duplicada na zona de pânico por não ter a informação que o nó recebeu a mensagem. Por um desses motivos, o nó *B* recebe novamente a mesma mensagem da infraestrutura, ilustrado pela seta de cor azul. Neste ataque a comunicação oportunista não é prejudicada, porque os nós egoístas apenas não enviam mensagens de reconhecimento positivo. Por exemplo, na Figura 2(b), o nó *B* encaminha a mensagem para o nó *J*, cooperando com a comunicação oportunista.

Com o ataque de não encaminhamento, o objetivo é reduzir a eficiência da comunicação oportunista. Este comportamento na prática pode não ser necessariamente



(a) Sem nós egoístas.

(b) Nó egoísta *B* não envia ACKs.

(c) Nó egoísta *B* não encaminha mensagens.

(d) Nó egoísta *B* não encaminha mensagens e não envia ACKs.

Figura 2. Comportamento dos nós egoístas.

visto como um ataque, mas acontece pelo fato dos usuários estarem mais preocupados com a conservação da vida útil da bateria dos seus dispositivos do que cooperarem com a comunicação oportunista, por exemplo. A Figura 2(c) ilustra este ataque. O nó *B* recebe a mensagem do nó *A*, em seguida, *B* tem uma oportunidade de contato com o nó *J*, porém não encaminha a mensagem. Como *J* não tem outra oportunidade de contato com outro nó, a infraestrutura envia a mensagem diretamente para ele. Este envio pode acontecer no momento que a infraestrutura reinjetar novas cópias da mensagem para atender a função objetivo ou no momento em que entra na zona de pânico para garantir que todos os nós recebam a mensagem. Neste ataque o cálculo da taxa de infecção não é afetado porque ao receber mensagens na oportunidade de contato, os nós enviam ACKs para a infraestrutura.

O ataque com a combinação dos comportamentos de não confirmação e não encaminhamento aumenta a probabilidade de reenvio de cópias desnecessárias e, assim, diminui a eficiência da utilização das redes oportunistas para aliviar a carga de tráfego da infraestrutura. Na Figura 2(d), o nó *B* não encaminha mensagem para o nó *J* e não envia ACKs para a infraestrutura. Neste exemplo, a carga de tráfego aumentará porque a infraestrutura terá que enviar duas novas mensagens: uma para o nó *J* e uma mensagem

duplicada para o nó *B*. Percebe-se os prejuízos deste comportamento quando se comparam as Figuras 2(a) e 2(d). No cenário sem nós egoístas, a infraestrutura envia somente 3 mensagens e no cenário com o ataque combinado envia 5 mensagens, um aumento de 40% da carga da infraestrutura nesse exemplo simples.

4. Cenário de Avaliação

O impacto dos nós egoístas na rede oportunista é avaliado por simulação. Para tanto, utiliza-se um simulador desenvolvido especificamente para avaliar o *Push-and-Track* e que foi cedido por seus autores [Whitbeck et al. 2011]. Esse simulador é uma adaptação do ONE (*Opportunistic Network Environment*) [Keränen et al. 2009]. Para analisar o comportamento dos nós egoístas, foi necessário modificar algumas classes do simulador para que nós da rede apresentassem um dos comportamentos egoístas descritos na Seção 3. Assim, nós podem não enviar ACKs ao receberem a mensagem através da comunicação oportunista ou/e não encaminhar mensagens para outros nós em uma oportunidade do contato. Uma vez que um nó é definido como egoísta no início de uma rodada de simulação ele mantém esse comportamento durante toda a rodada. Os nós egoístas são escolhidos aleatoriamente a cada rodada de simulação.

No cenário avaliado, existe apenas uma célula e dentro dessa célula os nós se movem com base em um registro real de mobilidade, o Rollernet [Benbadis 2009]. O conjunto de dados desse registro foi coletado em um período de cerca de 3 horas em um experimento no qual foram distribuídos 62 iMotes para participantes de um circuito de patinação, que acontece regularmente em Paris. No registro de dados foram considerados os 62 iMotes e mais 1050 dispositivos externos que tiveram contato com os iMotes.

Em todos os cenários de simulação, define-se que taxa de transferência *downlink* da infraestrutura é 100 KB/s e *uplink* é 10 KB/s. Esses são valores típicos de uma rede celular definidos por Whitbeck *et al.* que afirmam que pesquisas na Europa e nos EUA mostram que a taxa média de *downlink* 3G é normalmente abaixo de 128 KB/s e *uplink* de 10 KB/s [Whitbeck et al. 2011]. Durante um contato, a taxa de transferência entre os nós é de 1 MB/s. O tamanho da mensagem de dados é de 1 MB e o dos ACKs é de 256 B. Novas mensagens de dados são geradas a cada 70 s e são do interesse de todos os nós. O algoritmo de roteamento utilizado em todas as simulações é o epidêmico [Ip et al. 2008]. Considera-se o tempo de vida das mensagens (TTL) igual a 60 s. A infraestrutura entra em zona de pânico 10 s antes de expirar o tempo de vida da mensagem, tempo este necessário para a infraestrutura enviar a mensagem diretamente para os usuários que não receberam com taxas de 100 KB/s. Os destinatários das cópias iniciais de uma mensagem são escolhidos aleatoriamente, assim como os nós da fase de reinjeção. Whitbeck *et al.* concluíram que a estratégia aleatória apresenta bons resultados e, portanto, não necessita-se da complexidade adicional de um canal de controle mais sofisticado. Nesse caso não é preciso armazenar informações sobre o tempo de permanência, localização e/ou informação de proximidade dos nós. É interessante destacar que o simulador restringe a comunicação com apenas um nó por vez no momento de um contato.

5. Resultados

O objetivo dos experimentos é mostrar que a presença de nós com diferentes comportamentos egoístas na rede reduz a eficiência do descarregamento de tráfego, indepen-

dentemente da função objetivo empregada pelo PnT. Cada comportamento egoísta descrito na Seção 3 é analisado para três funções objetivos: *Fast Start*, *Slow Start* e adaptativa. A função objetivo *Slow Start* é dada pela seguinte expressão $\frac{x}{2}$, se $t < TTL/2$; $\frac{3x}{2} - \frac{1}{2}$, se $t \geq TTL/2$. A função *Fast Start* é dada por $\frac{3x}{2}$, se $t < TTL/2$; $\frac{x}{2} + \frac{1}{2}$, se $t \geq TTL/2$. Os valores de x são encontrados através da divisão do tempo de vida atual pelo o tempo de vencimento da mensagem [Whitbeck et al. 2012]. A função adaptativa proposta por Rebecchi *et al.* evita períodos com taxas de infecção constante e superior ao valor determinado pela função objetivo. Diferente das duas primeiras funções, na função adaptativa mantém-se o histórico da taxa de infecção e compara-se esse valor. Caso ele se mantenha constante, a infraestrutura envia novas cópias para a rede [Rebecchi et al. 2014]. Para cada configuração são executadas 10 rodadas de simulação. Em cada rodada, sorteia-se um novo conjunto de nós egoístas.

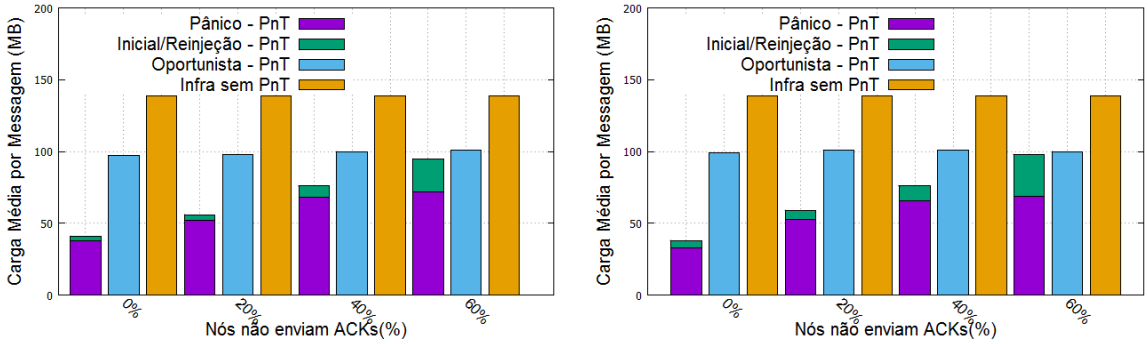
5.1. Cenário 1: Nós egoístas não enviam reconhecimentos positivos (ACKs)

Neste primeiro cenário, avalia-se o ataque de não-confirmação, ou seja, nós egoístas recebem e encaminham mensagens para outros nós de forma oportunista, mas não enviam ACKs para a infraestrutura. Assim, a infraestrutura não terá controle dos nós que receberam as mensagens através do contato com outros nós, fazendo com que a estimativa da taxa de infecção seja prejudicada. Portanto, o objetivo deste ataque é reduzir a eficiência do sistema de controle do PnT.

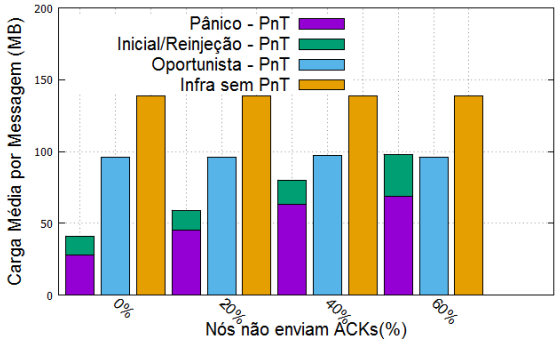
Cada grupo de barras da Figura 3 representa a carga de tráfego média necessária para entregar uma mensagem para todos os nós considerando percentuais específicos de nós egoístas. A barra de coloração laranja representa a carga média sem utilização de qualquer mecanismo de descarregamento. A barra de cor azul mostra a carga de tráfego média entregue pela comunicação oportunista entre os nós utilizando o PnT. A barra de coloração verde e roxa representa a carga média total por mensagem entregue pela infraestrutura com PnT. A porção verde da barra representa a carga de tráfego gerado pelo envio das mensagens na fase inicial e nas fases de reinjeção para atender a função objetivo. A porção roxa indica a carga gerada pelo envio de mensagens durante a zona de pânico.

Observa-se nos resultados apresentados na Figura 3 que a carga média por mensagem da comunicação oportunista mantém-se em aproximadamente 100 MB com o aumento dos nós egoístas em todos os cenários, mesmo utilizando funções objetivo diferentes. A carga de tráfego da comunicação oportunista não é afetada com o aumento do número de nós que não envia ACKs, uma vez que nesse cenário os nós egoístas continuam a encaminhar mensagens para outros nós quando há um contato.

Conforme aumenta o percentual de nós egoístas na rede cresce a carga de tráfego por mensagem da infraestrutura com o PnT. Diminui-se, assim, a eficiência do descarregamento. Por exemplo, observa-se na Figura 3(a) que a carga de tráfego é de 42 MB quando não existem nós egoístas. Com 20% de nós que não enviam ACKs, a carga cresce para 57 MB e chega 77 MB com 40% de nós egoístas, um aumento de aproximadamente 90% da carga. Mesmo utilizando funções objetivos diferentes (Figuras 3(b) e 3(c)), o desempenho do descarregamento de tráfego sofreu praticamente o mesmo impacto com o aumento do percentual dos nós egoístas. No entanto, é importante ressaltar que mesmo com 60% dos nós da rede não enviando ACKs a infraestrutura com o PnT ainda enviou



(a) Função Objetivo *Slow Start.* (b) Função Objetivo *Fast Start.*



(c) Função Objetivo Adaptativa.

Figura 3. Carga de tráfego para o ataque de não confirmação.

aproximadamente 50 MB menos do que a infraestrutura sem PnT. Ou seja, mesmo na presença de nós egoístas o PnT ainda descarrega o tráfego da infraestrutura.

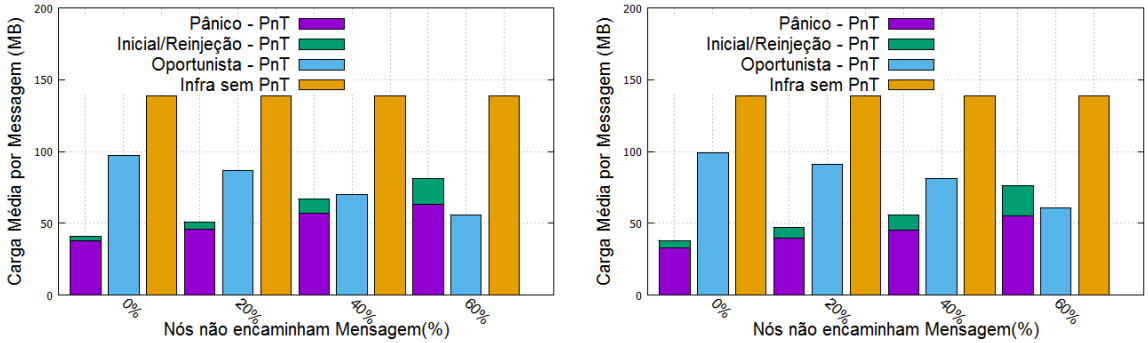
O ataque de não confirmação aumenta a carga da infraestrutura com o PnT por dois motivos. O sistema de controle é prejudicado porque os nós não enviam ACKs ao receberem a mensagem através da comunicação oportunista. Assim a infraestrutura calcula a taxa de infecção com um valor inferior ao valor real do número de nós que receberam a mensagem. Este valor inferior pode ser menor que a função objetivo e provocar envio de mais cópias na fase de reinjeção para atender a função objetivo. Quando a infraestrutura com o PnT entra na zona de pânico, ela envia cópias duplicadas para nós que receberam a mensagem e não confirmaram, devido à infraestrutura não ter o controle de quais nós receberam a mensagem.

5.2. Cenário 2: Nós egoístas não encaminham mensagens

No segundo cenário avalia-se o ataque de não encaminhamento, ou seja, nós egoístas recebem mensagens pelo canal primário e pelo secundário não encaminham para outros nós, prejudicando assim a comunicação oportunista entre os nós.

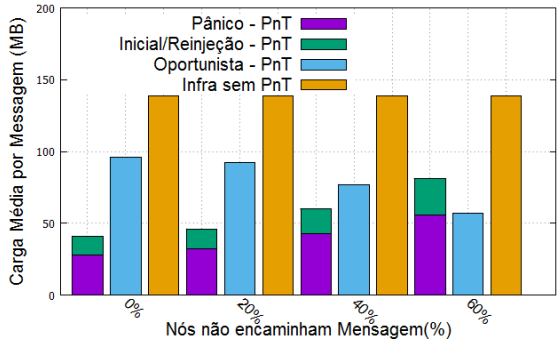
A carga de tráfego gerada na comunicação oportunista no ataque de não encaminhamento difere da carga gerada no ataque de não confirmação. Observa-se na Figura 4 que para todas as funções objetivos analisadas a carga de tráfego média por mensagem na comunicação oportunista diminui com o aumento do percentual de nós que não encaminham as mensagens na oportunidade de contato. Com 60% de nós que não encaminham mensagens a carga da comunicação oportunista diminui aproximadamente 44 MB (*Slow*

Start), 39 MB (*Slow Start*) e 43 MB (adaptativa) comparados com os resultados apresentados na Figura 3. No Cenário 1, mesmo atacando a rede ao não enviar ACKs, os nós egoístas continuam a encaminhar as mensagens na oportunidade de contato. Para todos os experimentos no Cenário 1, a carga de tráfego é de aproximadamente 100 MB.



(a) Função objetivo *Slow Start*.

(b) Função objetivo *Fast Start*.



(c) Função objetivo adaptativa.

Figura 4. Carga de tráfego para o ataque de não encaminhamento.

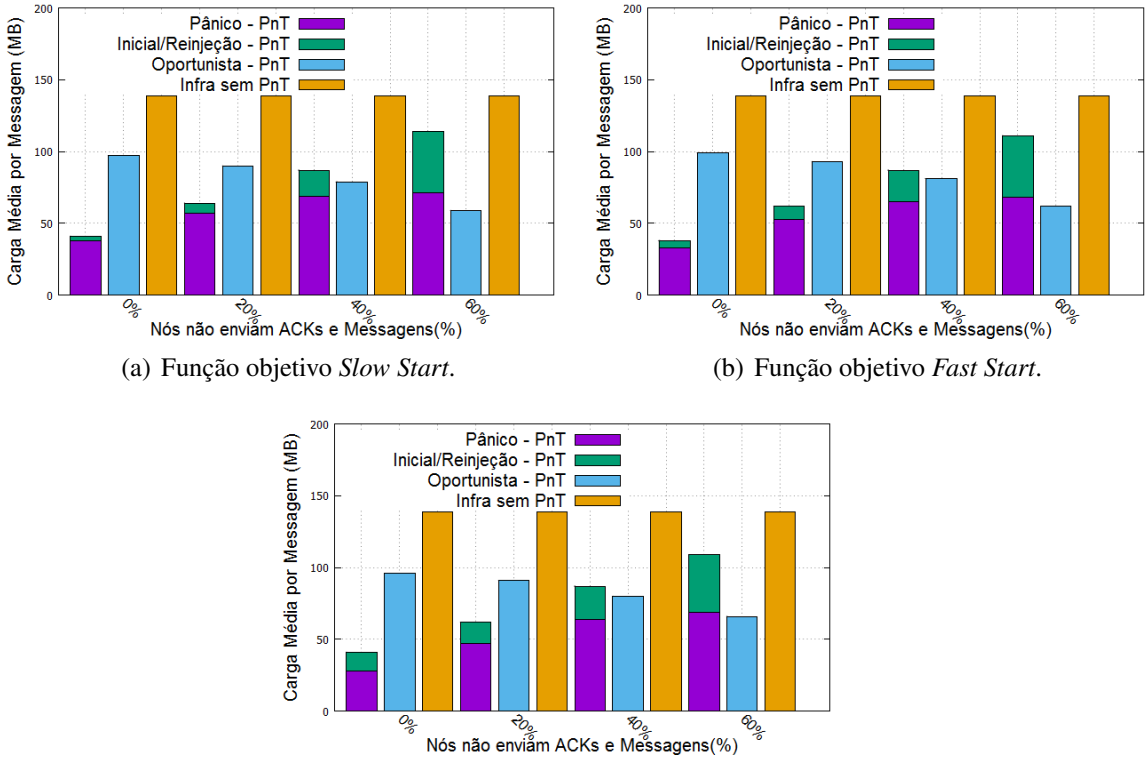
Com o aumento do número de nós egoístas a carga da infraestrutura com o PnT cresce para todas as funções objetivo analisadas. Assim, diminui-se a eficiência do descarregamento. Com 20% de nós que não encaminham mensagens, a carga aumenta para 51 MB, 47 MB e 47 MB, com 40% aumenta para 68 MB, 58 MB e 61 MB para as funções *Slow Start*, *Fast Start* e adaptativa, respectivamente. Justifica-se esse aumento na carga da infraestrutura com o PnT pelo aumento da probabilidade de contato de nós legítimos com nós que não encaminham mensagens. Observa-se que a carga da infraestrutura com PnT com a função objetivo *Slow Start* (Figura 4(a)) é maior do que com as outras funções objetivo. Os valores da função objetivo *Slow Start* na primeira metade de vida da mensagem são calculados pela expressão $\frac{x}{2}$, que são menos agressivos que os valores da função objetivo *Fast Start* (Figura 4(b)). Em outras palavras, a função objetivo *Slow Start* envia um número menor de cópias da mensagem para a rede. E neste cenário, um nó tem maior probabilidade de não receber a mensagem. A função adaptativa (Figura 4(c)) apresentou resultados semelhantes aos da função objetivo *Fast Start*.

Comparando os resultados apresentados nos Cenários 1 e 2, observa-se que o ataque de não encaminhamento é menos prejudicial para o desempenho do descarregamento de tráfego. Com aumento do percentual dos nós que não enviam ACKs, a infraestrutura com o *Push-and-Track* não tem o controle de quais e quantos nós receberam a mensagem,

provocando reenvio de cópias desnecessárias na fase de reinjeção e na zona de pânico.

5.3. Cenário 3: Nós egoístas não encaminham mensagens e não enviam reconhecimentos positivos

Neste cenário é analisada a influência do ataque combinado, ou seja, quando nós egoístas não encaminham mensagens e não enviam ACKs para a infraestrutura. Nota-se na Figura 5 que com o aumento do percentual de nós egoístas na rede, a carga de tráfego da infraestrutura com o *Push-and-Track* aumenta consideravelmente, reduzindo a eficiência do descarregamento de tráfego. Observa-se na Figura 5(b) que com 60% de nós egoístas, a carga gerada pela infraestrutura com o PnT é de 112 MB. No Cenário 1, utilizando a função objetivo *Fast Start* e com 60% de nós que não enviam ACKs, a carga da infraestrutura com o PnT é de 98 MB. Com o mesmo percentual de nós que não encaminham mensagens (Cenário 2) a carga é de 77 MB.



(a) Função objetivo *Slow Start*.

(b) Função objetivo *Fast Start*.

(c) Função objetivo adaptativa.

Figura 5. Carga de tráfego para o ataque combinado.

O aumento da carga da infraestrutura com o *Push-and-Track* ocorre pela junção dos problemas apresentados nos cenários anteriores. O não encaminhamento das mensagens de forma oportunista faz com que a infraestrutura tenha que enviar mais cópias para atender a função objetivo. Por sua vez, o não envio de reconhecimentos positivos, prejudica o cálculo da taxa de infecção, o que causará maior reenvio de cópias da mensagem desnecessariamente pela infraestrutura. Outra consideração, é que a soma da carga de tráfego da comunicação oportunista mais a carga de tráfego da infraestrutura com o PnT difere da carga de tráfego da infraestrutura sem PnT, também em virtude da estimativa errada da taxa de infecção pelo não envio de ACKs, como ocorre no Cenário 1.

Tabela 1. Eficiência do descarregamento de tráfego para os três ataques analisados.

		Funções objetivo		
		Slow Start	*Fast Start*	Adaptativa
Cenário 1	0%	70%	72%	70%
	20%	59%	57%	57%
	40%	45%	45%	42%
	60%	32%	29%	29%
Cenário 2	0%	70%	72%	70%
	20%	63%	65%	66%
	40%	51%	58%	56%
	60%	40%	44%	42%
Cenário 3	0%	70%	72%	70%
	20%	54%	55%	51%
	40%	36%	37%	37%
	60%	18%	20%	21%

A Tabela 1 mostra a eficiência do descarregamento de tráfego para os três ataques analisados. A eficiência do descarregamento de tráfego é calculada pela expressão $(1 - \frac{L_{PnT}}{L_{infra}}) * 100$, onde L_{PnT} é carga de tráfego média por mensagem da infraestrutura com o PnT e L_{infra} é a carga da infraestrutura sem o PnT. Em todos os cenários, mesmo com um aumento significativo de nós egoístas, há descarregamento de tráfego da infraestrutura com o PnT, porém menos significativo. O resultado menos significativo é com o ataque combinado com 60% de nós egoístas com a função objetivo *Slow Start*.

6. Trabalhos Relacionados

Naves e Moraes avaliaram o ataque de falsificação de reconhecimentos positivos (ACKs) em redes oportunistas [Naves and Moraes 2014]. Nesse trabalho, nós maliciosos forjam reconhecimentos para que os nós legítimos descartem mensagens ainda não entregues, reduzindo o desempenho da rede. Analisa-se também uma contramedida proposta na literatura. Portanto, diferencia-se da proposta deste artigo nos seguintes aspectos: não avaliam o desempenho da rede oportunista aplicada como um canal secundário para auxiliar a infraestrutura e não analisam o caso em nós não cooperam com o encaminhamento das mensagens.

Theja e Ramesh avaliaram o impacto de nós não cooperativos, ou seja, nós que não encaminham mensagens para outros nós, no tempo de vida das mensagens [Theja and Ramesh 2012]. Tal avaliação se diferencia deste trabalho, por não avaliar a carga de tráfego, e a utilização das redes oportunistas no descarregamento de tráfego e por não considerar que os nós não enviam ACKs diretamente para a infraestrutura ao receberem cópias das mensagens através da comunicação oportunista.

Rebecchi *et al.* propõem modificações na proposta de descarregamento de tráfego com o *Push-and-Track* e denominam essa nova versão como *Droid (Derivative Reinjection to Offload Data)* [Rebecchi et al. 2014]. Basicamente, eles definem uma nova função objetivo, que evita períodos de planalto, ou seja, momentos em que a taxa de

infecção mantém-se constante ou superior à função objetivo. Portanto, também não analisam o comportamento dos nós egoístas no desempenho da proposta, assim como no trabalho original do PnT.

Liu *et al.* também introduzem um mecanismo de descarregamento de tráfego através das redes oportunistas [Liu et al. 2013]. Os autores definem uma política para selecionar o número de réplicas iniciais e uma política para distribuir as réplicas iniciais limitadas sob a influência de comportamentos egoístas. Nesta proposta, entretanto, os autores não analisaram o impacto dos nós egoísta na eficiência do descarregamento de tráfego. O enfoque era o aumento do tempo médio da entrega das mensagens. Além disso, a proposta não garante que 100% das mensagens serão entregues, assim como faz o *Push-and-Track*.

7. Conclusões e Trabalhos Futuros

Neste artigo, avaliou-se a eficiência do descarregamento de tráfego com o *framework Push-and-Track* (PnT) na presença de nós egoístas. Esses nós não encaminham mensagens para outros nós, não enviam reconhecimentos positivos para infraestrutura ou combinam esses dois comportamentos. O desempenho do PnT foi avaliado para três funções objetivo diferentes: *Slow Start, Fast Start* e adaptativa.

Os resultados mostraram que quando 40% de nós não enviam ACKs para a infraestrutura, houve um aumento na carga da infraestrutura com o PnT de até 90% comparado com o cenário perfeito, no qual todos os nós enviam ACKs. Esse comportamento é semelhante independentemente da função objetivo usada. Observou-se também que o ataque de não encaminhamento é menos prejudicial para o desempenho do descarregamento de tráfego do que o ataque de não confirmação. Isso porque com aumento do percentual dos nós que não enviam ACKs, a infraestrutura com o PnT não tem o *feedback* de quais e quantos nós receberam a mensagem, provocando reenvio de cópias desnecessárias na fase de reinjeção e na zona de pânico. Quando combinados os ataques, a eficiência do descarregamento de tráfego com o PnT foi reduzida de 70% para 18%.

Como trabalhos futuros, pretende-se propor uma contramedida para identificar os nós egoístas na rede, visando melhorar a eficiência do descarregamento de tráfego através da comunicação oportunista com o PnT. Também pretende-se estudar e analisar outros ataques a redes oportunistas no descarregamento de tráfego e propor novas contramedidas.

Agradecimentos

Os autores agradecem a J. Whitbeck e a F. Rebecchi pelo simulador disponibilizado. Em especial a CAPES, pelo financiamento do DINTER IFTM/UFF.

Referências

Benbadis, F. (2009). CRAWDAD data set upmc/rollernet (v. 2009-02-02). Downloaded from http://crawdad.org/upmc/rollernet/.

Chaintreau, A., Hui, P., Crowcroft, J., Diot, C., Gass, R., and Scott, J. (2006). Impact of human mobility on the design of opportunistic forwarding algorithms. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–13.

Han, B., Hui, P., Kumar, V. A., Marathe, M. V., Pei, G., and Srinivasan, A. (2010). Cellular traffic offloading through opportunistic communications: A case study. In *Proceedings of the 5th ACM Workshop on Challenged Networks*, CHANTS '10, pages 31–38, New York, NY, USA. ACM.

Ip, Y.-K., Lau, W.-C., and Yue, O.-C. (2008). Performance modeling of epidemic routing with heterogeneous node types. In *Communications, 2008. ICC '08. IEEE International Conference on*, pages 219–224.

Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The ONE Simulator for DTN Protocol Evaluation. In *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, New York, NY, USA. ICST.

Li, Y., Qian, M., Jin, D., Hui, P., Wang, Z., and Chen, S. (2014). Multiple mobile data offloading through disruption tolerant networks. *Mobile Computing, IEEE Transactions on*, 13(7):1579–1596.

Liu, Z., Wu, Y., and Deng, S. (2013). Optimal mobile data offloading policy through delay tolerant networks with selfish nodes. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 3(5):386–390.

Naves, J. F. and Moraes, I. M. (2014). Uma avaliação do ataque de falsificação de reconhecimentos positivos em redes tolerantes a atrasos e desconexões. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos SBRC2014*, pages 105–118.

Oliveira, C. T., Moreira, M. D. D., Rubinstein, M. G., Costa, L. H. M. K., and Duarte, O. C. M. B. (2007). Redes tolerantes a atrasos e desconexões. In *Minicursos Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos SBRC2007*, Belém, PA, Brasil.

Rebecchi, F., Dias de Amorim, M., and Conan, V. (2014). Droid: Adapting to individual mobility pays off in mobile data offloading. In *Networking Conference, 2014 IFIP*, pages 1–9.

Rebecchi, F., Dias de Amorim, M., Conan, V., Passarella, A., Bruno, R., and Conti, M. (2015). Data offloading techniques in cellular networks: A survey. *Communications Surveys Tutorials, IEEE*, 17(2):580–603.

Theja, R. and Ramesh, Y. (2012). The impact of message lifetime on delay-tolerant networks with non-cooperative nodes. In *Internet (AH-ICI), 2012 Third Asian Himalayas International Conference on*, pages 1–4.

Whitbeck, J., Amorim, M., Lopez, Y., Leguay, J., and Conan, V. (2011). Relieving the wireless infrastructure: When opportunistic networks meet guaranteed delays. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*, pages 1–10.

Whitbeck, J., Amorim, M., Lopez, Y., Leguay, J., and Conan, V. (2012). Push-and-track: Saving infrastructure bandwidth through opportunistic forwarding. *Pervasive and Mobile Computing*, 8(5):682–697.

Zhuo, X., Gao, W., Cao, G., and Dai, Y. (2011). Win-coupon: An incentive framework for 3g traffic offloading. In *Network Protocols (ICNP), 2011 19th IEEE International Conference on*, pages 206–215.

