UNIVERSIDADE FEDERAL FLUMINENSE

CLAITON LUIZ SOARES

COMPORTAMENTO EGOÍSTA DE NÓS NO DESCARREGAMENTO DE TRÁFEGO COM REDES OPORTUNISTAS

NITERÓI

2018

UNIVERSIDADE FEDERAL FLUMINENSE

CLAITON LUIZ SOARES

COMPORTAMENTO EGOÍSTA DE NÓS NO DESCARREGAMENTO DE TRÁFEGO COM REDES OPORTUNISTAS

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Doutor em Computação. Área de concentração: Sistemas de Computação.

Orientador:
IGOR MONTEIRO MORAES

NITERÓI

2018

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

S676c Soares, Claiton Luiz
Comportamento Egoísta de Nós no Descarregamento de Tráfego com Redes Oportunistas / Claiton Luiz Soares ; Igor Monteiro Moraes, orientador. Niterói, 2018.
88 f. : il.

Tese (doutorado)-Universidade Federal Fluminense, Niterói, 2018.

DOI: http://dx.doi.org/10.22409/PGC.2018.d.06139908620

1. Redes Oportunistas. 2. Redes Tolerantes a Atrasos e Desconexões. 3. Comportamento Egoísta. 4. Segurança. 5. Produção intelectual. I. Moraes, Igor Monteiro, orientador. II. Universidade Federal Fluminense. Escola de Engenharia. III. Título.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

CLAITON LUIZ SOARES

COMPORTAMENTO EGOÍSTA DE NÓS NO DESCARREGAMENTO DE TRÁFEGO COM REDES OPORTUNISTAS

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Doutor em Computação. Área de concentração: Sistemas de Computação.

Aprovada em 07 de Dezembro de 2018.

BANCA EXAMINADORA

Prof. Igor Monteiro Moraes, D.Sc., UFF (Orientador)

Prof. Miguel Elias Mitre Campista, D.Sc., UFRJ

Prof. Luís Henrique Maciel Kosmalski Costa, Dr., UFRJ

Prof. Célio Vinicius Neves de Albuquerque, Ph.D., UFF

Prof. Diego Gimenez Passos, D.Sc., UFF

Niterói

2018

Dedico este trabalho à minha esposa e filha, Chrystal e Maria Luíza.

Agradecimentos

Gostaria de agradecer em primeiro lugar a Deus, pela força para continuar perseguindo meus objetivos, mesmo nos momentos de dificuldade.

Meus maiores agradecimentos à minha esposa, Chrystal, por sempre me apoiar e estar do meu lado. E à minha família pelo apoio de sempre.

Agradeço aos professores da Universidade Federal Fluminense, que contribuíram imensamente com este trabalho. Em especial, meus mais sinceros agradecimentos ao meu orientador, Igor Monteiro Moraes, pela força e pelos sábios conselhos e apontamentos.

Aos amigos que fiz em Niterói, em especial à Marister e aos meus amigos do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro.

Agradeço aos membros da banca por terem aceitado o convite para participar da defesa.

Finalmente, agradeço aos amigos Fieno, Heraldo, Ronaldo, Júlio e a todos que de alguma forma contribuíram com este trabalho. Em especial à CAPES e IFTM, pelo financiamento do DINTER IFTM/UFF.

Resumo

A infraestrutura celular está sobrecarregada com o crescente número de dispositivos e aplicações móveis. De acordo com a Cisco, o tráfego global de dados das redes celulares representa hoje 20% do tráfego IP na Internet quando em 2016 representava apenas 8%. Além disso, em 2021, o tráfego gerado por *smartphones* vai ultrapassar o tráfego gerado por computadores pessoais. 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 esse canal secundário. As redes oportunistas permitem que dois nós consigam se comunicar mesmo que nunca exista um caminho fim-a-fim entre eles.

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. Esta tese avalia a influência dos nós egoístas no descarregamento de tráfego com redes oportunistas através de um estudo de caso. Por simplificação, nós egoístas são aqueles que não encaminham mensagens para outros nós ou que falham ao enviar reconhecimentos positivos para infraestrutura ou que combinam ambos os comportamentos. O impacto dos nós egoístas no descarregamento de tráfego com rede oportunista é avaliado por simulação. Resultados mostram que a eficiência do descarregamento é reduzida de 77% para até 19% com a presença de nós egoístas na rede.

Em função dos resultados obtidos, esta tese propõe contramedidas com o objetivo de minimizar os efeitos da presença de nós egoístas, chamadas de ACKs duplamente identificados e *ranking* de encaminhamento. Com o ACK duplamente identificado, no momento em que um nó recebe a cópia de uma mensagem através do canal secundário, ele encaminha um ACK para a infraestrutura informando que recebeu a mensagem e de qual nó a recebeu na oportunidade do contato. Desta forma, a infraestrutura terá o controle de quais nós não estão enviando ACKs e prejudicando o calculo da taxa de infecção. Com o *ranking* de encaminhamento, a infraestrutura contabiliza o número de mensagens encaminhadas por cada nó com base nos ACKs enviados. A lista ordenada com o número de encaminhamentos de cada nó servirá como critério de escolha para determinar para quais nós a infraestrutura irá enviar cópias da mensagem inicialmente e na fase de reinjeção para atender a função objetivo. Os resultados apresentaram uma diminuição na carga de tráfego da infraestrutura em todos os cenários analisados, aumentando assim a eficiência do descarregamento de tráfego na presença de nós egoístas. No cenário em que os nós falham ao enviar ACKs e/ou não enviam mensagens para outros nós, com 60% de nós egoístas usando a função de objetivo *Slow Linear*, há um aumento na eficiência do descarregamento de tráfego de 19% para 44%.

Palavras-chave: Redes Oportunistas, Redes tolerantes a atrasos e desconexões, comportamento egoísta, segurança.

Abstract

The cellular infrastructure is overloaded because of the increasing number of mobile devices and applications. Cisco states that today's global data traffic from cellular networks corresponds to 20% of total IP traffic in the Internet against 8% in 2016. In addition, in 2021, the smartphones 'traffic will surpass personal computers' traffic. 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. Opportunistic networks allow two nodes to communicate even if there is no an end-to-end path between them.

To be effective, however, opportunistic communication relies that nodes cooperate with each other in order to forward messages and to confirm to the infrastructure the successful reception of messages sent by other nodes. This thesis evaluates the impact of selfish nodes on the performance of the traffic offloading with opportunistic networks. For simplicity, selfish nodes are those nodes that do not forward messages to other nodes or nodes that fail to send acknowledgment messages to the infrastructure or combine both behaviors. The impact of selfish nodes with the opportunistic network traffic offloading is evaluated by simulation. Results show that the offloading efficiency decreases from 77% to up to 19% if selfish nodes are in the network.

We propose two countermeasures in order to reduce the negative effects of selfish nodes, referred to as doubly identified ACKs and forwarding ranking. With doubly identified ACK, at the time a node receives the copy of a message through the secondary channel, this nodes sends an ACK for the infrastructure stating that it successfully received the message and which node forwarded the message to her during a contact. In this way, the infrastructure has control of which nodes are not sending ACKs and degrading the calculation of the infection rate. With the forwarding ranking, the infrastructure counts the number of messages forwarded by each node based on sent ACKs. The ordered list with the number of forwarded messages by each node serves as the criteria to determine to which nodes the infrastructure will initially send copies of the message and to meet the objective function during the reinjection phase. The results present a decrease in the infrastructure traffic load in all scenarios analyzed, thus increasing the traffic offloading efficiency in the presence of selfish nodes. In the scenario where nodes fail to send ACKs and do not forward messages to other nodes, with 60% of selfish nodes using *Slow Linear* objective function, there is an efficiency increase in traffic offloading from 19% to 44%.

Keywords: Opportunistic network, Delay and disruption tolerant networks, selfish behavior, security.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ACK	:	*Acknowledgement*;
AP	:	*Access Point*;
BS	:	*Base Station*;
DTN	:	*Delay and Disruption Tolerant Network*;
DTNRG	:	*Delay Tolerant Networking Research Group*;
D2D	:	*Device-to-Device*;
EAP	:	*Extensible Authentication Protocol*;
ER	:	*Registro de Encontro*;
IPN	:	*Interplanetary Network*;
IRTF	:	*Internet Research Task Force*;
LTE	:	*Long Term Evolution*;
MANET	:	*Mobile Ad Hoc Network*;
MINEIRO	:	*Messagebased INcentive mechanism for End-user Improvement*
	:	*of Routing Opportunities* ;
ONE	:	*Opportunistic Network Environment*;
PnT	:	*Push-and-Track*;
RSSI	:	*Received Signal Strength Indication*;
SINR	:	*Signal to Interference Plus Noise Ratio*;
VOIP	:	*Voice over IP*;
3GPP	:	*3rd Generation Partnership Project.*

Sumário

Capítulo 1

Introdução

A crescente popularização dos dispositivos móveis inteligentes modifica drasticamente o estilo de vida dos indivíduos que cada vez mais usam e confiam nas redes celulares para os mais diferentes fins. Aplicações consumidoras de dados, como distribuição de vídeo e redes sociais, estão entre as mais populares. De acordo com a previsão da Cisco [21], o tráfego global de dados móveis aumentará 7 vezes entre 2016 e 2021, enquanto o tráfego de vídeo móvel crescerá 8,7 vezes entre 2016 e 2021. O tráfego de vídeo móvel representará mais de 78%, sendo a categoria de aplicações móveis de maior crescimento. Em 2021, o tráfego gerado por *smartphones* vai ultrapassar o tráfego gerado por computadores pessoais.

A crescente demanda de tráfego faz com que a infraestrutura de rede celular se aproxime do seu limite. Consequentemente, os usuários da rede celular poderão experimentar uma redução da qualidade do serviço, por exemplo, chamadas perdidas, e velocidade reduzida de acesso à Internet. Uma solução simples em termos técnicos é aumentar o número de estações base para aumentar a capacidade da rede celular. Porém, os aplicativos móveis estão se tornando cada vez mais exigentes em termos de processamento e largura de banda [21]. Uma alternativa é desenvolver e implantar uma nova geração de redes celulares. A expectativa é que até 2020 a rede celular de quinta geração (5G) esteja padronizada e ofereça dez vezes mais largura de banda do que a geração atual [58]. No entanto, esta solução pode não ser suficiente. Isso ocorre porque a atualização da rede celular geralmente é cara e o retorno financeiro pode ser baixo. Além disso, prevê-se que até mesmo a nova geração de redes celulares não vai ser capaz de lidar com a enorme demanda de tráfego de dados dos usuários nos próximos anos [44].

Uma possível solução para este problema é utilizar uma técnica conhecida como descarregamento de tráfego (*Traffic Offloading*) [67, 33]. O objetivo dessa técnica não é

substituir a rede celular, que seria o canal principal de comunicação, mas empregar um canal secundário de comunicação para reduzir o volume de dados transportado na rede celular [67]. Neste contexto, muitos usuários estão interessados em um mesmo conteúdo, premissa que é válida para muitos conteúdos na Internet [89]. 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.

Existem na literatura diferentes propostas de implementação do descarregamento de tráfego [67]. Algumas propostas utilizam uma infraestrutura auxiliar, nesse caso, ponto de acesso (*Access Points* - APs) WiFi. Outras utilizam um mecanismo de descarregamento que emprega apenas a comunicação dispositivo-a-dispositivo (*Device-to-Device* - D2D). Esta tese estuda a implementação do descarregamento de tráfego com redes oportunistas [33], uma solução promissora para aliviar a sobrecarga da rede celular que explora a comunicação D2D. Com as redes oportunistas, os nós não precisam recuperar exclusivamente um conteúdo da sua fonte. Alguns nós móveis recuperam conteúdos populares através da rede celular e transmitem esses conteúdos para outros nós. A comunicação entre os nós é feita de forma *ad hoc* através de outras interfaces de rede sem-fio cada vez mais comuns nos dispositivos móveis, como WiFi e Bluetooth. Desta forma, nós podem obter o conteúdo solicitado sem acessar a Internet através do canal secundário, o que ajuda a reduzir significativamente a carga de tráfego na rede celular. 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 [93]. Ao contrário do descarregamento baseado em APs WiFi, esse novo tipo de descarga de tráfego depende da comunicação entre os nós móveis.

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 and Disruption Tolerant Networking*) [55]. As DTNs encaminham as mensagens segundo o paradigma armazena-carrega-e-encaminha (*store-carry-and-forward*), no qual cada nó é dotado de um *buffer*. Assim, se não existe um caminho fim-a-fim entre uma fonte e um destino num determinado momento, os nós armazenam as mensagens no *buffer* e as carregam 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 [16].

É comum que as propostas de mecanismos de descarregamento de tráfego com redes oportunistas assumam que todos os nós têm interesse em encaminhar mensagem para 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 de mensagens entre os nós e pode provocar reenvios desnecessários das mensagens.

1.1 Objetivos

Esta tese avalia a influência dos nós egoístas e propõe contramedidas para reduzir o impacto negativo causado pela presença desses nós no descarregamento de tráfego com redes oportunistas. Para tanto, considera o *framework Push-and-Track* (PnT) [87] como estudo de caso. 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. Em seguida, os nós que receberam uma dessas cópias encaminham a mensagem para outros nós através do canal secundário 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 necessidade de reenviar novas cópias da mensagem. Se a infraestrutura percebe que o encaminhamento 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. Avalia-se a influência dos nós egoístas, que não encaminham mensagens para outros nós ou que falham ao enviar 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 77% para 58% quando

20% dos nós tem o comportamento egoísta combinado. Se 60% dos nós são egoístas, a eficiência é reduzida para 19%.

Esta tese também propõe contramedidas que aumentem a eficiência do descarregamento de tráfego na presença de nós com comportamentos egoístas Para tanto, o PnT foi alterado para que ele use ACK duplamente identificado e um *ranking* de encaminhamento. Com o ACK duplamente identificado, quando um nó recebe a cópia da mensagem através do canal secundário, esse nó enviará um ACK para a infraestrutura informando que ele recebeu a mensagem e também de qual nó ele recebeu a mensagem, juntamente com o registro de encontro. Assim, a infraestrutura terá o controle através desta mensagem de quais nós receberam as mensagens e que falharam ao enviar o ACK. Com o *ranking* de encaminhamento, a infraestrutura da rede celular manterá uma lista que contabiliza o número de encaminhamentos de cada nó através da comunicação oportunista com base no ACKs duplamente identificados recebidos. Com base nesta lista, a infraestrutura envia cópias da mensagem para os nós que mais encaminham mensagens evitando, assim, nós que não encaminham cópias da mensagem para outros nós na oportunidade de contato.

1.2 Organização do Trabalho

O restante desta tese está organizada da seguinte forma. O Capítulo 2 apresenta o estado da arte do descarregamento de tráfego em redes celulares e uma taxonomia das propostas de alguns dos mecanismos de descarregamento existentes na literatura. O Capítulo 3 detalha o descarregamento de tráfego com redes oportunistas e o funcionamento do *Push-and-Track*, que é o mecanismo usado como estudo de caso para avaliar o impacto de comportamentos egoístas. O Capítulo 4 define os modelos de ataque empregados, apresenta os parâmetros de configuração e os cenários de avaliação utilizados nas simulações, analisa e discute os resultados. O Capítulo 5 apresenta e avalia as contramedidas para o PnT, chamadas de ACK duplamente identificado e *ranking* de encaminhamento. Por fim, o Capítulo 5 apresenta as considerações finais e discute as direções futuras deste trabalho.

Capítulo 2

Descarregamento de Tráfego em Redes Celulares

O aumento do número de *smartphones* e do seu uso para acesso à Internet tem impactado diretamente às redes de operadoras de telefonia celular, devido à grande demanda de uso de dados. Uma solução promissora e de baixo custo para lidar com esse aumento da carga de tráfego na rede celular é o descarregamento de tráfego [67, 63]. A ideia do descarregamento de tráfego não é substituir a rede celular, mas sim aproveitar interfaces de rede disponíveis nos *smartphones*, como o WiFi e o Bluetooth, como canais secundários de comunicação para reduzir a quantidade de tráfego transportada pelo canal primário. Para tornar isto possível, é preciso modificar mecanismos e protocolos de comunicação usados nas redes celulares para que eles considerem a existência dos vários canais alternativos de comunicação. Este capítulo, apresenta o estado da arte do descarregamento de tráfego em redes celulares e uma taxonomia das propostas de mecanismo de descarregamento existentes na literatura.

2.1 Motivação

Um dos maiores desafios para as operadoras de telefonia celular atualmente é como gerenciar o crescimento do tráfego de dados. O tráfego das redes celulares em todo o mundo crescerá nos próximos anos graças ao crescimento do número de dispositivos móveis e à oferta de planos de dados mais acessíveis pelas operadoras de telefonia celular. Além disso, aplicações consumidoras de tráfego, como distribuição de áudio e vídeo, compartilhamento de conteúdos em redes sociais e aplicações em nuvem, são cada vez mais populares entre os usuários. De acordo com a Cisco [21], o tráfego de dados global das redes celulares hoje representa 20% do tráfego IP na Internet enquanto em 2016 repre-

sentava apenas 8%. No Brasil, o tráfego de dados móveis terá um crescimento duas vezes mais rápido que o tráfego IP entre 2016 e 2021, e 77% das conexões móveis no país serão conexões por dispositivos móveis até 2021, comparados com 52% em 2016. A distribuição de vídeo pela rede celular crescerá 8,7% entre 2016 e 2021, sendo a categoria de aplicações móveis de maior crescimento. O vídeo móvel representará 78% de todo o tráfego móvel em 2021, com ou sem requisitos de tempo real. Até 2021, o tráfego global de dados móveis atingirá 49 exabytes por mês ou 587 exabytes anualmente. A taxa anual prevista de 587 exabytes de tráfego de dados móveis para 2021 é equivalente a 122 vezes mais do que todo o tráfego móvel global gerado em 2011, apenas 10 anos antes.

Com a crescente demanda de acesso à Internet através das redes celulares, as operadoras estão sob pressão tentando lidar com essa sobrecarga de tráfego. Por regulamentação, as operadoras de telefonia celular utilizam apenas uma faixa fixa e predeterminada do espectro de radiofrequência, que é extremamente cara. Os usuários devem compartilhar os recursos limitados de banda passante sem possibilidade de aumento da faixa de espectro reservada. Se a demanda de tráfego é maior do que a capacidade projetada para a rede, o desempenho e a qualidade do serviço (QoS) percebida pelos usuários são afetados. Durante os horários de pico em ambientes metropolitanos densos, por exemplo, os usuários experimentam altas latências, baixa taxa de transferência e interrupções de rede devido ao congestionamento [83]. Infelizmente, esta tendência se agravará no futuro, devido o maior número de dispositivos conectados à rede celular e ao surgimento de novas aplicações que demandam mais banda passante, como os veículos autônomos e as aplicações de cidades inteligentes [4].

Em função da alta demanda de tráfego, é necessário, portanto, desenvolver métodos alternativos para reduzir a quantidade de tráfego transportada pelas redes celulares. Como primeira opção, as operadoras de telefonia móvel passaram a limitar a taxa de transmissão da conexão e o uso de dados pelos usuários [89]. No entanto, essas práticas afetam negativamente a satisfação do cliente que paga por um serviço com restrições. Por essa razão, surgiram propostas de descarregamento de tráfego em redes celulares. A premissa de funcionamento do descarregamento de tráfego é que os dispositivos móveis possuem outras interfaces de diferentes tecnologias de rede além da rede celular. Por isso, podem aproveitar a largura de banda não utilizada por essas interfaces para transportar tráfego que antes seria transportado pela rede celular. Criam-se, assim, canais secundários de comunicação. O descarregamento de tráfego se destaca como uma solução promissora e de baixo custo porque não exige a adição de novas interfaces de rede nos dispositivos móveis e porque a criação dos canais secundários de comunicação pode ser feita ou com a

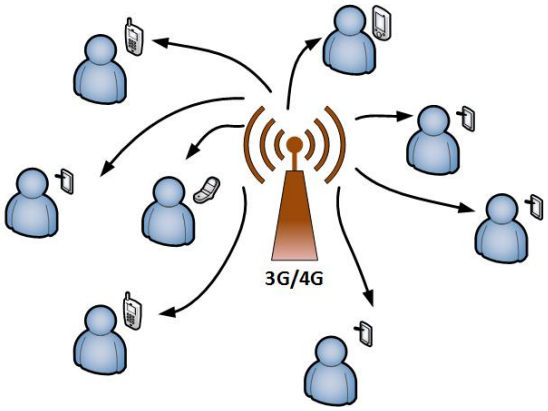
instalação de uma infraestrutura de menor custo do que a infraestrutura da rede celular ou com a comunicação direta entre os dispositivos móveis, como detalhado a seguir.

2.2 Uma Taxonomia dos Mecanismos de Descarregamento de Tráfego

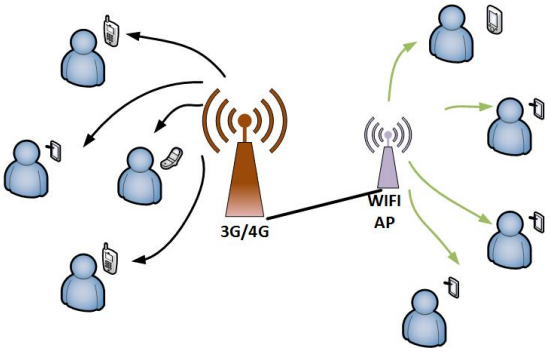
A taxonomia apresentada neste seção adota dois critérios para classificar os mecanismos de descarregamento de tráfego: (i) se os mecanismos empregam alguma infraestrutura auxiliar ou consideram a comunicação direta entre dispositivos móveis ou (ii) de acordo com os requisitos de QoS das aplicações para as quais se propõe descarregar o tráfego.

A Figura 2.1 compara o funcionamento da rede celular tradicional, da rede celular com um mecanismo de descarregamento que emprega uma infraestrutura auxiliar e da rede celular com um mecanismo de descarregamento que emprega apenas a comunicação dispositivo-a-dispositivo (*Device-to-Device* - D2D). Na rede celular convencional, Figura 2.1(a), cada dispositivo móvel possui uma conexão com a estação base da rede celular. A Figura 2.1(b), por outro lado, ilustra a abordagem em que há uma infraestrutura auxiliar, nesse caso, um ponto de acesso WiFi. Esse AP está ligado através de uma rede cabeada à estação base. Tal abordagem apresenta uma solução convencional para reduzir o tráfego nas redes celulares porque os usuários localizados dentro da área de cobertura do AP podem usá-lo como uma alternativa interessante para a rede celular quando precisam trocar dados. APs baseados na tecnologia IEEE 802.11 geralmente fornecem maior taxa de transferência do que redes celulares [23]. No entanto, a área de cobertura de um AP WiFi normalmente é muito menor que uma macrocélula da rede celular. Logo, a cobertura é limitada e a mobilidade é, em geral, restringida dentro da área do AP. Como o custo monetário da implantação de uma série de APs WiFi é muito menor do que a implantação de uma única estação base, algumas das principais operadoras de telefonia celular começaram a integrar um número crescente de APs WiFi em suas redes celulares para incentivar o descarregamento de tráfego [2].

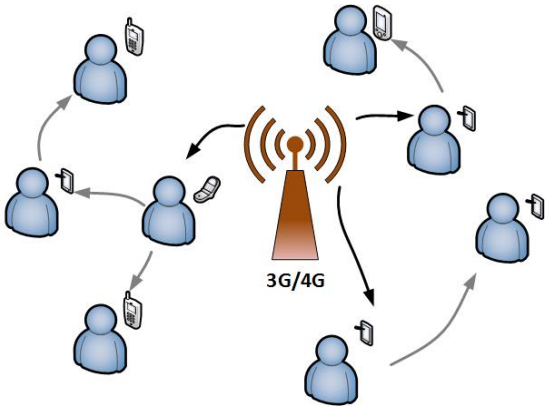
Com dispositivos móveis cada vez mais potentes, em termos de processamento, memória e autonomia de bateria, é possível implantar uma rede *ad hoc*, na qual os dispositivos móveis se comunicam diretamente sem a necessidade de uma infraestrutura de rede, conforme pode ser observado na Figura 2.1(c) [70]. Essa abordagem é conhecida como comunicação dispositivo-a-dispositivo, ou simplesmente D2D. A premissa de funcionamento dos mecanismos de descarregamento de tráfego baseados na comunicação D2D é



(a) Rede Celular Tradicional.



(b) Baseado em AP.



(c) Baseado em D2D.

Figura 2.1: Diferentes tipos de descarregamento de tráfego.

que vários usuários estão interessados no mesmo conteúdo [89, 57]. 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 do canal secundário, diminuindo assim a carga de tráfego do canal primário da infraestrutura. Beneficiando-se de interesses compartilhados entre usuários que estejam próximos, as operadoras podem decidir enviar conteúdo popular apenas para um pequeno subconjunto de usuários através da rede celular, e deixar esses usuários espalharem as informações através de comunicações D2D, aproveitando-se assim, do canal secundário destes dispositivos para encaminhamento do conteúdo.

Outro critério usado para classificar os mecanismos de descarregamento de tráfego são os requisitos de QoS das aplicações para as quais o mecanismo se propõe a descarregar o tráfego. Rebecchi *et al.* [67] classificam os mecanismos de acordo com o atraso de entrega que os dados de uma aplicação podem tolerar.

No descargamento não sensível ao atraso, a entrega do conteúdo pode ser atrasada intencionalmente até certo ponto, a fim de alcançar condições de entrega mais favoráveis. Incluem-se nesta categoria os seguintes tipos de tráfego: (i) tráfego com requisitos "frouxos" de QoS, isto é, pacotes individuais podem ser atrasados, mas todo o conteúdo deve atingir o usuário dentro de um determinado prazo, e (ii) tráfego verdadeiramente tolerante ao atraso, isto é, possivelmente sem garantias de atraso. A flexibilidade na restrição de entrega permite também encaminhar o tráfego oportunisticamente, o que, por definição, só pode garantir um tempo de entrega probabilístico. Se a transferência de dados não terminar no prazo esperado, o canal primário é empregado como um meio de retorno para completar a transferência, garantindo uma QoS mínima. Apesar da perda do suporte em tempo real devido ao atraso de transmissão adicional, observa-se que muitos aplicativos para dispositivos móveis geram conteúdo intrinsecamente tolerante a atrasos, como sincronização de emails ou *podcasts*. É importante ressaltar que os mecanismos descarregamento não sensíveis ao atraso dependem da mobilidade dos usuários. Graças à mobilidade, os usuários podem alcançar um AP WiFi ou um vizinho que carrega o conteúdo de interesse, aumentando a capacidade de descarregamento.

No descargamento sensível ao atraso, por outro lado, cada pacote apresenta uma restrição de atraso de entrega definida pela aplicação, que em geral é independente da rede. Nenhum atraso extra é adicionado à entrega de dados para preservar os requisitos de QoS além do atraso devido ao processamento de pacotes, atraso de espera em fila, propagação, transmissão e acesso ao rádio. Assim, a rede deve cumprir esse prazo para garantir o funcionamento adequado da aplicação. No descarregamento sensível ao atraso, a mobilidade muitas vezes representa um grande obstáculo e requer um esforço substancial para que os requisitos de tempo de entrega sejam atendidos. Em cenários de baixa mobilidade, é possível entregar dados com garantias restritas de atraso tanto usando comunicações D2D quanto o auxílio de uma infraestrutura de pontos de acesso WiFi. Por outro lado, o descarregamento sensível ao atraso é essencialmente desafiador em redes oportunistas, uma vez que o atraso acumulado fim-a-fim ao longo do caminho de transmissão pode ser muito alto em relação aos requisitos de entrega limitados. Principalmente, por causa da mobilidade dos nós e por não ter garantias que haverá contatos entre os nós.

A maior diferença entre os mecanismos sensíveis ao atraso e os não sensíveis ao atraso é a forma como a pontualidade de entrega de conteúdo é tratada. No descarregamento sensível ao atraso, o atraso adicional gerado pelo canal secundário é extramente limitado, enquanto no descarregamento não sensível ao atraso o canal secundário adiciona algum atraso, seja pelo fato de que o usuário precisa esperar até que chegue perto o suficiente

de um AP WiFi, ou a espera por obter mensagens através da comunicação D2D.

Esta tese, assim como feito por Rebecchi *et al.* [67], classifica o descarregamento considerando as garantias de atraso de entrega e a maneira como ocorre o descarregamento baseado em AP ou em D2D. Assim, classificam-se os mecanismo de descarregamento em quatro combinações discutidas nas próximas seções: (i) descarregamento sensível ao atraso baseado em AP; (ii) descarregamento sensível ao atraso baseado em D2D; (iii) descarregamento não sensível ao atraso baseado em AP e (iv) descarregamento não sensível ao atraso baseado em D2D.

2.2.1 Descarregamento Sensível ao Atraso Baseado em Pontos de Acesso

A ideia do descarregamento sensível ao atraso baseado em APs é que dados em tempo real e interativos, como distribuição de vídeo e VoIP (*Voice over IP*), possam se beneficiar do uso de um canal secundário de comunicação além da rede celular. Uma possível solução é a instalação de pontos de acesso WiFi para servirem de canal secundário, devido a sua ampla difusão, desempenho e baixo custo. Há inúmeros exemplos de operadoras de telefonia que incentivam seus assinantes, oferecendo dados ilimitados por meio de pontos de acesso WiFi. Alguns desses exemplo são descritos a seguir. Sobre a questão do custo, as operadoras Oi, Claro, e TIM, anunciaram que o preço por megabyte transportado por pontos de acesso WiFi é 30% inferior ao preço do megabyte transportado pela infraestrutura da rede celular [76].

Do ponto de vista técnico, as estações base das redes celulares são projetadas para cobrir grandes áreas, enquanto pontos de acesso do padrão IEEE 802.11 possuem raio de alcance de uma ou poucas centenas de metros. Em contraste, a taxa de transmissão é geralmente maior em redes locais WiFi do que nas tecnologias celulares. Portanto, como sugerido em alguns trabalhos, é possível aproveitar essa complementaridade de tecnologias, combinando adequadamente os pontos fortes de cada uma [30, 41].

Existem atualmente diversos exemplos do emprego do descarregamento de tráfego de redes celulares utilizando APs WiFi por algumas operadoras do Brasil. Por exemplo, a TIM reestruturou a sua política de instalação de APs WiFi criando a TIM WiFi [78, 76]. A operadora adotou estratégia de instalar APs da rede WiFi em regiões de alta utilização de acessos à rede de dados. O princípio é garantir que a rede WiFi seja uma rede complementar à sua oferta na rede móvel. Encontra-se em funcionamento no Rio de Janeiro e São Paulo o redirecionamento automático dos clientes da operadora de telefonia para

a rede de APs WiFi, com *login* transparente ao usuário. Os clientes que utilizam equipamentos que suportam a tecnologia EAP (*Extensible Authentication Protocol*) efetuam automaticamente a autenticação. A rede WiFi, após identificar os clientes TIM, passa a redirecionar a sua navegação.

A operadora Oi adotou a estratégia de instalar APs WiFi, a partir do momento em que comprou a "Vex", a provedora com o maior número de APs WiFi instalados do Brasil, criando, assim, o serviço Oi WiFi [54, 76]. Todos os APs foram imediatamente atualizados com a marca da Oi, e clientes da banda larga fixa Velox ou dos pacotes de dados 3G/4G, ganharam acesso gratuito ao serviço. A operadora investiu na instalação de novos APs em lugares estratégicos como a orla de Ipanema, Leblon e Copacabana no Rio de Janeiro. Em Salvador na Bahia, o mesmo acontece com a Praia da Barra e o Pelourinho. Além disso, a Oi instala APs durante grandes eventos, como os festivais *Rock in Rio* e *Lollapalooza*.

A operadora Claro conta com um número alto de assinantes que já experimentaram o serviço WiFi da operadora, denominado de Claro "NeT-Claro-WiFi" [22, 76]. A rede que compartilha a infraestrutura WiFi da Claro é a "Net Serviços", que está presente em mais de 6 mil pontos nas cidades do Rio de Janeiro, São Paulo, Campinas, Brasília, Belo Horizonte, Porto Alegre, Curitiba, Recife, Salvador e Fortaleza. O serviço está disponível de graça para clientes da operadora com planos de dados. Para acessar a rede automaticamente é necessário ter um aparelho compatível com a tecnologia EAP. Outro modo é informar o *login* e senha pelo portal de autenticação do serviço.

Os mecanismos de descarregamento baseados em APs são atualmente acionados pelos usuários. Isso significa que os usuários devem habilitar explicitamente o canal secundário de comunicação. Essa abordagem é atraente no início, pois não exige modificações na infraestrutura de rede. Porém, apresenta algumas limitações, como a mobilidade restrita e a falta de continuidade de sessão, que dificultam sua adoção em larga escala [11]. Para aumentar a qualidade de experiência do usuário, as operadoras buscam aumentar o controle do processo de descarregamento. As operadores estão cada vez mais voltadas para uma integração entre redes alternativas de acesso e sua infraestrutura de rede celular. O processo de integração envolve parcerias entre as operadoras celulares e de pontos de acesso WiFi, com políticas comuns de faturamento e contabilidade, bancos de dados de assinantes compartilhados para autenticação e autorização.

Além das iniciativas das operadoras, existem avaliações e propostas na literatura para demonstrar a viabilidade do descarregamento de tráfego sensível ao atraso com a instalação de APs WiFi. Lee *et al.* [41] apresentam um dos primeiros estudos quantitativos

sobre o benefício que a transferência de dados por meio de APs pode trazer para as operadoras celulares e usuários finais. Os autores realizam um estudo quantitativo sobre o desempenho do descarregamento de dados móveis 3G através de pontos de acesso WiFi. Eles analisam 97 usuários de iPhone de áreas metropolitanas e coletam estatísticas sobre sua conectividade WiFi durante um período de duas semanas e meia em fevereiro de 2010. Os resultados baseados nos *traces* coletados apresentam que se consegue descarregar utilizando APs WiFi cerca de 65% do tráfego total de dados móveis e se economiza 55% da energia da bateria sem usar nenhuma transmissão atrasada. Fuxjager *et al.* [30] tentam estimar o grau real de utilização do espectro WiFi, ou seja, o número médio de bytes transmitidos pelos pontos de acesso WiFi. Esses estudos revelam que, nas áreas metropolitanas, a disponibilidade de WiFi é alta.

Uma estratégia interessante para aumentar o desempenho do descarregamento é posicionar os APs de forma otimizada para maximizar o tráfego que flui pelo canal secundário. Como o problema de posicionamento ótimo torna-se rapidamente intratável (NP-difícil) a medida que a quantidade de APs aumenta, vários algoritmos sub-ótimos foram propostos na literatura. Hu *et al.* [36] avaliam o desempenho do descarregamento sensível ao atraso em função do número de APs instalados. São realizadas simulações com um modelo de propagação de rádio em um cenário urbano sem mobilidade dos usuários. Os resultados revelam que a medida que a densidade de APs aumenta há um aumento linear na taxa de transferência média por usuário. Bulut *et al.* [11] e Ristanovic *et al.* [68], também propõem algoritmos de implantação de APs visando maximizar a fração de tráfego descarregado. Todas essas abordagens são semelhantes, propondo uma solução heurística para o problema da implementação ótima do AP, que é problema NP-difícil. A ideia é colocar os APs próximos aos locais com maior densidade de solicitações de dados móveis ou maior número de usuários. Os resultados da simulação mostram que é possível reduzir o tráfego celular em 20% a 70%, dependendo da densidade do ponto de acesso. Além dos resultados da simulação, os modelos analíticos ajudam a derivar os limites teóricos de desempenho.

O compartilhamento do espectro sem-fio é uma grande preocupação dos administradores de rede. Pontos de acesso na mesma rede podem interferir uns com os outros, degradando seu desempenho. Assim, adicionar muitos APs pode aumentar a interferência mútua entre os APs e degradar o desempenho da rede. Uma outra área de pesquisa interessante diz respeito à seleção do AP ideal quando vários APs estão disponíveis simultaneamente. Singh *et al.* [72] descrevem um modelo de descarregamento considerando que há congestionamento nos APs. A estratégia resultante maximiza o número de usuá-

rios capazes de atingir suas taxas máximas de dados levando em conta a SINR (*Signal to Interference Plus Noise Ratio*) recebido e a distribuição espacial de usuários e APs. Balbi *et al.* [6] propõem um algoritmo de alocação de canais projetado para controladores centrais das redes IEEE 802.11 infraestruturadas. O algoritmo proposto reduz a interferência nos pontos de acesso controlados através da escolha dinâmica de seus canais operacionais e, ao contrário de outras propostas, é projetado para operar em uma rede composta por dispositivos de baixo custo de diferentes marcas e software de código aberto. Considera-se a interferência causada por redes não gerenciadas, ajustando as configurações dos pontos de acesso gerenciados de acordo com o ambiente sem-fio. A proposta foi implementada e avaliada em um *testbed* aberto e os resultados mostram que o controlador gerencia eficientemente o espectro com equipamentos de baixo custo e um algoritmo de baixa complexidade.

2.2.2 Descarregamento Sensível ao Atraso Baseado em Comunicação Dispositivo-a-Dispositivo

O descarregamento sensível ao atraso baseado em D2D é geralmente implementado através do emprego de estratégias cooperativas de recuperação de dados de maneira distribuída. A ideia da maioria dos mecanismos cooperativos é que um conjunto de nós seja responsável por receber um conteúdo através da rede celular e que, em seguida, esses nós sejam responsáveis por encaminhar o conteúdo aos demais nós interessados. Há, portanto, desafios como o critério de seleção do conjunto de nós retransmissores, descoberta de nós interessados no mesmo conteúdo etc. Há ainda a questão de qual interface deve ser usada para a comunicação direta entre os dispositivos. Há mecanismos que empregam tecnologias de comunicação alternativas não licenciadas para estabelecer comunicações D2D fora de banda. Há mecanismos, por sua vez, que dedicam parte da banda celular licenciada às comunicações D2D, chamada de comunicação em banda [4]. Na categoria fora de banda, o WiFi e o Bluetooth são escolhas comuns, já que são as tecnologias sem-fio mais populares atualmente presentes nos *smarthphones*. Para a categoria de descarregamento em banda, desenvolvimentos recentes do padrão LTE-A (*Long Term Evolution-Advanced*), especificado pelo 3GPP (*3rd Generation Partnership Project*) versão 12, propõem integrar as capacidades de comunicação do D2D em futuras arquiteturas celulares [1] [9].

Stiemerling *et al.* [75] e Karanakaran *et al.* [39] consideram a comunicação D2D fora da banda. O primeiro avalia a aplicação de distribuição de vídeo em um cenário de alta mobilidade dos nós. A ideia básica é fazer o *download* de cada fragmento de vídeo apenas

uma vez pelo canal da rede celular e compartilhá-lo através de um canal secundário. Os acessos celulares precisam ser coordenados entre os nós dispostos a aliviar a rede celular. Um nó atua como o controlador central e estima a taxa de transferência disponível no canal celular para cada nó, de modo a coordenar a recuperação de conteúdo entre os pares. Os resultados da simulação fornecem o número mínimo de nós cooperativos necessários para atingir os valores-alvo de taxa de transferência e recepção. Karunakaran *et al.* [39] consideram a variação da taxa de transmissão de dados que os usuários de celular podem alcançar para transmitir dados somente àqueles usuários com a melhor qualidade de canal. Em seguida, os dados são transmitidos para todos os outros nós por meio de transmissões D2D. Os resultados mostram economia significativa de energia quando todos os usuários estão solicitando os mesmos dados. Comparado com a distribuição somente pela rede celular, a taxa apresenta melhor desempenho em termos de consumo de energia, com redução em até 70%.

A principal desvantagem dos mecanismos que empregam a comunicação em banda é a interferência causada pelas comunicações D2D nas comunicações do canal primário e vice-versa. Assim, os mecanismos precisam lidar com questões como interferência mútua e alocação de recursos, já que as comunicações D2D ocorrem na mesma faixa das comunicações entre os dispositivos e a estação base [4, 29]. Alwan *et al* [3] citam que ativar as comunicações D2D em uma rede celular apresenta grandes desafios. Primeiro, a interferência causada aos usuários de celular por dispositivos D2D poderia afetar criticamente o desempenho dos dispositivos celulares. Outro desafio é garantir os requisitos mínimos das comunicações D2D.

No LTE-*Advanced* [9] a comunicação D2D foi introduzida pelo 3GPP para descarregar o tráfego de usuários e ao mesmo tempo para melhorar a utilização do espectro nas redes LTE. Phunchongharn *et al.* [61] introduzem um novo esquema de alocação de recursos para comunicações D2D em redes LTE para maximizar a utilização do espectro, encontrando o comprimento mínimo de transmissão em termos de intervalos de tempo para comunicação D2D, protegendo os usuários de celulares contra interferências prejudiciais e garantindo a QoS nas comunicações D2D.

Moura *et al.* [51] investigam o desempenho da comunicação D2D em redes LTE-A. Eles afirmam no trabalho que mesmo com um pequeno número de estações móveis aumenta-se a área de cobertura da rede celular e tem-se ganhos de vazão. Li *et al.* [46] estudam o limite de uma estratégia de descarregamento que explora o LTE-D2D num cenário de grande escala. Os nós são divididos em *downloaders* e *helpers*, que podem

ajudar a rede celular a entregar o conteúdo para *downloaders*. A estratégia de distribuição ótima é formulada como um problema de otimização e avaliada por meio de simulações. Ao conhecer o padrão de mobilidade dos usuários, é elaborado um limite superior de desempenho. Os resultados da simulação confirmam que o aumento do número de usuários na célula se beneficia amplamente do descarregamento, aumentando sua eficiência. Nesse caso, as transmissões D2D são responsáveis por até 50% do tráfego.

2.2.3 Descarregamento Não Sensível ao Atraso Baseado em Pontos de Acesso

A ideia dos mecanismos de descarregamento de tráfego não sensíveis ao atraso é adicionar um atraso não negligenciável à recepção do conteúdo. Exploram-se assim aplicações que podem tolerar um certo grau de atraso sem afetar o grau de satisfação dos usuários dessas aplicações. Alguns conteúdos podem ter um limite de atraso de entrega explícito, outros podem ser verdadeiramente tolerantes a atrasos, tais como emails e *podcasts*. Estes são, portanto, conteúdos candidatos a serem descarregados com limites de entrega.

As estratégias baseadas em APs aproveitam-se de um conjunto de APs, geralmente formado por APs WiFi fixos, para fornecer dados através do canal secundário. Conforme abordado na Seção 2.2.1, a rede de acesso usada como canal secundário pode fazer parte da rede das operadoras de celular, ou pode ser completamente independente. Neste último caso, deve ser previsto um acordo entre as operadoras. No início, essa abordagem é semelhante ao caso não atrasado. O princípio de funcionamento dos mecanismos baseados em AP tanto sensíveis quanto os não sensíveis ao atraso é semelhante: dispositivos móveis obtém dados de interesse através dos APs WiFi e não pela rede celular. A diferença é que os mecanismos não sensíveis ao atraso buscam explorar a mobilidade dos usuários para criar oportunidades de contato entre os usuários e outros APs para aumentar a eficiência do descarregamento. Há, portando, diferentes desafios de pesquisa nessa área, como prever o potencial de descarregamento através de comportamentos passados de usuários como mobilidade, contatos com diferentes APs e taxa de transferência. Usando essa previsão, pode-se usar um coordenador de descarregamento para decidir qual fração de dados descarregar, quando e para quem. Possivelmente, o conteúdo é dividido em várias partes, que são enviadas pró-ativamente para APs que os nós provavelmente encontrarão no futuro. Outra área de pesquisa visa identificar o número ideal de pontos de acesso fixos e sua localização geográfica, a partir do padrão de mobilidade de um usuário conhecido.

Os usuários móveis geram quantidades cada vez maiores de dados digitais, como do-

cumentos, fotos e vídeos, que são carregados enquanto estão em trânsito, principalmente devido ao surgimento de aplicações de compartilhamento social. A conectividade de Internet através da infraestrutura celular permite que os usuários de dispositivos móveis façam *upload* de seus dados, que consomem seus recursos de bateria dos dispositivos e sobrecarregam os provedores de serviços móveis. O descarregamento de dados *upload* baseado em AP WiFi supera os problemas mencionados anteriormente para dados tolerantes a atraso. No entanto, ocorre a custo da mobilidade restrita para os usuários, já que eles precisam permanecer em uma determinada área de cobertura do AP WiFi enquanto os dados são carregados. Huguenin *et al.* [37], propõem um mecanismo denominado de Hoop, um sistema para descarregar dados *upload* de dispositivos móveis. Os autores descrevem que o Hoop é seguro, não requer mudanças nos *gateways*, servidores da web, nos protocolos ou navegadores existentes.

Siris *et al.* [73] combinam a previsão da mobilidade do nó com o conhecimento da geolocalização de APs fixos para melhorar a eficiência do processo de descarregamento. Há um nó coordenador e um preditor que informam ao coordenador quantos APs um nó móvel irá encontrar durante sua rota, quando eles serão encontrados e por quanto tempo o usuário estará no alcance do AP. O algoritmo procura maximizar a quantidade de dados tolerantes a atraso a serem descarregados pelo canal secundário WiFi, garantindo também que os dados sejam transferidos dentro de seu prazo de entrega.

Da mesma forma, a arquitetura MobTorrent [17] explora a infraestrutura híbrida, a pré-busca de dados e a replicação de *cache* em APs fixos. As solicitações de *download* são emitidas por meio do canal de primário. Os dados solicitados são armazenados em *cache* antecipadamente nos APs usando informações de localização e o histórico de mobilidade dos usuários.

Dimatteo *et al.* [23] propõem arquitetura para a integração de redes WiFi e *Pocket Switched Networks*(PSN) com redes celulares para fornecer uma solução de baixo custo para lidar com o crescimento exponencial do tráfego de dados móveis. A MADNet emprega a rede celular como um canal de controle. Quando um usuário móvel solicita algum conteúdo, o coordenador de descarregamento responde com a lista dos APs adjacentes, nos quais ele pode recuperar os dados solicitados. O coordenador de descarregamento prevê os APs vizinhos explorando as informações de posicionamento enviadas pelos usuários por meio do canal de controle. Os principais resultados, obtidos por meio de simulação, mostram que algumas centenas de APs implantados em toda a cidade de São Francisco poderiam descarregar metade do tráfego da rede celular.

Ra *et al.* [64] propõem um algoritmo de otimização centralizado chamado SALSA. Esse algoritmo determina quando adiar uma transmissão, adaptando o processo de descarregamento à disponibilidade de rede e informações de localização. A principal contribuição do trabalho é explorar a eficiência energética das transmissões não sensíveis ao atraso, porque o envio e recepção de dados usando WiFi consome menos energia do que transmissões e recepções na rede celular. A decisão de transmissão baseia-se na previsão da largura de banda disponível para cada rede de acesso possível, estimada como a taxa média alcançada em transmissões passadas, ou em função da RSSI (*Received Signal Strength Indication*) recebida. Os autores também realizaram experimentos sintéticos e reais para confirmar o bom desempenho do SALSA, que pode economizar até 40% de energia se comparado a outros mecanismos de descarregamento.

Balasubramanian *et al.* [5] propõem um algoritmo capaz de explorar a tolerância de atraso do conteúdo e os contatos com APs WiFi fixos. O algoritmo chamado de Wiffler prevê futuros encontros com APs, adiando a transmissão apenas se isso evitar o transporte de tráfego na rede celular, empregando uma heurística. O algoritmo Wiffler prevê o tempo de transferência WiFi com base nos encontros anteriores com os APs. O histórico de contatos é empregado para estimar o tempo entre contatos e a taxa de transferência média por contato. Por meio de simulações baseadas em *traces* reais, os autores mostram que com uma previsão baseada apenas nos últimos quatro encontros, o Wiffler obtém um erro de previsão baixo para intervalos futuros de cerca de um minuto. O sistema é capaz de descarregar entre 20% a 40% da carga da rede celular, dependendo da tolerância de atraso do conteúdo.

Zhang *et al.* [91] concentram em como encontrar o instante ideal para adiar a transferência de dados pela redes celulares. Embora transferências não sensíveis ao atraso aumentam substancialmente o desempenho de descarregamento de tráfego, adiar todas as transferências até a tolerância máxima de atraso é muitas vezes uma estratégia ineficaz. Em caso de ausência de WiFi, cada transmissão atrasada frustra a experiência do usuário. Uma solução ideal é identificar o instante ideal de tempo um usuário deve parar de adiar as transmissões e começar a transferir dados usando a rede celular, considerando a eficiência de descarregamento e a satisfação do usuário. Por esse motivo, o algoritmo proposto maximiza uma função de utilidade dependendo dos dados transferidos e da satisfação do usuário. A satisfação do usuário é modelada como uma função de satisfação do período de atraso. Os autores usam um algoritmo de enumeração da sequência de contato e um modelo semi-Markov para prever o volume médio de dados descarregados. Através de extensas simulações e resultados numéricos, o esquema mostra sua alta eficácia

e flexibilidade

Lee *et al.* [41] demonstram que o aumento da tolerância ao atraso aumenta quantidade de tráfego descarregado. Discutem também que o tempo médio de entrega com mecanismos de descarregamento não sensível ao atraso é sempre muito menor do que o prazo máximo de entrega. Os autores inclusive mostram que, para conteúdos de grande tamanho, atrasar a transmissão pode resultar em tempos de entrega menores que quando a transmissão não é atrasada. Isso porque a tecnologia WiFi geralmente oferece taxas de dados mais altas do que as redes celulares, o que se traduz em tempos de entrega agregados mais curtos.

Trestian *et al.* [79] sugerem atualizar a capacidade da rede em um número limitado de locais, chamados *Drop Zones*. A premissa de bom funcionamento é que a maioria dos usuários passa por um número limitado de locais durante seus deslocamentos diários. A contribuição original deste trabalho é o algoritmo para alocação dos *Drop Zones*, que visa reduzir tanto o número de APs quanto o atraso médio de entrega. Este é um problema mínimo de seleção de conjuntos, com uma solução ótima NP-díficil. O artigo propõe também um algoritmo guloso sub-ótimo que garante uma redução de 24% na alocação de APs em relação às estratégias sensíveis ao atraso.

2.2.4 Descarregamento Não Sensível ao Atraso Baseado em Comunicação Dispositivo-a-Dispositivo

Os mecanismos de descarregamento não sensíveis ao atraso baseados em D2D exploram a mobilidade dos usuários para criar oportunidades de comunicação, os chamados contatos. Como efeito colateral, o desempenho desses mecanismos é fortemente dependente do padrão de mobilidade dos usuários. Para contornar esse problema, tais mecanismos confiam na rede celular para inicialmente disseminar cópias de um conteúdo entre os usuários interessados. O objetivo é garantir requisitos mínimos de QoS das aplicações. Antes do prazo de entrega expirar, o conteúdo é de preferência encaminhado pelo canal secundário de comunicação. Como as mensagens são encaminhadas apenas durante períodos de contato entre usuários, a análise estatística desses contatos é fundamental para o bom funcionamento dos mecanismos. Informações tais como a frequência em que os contatos acontecem, quando ocorrem, o tempo que eles duram ajudam a prever o número de mensagens que podem ser descarregadas.

No descarregamento não sensível ao atraso baseado em D2D, a distribuição de conteúdo é de responsabilidade dos próprios usuários da rede. A mobilidade de usuários

que "carregam" dado conteúdo, por sua vez, cria oportunidades para que esses usuários transfiram conteúdos usando uma abordagem tolerante a atrasos, baseada na arquitetura DTN [26]. Para exemplificar a utilidade do descarregamento baseado em DTN, Vukadinovic *et al.* [82] propõem um sistema especialmente projetado para distribuição de *podcast*. Os *podcasts* são conteúdos populares e tolerantes a atrasos. Logo, ideais para servirem de estudo de caso do emprego da arquitetura DTN. Os resultados demonstram que a distribuição de conteúdo oportunista é um método eficiente em termos de recursos para aumentar a eficiência e a taxa de transferência da rede, a um custo menor do que a implantação de infraestrutura adicional de rede celular. O Capítulo 3 abordará de uma forma mais detalhada as redes DTNs e o descarregamento de tráfego utilizando redes oportunistas.

2.3 Considerações Finais

Este capítulo apresentou o estado da arte do descarregamento de tráfego, classificou e apresentou alguns trabalhos referentes ao descarregamento de tráfego: sensível ao atraso baseado em AP, sensível ao atraso baseado em D2D, não sensível ao atraso baseado em AP e não sensível ao atraso baseado em D2D. As operadoras de telefonia celular estão particularmente interessadas no desenvolvimento de mecanismos capazes de prever ganhos adicionais proporcionados pela ativação do descarregamento e planejar quanto tráfego podem desviar de sua rede principal. Os desafios futuros incluem o desenvolvimento de novos mecanismos de coordenação e políticas de programação inter-tecnológica para controlar a recuperação de conteúdo entre múltiplas tecnologias de acesso e comunicação D2D.

Capítulo 3

Descarregamento de Tráfego com Redes Oportunistas

Por definição, redes oportunistas são aquelas em que dois nós podem se comunicar mesmo que nunca haja um caminho fim-a-fim entre eles [89]. A ausência de caminhos fim-a-fim fixos em redes sem-fio é comum devido à mobilidade dos nós e à variabilidade da qualidade dos enlaces pelas características do meio de transmissão sem-fio. Se prejudica o estabelecimento de caminhos fim-a-fim, a mobilidade dos nós, entretanto, pode criar caminhos de comunicação oportunistas entre nós. Quando dois nós não adjacentes se movem para o alcance de comunicação um do outro, eles podem se comunicar por meio de uma tecnologia de comunicação de curto alcance, por exemplo, WiFi e Bluetooth. Para aumentar a probabilidade de contatos entre os nós, as redes oportunistas comumente empregam uma arquitetura chamada de Rede Tolerante a Atrasos (*Delay and Disruption Tolerant Network* - DTN) [14], cuja principal característica é assumir que os nós da rede possuem um *buffer* para armazenar mensagens persistentemente. Nesse caso, o preço a se pagar na comunicação oportunista é que a entrega de conteúdo sofrerá um certo atraso aleatório ou tornar tipicamente alto. Assim, as redes oportunistas podem ser usadas para implementar mecanismos de descarregamento de tráfego não sensíveis ao atraso. Outra característica é que não há custo monetário envolvido para os usuários que colaboram na comunicação oportunista. A popularidade do conteúdo também é determinante para o bom funcionamento dos mecanismos de descarregamento. Popularidade significa que o conteúdo é de interesse para muitos usuários. Em outras palavras, o conteúdo é redundante na rede. Este capítulo aborda com mais detalhes o descarregamento de tráfego com redes oportunistas.

3.1 Arquitetura DTN

A arquitetura DTN [13] [14] foi proposta pelo DTNRG (*Delay Tolerant Networking Research Group*) [26], grupo de pesquisa criado pelo o IRTF (*Internet Research Task Force*). O DTNRG descreveu uma proposta de arquitetura para DTNs que é uma evolução da arquitetura do projeto Rede Interplanetária (*Interplanetary Network*– IPN) [13]. As DTNs encaminham as mensagens segundo o paradigma armazena-carrega-e-encaminha (*store-carry-and-forward*) [55]. 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 [28]. Nas DTNs não se pode afirmar que todos os nós são alcançáveis e podem ser contatados a qualquer instante. Essa característica das DTNs contrasta fortemente com o que é assumido para a Internet convencional, que considera que as entidades comunicantes estão sempre alcançáveis.

As DTNs permitem que dois nós consigam se comunicar mesmo que nunca exista um caminho fim-a-fim entre eles, como na definição das redes oportunistas [55]. A existência de um caminho fim-a-fim entre a fonte e destino de uma mensagem é uma das premissas de bom funcionamento da arquitetura TCP/IP usada na Internet. Por este motivo, essa não é uma arquitetura de rede mais indicada para ser usada nas DTNs. Algumas premissas necessárias ao bom funcionamento da arquitetura TCP/IP não são encontradas em determinados ambientes, tornando o perfil de protocolos da Internet inadequado e pouco robusto [27]. Exemplos de tais ambientes são: comunicações sem fio, comunicações entre dispositivos móveis, comunicações entre dispositivos com restrições de energia, comunicações rurais, comunicações em campo de batalha, comunicações submarinas, comunicações interplanetárias etc. Estes ambientes, considerados "desafiadores", possuem em comum a dificuldade de manter uma comunicação fim-a-fim com baixa latência e pequena perda de pacotes [25]. A principal causa para a arquitetura atual da Internet não funcionar bem em tais redes está no modo de operação da pilha de protocolo TCP/IP que não foi projetado para operar nestes cenários [27]. Para o bom funcionamento do serviço provido pelo protocolo TCP é necessário um caminho fim-a-fim entre a fonte e o destino durante todo o período correspondente à sessão de comunicação, atrasos de comunicação relativamente pequenos e baixa taxa de erros.

Nas redes DTNs, quando o nó entra no raio de alcance de outro nó e tem uma oportunidade de encaminhamento, todos os nós encontrados podem ser candidatos a receberem cópias das mensagens carregadas. Portanto, as DTNs dependem da mobilidade e cooperação dos nós para proverem pelo menos caminhos esporádicos para que a informação

possa ser devidamente entregue ao destino baseado em contatos [16].

O contato é um importante conceito que deve ser explicado na arquitetura DTN. Um contato corresponde a uma ocasião favorável para os nós trocarem mensagens. Nestes contatos podem existir falhas, por exemplo o instante de tempo necessário para envio de toda mensagens é maior que o período do contato. Porém, dependendo do tipo de contato, as falhas podem ser mais frequentes, como é o caso dos contatos previsíveis. Oliveira *et al.* [55] classificam os tipos de contatos na arquitetura DTN em:

- persistente: são aqueles que estão sempre disponíveis.
- sob demanda: são aqueles que requerem alguma ação para que sejam instanciados, mas que, uma vez acionados, funcionam como contatos persistentes até serem encerrados.
- programado: são aqueles em que se estabelece uma agenda de contatos pode ser preestabelecida entre dois ou mais nós antes que ocorra a troca de informações, caso horário e a duração de cada contatos previamente entre os nós comunicantes. Assim, exige-se uma sincronização do tempo na rede para que a troca de informações seja realizada com sucesso.
- previsível: são aqueles nos quais os nós podem fazer previsões sobre o horário e a duração dos contatos com base em históricos de contatos previamente realizados. Ao contrário dos contatos programados, os contatos previsíveis possuem certo grau de incerteza do contato.
- oportunistas: são aqueles que ocorrem diante de encontros não previamente programados entre os nós. Esse tipo de contato tem como objetivo obter vantagens de contatos realizados totalmente ao acaso para realizar a comunicação com qualquer nó que esteja fora do alcance de um nó fonte. Assim, utiliza-se a capacidade dos nós se comunicarem localmente com os seus vizinhos para criar possibilidades de comunicação com outros nós que estão fora do alcance. O conceito de contato oportunista permite comunicação entre nós na qual em nenhum momento existe um caminho inteiramente conectado entre eles. Geralmente, os nós que estabelecem contatos oportunistas desconhecem qualquer informação acerca do estado, da localização ou dos padrões de mobilidade dos outros nós.

As redes oportunistas são consideradas uma evolução das MANETs (*Mobile Ad Hoc Network*) e um subcategoria de Redes Tolerantes a Atrasos e Desconexões [69, 90], basea-

das em contatos oportunistas. As redes oportunistas herdam todas as características das DTNs, porém elas exploram a mobilidade e os contatos oportunistas entre os nós como forma de proporcionar a entrega de dados. O descarregamento com redes oportunistas é uma forma de implementar o descarregamento não sensível a atraso baseado em D2D.

3.2 Descarregamento de Tráfego com Redes Oportunistas

O descarregamento de tráfego utilizando redes oportunistas [33, 94] é uma solução promissora para aliviar a sobrecarga da rede celular. A ideia básica do descarregamento de tráfego com redes oportunistas é aproveitar as oportunidades de contato entre os dispositivos móveis para encaminhar conteúdos. Para tanto, um subconjunto de dispositivos (ou nós) desempenham o papel de retransmissores com outros dispositivos e com a infraestrutura. Alguns nós móveis baixam conteúdos populares através da rede celular e transmitem esses conteúdos para outros nós por meio de um canal secundário através da comunicação oportunista. Desta forma, nós podem obter o conteúdo solicitado sem acessar a Internet através do canal secundário, o que ajuda a reduzir significativamente a carga de tráfego na rede celular. O descarregamento oportunista é viável e eficiente devido às seguintes razões [89]:

- Há muitas aplicações, como *podcast*, previsão do tempo, redes sociais, dentre outras, que não possuem requisitos estritos de tempo, ou seja, podem tolerar algum atraso na entrega dos dados. Neste caso, a operadora de celular pode enviar dados para um pequeno número de usuários selecionados, que então encaminham os dados para outros usuários.

- O *download* de conteúdos populares é responsável por uma enorme quantidade de transmissões de dados redundantes na rede. Segundo as estatísticas, 10% dos principais vídeos populares são responsáveis por 80% das visualizações no Youtube [15]. Na verdade, apenas um pequeno subconjunto de nós precisa baixar o conteúdo popular através da rede celular. Outros podem obter o conteúdo desses nós por meio de comunicação oportunista. Em outras palavras, o conteúdo é redundante na rede. Assim, se um grupo de nós estiver interessado no mesmo vídeo, poderá apenas um nó fazer o *download* do vídeo por meio do canal primário e transmitir o conteúdo para outros membros do grupo nas proximidades por meio da comunicação oportunista. Dessa forma, uma grande quantidade de tráfego celular pode ser transferido

através da comunicação oportunista e a eficiência do descarregamento de tráfego se torna muito alta. Por outro lado, se o conteúdo for de interesse para apenas um nó, a eficiência de descarregamento será zero [15].

- O descarregamento oportunista faz sentido econômico - não há quase nenhum custo monetário extra envolvido. Os dados são transmitidos diretamente entre os nós móveis, que descarregam a enorme quantidade de tráfego da rede celular e ajudam a evitar o congestionamento da rede. Logo, o descarregamento oportunista é benéfico para a operadora de celular e o usuário não deve ser cobrado por ela.

Portanto, a eficiência do descarregamento depende da popularidade do conteúdo, ou de seu nível de redundância, e da tolerância do conteúdo ao atraso. De acordo com a direção do fluxo [89], o descarregamento de tráfego pode ser dividido em duas categorias, descarregamento de tráfego *download* e descarregamento *upload*. No descarregamento de tráfego *download*, o operador de celular seleciona um subconjunto de usuários móveis como nós de descarregamento com base em algumas estratégias de seleção e envia o conteúdo a esses nós. Para reduzir a quantidade de tráfego da rede celular, o subconjunto de nós de descarregamento deve ser minimizado. Os nós de descarregamento podem ser escolhidos inicialmente baseados em um critério, tal como, os nós que mais encaminham o conteúdo para outros nós ou que apresentam melhores recursos de bateria e armazenamento. Estes nós encaminham o conteúdo para outros nós através de comunicações com um salto ou vários saltos. A entrega em um salto significa que o nó de descarregamento selecionado pode entregar o conteúdo a um nó diretamente, porque esse nó está dentro do seu raio de alcance. Em contraste, a entrega em múltiplos saltos é necessária, se um nó estiver fora do raio de alcance do nó de descarregamento. Neste caso, nós de retransmissão podem encaminhar o conteúdo para outros nós de retransmissão que podem, eventualmente, entregar o conteúdo ao nó destino por meio do mecanismo armazena-carrega-e-encaminha. No entanto, o modo de um salto deve ser adotado se os nós móveis não cooperarem, ou seja, se os nós não estiverem dispostos a atuar como retransmissores para outros nós. No descarregamento *upload*, os nós móveis com dados para *upload* primeiro entregam os dados aos nós de retransmissão selecionados com base em algumas estratégias. Estes nós de retransmissão, em seguida, carregam os dados e encaminham para outros nós de retransmissão ou para infraestrutura da rede celular. Esta tese analisa somente o descarregamento de tráfego *download*.

3.3 Trabalhos relacionados

Nas redes oportunistas, às vezes é impossível manter rotas fim-a-fim entre os nós devido às constantes mudanças topológicas da rede. Mesmo assim, o uso de nós encaminhadores ou retransmissores possibilita a troca de dados entre nós mesmo não estando eles conectados ao mesmo tempo na rede. Um tema de pesquisa de interesse no descarregamento baseado em redes oportunistas é a seleção destes nós.

Li *et al.* [45] consideram a seleção de um subconjunto ideal de retransmissores como um problema de maximização de utilidade sob múltiplas restrições lineares, como heterogeneidade de tráfego, mobilidade do usuário e armazenamento disponível. O problema de seleção de subconjuntos é NP-difícil, similarmente ao caso do problema mínimo de seleção de conjunto de APs estudado por Trestian *et al.* [79]. Ambos os trabalhos propõem algoritmos de seleção gulosa para identificar um conjunto de metas abaixo do ideal. Um ponto em comum para todas as estratégias de seleção de subconjuntos é que o provedor de rede deve ser capaz de coletar informações sobre as taxas de contato do nó para calcular o melhor subconjunto.

Barbera *et al.* [7, 8] aproveitam os atributos sociais de nós móveis para selecionar nós móveis socialmente importantes como nós de descarregamento. Os autores constroem um grafo social de nós móveis em uma determinada área durante um certo período de observação e analisam as características dos contatos entre os nós e os padrões de mobilidade. Eles calculam os valores dos atributos sociais para quantificar a importância de cada nó móvel na área com a ajuda do grafo social. A importância dos usuários dentro da rede é dada em termos de atributos sociais bem conhecidos, tais como centralidade (intermediação, grau e proximidade) e *PageRank*. O grafo social pode ser dividido em várias comunidades através da aplicação do algoritmo *k-clique*. Dois algoritmos gulosos diferentes são propostos para selecionar os nós móveis socialmente importantes como VIPs, que desempenham o papel de "ponte" entre a rede celular e os usuários móveis em todas as comunidades [8]. Os VIPs são os nós retransmissores escolhidos com base em métricas sociais. Desta forma, os VIPs replicam oportunisticamente dados recebidos da infraestrutura para outros nós.

Wang *et al.* [85] também propõem construir um grafo social, no entanto usam dados de aplicações de redes sociais para quantificar a importância dos nós. Especificamente, eles aproveitam o impacto do espalhamento *on-line* e o padrão de mobilidade *off-line* para selecionar um subconjunto de nós de descarregamento para baixar conteúdo diretamente

da rede celular e compartilhar o conteúdo com outros nós solicitantes nas proximidades.

Zhigang *et al.* [92] propõem o algoritmo *NodeRank* para selecionar o subconjunto de nós de descarregamento baseado nas características temporais e espaciais da mobilidade humana. O objetivo desse esquema de descarregamento é maximizar o número de nós que obtêm o conteúdo solicitado por meio da rede oportunista. O *NodeRank* constrói um grafo de contatos baseado em informações do histórico de contatos e calcula a importância de cada nó no grafo. O *NodeRank* não só leva em conta as taxas de contato entre nós móveis, mas também a duração do contato e o tempo entre contatos para garantir a entrega do conteúdo. Wenxiang *et al.* [24] também estudam a questão da escolha dos nós de descarregamento com base em atributos sociais.

Peng *et al.* [59] propõem descarregar o tráfego da rede celular através do grau de proximidade, considerando a importância topológica do usuário e a agregação de interesse. A importância de um nó é calculada com base na centralidade de intermediação e o interesse agregado de um nó para um conteúdo é estimado com base na demanda pelo conteúdo pelo nó e seus vizinhos. Uma equação é dada para calcular a probabilidade de cada nó adicionar a seleção de nós de descarregamento. Quando um nó solicita um conteúdo, o *download* através da rede celular ou rede oportunista não começa imediatamente. Em vez disso, o nó decide primeiro se deseja baixar o conteúdo através da rede celular ou através da rede oportunista de acordo com essa equação de probabilidade. Se o nó fizer o *download* do conteúdo através da rede celular, ele se tornará um nó de descarregamento para infectar outros nós interessados de maneira epidêmica.

Mota *et al.* [50] propõem o OppLite um algoritmo baseado em múltiplos critérios, incluindo o número de vizinhos, nível de bateria e qualidade do canal, para selecionar os nós de descarregamento. O OppLite considera a disposição do usuário para se tornar um retransmissor ou um nó oportunista com base em um conjunto de propriedades das redes e dos dispositivos. Especificamente, uma função de utilidade multicritério é usada para decidir se um nó deve obter o conteúdo solicitado através da rede celular ou via rede oportunista, bem como se um nó pode ser selecionado como nó de descarregamento ou não.

Vigneri *et al.* [81] propõem transformar veículos em nós de descarregamento que podem baixar conteúdo popular e transmitir o conteúdo para outros usuários solicitantes quando eles estão passando por eles. Nesta arquitetura, existem três tipos de nós: nó de infraestrutura, nó de nuvem e nó móvel. Nós de infraestrutura são estações base. Os nós da nuvem são veículos, como táxis e ônibus, que são nós de descarregamento pré-

determinados. Nós móveis são usuários comuns com *smartphones*. Os nós da nuvem baixam conteúdo popular dos nós de infraestrutura por meio do canal celular. Um nó móvel pode enviar uma solicitação ao nó da nuvem próximo. Se o nó da nuvem contiver o conteúdo solicitado no *cache*, o nó solicitante poderá baixar o conteúdo por meio da técnica de comunicação de curto alcance. Caso contrário, o nó móvel pode aguardar outro nó da nuvem. Quando o prazo é passado, o nó solicitante deve obter o conteúdo via canal celular.

Han *et al.* [33] estudam o problema de selecionar nós de descarregamento para melhorar a eficiência do descarregamento de tráfego nas redes celulares. Eles também projetam o Opp-Off [34], um protótipo implantado nos *smartphones* para demonstrar a viabilidade da comunicação oportunista usando o Bluetooth para transmitir conteúdo. Han *et al.* [35] propõem a rede de entrega avançada metropolitana (MADNet) para estudar o problema de descarregamento na área metropolitana com a cooperação de redes celulares, WiFi e oportunistas. Eles adotam uma abordagem de seleção de nós retransmissores que escolhem os nós de descarregamento baseados nas probabilidades de contato entre nós móveis.

Wang *et al.* [84] projetam um esquema de descarregamento aprimorado. Nesse esquema, além de selecionar os nós de descarregamento, eles também selecionam os retransmissores com maior probabilidade de encontrar nós de assinantes do que os de descarregamento. Além disso, existem dois tipos de nós de descarregamento, nós de descarregamento móveis e nós de descarregamento fixos. Ao solicitar um conteúdo, o nó de assinante ou a operadora de celular pode indicar vários retransmissores para ajudar. Um nó retransmissor faz o *download* do conteúdo solicitado de um nó de descargamento por meio do canal secundário quando eles se encontram. Quando o nó do assinante encontra um nó de descarregamento ou retransmissor que possui o conteúdo, o conteúdo é encaminhado para o nó do assinante por meio do canal secundário por meio da comunicação D2D. Se o nó do assinante não quiser esperar, ele poderá optar por obter o conteúdo por meio do canal primário. Ao receber o conteúdo solicitado, o nó do assinante precisa enviar uma notificação para os nós retransmissores selecionados para que eles parem de encaminhar o conteúdo que acaba de ser entregue. Os nós de descargamento móvel podem ser encorajados a compartilhar seus recursos por um mecanismo de incentivo [93, 49], e os nós de descarregamento fixo são fornecidos pela operadora.

Chuang *et al.* [20] selecionam os nós de descarregamento com base nas probabilidades de encontro dos nós com comunidades sociais disjuntas. O esquema proposto base-

ado na comunidade melhora a quantidade de tráfego celular descarregado em até 29%. Além disso, os usuários experimentam uma latência significativamente menor. Cheng *et al.* [18] projetam um esquema de reconhecimento de preferências, chamado PrefCast. Esse esquema considera a heterogeneidade de preferência dos usuários, que leva em conta conjuntamente os problemas de seleção de nós de transferência e encaminhamento. O PrefCast, de acordo com a estrutura da comunidade e a preferência do usuário, seleciona os nós de descarregamento, calculando o utilidade para cada nó e selecionando os principais nós com os valores de utilidade mais altos como nós de descarregamento.

Proulx *et al.* [62] propõem pré-carregar o tráfego celular para aliviar o pico de tráfego da rede celular. Eles aproveitam a rede social para prever a demanda de tráfego e fazer o pré-carregamento do tráfego para um subconjunto de nós de descarregamento. Com este pré-carregamento, nós de transferência podem transmitir o conteúdo para outros nós interessados através de rede oportunista para minimizar o uso da rede celular durante o horário de pico. A seleção de nós de descarregamento é baseada em um algoritmo guloso. Da mesma forma, os nós podem armazenar proativamente o conteúdo para os vizinhos, como proposto por Gu *et al.* [32, 31].

Radu *et al.* [65] propõem um mecanismo de detecção de nós egoístas para redes móveis *Ad Hoc* e DTNs, usam uma abordagem colaborativa para detectar nós egoístas e espalhar estas informações na rede. Em tal abordagem, se um nó detectou previamente um nó egoísta, transmite esta informação para os outros nós encontrados. Afirmam que o problema em tais redes é como decidir qual o próximo salto, uma vez que os nós não têm uma visão global da rede. Propõem usar as informações da rede social de um nó ao executar o encaminhamento, pois é mais provável que um nó encontre membros de sua própria comunidade social do que outros nós. Além disso, mostram que pode prever seu comportamento futuro com base no histórico de contato.

Wenjie *et al.* [86] apresentam uma abordagem totalmente distribuída que permite que cada nó DTN identifique rapidamente que outros nós estão produzindo dados com falha. A presença de nós maliciosos, que tentam perturbar o processo de detecção de nós egoístas, também é levado em conta. As taxas de detecção e alarme falso são estimadas comparando os resultados teóricos e de simulação. Os resultados numéricos avaliam a eficácia da solução proposta e podem ser usados para fornecer diretrizes para o projeto do algoritmo.

Em [19] é proposto um mecanismo de incentivo baseado em créditos. A principal contribuição é o fato do mecanismo não utilizar um banco virtual para a distribuição os

créditos (recompensa pelo encaminhamento das mensagens), mas sim uma abordagem descentralizada. Além disso, foi proposta uma modelagem matemática para representar a cobrança e distribuição de créditos buscando evitar ataques do tipo *Edge Insertion*, em determinados casos. Por fim, o mecanismo proposto foi avaliado através de simulação, utilizando *traces* reais de mobilidade e diferentes protocolos de roteamento, e comparado seu desempenho com o mecanismo de incentivo RELICS [80]. Com base nos resultados obtidos pode-se dizer que o mecanismo proposto é promissor no sentido de diminuir a ocorrência de nós egoístas. Mecanismos de incentivo são cada vez mais necessários em redes oportunistas que contém nós com o comportamento egoísta. Para isso, existem mecanismos baseados em crédito mas, que necessitam de uma banco virtual (entidade central) para promover o incentivo. Entretanto, a existência desta entidade central em uma rede oportunista pode ser possível no descarregamento de tráfego com redes oportunista, pois nesta rede existe uma entidade central da rede móvel.

Moreira *et al.* [48] propõem uma arquitetura de detecção de nós egoístas utilizando um modelo de reputação para redes oportunistas, que possibilita aos nós da rede atestarem a integridade do comportamento dos nós. Esse mecanismo viabiliza atribuir mais pontuação para os nós que cooperam com a rede. Além disso, utilizam uma metologia de agrupamento, também conhecida como *clustering* para realizar a classificação dos nós em egoístas ou não egoístas. Assim, não precisa de informações sobre um nó até que a reputação desse nó ultrapasse certo limiar. Desse modo demonstram que é preciso muito menos informações adquiridas para realizar a classificação dos nós.

Souza *et al.* [74] descrevem um algoritmo leva em consideração o egoísmo dos nós para decidir que mensagem descartar do *buffer*. A força da amizade entre dois nós, preponderante para essa decisão, é classificada utilizando-se uma técnica de aprendizagem de máquina. Para melhorar a qualidade dessa classificação, utiliza-se como dados de treinamento características de amizades extraídas de um experimento realizado por pesquisadores do MIT com usuários do campus universitário. Para validar o algoritmo proposto, um conjunto de experimentos considerando métricas relacionadas à entrega de mensagens na rede foi realizado em dois cenários de mobilidade real: Cambridge e Reality. Apesar de se levantarem algumas hipóteses negativas com relação ao uso do egoísmo no gerenciamento do *buffer* para DTNs, os resultados obtidos indicam que em ambos os cenários, o desempenho do algoritmo proposto mostrou-se muito promissor e inclusive superou outros algoritmos de gerenciamento existentes na literatura em termos da taxa de entrega e do atraso médio de entrega, além de obter um valor razoável de média de saltos.

Mota *et al.* [49] propõem um mecanismo de incentivo que constrói uma tabela de reputação baseada na fonte das mensagens recebidas por nós intermediários, batizado de MINEIRO (*Message-based INcentive mechanism for End-user Improvement of Routing Opportunities*). Observa-se que a rede suporta até 60% de nós com comportamento egoísta sem degradação de desempenho em um cenário de mobilidade aleatório. Após esse limite, MINEIRO manteve a taxa de entrega de mensagens e o atraso constante. Enquanto isso, em um cenário com mobilidade baseada em modelos sociais, o comportamento egoísta degrada o desempenho da rede rapidamente.

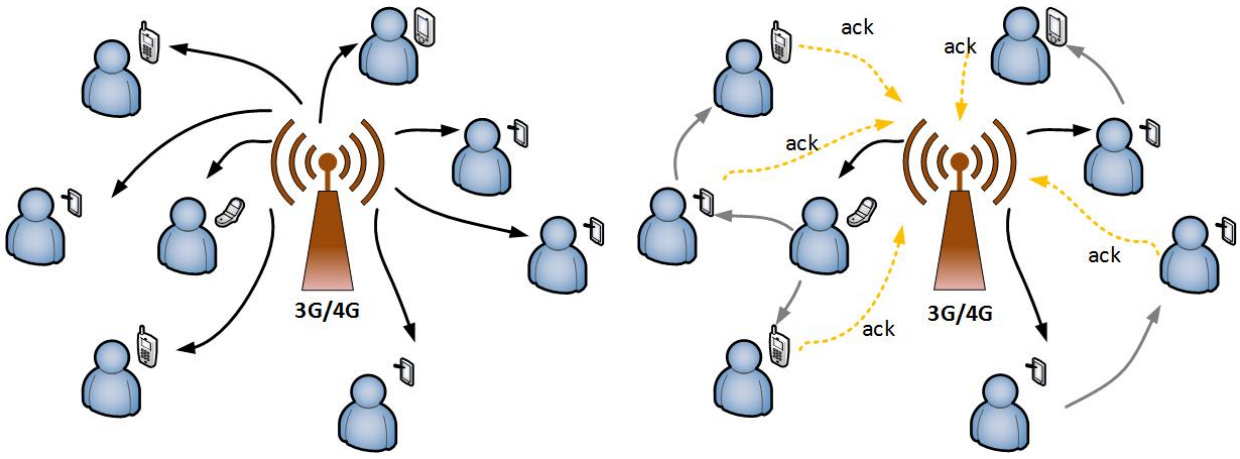
Liu *et al.* [47] também introduzem um mecanismo de descarregamento de tráfego que usa redes oportunistas. Os autores definem uma política para selecionar o número de réplicas iniciais e uma política para distribuir as réplicas iniciais limitadas sob a influência de comportamentos egoístas. Theja *et al.* [77] também avaliaram o impacto de nós não cooperativos, ou seja, nós que não encaminham mensagens para outros nós, no tempo de vida das mensagens. Nestas propostas, entretanto, os autores não analisaram o impacto dos nós egoístas na eficiência do descarregamento de tráfego. O enfoque era o aumento do tempo médio da entrega das mensagens.

Em alguns trabalhos consideração a falsificação de reconhecimentos positivos, nós egoístas enviam reconhecimentos positivos falsificados com o objetivo de expurgar da rede mensagens que ainda não chegaram ao destino, impactando negativamente na taxa de entrega média da rede. De acordo com Li *et al.* [42], ao forjar métricas e distribuí-las aos demais nós da rede com os quais um nó egoísta faz contato, com o objetivo de atrair um maior número de pacotes para ele, este nó egoísta, pode descartar estes pacotes ou utilizá-los para iniciar outros ataques mais sofisticados. Como exemplo é mencionado que após atrair os pacotes um nó poderia disseminar reconhecimentos positivos falsificados, realizando um ataque de falsificação de reconhecimentos positivos. Em Burgess*et al.* [12] avaliaram o ataque de falsificação de reconhecimentos positivos em redes oportunistas. Os autores propuseram uma contramedida, onde as mensagens são encaminhadas de nós próximos a fonte até nós próximos ao destino. Por sua vez, os reconhecimentos positivos percorrem o caminho contrário e são encaminhados de nós próximo ao destino até nós próximos a fonte. Com a contramedida, nós somente aceitarão um reconhecimento positivo como legítimo se já tiverem recebido a mensagem para qual este reconhecimento positivo foi gerado. Através de simulações, os autores demonstram que a contramedida é efetiva contra o ataque de falsificação de reconhecimentos positivos. Naves *et al.* [52, 53] também avaliaram o ataque de falsificação de reconhecimentos positivos (ACKs) em redes oportunistas. 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 trabalho 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 que os nós não cooperam com o encaminhamento das mensagens.

3.4 *Push-and-Track*

Uma das propostas de mecanismos de descarregamento de tráfego que usam redes oportunistas é o *framework Push-and-Track* (PnT) [87, 88]. A principal característica do PnT é garantir a entrega de todas as mensagens mesmo usando uma rede oportunista para aliviar a carga da infraestrutura de rede celular. A Figura 3.1 compara os modos de operação simplificados de uma rede celular na qual somente a infraestrutura entrega as mensagens e com o *Push-and-Track* funcionando. Na Figura 3.1(a), a infraestrutura envia uma cópia da mensagem diretamente para cada um dos nós da rede interessados no mesmo conteúdo. Sem o PnT, portanto, a infraestrutura envia oito cópias da mensagem. Logo, a carga da rede está relacionada com o número de nós interessados nesse conteúdo. Na Figura 3.1(b), com o PnT, a infraestrutura envia um número de cópias iniciais para alguns nós da rede, três no caso do exemplo, e espera a difusão da mensagem através da comunicação oportunista. Cada nó ao receber a mensagem 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 3.1: Modos de Operação: sem e como o *Push-and-Track*.

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 a função objetivo como uma métrica predefinida que deve ser atendida no processo de divulgação da mensagem através da comunicação oportunista. A taxa de infecção corresponde ao número de nós que receberam a mensagem até um dado instante de tempo e é calculada pelo número de ACKs recebidos pela infraestrutura. Em intervalos de tempo curtos, o PnT compara a função objetivo com a taxa de infecção. Caso a taxa de infecção seja menor do que a função objetivo, a infraestrutura envia cópias da mensagem pelo canal primário para outros nós que ainda não receberam o conteúdo para acelerar a disseminação. Os resultados apresentados mostraram uma alta eficiência do descarregamento com o PnT.

A Figura 3.2 apresenta a evolução da taxa de infecção sobre o percentual do tempo de vida da mensagem. Primeiramente, apresenta um comparativo com a infraestrutura enviando apenas 1 mensagem, 10 mensagens e 100% da mensagens. O PnT apresenta alguns funções objetivos com características diferentes. Whitbeck *et al.* [87, 88] 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 Linear, Quadratic*) e funções com taxas mais rápidas (*Fast Linear, Square Root*). A função objetivo *Slow Linear* é dada pela seguinte expressão $\frac{x}{2}$, se $t < TTL/2$; $\frac{3x}{2} - \frac{1}{2}$, se $t \geq TTL/2$. Os valores de x são encontrados através da divisão do tempo atual t pelo o tempo de vida da mensagem (TTL) [88]. A função *Fast Linear* é dada por $\frac{3x}{2}$, se $t < TTL/2$; $\frac{x}{2} + \frac{1}{2}$, se $t \geq TTL/2$. A função *Quadratic* é $\sqrt{x}$ e a função *Square Root* é x^2.

Para tomar a decisão para quais nós enviar novas cópias, pode-se utilizar estratégias aleatórias, baseadas no tempo de permanência, localização e conectividade [87, 88]. 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

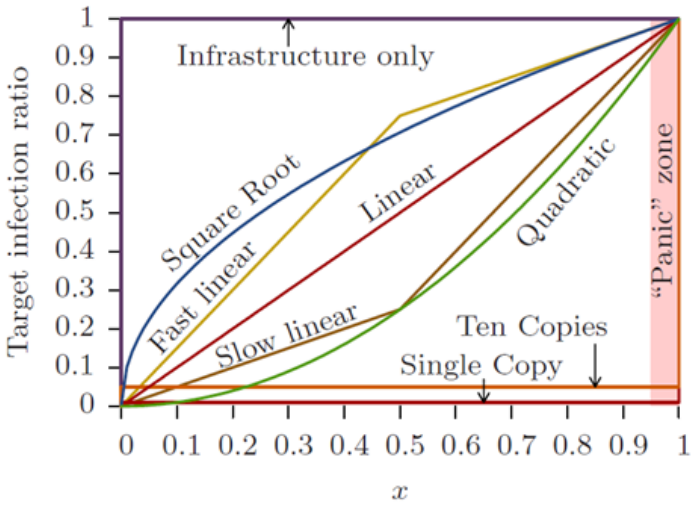


Figura 3.2: Função Objetivo do *Push-and-Track [87, 88].*

de um intervalo máximo de tempo, o PnT define uma zona de pânico (Figura 3.2). 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 de 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.

Rebecchi *et al.* propõem modificações na proposta de descarregamento de tráfego com o *Push-and-Track* e denominam essa nova versão do mecanismo como *Droid (Derivative Re-injection to Offload Data)* [66]. Basicamente, os autores definem uma nova função objetivo, que evita períodos de planalto, ou seja, momentos em que a taxa de infecção mantém-se constante e superior à função objetivo. Portanto, também não analisam o comportamento dos nós egoístas no desempenho da proposta, assim como no trabalho original do PnT.

3.5 Considerações Finais

O desempenho de um esquema de descarregamento baseado em redes oportunistas pode depender amplamente da seleção de nós de descarregamento. O número de nós de

descarregamento deve ser pequeno para reduzir a carga na rede celular. Mas um número muito pequeno de nós de descarregamento poderá resultar em baixa eficiência de descarregamento. Portanto, o número de nós de descarregamento é uma compensação entre esses dois requisitos conflitantes. Que tipo de informação usada para selecionar o nó de descarregamento também é importante para o desempenho de descarregamento possível. Na literatura, muitas pesquisas se concentram em utilizar o padrão de encontro entre nós móveis e outras métricas, como energia, justiça e etc. Por outro lado, adotar um salto ou salto múltiplo para distribuir o conteúdo influencia o desempenho alcançável de um esquema de descarregamento. Usar um salto é muito conservador, pois não pode explorar todo o potencial das comunicações oportunistas. Usar múltiplos saltos, enquanto explora melhor as comunicações oportunistas, pode não ser realista, pois alguns nós podem não estar dispostos a agir como retransmissores. Muitas pesquisas estudam os comportamentos humanos e investigam como incentivar os nós móveis, isto é, os seres humanos, a participar no encaminhamento de conteúdo para outros nós. Essa direção de pesquisa tem um grande potencial para melhorar o desempenho de descarregamento.

Capítulo 4

Avaliação do Comportamento Egoísta dos Nós: Um Estudo de Caso

Whitbeck *et al.* [87, 88] mostram uma alta eficiência do descarregamento de tráfego com o PnT. Porém, tais resultados são obtidos em um cenário perfeito, no qual todos os nós cooperam com a comunicação oportunista e não existe falha ou perda no envio das mensagens de reconhecimento positivo para a infraestrutura. Na prática, os nós podem apresentar comportamento egoísta não encaminhando mensagens para outros nós. Isso pode acontecer simplesmente 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. Este capítulo apresenta um estudo de caso no qual é analisada a influência destes comportamentos egoístas no desempenho do descarregamento de tráfego com o PnT.

4.1 Modelos de Ataque e Falha

No estudo de caso, são considerados comportamentos egoístas e falha de comunicação dos nós, por simplificação define em ambos cenários os nós de egoístas:

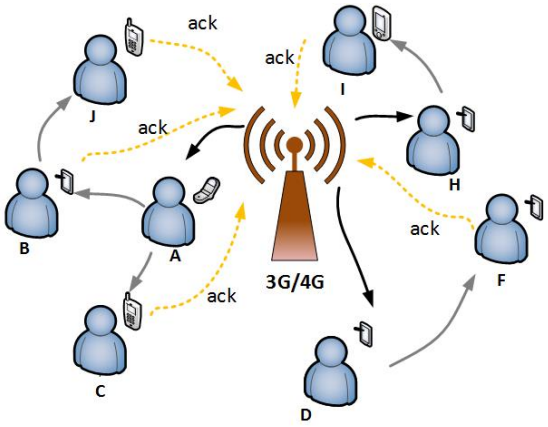
- Cenário de falha ao enviar ACKs, no qual nós recebem as mensagens através da rede oportunista, mas não enviam ACKs para a infraestrutura pelo motivo ocorrer uma falha na comunicação dos nós ou perda da mensagem de confirmação;
- Ataque de não encaminhamento, no qual nós egoístas recebem as mensagens da infraestrutura ou da rede oportunista, mas não encaminham as mensagens para outros nós;

- Ataque combinado, no qual nós egoístas recebem as mensagens da infraestrutura ou da rede oportunista, mas não encaminham as mensagens para outros nós e/ou não enviam ACKs para a infraestrutura pelo motivo de uma falha na comunicação ou perda de confirmação.

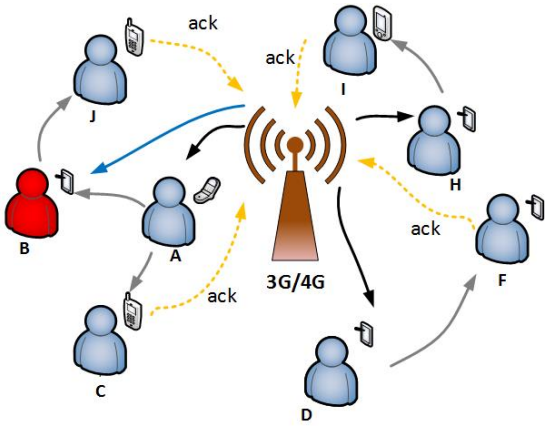
No cenário de falha ao enviar ACKs, a infraestrutura não recebe ACKs de alguns nós, assim não terá controle dos nós que receberam as mensagens através da comunicação oportunista. Na Figura 4.1(b), o nó B apresenta uma falha na comunicação no envio do ACK. B recebe a mensagem através do contato oportunista com o nó A, porém a infraestrutura não recebe o ACK pelo motivo de ter ocorrido uma falha na comunicação ou perda da mensagem. Este cenário 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 cenário a comunicação oportunista não é prejudicada, porque os nós apenas não enviam mensagens de reconhecimento positivo por motivo de falha. Por exemplo, na Figura 4.1(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 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 4.1(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.

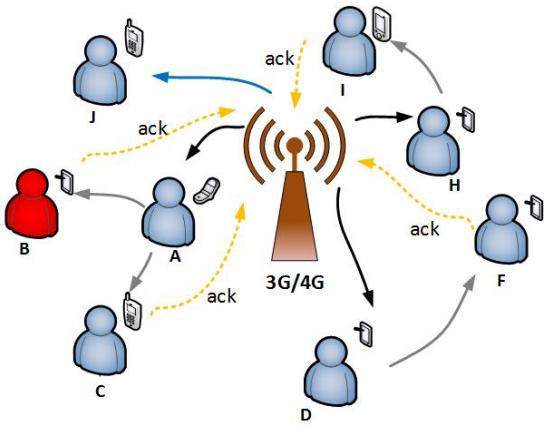
O ataque com a combinação dos comportamentos do cenário de falha e não encaminhamento aumenta a probabilidade de reenvio de cópias desnecessárias e, assim, diminui



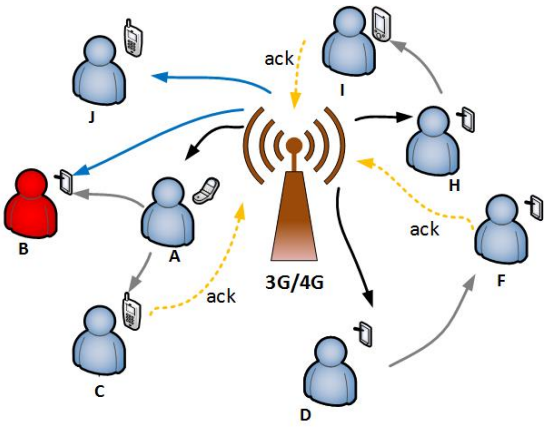
(a) Sem nós egoístas e perda de ACK.



(b) Nó B não envia ACKs por motivo de falha.



(c) Nó egoísta B não encaminha mensagens.



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

Figura 4.1: Comportamento dos nós egoístas e cenário de falha.

a eficiência da utilização do PnT para aliviar a carga de tráfego da infraestrutura. Na Figura 4.1(d), o nó B não encaminha mensagem para o nó J e falha ao 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. Percebem-se os prejuízos causados por esse comportamento quando se comparam as Figuras 4.1(a) e 4.1(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.

4.2 Cenário de Avaliação: Rollernet

O impacto dos nós egoístas no descarregamento de tráfego com 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 [87]. Esse simulador

é uma adaptação do ONE (*Opportunistic Network Environment*) [40]. Para analisar o comportamento dos nós egoístas e o cenário de falha, foi necessário modificar algumas classes do simulador para que nós da rede apresentassem um dos comportamentos egoístas descritos na seção 4.1. Assim, nós falham ao enviar ACKs ao receberem a mensagem através da comunicação oportunista e/ou não encaminham 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 [10]. 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 [87]. Durante um contato, a taxa de transferência do canal secundário 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. O algoritmo de roteamento utilizado em todas as simulações é o epidêmico [38]. Considera-se o tempo de vida das mensagens (TTL) igual a 120 s. Novas mensagens de dados são geradas com intervalo de 130 s e são do interesse de todos os nós. 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.* [87, 88] 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.

O objetivo dos experimentos é mostrar que a presença de nós que não encaminham mensagens e que apresentam falha no envio do ACK na rede reduz a eficiência do descar-

regamento de tráfego, independentemente da função objetivo empregada pelo PnT. Cada comportamento egoísta descrito na seção 4.1 é analisado para três funções objetivos: *Fast Linear*, *Slow Linear* e adaptativa. A função objetivo *Slow Linear* apresenta como métrica a difusão de um número menor das cópias da mensagem entregues na primeira metade do tempo de vida da mensagem e com a função *Fast Linear* ocorre o contrário, expectativa de difusão da mensagem entre os nós maior na primeira metade do tempo de vida da mensagem, na seção 3.4 apresenta com mais detalhes as funções objetivos. A função adaptativa proposta por Rebecchi *et al.* [66] 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. Para cada configuração são executadas 10 rodadas de simulação. Em cada rodada, sorteia-se um novo conjunto de nós egoístas.

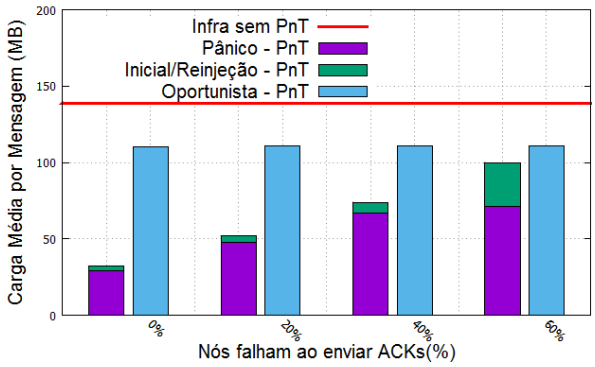
4.2.1 Cenário 1: Falha no envio de reconhecimentos positivos (ACKs)

Neste primeiro cenário, avalia-se o cenário de falha no envio de ACKs ou seja, nós recebem e encaminham mensagens para outros nós de forma oportunista, mas não enviam ACKs para a infraestrutura, por alguma falha na comunicação ou perda dos ACKs. 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, esta falha diminui a eficiência do sistema de controle do PnT.

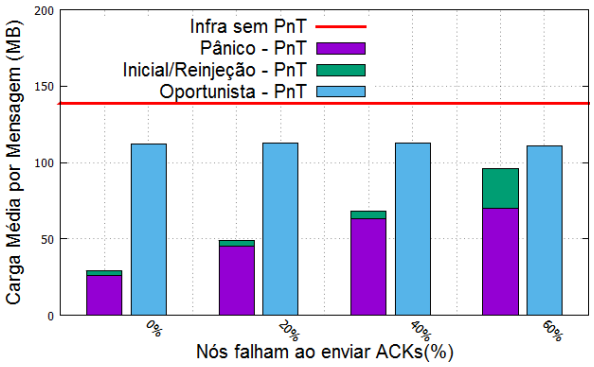
Cada grupo de barras da Figura 4.2 representa a carga de tráfego média necessária para entregar uma mensagem para todos os nós considerando percentuais específicos de nós egoístas. A linha de cor vermelha representa a carga média sem utilização de qualquer mecanismo de descarregamento. A barra de cor 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 média da carga 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 4.2 que a carga média por mensagem da comunicação oportunista mantém-se em aproximadamente 110 MB com o aumento dos nós que falham ao ACKs em todos os cenários, mesmo utilizando funções objetivo

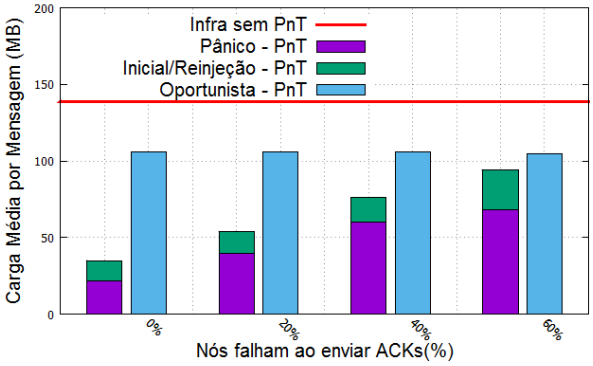
diferentes. A carga de tráfego da comunicação oportunista não é afetada com o aumento do número de nós que não enviam ACKs pelo motivo de falha ou perda de ACKs, uma vez que nesse cenário os nós continuam a encaminhar mensagens para outros nós quando há um contato.



(a) Função Objetivo *Slow Linear*.



(b) Função Objetivo *Fast Linear*.



(c) Função Objetivo Adaptativa.

Figura 4.2: Carga de tráfego quando acontece falha no envio de ACKs.

Conforme aumenta o percentual de nós que falham ao enviar ACKs, 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 4.2(a) que a carga de tráfego é de 32 MB quando não existem perdas de ACKs. Com 20% de nós que não enviam ACKs, a carga cresce para 52 MB e chega 74 MB com 40% de nós que falham no envio de ACKs, ocorre um aumento maior que 100% da carga, indicada pela barra roxa e verde. Mesmo utilizando funções objetivos diferentes (Figuras 4.2(b) e 4.2(c)), o desempenho do descarregamento de tráfego sofreu praticamente o mesmo impacto com o aumento do percentual de nós que falham. No entanto, é importante ressaltar que mesmo com 60% dos nós da rede não enviando ACKs a carga de tráfego da infraestrutura com o PnT foi 100 MB, aproximadamente 40 MB menor do que a infraestrutura sem PnT. Ou seja, mesmo na presença de um percentual muito alto de nós que falham no envio de ACKs o

PnT conseguiu descarregar aproximadamente 28% do tráfego da rede.

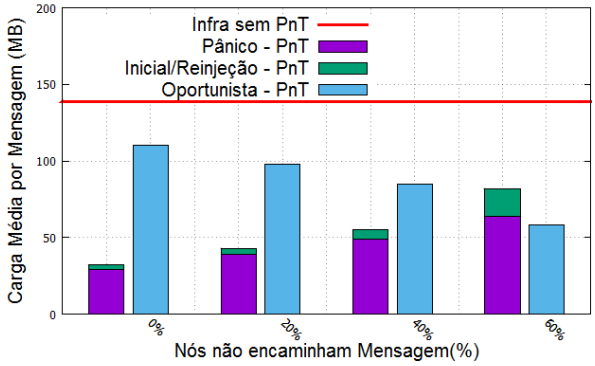
No cenário de falha no envio de ACKs aumenta a carga da infraestrutura com o PnT por dois motivos. O sistema de controle é prejudicado porque os nós falham ao enviar ACKs ao receberem a mensagem através da comunicação oportunista. Assim, a infraestrutura calcula a taxa de infecção com um valor inferior 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.

4.2.2 Cenário 2: Nós egoístas não encaminham mensagens

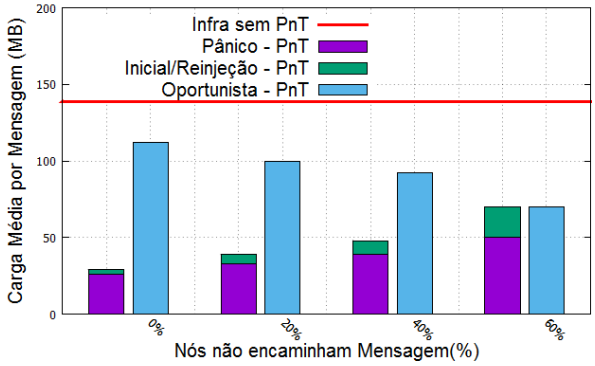
No segundo cenário avalia-se o ataque de não encaminhamento, ou seja, nós egoístas recebem mensagens pelo canal primário e pelo secundário e não as encaminham para outros nós prejudicando assim a comunicação oportunista entre os nós.

A carga de tráfego gerada na comunicação oportunista no ataque de não encaminhamento difere da carga gerada no cenário de falha no envio de ACKs. Observa-se na Figura 4.3 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, indicada pelas barras azuis, diminui aproximadamente para 58 MB (*Slow Linear*), 70 MB (*Fast Linear*) e 67 MB (adaptativa). No Cenário 1, mesmo com nós que falham ao enviar ACKs, os nós continuam a encaminhar as mensagens na oportunidade de contato. Para todos os experimentos no Cenário 1, a carga de tráfego da comunicação oportunista é de aproximadamente 110 MB.

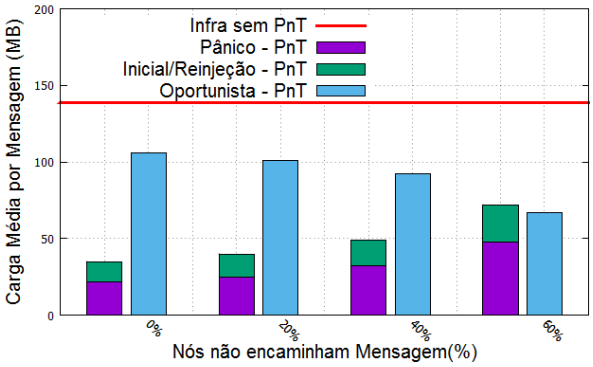
Com o aumento do número de nós egoístas, a carga da infraestrutura com o PnT cresce para todas as funções objetivo analisadas. Assim, diminui-se a eficiência do descarregamento. Com 20% de nós que não encaminham mensagens, a carga aumenta, representada pelas barras roxas e verdes, para 42 MB, 39 MB e 40 MB, com 40% aumenta para 55 MB, 48 MB e 49 MB para as funções *Slow Linear*, *Fast Linear* 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 Linear* (Figura 4.3(a))



(a) Função objetivo *Slow Linear*.



(b) Função objetivo *Fast Linear*.



(c) Função objetivo adaptativa.

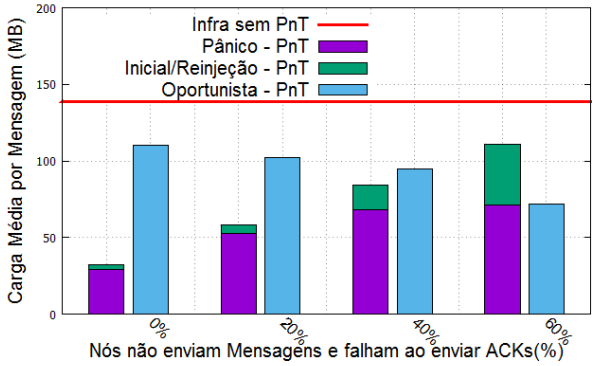
Figura 4.3: Carga de tráfego para o ataque de não encaminhamento.

é maior do que com as outras funções objetivo. Os valores da função objetivo *Slow Linear* 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 Linear* (Figura 4.3(b)). Em outras palavras, a função objetivo *Slow Linear* 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 4.3(c), apresentou resultados semelhantes aos da função objetivo *Fast Linear*.

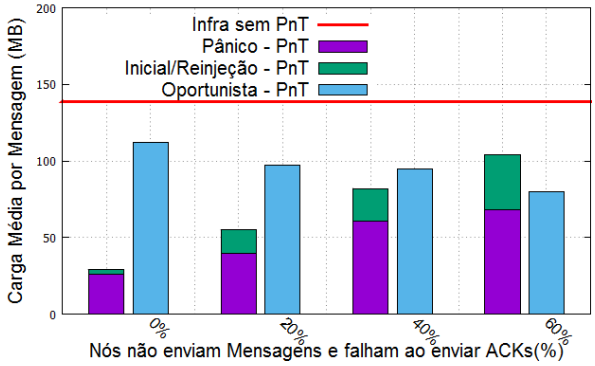
Comparando as cargas de tráfego da infraestrutura com PnT apresentados nos Cenários 1 e 2, observa-se que o ataque de não encaminhamento foi menos prejudicial para o desempenho do descarregamento de tráfego. Devido à infraestrutura com o *Push-and-Track* não ter o controle de quais e quantos nós receberam a mensagem, provocando reenvio de cópias desnecessárias na fase de reinjeção e na zona de pânico, com aumento do percentual dos nós que falham ao enviar ACKs.

4.2.3 Cenário 3: Nós egoístas não encaminham mensagens e/ou falham no envio de reconhecimentos positivos

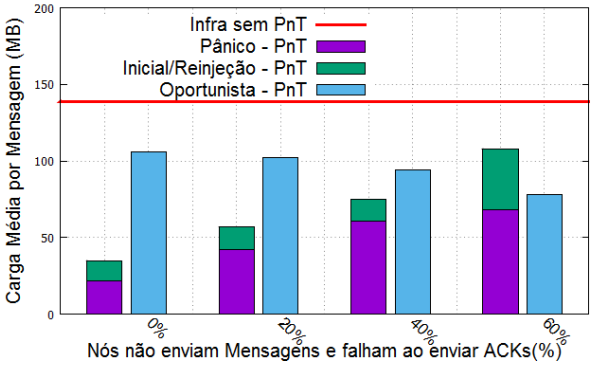
Neste cenário é analisada a influência do ataque combinado, ou seja, quando nós egoístas não encaminham mensagens e/ou falha ao enviar ACKs para a infraestrutura. Nota-se na Figura 4.4 que com o aumento do percentual de nós egoístas na rede, a carga de tráfego da infraestrutura com o *Push-and-Track* aumenta consideravelmente, reduzindo a eficiência do descarregamento de tráfego. Observa-se na Figura 4.4(b) que com 60% de nós egoístas, a carga gerada pela infraestrutura com o PnT é de 104 MB, barra roxa e verde. No Cenário 1, utilizando a função objetivo *Fast Linear* e com 60% de nós que não enviam ACKs, a carga da infraestrutura com o PnT é de 96 MB. Com o mesmo percentual de nós que não encaminham mensagens (Cenário 2) a carga é de 70 MB.



(a) Função objetivo *Slow Linear*.



(b) Função objetivo *Fast Linear*.



(c) Função objetivo adaptativa.

Figura 4.4: 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, a falha no envio de reconhecimentos positivos prejudica o cálculo da taxa de infecção, o que causará maior reenvio de cópias da mensagem de forma

Tabela 4.1: Eficiência do descarregamento de tráfego para os três ataques analisados.

		Funções Objetivos		
		Slow Linear	*Fast Linear*	Adaptive
Cenário 1	0%	77%	79%	74%
	20%	62%	64%	61%
	40%	46%	51%	45%
	60%	28%	30%	32%
Cenário 2	0%	77%	79%	74%
	20%	69%	71%	71%
	40%	60%	65%	64%
	60%	41%	49%	48%
Cenário 3	0%	77%	79%	74%
	20%	58%	60%	58%
	40%	39%	41%	46%
	60%	19%	25%	22%

desnecessária 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 dos ACKs, como ocorre no Cenário 1.

A Tabela 4.1 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 Linear*. Em todos os cenários avaliados a taxa de entrega das mensagens foi de 100% característica garantida pelo modo de funcionamento do PnT ao entrar em zona de pânico.

4.3 Considerações Finais

Neste capítulo, 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, falham no envio de reconhecimentos positivos para infraestrutura ou combinam esses dois comportamentos. O desempenho do PnT foi avaliado para três funções objetivo diferentes: *Slow Linear, Fast Linear* e adaptativa.

Os resultados mostraram que quando 40% de nós que falham ao enviar ACKs para a infraestrutura, houve um aumento na carga da infraestrutura com o PnT de aproximadamente 100% 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 cenário de falha no envio de ACKs. Isso porque com aumento do percentual dos nós que falham no envio 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 77% para 19%.

Capítulo 5

Contramedidas

Os resultados apresentados no capítulo anterior motivam propostas de contramedidas para o cenário de falha ao enviar ACKs para a infraestrutura e para ataques de não encaminhamento e combinado. A eficiência do descarregamento é extremamente degradada quando 40% dos nós falham ao enviar ACKs para a infraestrutura. Houve um aumento na carga da infraestrutura com o PnT de aproximadamente 100% comparado com o cenário perfeito, no qual todos os nós enviam ACKs. No pior caso, quando combinados os comportamentos, a eficiência do descarregamento de tráfego com o PnT foi reduzida de 77% para 19%. Este capítulo apresenta contramedidas para minimizar os efeitos do cenário de falha e dos ataques no PnT, denominadas de ACKs duplamente identificados e *ranking* de encaminhamento. O mecanismo de ACKs duplamente identificados é proposto para minimizar os efeitos do cenário de falha do envio de ACKs no descarregamento de tráfego evitando que a infraestrutura com o PnT calcule de forma imprecisa a taxa de infecção. Para que a infraestrutura não escolha nós egoístas na fase inicial e de reinjeção, a infraestrutura consulta a lista com o número de encaminhamentos recentes de cada nó gerada pela proposta do *ranking* de encaminhamento. No decorrer do capítulo serão apresentadas as contramedidas propostas bem como uma análise detalhada dessas contramedidas.

5.1 Propostas de Contramedidas

Esta seção apresenta as contramedidas propostas para melhorar a eficiência dos descarregamento na presença de nós que falham no envio de ACKs e não encaminham mensagens na oportunidade do contato oportunista.

5.1.1 ACKs Duplamente Identificados

Os resultados da seção 4.2 mostram que a eficiência do descarregamento de tráfego diminui com o aumento de nós que falham ao enviar ACKs para infraestrutura ao receberem cópias da mensagem pelo canal secundário, denominado como cenário de falha de envio de ACKs. Para evitar este ataque, esta tese altera o PnT para que ele use um mecanismo denominado de ACKs duplamente identificados. A modificação proposta é simples. No momento que um nó recebe a cópia da mensagem através do canal secundário, esse nó enviará um ACK para a infraestrutura informando que ele recebeu a mensagem e também de qual nó ele recebeu a mensagem, definido como nó encaminhador. Assim, mesmo que o nó encaminhador da mensagem tenha falhado no envio do ACK a infraestrutura será capaz de saber que ele recebeu a mensagem por conta do ACK modificado contendo os dois identificadores enviado pelo nó que acaba de receber a mensagem através da comunicação oportunista. A infraestrutura, nesse caso, pode identificar alguns nós que falharam ao enviar ACKs.

Na Figura 5.1, os nós B e D apresentam falhas no envio dos ACKs, B e D recebem a mensagem através do contato oportunista com os nós A e C, respectivamente, porém a infraestrutura não recebem ACKs confirmando que receberam a mensagem. Os nós B e D encaminham a mensagem para os nós J e F. Ao receberem as mensagens, os nós J e F enviam para a infraestrutura ACKs duplamente identificados, informando que receberam a mensagem e de quais nós receberam a mensagem. Assim, a infraestrutura ao receber ACKs duplamente identificados atualiza a lista dos nós infectados e verifica se os nós encaminhadores já foram reconhecidos. Caso não, atualiza a lista e calcula a taxa de infecção. Evita-se assim a reinjeção de mais cópias desnecessárias para atingir a função objetivo ou reenvio de cópias duplicadas na zona de pânico.

Esta contramedida assume que os nós da rede estão autenticados para que seja possível ter certeza da identidade do nó que encaminhou a mensagem. Somente desta forma é possível afirmar a identidade de um nó que já recebeu a mensagem e não enviou um ACK para a infraestrutura. Vale ressaltar que os usuários de uma rede celular devem se autenticar para poder usá-la [56] e, por isso, a suposição para o bom funcionamento da contramedida é válida.

Há ainda um outro ponto que pode ser explorado na contramedida proposta. Um nó malicioso pode enviar um ACK duplamente identificado falsificado contendo sua identificação e a identificação de um outro nó da rede do qual não tenha recebido a mensagem. No exemplo da Figura 5.1, suponha que o nó malicioso I envie um ACK falsificado para

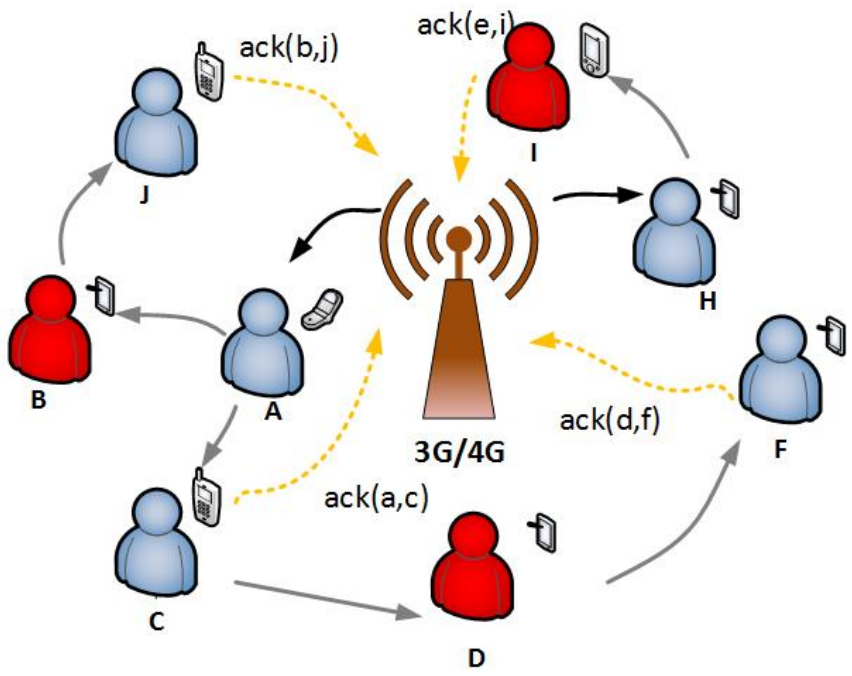


Figura 5.1: Modo de funcionamento do ACK Duplamente Identificado.

a infraestrutura informando que recebeu a mensagem do nó *E*. Assim, a infraestrutura assumirá que *E* já recebeu a mensagem, o que na verdade ainda não ocorreu.

Para evitar a falsificação de ACKs, a contramedida assume também que há uma Infraestrutura de Chaves Públicas (*Public Key Infrastructure* - PKI) na rede celular. Cada nó, então, possui um par de chaves pública e privada. Além disso, a cada encaminhamento de mensagens através da comunicação oportunista gerará um registro de encontro (*Encounter Record* - ER) [60, 43]. Este registro de encontro inclui a identificação do nó que enviou a mensagem, a identificação do nó que recebeu a mensagem, data e hora do encontro, a identificação da mensagem trocada entre eles. Ainda, ambos assinam este registro de encontro com suas chaves privadas e o armazenam. Um nó, portanto, enviará à infraestrutura o ACK duplamente identificado com sua identificação e a do nó que lhe encaminhou a mensagem e registro de encontro gerado para comprovar que realmente a mensagem foi trocada entre os nós identificados no ACK. A infraestrutura ao receber ACKs duplamente identificados verificará a autenticidade da identificação de cada nó e se houve o encontro com base no registro de encontro. Para isso, utiliza as chaves dos nós para decifrar se o registro de encontro foi realmente assinado por eles. Caso as informações estejam corretas, ela atualiza a lista de nós infectados e verifica se o nó que encaminhou a mensagem também encaminhou ACK. Caso não tenha enviado, atualiza a lista e calcula a taxa de infecção.

O pseudocódigo (Algoritmo 1) apresenta as ações executadas pela infraestrutura ao receber um ACK duplamente identificado. O valor de *IdFrom* é a identificação do nó que encaminhou o ACK, *IdFrom2* é a identificação do nó encaminhador da mensagem através da rede oportunista, *ListInfected* é a lista que contém os nós que receberam a mensagem. Primeiro verifica a autenticidade da identificação de cada nó e se houve o encontro com base no registro de encontro, caso a mensagem não seja autentica ela é descartada. Em seguida adiciona a identificação do nó *IdFrom* na lista dos nós que receberam a mensagem (*ListInfected*), caso o nó encaminhador *IdFrom2* não esteja na lista, adiciona-o e calcula a taxa de infecção.

Algoritmo 1: Pseudocódigo: ACK duplamente identificado.

Entrada: Infraestrutura recebe ACK duplamente identificado

```
1  início
2      se ACK é autentico então
3          Adiciona IdFrom na ListInfected;
4          Calcula taxa de infecção;
5          se IdFrom2 não está ListInfected então
6              Adiciona IdFrom2 na ListInfected;
7              Calcula taxa de infecção;
8          fim
9      fim
10     senão
11         Descarta o ACK;
12     fim
13 fim
```

O objetivo principal da proposta do ACK duplamente identificado é reconhecer os nós que falharam ao enviar ACK para infraestrutura.

5.1.2 *Ranking* de Encaminhamento

Para evitar que a infraestrutura envie mensagens para nós que apresentem comportamento egoísta, isto é, nós que não encaminham mensagens, propõe-se que a infraestrutura mantenha uma lista ordenada que contabilize o número de encaminhamentos recentes de cada nó através da comunicação oportunista. Esse mecanismo é denominado *ranking* de encaminhamento. A lista será criada e atualizada utilizando as informações dos ACKs duplamente identificados. Assim, a infraestrutura ao receber um ACK duplamente iden-

tificado consulta a identificação do nó encaminhador, o nó que encaminhou a mensagem através da comunicação oportunista, e atualiza o número de encaminhamento deste nó na lista. O *ranking* de encaminhamento serve como critério de escolha para determinar para quais nós a infraestrutura irá enviar cópias da mensagem inicialmente e na fase de reinjeção de novas cópias para atender a função objetivo do PnT. O número de nós a serem escolhidos n é definido pela função objetivo. A infraestrutura, então, consulta a lista para os escolher os n com maior número de encaminhamento ao enviar mensagens na fase inicial e reinjeção. Assim, evitará nós que não encaminham mensagens para outros nós através do canal secundário, não contribuindo com a eficiência do descarregamento. O *ranking* de encaminhamento gerará uma nova lista a cada intervalo de tempo definido pela infraestrutura. Assim, o número de encaminhamento de cada nó é zerado e uma nova lista é criada.

Suponha que a função objetivo determinou o envio de duas cópias pela infraestrutura. Na Figura 5.2, os nós A e H são os escolhidos para receberem as mensagens da infraestrutura através do canal primário. Estes nós são os que apresentam maior número de encaminhamentos, 10 e 8, respectivamente. A infraestrutura os escolheu após consultar a lista gerada pelo *ranking* de encaminhamento com base nos ACKs duplamente identificados recebidos. Assim, a infraestrutura não envia mensagens através do canal primário para os nós I e J nas fases iniciais e na fase de reinjeção, pois apresentam comportamentos egoístas.

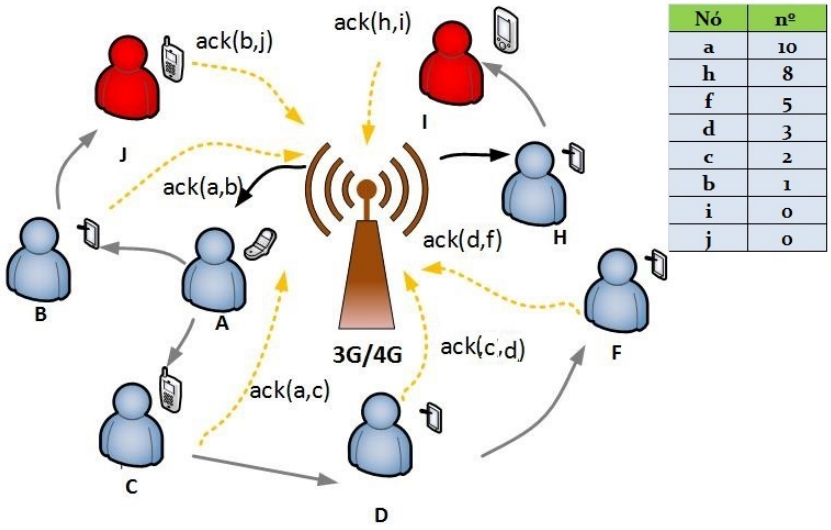


Figura 5.2: Modo de funcionamento do *Ranking* de Encaminhamento.

A infraestrutura mantém uma lista ordenada *ListRanking* com o número de encaminhamento de cada nó, utilizando o ACK duplamente identificado para construir está lista.

A infraestrutura utiliza esta lista para enviar cópias da mensagem na fase inicial. E na fase reinjeção, caso a função objetivo for menor a taxa de infecção a infraestrutura escolhe os n nós a enviar cópias da mensagem usando a lista ordenada *ListRanking* e na zona de pânico a infraestrutura envia a mensagem para todos os nós que ainda não receberam a mensagem usando a lista *ListSane*. Os pseudocódigos descritos no Algoritmo 2 descreve as ações realizadas pela infraestrutura ao enviar mensagens.

Algoritmo 2: PSEUDOCÓDIGO: *Ranking* DE ENCAMINHAMENTO.

```
1  início
2      se Fase inicial então
3          Consulta função objetivo para decidir quantas n mensagens enviar;
4          Consulta a ListRanking para escolher os n nós;
5          Envia cópia da mensagem para os n nós;
6          Adiciona os IdFrom dos n nós na ListInfected;
7          Calcula taxa de infecção;
8      fim
9      ...
10     se Função Objetivo < Taxa de infecção então
11         Consulta função objetivo para decidir quantas n mensagens enviar;
12         Consulta a ListRanking para escolher os n nós;
13         Envia cópia da mensagem para os n nós;
14         Adiciona os IdFrom dos n nós na ListInfected;
15         Calcula taxa de infecção;
16     fim
17     ...
18     se Zona de Pânico então
19         Envia cópia da mensagem para todos os n da ListSane;
20         Adiciona os IdFrom dos n nós na ListInfected;
21         Calcula taxa de infecção;
22     fim
23 fim
```

5.1.3 Combinação das Contramedidas

Propõe-se usar a combinação das duas contramedidas para aumentar a eficiência do descarregamento de tráfego quando nós não encaminham mensagens na oportunidade de

contato e/ou falham ao enviar ACKs ao receberem uma cópia da mensagem de outros nós. A infraestrutura tem o controle através do *ranking* de encaminhamento do número de mensagens que cada nó encaminhou através da comunicação oportunista e usa está informação para futuras tomadas de decisão para escolha de quais nós encaminhar novas mensagens na fase inicial e na fase de reinjeção. Assim, a infraestrutura não enviará cópias da mensagem para nós que não encaminham para outros nós através do canal secundário. Com os ACKs duplamente identificados a infraestrutura terá informação de quais nós receberam cópias da mensagem e falharam ao enviar ACKs, evitando a reinjeção de mais cópias desnecessárias para atingir a função objetivo ou reenvio de cópias duplicadas na zona de pânico.

Com as proposta combinadas a infraestrutura realiza as seguintes ações ao receber um ACK duplamente identificado, descritas no Algoritmo 3. Primeiro verifica a autenticidade do ACK, conforme descrito no Algoritmo 1, porém contabiliza mais um encaminhamento para $IdFrom2$ na lista ordenada $ListRanking$. A infraestrutura sempre que precisar enviar alguma cópia da mensagem, realiza as ações descritas nos pseudocódigos do Algoritmo 2.

Algoritmo 3: Pseudocódigo: Combinação das Contramedidas.

Entrada: Infraestrutura recebe ACK duplamente identificado

```
1  início
2      se ACK é autentico então
3          Adiciona IdFrom na ListInfected;
4          Calcula taxa de infecção;
5          Contabiliza mais um encaminhamento para IdFrom2 na ListRanking;
6          Ordena ListRanking;
7          se IdFrom2 não está ListInfected então
8              Adiciona IdFrom2 na ListInfected;
9              Calcula taxa de infecção;
10         fim
11     fim
12     senão
13         Descarta o ACK;
14     fim
15 fim
```

5.2 Avaliação das Contramedidas

As contramedidas foram implementadas no simulador, descrito na seção 4.2. As principais alterações aconteceram na classe ACK e PnTRouter. Adicionou mais parâmetros na classe ACK para que no momento em que um nó receber uma mensagem através do canal secundário, ele encaminhe para a infraestrutura a informação de qual nó ele recebeu a cópia da mensagem e o registro de encontro. Na classe PnTRouter, implementou-se uma lista com os nós autenticados pela infraestrutura. Nesta lista ordenada a infraestrutura manterá registro do número de mensagens que cada nó encaminhou. A infraestrutura utilizará a lista para escolher quais nós encaminharam novas mensagens na fase inicial e na fase de reinjeção, minimizando as chances de encaminhar cópias da mensagem para nós que apresentem comportamento egoístas.

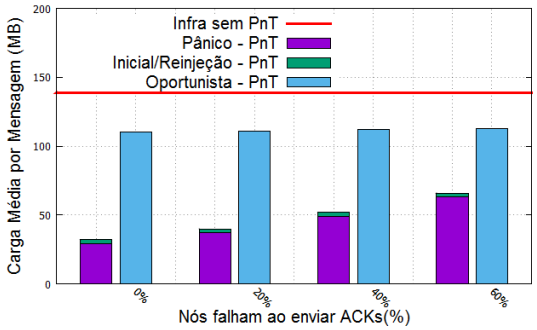
A taxa de transferência *downlink* da infraestrutura é 100 Kb/s e *uplink* é 10 Kb/s. Durante o contato, a taxa de transferência entre os nós é de 1 MB/s. O tamanho da mensagem de dados é de 1 MB e o dos ACKs é de 256 B. Novas mensagens de dados são geradas a cada 130 s e são do interesse de todos os nós. O algoritmo de roteamento utilizado em todas as simulações é o epidêmico [38]. Considera-se o tempo de vida das mensagens (TTL) igual a 120 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.

5.2.1 Cenário 1: Falha no envio de reconhecimentos positivos (ACKs)

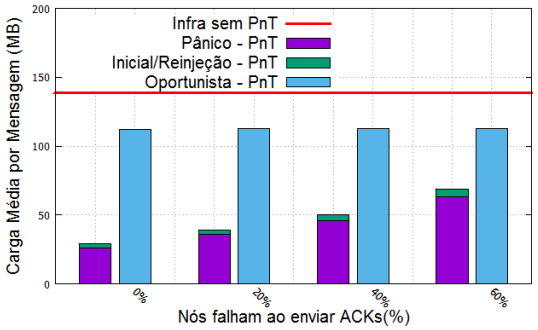
Nesta seção avalia-se o cenário de falha no envio de ACKs. Observa-se que os resultados da Figura 5.3 com as contramedidas implementadas apresentam aumento na carga de tráfego média comparado com os resultados da Figura 4.2 sem as contramedidas. A carga média de tráfego por mensagem da comunicação oportunista mantém-se em aproximadamente 110 MB com o aumento dos nós que falham a enviar ACKs em todos os cenários, mesmo utilizando funções objetivo diferentes. A carga de tráfego da comunicação oportunista não foi afetada com o aumento do número de nós que falham ao enviar ACKs porque este nós continuam a encaminhar mensagens para outros nós quando há um contato.

Os nós enviam ACKs duplamente identificados para a infraestrutura ao receberam cópias da mensagem através da comunicação oportunista. Informam que receberam e

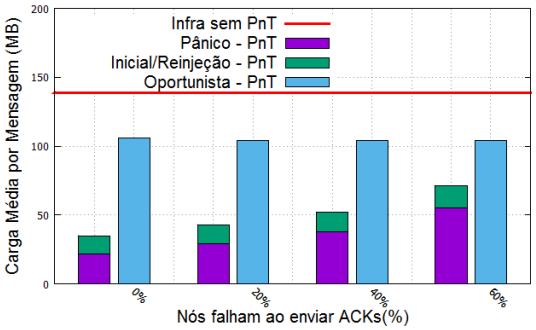
de qual nó receberam a mensagem. Desta forma, minimiza os efeitos dos nós egoístas na rede. Observa-se que os resultados da Figura 5.3 apresentam uma carga de tráfego média menor comparada com os resultados da Figura 4.2, aumentando assim a eficiência do descarregamento de tráfego. No cenário com 40% de nós egoísta a carga de tráfego diminuiu de 74 MB (*Slow Linear*), 68 MB (*Fast Linear*) e 76 MB (Adaptativa) para 51 MB (*Slow Linear*), 50 MB (*Fast Linear*) e 52 MB (Adaptativa) com as contramedidas. Com o ACK duplamente identificado, a infraestrutura reconhecerá mais nós que receberam a mensagem, reduzindo o impacto da presença de nós falham ao enviar ACKs no cálculo da taxa de infecção. A infraestrutura reconhecerá alguns nós receberam as mensagens e falharam ao enviar ACK. Consequentemente, evita mais cópias desnecessárias na fase de reinjeção para atingir a função objetivo ou reenvio de cópias duplicadas na zona de pânico.



(a) Função Objetivo *Slow Linear*.



(b) Função Objetivo *Fast Linear*.

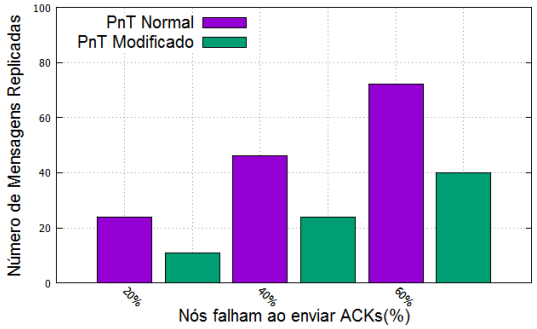


(c) Função Objetivo Adaptativa.

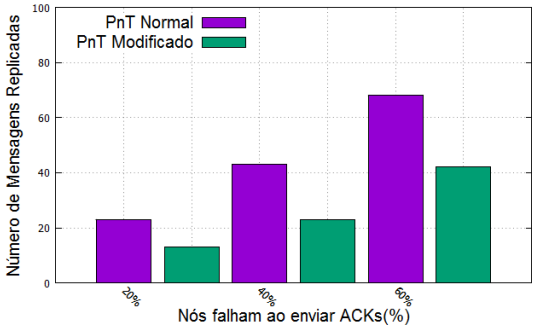
Figura 5.3: Carga de tráfego quando acontece falha no envio de ACKs com as contramedidas.

A Figura 5.4 compara o número de mensagens replicadas utilizando o PnT normal com o PnT modificado com a contramedida ACK duplamente identificado. Observa-se que em todos os cenários utilizando as três funções diferentes o PnT modificado com a contramedida apresentou um número menor de mensagens replicadas. Com 40% de nós egoístas utilizando a função objetivo *Slow Linear* o número de mensagens replicadas é

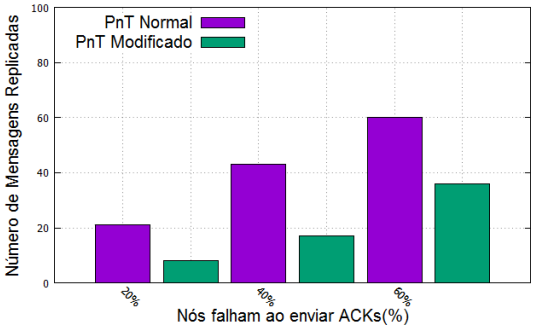
aproximadamente a metade comparado com o PnT normal. A infraestrutura ao receber a mensagem de confirmação de entrega através do ACK duplamente identificado reconhece um número maior de nós que não enviaram ACKs. Assim, a infraestrutura evita o envio de cópias da mensagem replicadas utilizando o canal primário, consequentemente diminui a carga de tráfego da infraestrutura conforme observado na Figura 5.3.



(a) Função Objetivo *Slow Linear*.

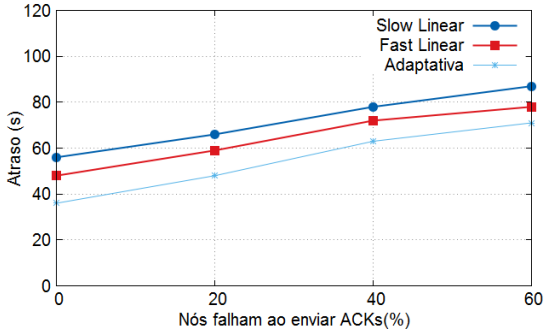


(b) Função Objetivo *Fast Linear*.

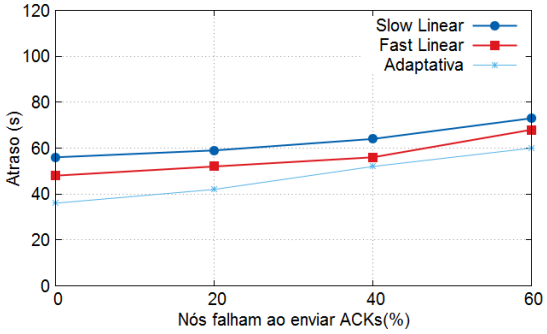


(c) Função Objetivo Adaptativa.

Figura 5.4: Número de mensagens replicadas quando acontece falha no envio de ACKs.



(a) PnT Normal.



(b) PnT Modificado.

Figura 5.5: Atraso na entrega das mensagens quando acontece falha no envio de ACKs.

A Figura 5.5 apresenta o atraso na entrega da mensagem com o PnT normal e com o PnT modificado as com contramedidas. Nota-se em todos os cenários analisados o atraso na entrega é menor com PnT modificado independente do percentual de nós que falham

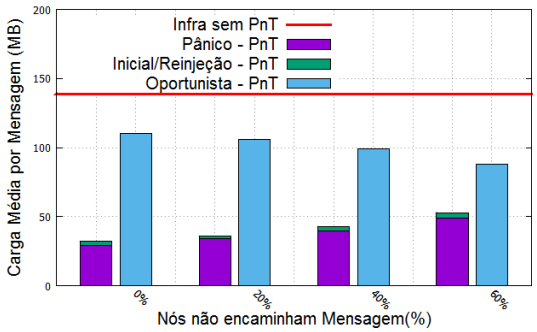
ao enviar ACKs. A função objetivo adaptativa apresentou os menores atrasos comparado com as outras funções objetivos. Devido ao seu mecanismo de atuação evitando períodos com a taxa de infecção constantes. Na presença de 60% de nós que falham ao enviar ACKs utilizando o PnT modificado com a contramedida e função adaptativa apresentou atraso na entrega da mensagem aproximadamente semelhante o da função *Slow Linear* sem a presença de nós egoístas. Em todos os cenários, houve um aumento de aproximadamente 30 s no atraso com 60% de nós egoístas comparando com um cenário sem nós que não falham ao enviar ACKs. Com 60% egoístas com o PnT modificado com a contramedida houve uma diminuição de aproximadamente 10 s comparando com o PnT normal.

5.2.2 Cenário 2: Nós egoístas não encaminham mensagens

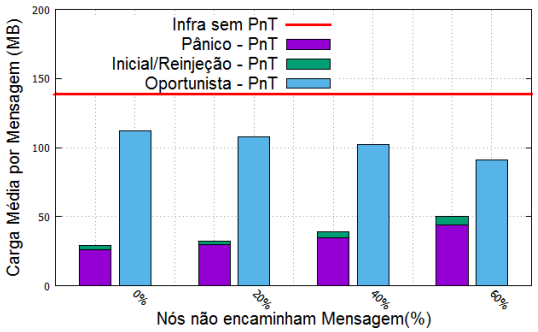
No segundo cenário avalia-se o ataque de não encaminhamento. Comparando a Figura 5.6 (que mostra o resultado com as contramedidas) com a Figura 4.3 (que mostra o resultado sem as contramedidas), nota-se um aumento na carga de tráfego gerada na comunicação oportunista na presença de nós egoístas. Por exemplo, na presença de 60% utilizando a função *Slow Linear* o uso das contramedidas aumenta a carga de tráfego da comunicação oportunista de 58 MB para 88 MB. A melhora na comunicação oportunista acontece porque a infraestrutura consulta os nós que mais encaminham mensagem na lista gerado pelo *ranking* de encaminhamento para enviar novas cópias da mensagem na fase de reinjeção.

Observa-se nos resultados quando se utiliza o *ranking* de encaminhamento (Figura 5.6) na presença de nós que não encaminham mensagens que a carga de tráfego da infraestrutura diminuiu comparado com os resultados da Figura 4.3 sem a contramedida. Isto ocorre, devido à infraestrutura utilizar a lista gerada pelo *ranking* de encaminhamento com base nos ACKs duplamente identificados recebidos para identificar os nós que mais encaminham mensagens. Assim, encaminhará cópias da mensagem para nós que mais cooperam com a comunicação oportunista e evitando nós com comportamento egoístas. Com 40% de nós egoístas utilizando a função *Fast Linear* a carga de tráfego na infraestrutura é de 55 MB (Figura 4.3(b)). Com o *ranking* de encaminhamento a carga de tráfego diminui para 43 MB (Figura 5.6(b)). Independente das funções objetivo utilizadas os ganhos na eficiência do descarregamento são significativos usando o *ranking* de encaminhamento.

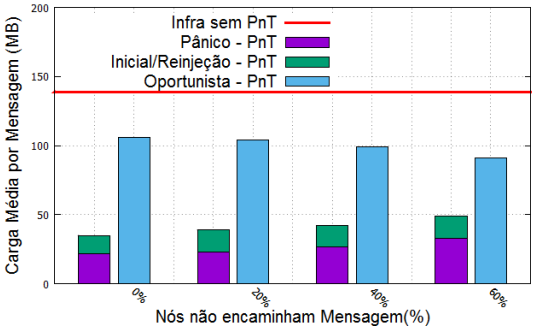
Diferentemente do primeiro cenário, o ataque de não encaminhamento não provoca mensagens replicadas. Em todos os cenários simulados não houve mensagens duplicadas, porque a infraestrutura recebe o ACK de todos os nós que receberam a mensagem atra-



(a) Função objetivo *Slow Linear*.



(b) Função objetivo *Fast Linear*.



(c) Função objetivo adaptativa.

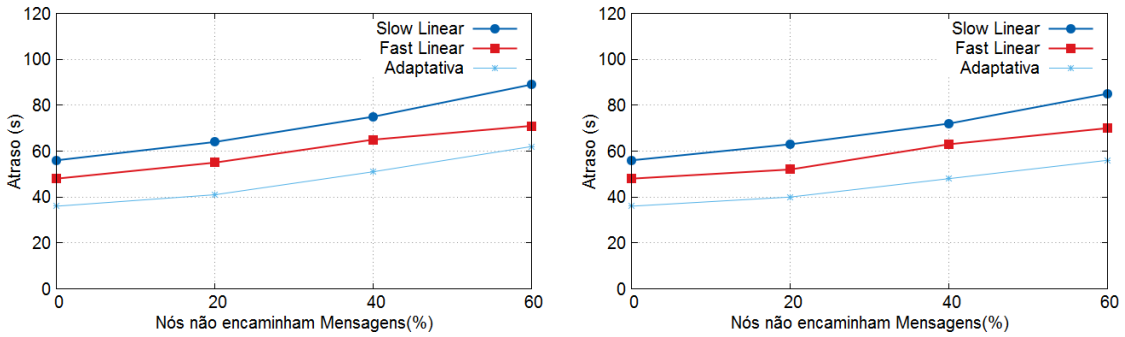
Figura 5.6: Carga de tráfego para o ataque de não encaminhamento com as contramedidas.

vés da comunicação oportunista. Assim, o sistema de controle da infraestrutura não é prejudicado como nó primeiro cenário.

A Figura 5.7 nota-se mesmo com o PnT modificado com a contramedida o ganho no atraso não foi tão significativo quanto no cenário 1. As funções objetivos *Fast Linear* e Adaptativa apresentaram atrasos menores com o PnT com e sem a contramedida comparados com o cenário 1. Porém, a funções objetivo *Slow Linear* apresentou atrasos maiores, devido ser uma função objetivo com métricas mais lentas na primeira metade do tempo de vida da mensagem, assim demora mais para reinjetar novas cópias da mensagem na rede na presença de nós que não encaminham mensagens através da comunicação oportunista na oportunidade do contato.

5.2.3 Cenário 3: Nós egoístas não encaminham mensagens e/ou falham no envio de reconhecimentos positivos

Neste cenário é analisada a influência do ataque combinado, alguns nós podem não encaminhar mensagens e/ou falham ao enviar ACK. Assim, ao receber uma mensagem o nó pode falhar ao enviar ACK para a infraestrutura e/ou não encaminhar a mensagem para outros nós na oportunidade de contato através da comunicação oportunista. Neste



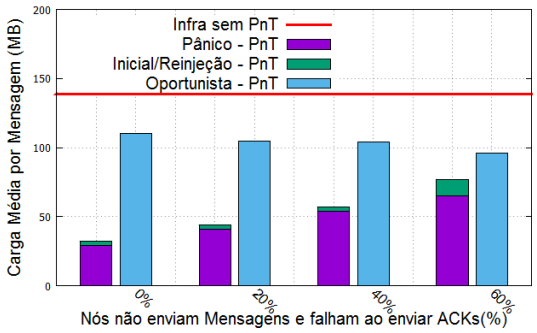
(a) PnT Normal. (b) PnT Modificado.

Figura 5.7: Atraso na entrega das mensagens quando nós não encaminham mensagens.

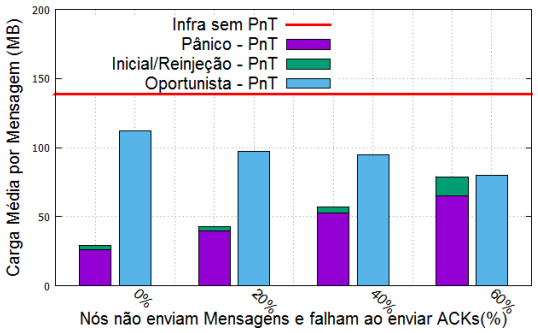
cenário varia o percentual de nós que falham ao enviar ACKs e o percentual de nós que não encaminham mensagem. Primeiro, é escolhido aleatoriamente os n nós que falham ao enviar ACKs e em seguida os n nós que não enviam mensagens. Com a interseção destes nós, tem-se os nós que falham ao enviar ACKs e não encaminham mensagens. Desta forma, têm-se três comportamentos dos nós na rede, nós que não encaminham mensagem, falham ao enviar mensagens e nós que não encaminham mensagens e falham ao enviar ACKs. Com 40% de nós egoísta, ou seja, 40% dos nós que não enviam mensagens e 40% dos nós que falham ao enviar ACKs, a carga de tráfego da infraestrutura diminuiu de 84 MB (*Slow Linear*), 82 MB (*Fast Linear*) e 75 MB (Adaptativa) para 57 MB (*Slow Linear*), 57 MB (*Fast Linear*) e 65 MB (Adaptativa) utilizando as contramedidas (Figura 4.4). O ataque combinado representa o que acontece na prática no descarregamento de tráfego, por exemplo, alguns nós mais preocupados com a conservação da carga da bateria e com movimentação aleatória que provoca falhas na comunicação oportunista.

Com a implementação das contramedidas a infraestrutura mantém o controle através do *ranking* de encaminhamento do número de mensagens que cada nó encaminhou através da comunicação oportunista, e utiliza esta informação para futuras tomadas de decisão na escolha de quais nós receberão novas cópias da mensagens na fase inicial e na fase de reinjeção. O número de cópias duplicadas será minimizado com os ACKs duplamente identificados. A infraestrutura terá mais informações de quais nós receberam cópias da mensagem e falharam ao enviar ACKs, evitando que mais cópias desnecessárias para atingir a função objetivo na fase de reinjeção e de zona de pânico.

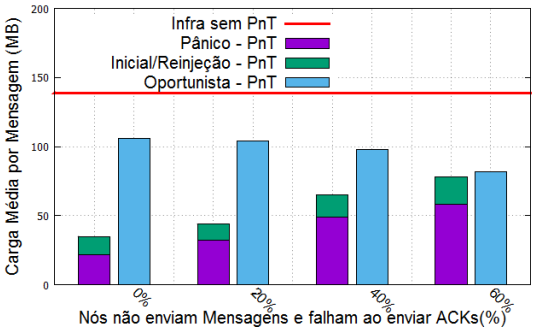
Em todos os cenários, mesmo com um aumento significativo de nós egoístas, a eficiência do descarregamento de tráfego aumentou utilizando as contramedidas, conforme pode ser observado na Tabela 5.1. Utilizando a função objetivo *Slow Linear* com o ataque combinado na presença 60% de nós egoístas a eficiência aumentou de 19% para 44%.



(a) Função objetivo *Slow Linear*.



(b) Função objetivo *Fast Linear*.



(c) Função objetivo adaptativa.

Figura 5.8: Carga de tráfego para o ataque combinado com as contramedidas.

Observa-se na Figura 5.9 que em todos os cenários utilizando o PnT modificado com as contramedidas apresentaram um número menor de mensagens replicadas comparado com o PnT normal. Utilizando a função objeto *Slow Linear* com 60% de nós egoístas apresentou resultados menos significativo comparado com as outras funções objetivos, devido a forma de atuação da função objetivo enviando um número menor de cópias da mensagem na primeira metade de tempo de vida da mensagem.

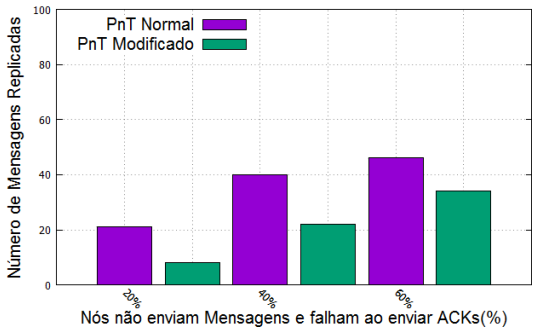
E por fim, na Figura 5.10 apresentou atrasos na entrega da mensagem maiores que os dos cenários 1 e 2, devido aos nós não encaminharem mensagens e/ou falharem ao enviar ACKs. Em todos os cenários o PnT com as contramedidas apresentou um atraso na entrega das mensagens menor comparando com o PnT normal. Assim, o PnT com as contramedidas apresentou uma maior eficiência do descarregamento de tráfego, menor número de mensagens replicas e menores atrasos.

5.2.4 Rollernet: Variando o TTL da Mensagem

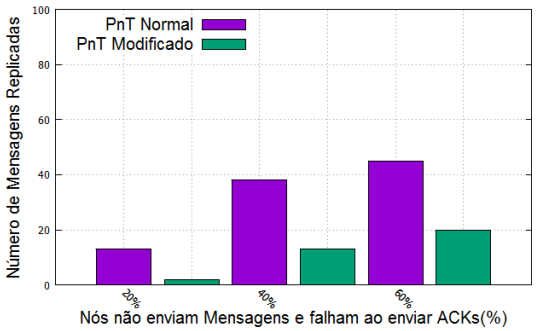
Neste cenário avalia a eficiência no descarregamento de tráfego com as contramedidas variando o tempo de vida da mensagem, TTL. Analisa os valores do TTL da mensagem para 30 s, 60 s, 120 s, 180 s e 240 s utilizando o *trace* do Rollernet. Os parâmetros

Tabela 5.1: Eficiência dos descarregamento de tráfego com as contramedidas.

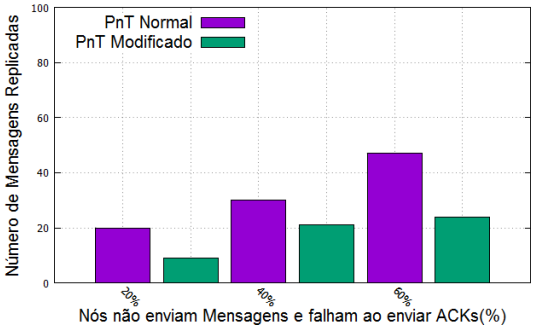
		Funções Objetivo		
		Slow Linear	*Fast Linear*	Adaptativa
Cenário 1	0%	77%	79%	74%
	20%	71%	72%	69%
	40%	62%	64%	62%
	60%	47%	50%	48%
Cenário 2	0%	76%	79%	74%
	20%	74%	77%	71%
	40%	69%	72%	69%
	60%	61%	64%	64%
Cenário 3	0%	77%	79%	74%
	20%	68%	69%	68%
	40%	58%	58%	53%
	60%	44%	43%	43%



(a) Função Objetivo *Slow Linear*.



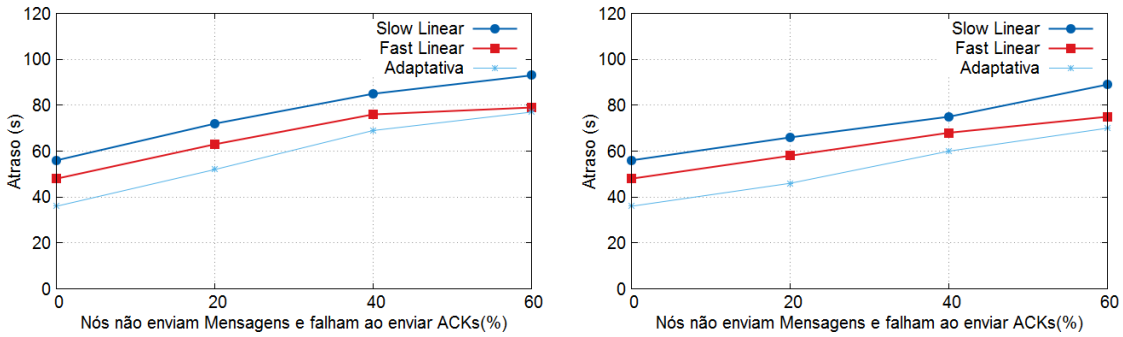
(b) Função Objetivo *Fast Linear*.



(c) Função Objetivo Adaptativa.

Figura 5.9: Número de mensagens replicadas para o ataque combinado.

de simulação são os mesmos utilizados nos cenários anteriores. Neste cenário utilizou a função objetivo *Fast Linear* e 40% de nós que não enviam mensagens e 40% de nós que falham a enviar ACKs em todas as rodadas de simulação. Observa-se na Figura 5.11 que quanto maior o valor do TTL maior é a eficiência do descarregamento de tráfego. Isto



(a) PnT Normal. (b) PnT Modificado.

Figura 5.10: Atraso na entrega das mensagens quando nós não enviam Mensagens e falham ao enviar ACKs.

acontece devido ao atraso na entrega da mensagem, aumento do TTL, assim aumenta as chances do nó receber as mensagens através da comunicação oportunista mesmo na presença de nós egoístas. Em todos os cenários, o PnT modificado apresentou desempenho superior ao PnT normal devido a implementação das contramedidas ACK duplamente identificado e *ranking* de encaminhamento, reconhecendo nós que falharam a enviar ACKs, escolhendo nós melhores encaminhadores na fase de inicial e de reinjeção, e evitando envio de mensagens duplicadas na zona de pânico. Com o TTL da mensagem de 240 s o PnT modificado com as contramedidas apresentou a eficiência no descarregamento de tráfego de 13% superior ao PnT normal.

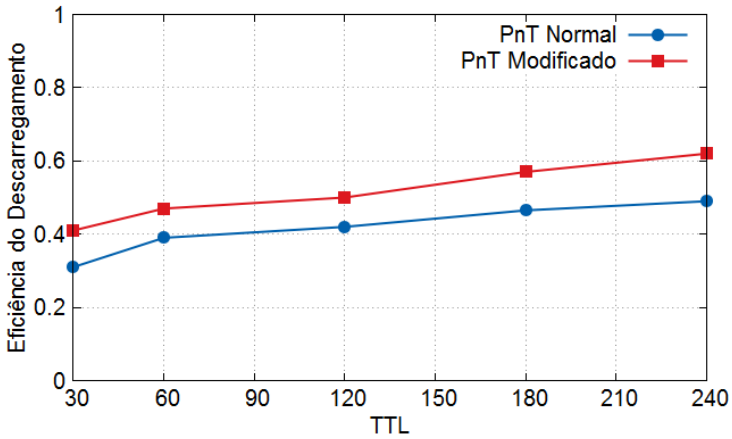


Figura 5.11: Eficiência do descarregamento variando o TLL.

5.2.5 Cenário de Mobilidade: Infocom

Como o objetivo de observar o impacto dos nós egoísta em outro cenário de mobilidade, esta seção avalia as contramedidas com o *trace* de mobilidade do Infocom [71]. Este conjunto de dados foi coletado através da distribuição de dispositivos de registros de

contatos, chamados de Intel *iMote*, para um dado número de participantes que carregam estes dispositivos durante a duração do experimento. Toda vez que um *iMote* descobre um novo vizinho, ele armazena a marca de tempo, a duração do contato e o identificador do vizinho encontrado. Os dados do conjunto de dados Infocom foram coletados pelo projeto Haggle. Este conjunto de dados foi coletado durante a conferência Infocom do ano de 2005. Contatos entre voluntários carregando *iMote* em torno da localização da conferência foram coletados por 41 dispositivos durante cerca de 3 dias. Neste cenário utiliza a função objetivo *Slow Linear* e os mesmos parâmetros de simulação utilizados nos cenários anteriores.

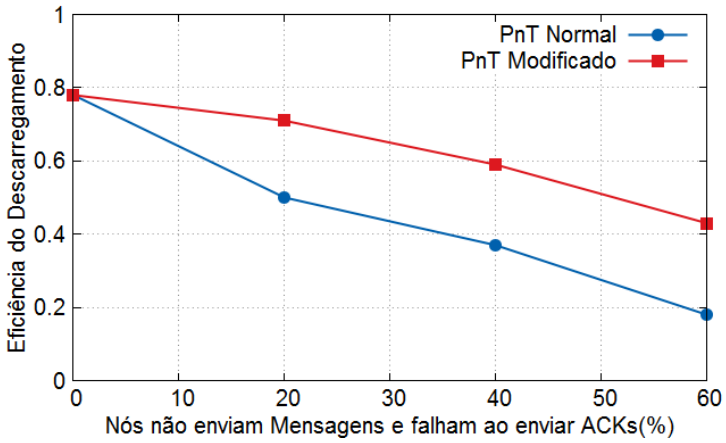


Figura 5.12: Eficiência do descarregamento de tráfego com o ataque combinado.

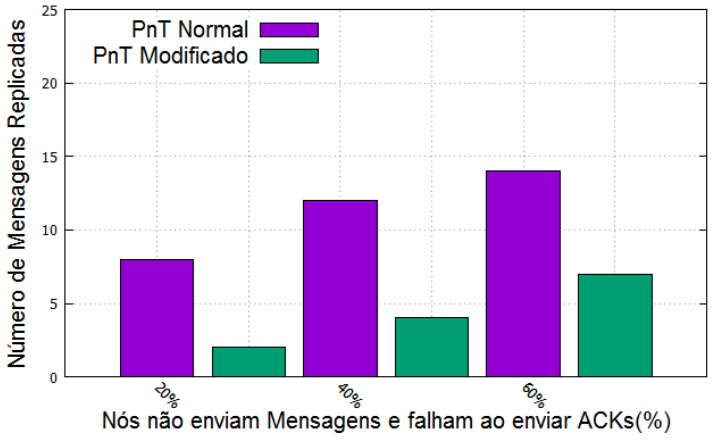


Figura 5.13: Número de mensagens replicadas com o ataque combinado.

Nota-se na Figura 5.12 que o desempenho do PnT modificado com as contramedidas na presença de 60% de nós egoístas, por exemplo, é superior ao desempenho do PnT sem contramedidas na presença de 40% de nós egoístas. Observa-se um aumento relevante na eficiência do descarregamento de tráfego com a implementação das contramedidas. Com o ataque combinado na presença de 60% de nós egoístas a eficiência aumentou de 19% para

42%, ganho superior a 100% na eficiência do descarregamento de tráfego. Na Figura 5.13 demostra que com o PnT modificado o número de mensagens replicadas diminui comparado com o PnT normal, consequentemente aumenta a eficiência do descarregamento de tráfego conforme observado na Figura 5.12.

A Figura 5.14 apresenta os atrasos variando o percentual de nós egoístas na redes, nós que não enviam mensagem e/ou falham ao enviar ACKs. Observa-se que com o aumento de nós egoístas na rede aumenta o atraso na entrega das mensagens. Na presença de nós egoísta utilizando o PnT modificado com as contramedidas diminuiu o tempo na entrega das mensagens de aproximadamente 9 s comparado com o PnT normal. Com 40% de nós egoístas, o atraso na entrega das mensagens é de 73 s com o PnT normal e de 62 s com o PnT modificado. Assim, com o PnT modificado aumentou a eficiência do descarregamento de tráfego, diminuiu o número de mensagens replicadas e o atraso na entrega das mensagens.

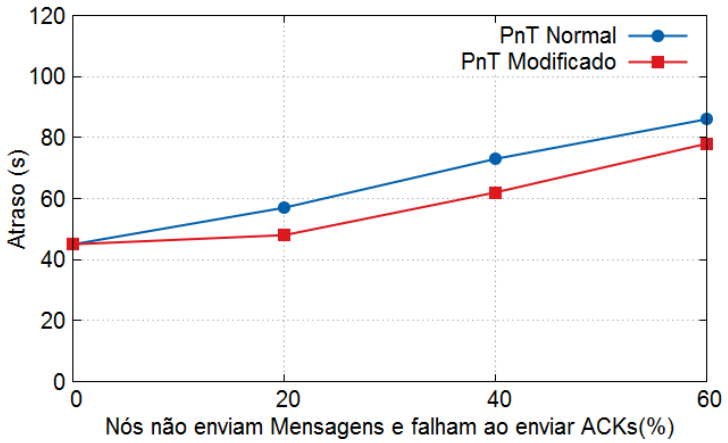


Figura 5.14: Atraso na entrega das mensagens com o ataque combinado.

5.3 Considerações Finais

O capítulo apresentou as contramedidas denominadas como ACKs duplamente identificados e *ranking* de encaminhamento. Com o ACK duplamente identificado, no momento em que um nó recebe a cópia de uma mensagem através do canal secundário, ele encaminha um ACK para a infraestrutura informando que recebeu a mensagem e de qual nó a recebeu na oportunidade do contato. Desta forma, a infraestrutura reconhecerá alguns nós que falharam ao enviar ACKs que prejudicam o cálculo da taxa de infecção. Assume-se que os nós da rede estão autenticados para que seja possível ter certeza da identidade do nó que encaminhou a mensagem. Na outra proposta, o *ranking* de encaminhamento,

a infraestrutura contabiliza o número de mensagens encaminhadas por cada nó com base nos ACKs duplamente identificados recebidos. A lista ordenada com o número de encaminhamento de cada nó servirá como critério de escolha para determinar para quais nós a infraestrutura irá enviar cópias da mensagem inicialmente e na fase de reinjeção para atender a função objetivo. A infraestrutura enviará cópias da mensagem para os nós que mais encaminham mensagens.

Avaliou-se as contramedidas através de simulação utilizando dois *traces* reais do Rolernet e Infocom. Realizou-se uma simulação mais detalhada utilizando o *trace* do Rollernet. Observou-se ganhos consideráveis no desempenho da eficiência do descarregamento de tráfego da infraestrutura em todos os cenários analisados com a presença de nós egoístas. Utilizando a função objetivo *Slow Linear* com o ataque combinado na presença de 60% de nós egoístas a eficiência melhorou de 19% para 44%. Analisou os valores do TTL da mensagem na presença de 40% de nós que falham ao enviar ACKs e/ou não encaminham mensagens com a função objetivo *Fast Linear* e observou que quanto maior o valor do TTL maior é a eficiência do descarregamento de tráfego. Com o TTL da mensagem de 240 s o PnT modificado com as contramedidas apresentou a eficiência no descarregamento de tráfego de 13% superior ao PnT normal.

Na avaliação utilizando o trace do Infocom observou-se uma melhorá relevante na eficiência do descarregamento de tráfego. Com o ataque combinado na presença de 60% de nós egoístas a eficiência aumento de 19% para 42%. Desempenho superior ao PnT sem as contramedidas na presença de 40% de nós egoístas.

Capítulo 6

Considerações Finais

O descarregamento de tráfego utilizando redes oportunistas é uma solução promissora para aliviar a sobrecarga da rede celular, causada pelo aumento do número de dispositivos móveis e aplicações consumidoras de dados. Com esses mecanismos, nós móveis baixam conteúdos populares através da rede celular e transmitem esses conteúdos para outros nós por meio de um canal secundário através da comunicação oportunista. Desta forma, nós podem obter o conteúdo solicitado sem acessar a Internet através do canal secundário, o que ajuda a reduzir significativamente a carga de tráfego na rede celular.

Uma das propostas de mecanismos de descarregamento de tráfego que usam redes oportunistas é o *framework Push-and-Track* (PnT) [87, 88]. A principal característica do PnT é garantir a entrega de todas as mensagens mesmo usando uma rede oportunista para aliviar a carga da infraestrutura de rede celular. 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. 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. Neste caso, um aumento significativo da carga de tráfego por mensagem.

O PnT, no entanto, assume que todos os nós cooperam com a comunicação oportunista e não falham no envio de mensagens de reconhecimento positivo (ACKs) para a infraestrutura. Nesta tese, avaliou-se a eficiência do descarregamento de tráfego com o *framework Push-and-Track* na presença de nós egoístas. Esses nós não encaminham mensagens para outros nós, falham ao enviar mensagens de reconhecimentos positivos para infraestrutura ou combinam esses dois comportamentos. O desempenho do PnT foi

avaliado para três funções objetivo diferentes: *Slow Linear, Fast Linear* e adaptativa. Os resultados mostraram que quando 40% de nós que falharam ao enviar ACKs para a infraestrutura, houve um aumento na carga da infraestrutura com o PnT de aproximadamente 100% 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 cenário de falha no envio de ACKs. Isso porque com aumento do percentual dos nós que falham ao enviar 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 duplicadas na zona de pânico. Quando combinados os ataques, a eficiência do descarregamento de tráfego com o PnT foi reduzida de 77% para 19%, a carga das mensagens replicadas é de 72 MB.

Por conta dos resultados obtidos, essa tese propõem duas contramedidas denominadas como ACKs duplamente identificados e *ranking* de encaminhamento. Com ACKs duplamente identificados, um nó ao receber cópia da mensagem através do contato oportunista com outro nó encaminha um ACK duplamente identificando confirmando que recebeu a mensagem e de qual nó a recebeu, juntamente com o registro do encontro. O registro de encontro contém a identificação do nó que enviou a mensagem, a identificação do nó que recebeu a mensagem, data e hora do encontro, a identificação da mensagem trocada entre eles. Ainda, ambos assinam este registro de encontro com suas chaves privadas. A infraestrutura ao receber os ACKs duplamente identificados realiza as seguintes ações: primeiro atualiza a lista de nós infectados identificando o nó, depois verifica se o nó que encaminhou a mensagem através do canal secundário foi identificado. Caso não, atualiza a lista de nós infectados e calcula novamente a taxa de infecção. Assim, a infraestrutura tem o controle de quais nós não estão enviando ACK. Evita-se que a infraestrutura encaminhe cópias duplicada da mensagem para estes nós na fase reinjeção e na zona de pânico. Assume que todos os nós da rede estão autenticados para que seja possível ter certeza da identidade do nó que encaminhou a mensagem.

O *ranking* de encaminhamento é um mecanismo que cria uma lista ordenada com o número de mensagens encaminhadas por cada nó com base nos ACKs duplamente identificados recebidos. A infraestrutura utiliza a lista para selecionar o conjunto de nós que mais encaminham mensagem através do canal secundário para enviar a mensagem na fase de inicial e reinjeção para atender a função objetivo. Assim, evita enviar cópias da mensagem para nós egoístas. Propõe-se usar a combinação das duas contramedidas para aumentar a eficiência do descarregamento de tráfego na presença de nós egoístas.

As contramedidas foram avaliadas utilizando dois *traces* de mobilidade, do Rollernet e Infocom. Na avaliação utilizando o *Rollernet* avaliou os três ataques conforme a analise inicial do comportamento dos nós egoístas. Em todos os cenários, a eficiência do descarregamento aumentou comparado com os cenários sem implementar as contramedidas. Destaca-se a análise utilizando a função objetivo *Slow Linear* com o ataque combinado na presença 60% de nós egoístas à eficiência aumentou de 19% para 44%, diminuiu a carga das mensagens replicadas para 40 MB. O mesmo aconteceu na avaliação utilizando o *trace* do Infocom, a eficiência do descarregamento de tráfego com o ataque combinado na presença de 60% de nós egoístas melhorou para 42%, desempenho superior ao PnT sem implementar as contramedidas na presença de 40% de nós egoístas.

Em todos os cenário analisados, o PnT com as contramedidas apresentou uma maior eficiência do descarregamento de tráfego, menor número de mensagens replicas e menores atrasos na entrega da mensagem.

Durante essa pesquisa identificaram-se algumas possíveis direções para as quais o trabalho atual poderia evoluir, além da avaliação da carga de tráfego e eficiência do descarregamento de tráfego. Poderia analisar o consumo de energia e *buffer* dos nós encaminhadores na presença de nós egoístas. Novos ataques podem ser considerados como nós falsificando suas identificações, por exemplo.

6.1 Artigo Publicado

SOARES, C. L.; MORAES, I. M; "Sobre a Influencia dos Nós Egoístas no Descarregamento de Tráfego com Redes Oportunistas", Artigo completo publicado no Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2016), Niterói/RJ, 2016.

6.2 Submissão de Artigo para Periódico

SOARES, C. L.; MORAES, I. M; "Influence of selfish nodes in the traffic offloading with opportunistic networks", Submissão artigo completo para o periódico *Computers and Electrical Engineering*, ISSN: 0045-7906.

Referências

[1] 3GPP. 3GPP TSG SA: Feasibility study for proximity services (prose) (rel. 12), 2012.

[2] Aijaz, A.; Aghvami, H.; Amani, M. A survey on mobile data offloading: technical and business perspectives. *IEEE Wireless Communications 20*, 2 (April 2013), 104–112.

[3] Alwan, S.; Fajjari, I.; Aitsaadi, N. Joint multicast routing and OFDM resource allocation in LTE-D2D 5G cellular network. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium* (April 2018), pp. 1–9.

[4] Asadi, A.; Wang, Q.; Mancuso, V. A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys Tutorials 16*, 4 (Fourthquarter 2014), 1801–1819.

[5] Balasubramanian, A.; Mahajan, R.; Venkataramani, A. Augmenting mobile 3G using WiFi. In *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services* (New York, NY, USA, 2010), MobiSys '10, ACM, pp. 209–222.

[6] Balbi, H.; Fernandes, N.; Souza, F.; Carrano, R.; Albuquerque, C.; Muchaluat-Saade, D.; Magalhaes, L. Centralized channel allocation algorithm for IEEE 802.11 networks. In *2012 Global Information Infrastructure and Networking Symposium (GIIS)* (Dec 2012), pp. 1–7.

[7] Barbera, M. V.; Stefa, J.; Viana, A. C.; de Amorim, M. D.; Boc, M. VIP delegation: Enabling VIPs to offload data in wireless social mobile networks. In *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)* (June 2011), pp. 1–8.

[8] Barbera, M. V.; Viana, A. C.; de Amorim, M. D.; Stefa, J. Data offloading in social mobile networks through VIP delegation. *Ad Hoc Networks 19* (2014), 92 – 110.

[9] Bastos, A, V.; Júnior, D. C. S. Comunicação D2D para a 5G de arquiteturas de redes celulares: Da teoria à prática. In *Minicursos Simpósio Brasileiro Telecomunicações e Processamento de Sinais SBRC2017* (Belém, PA, Brasil, 2017).

[10] Benbadis, F. CRAWDAD data set UPMC/Rollernet (v. 2009-02-02). Disponível em: http://crawdad.org/upmc/rollernet/, Feb. 2009.

[11] Bulut, E.; Szymanski, B. K. WiFi access point deployment for efficient mobile data offloading. In *Proceedings of the First ACM International Workshop on Practical*

Issues and Applications in Next Generation Wireless Networks (New York, NY, USA, 2012), PINGEN '12, ACM, pp. 45–50.

[12] Burgess, J.; Dean Bissias, G.; D. Corner, M.; Neil Levine, B. Surviving attacks on disruption-tolerant networks without authentication. pp. 61–70.

[13] Caini, C.; Cruickshank, H. S.; Farrell, S.; Marchese, M. Delay- and disruption-tolerant networking (DTN): An alternative solution for future satellite networking applications. *Proceedings of the IEEE 99*, 11 (2011), 1980–1997.

[14] Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K.; Weiss, H. Delay-Tolerant Networking Architecture. RFC 4838 (Informational), Apr. 2007.

[15] Cha, M.; Kwak, H.; Rodriguez, P.; Ahn, Y.-Y.; Moon, S. I tube, you tube, everybody tubes: Analyzing the world's largest user generated content video system. In *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement* (New York, NY, USA, 2007), IMC '07, ACM, pp. 1–14.

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

[17] Chen, B. B.; Chan, M. C. Mobtorrent: A framework for mobile Internet access from vehicles. In *IEEE INFOCOM 2009* (April 2009), pp. 1404–1412.

[18] Cheng, H.; Lin, K. C. Source selection and content dissemination for preference-aware traffic offloading. *IEEE Transactions on Parallel and Distributed Systems 26*, 11 (Nov 2015), 3160–3174.

[19] Christiani, D. d. M. C.; Rocha, A. A. d. A.; Campos, C. A. V. Um mecanismo distribuído de incentivo baseado em crédito para redes oportunistas. In *16º Workshop em Desempenho de Sistemas Computacionais e de Comunicação (WPerformance 2017)* (Porto Alegre, RS, Brasil, 2017), vol. 16, SBC.

[20] Chuang, Y.; Lin, K. C. Cellular traffic offloading through community-based opportunistic dissemination. In *2012 IEEE Wireless Communications and Networking Conference (WCNC)* (April 2012), pp. 3188–3193.

[21] Cisco. O tráfego mundial de dados móveis aumentará 7 vezes entre 2016 e 2021. Disponível em: `https://www.cisco.com/c/pt_pt/about/press/news-archive-2017/20170208.html/`, 2018. Acessado em: 16 agosto de 2018.

[22] Claro. Net Claro WiFi. Disponível em: `https://www.claro.com.br/internet/rede-net-claro-wifi/`. Acesso em: 10 de outubro de 2018, 2018.

[23] Dimatteo, S.; Hui, P.; Han, B.; Li, V. O. K. Cellular traffic offloading through WiFi networks. In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems* (Oct 2011), pp. 192–201.

[24] Dong, W.; Chen, J.; Yang, Y.; Zhang, W. Epidemic-like proximity-based traffic offloading. *China Communications 12*, 10 (Oct 2015), 91–107.

[25] Fall, K. A delay-tolerant network architecture for challenged Internets. In *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (New York, NY, USA, 2003), SIGCOMM '03, ACM, pp. 27–34.

[26] Fall, K.; Farrell, S. DTN: an architectural retrospective. *IEEE Journal on Selected Areas in Communications 26*, 5 (June 2008), 828–836.

[27] Farrell, S.; Cahill, V.; Geraghty, D.; Humphreys, I.; McDonald, P. When TCP breaks: Delay- and disruption- tolerant networking. *IEEE Internet Computing 10*, 4 (July 2006), 72–78.

[28] Farrell, S.; Symington, S. F.; Weiss, H.; Lovell, P. Delay-tolerant networking security overview. Internet-Draft, September 2009. draft-irtf-dtnrg-sec-overview-06.

[29] Fengming, C.; Ping, G.; Kai, N. Reference signal design for LTE-based D2D communications. In *2014 4th IEEE International Conference on Network Infrastructure and Digital Content* (Sept 2014), pp. 317–321.

[30] Fuxjager, P.; Gojmerac, I.; Fischer, H. R.; Reichl, P. Measurement-based small-cell coverage analysis for urban macro-offload scenarios. In *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)* (May 2011), pp. 1–5.

[31] Gu, J.; Wang, W.; Huang, A.; Shan, H. Proactive storage at caching-enable base stations in cellular networks. In *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (Sept 2013), pp. 1543–1547.

[32] Gu, J.; Wang, W.; Huang, A.; Shan, H.; Zhang, Z. Distributed cache replacement for caching-enable base stations in cellular networks. In *2014 IEEE International Conference on Communications (ICC)* (June 2014), pp. 2648–2653.

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

[34] Han, B.; Hui, P.; Kumar, V. S. A.; Marathe, M. V.; Shao, J.; Srinivasan, A. Mobile data offloading through opportunistic communications and social participation. *IEEE Transactions on Mobile Computing 11*, 5 (May 2012), 821–834.

[35] Han, B.; Hui, P.; Srinivasan, A. Mobile data offloading in metropolitan area networks. *SIGMOBILE Mob. Comput. Commun. Rev. 14*, 4 (Nov. 2010), 28–30.

[36] Hu, L.; Coletti, C.; Huan, N.; Kovács, I. Z.; Vejlgaard, B.; Irmer, R.; Scully, N. Realistic indoor Wi-Fi and femto deployment study as the offloading solution to LTE macro networks. In *2012 IEEE Vehicular Technology Conference (VTC Fall)* (Sept 2012), pp. 1–6.

[37] Huguenin, K.; Merrer, E. L.; Scouarnec, N. L.; Straub, G. Efficient and transparent Wi-Fi offloading for HTTP(S) POSTs. *IEEE Transactions on Mobile Computing 15*, 4 (April 2016), 826–839.

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

[39] Karunakaran, P.; Bagheri, H.; Katz, M. Energy efficient multicast data delivery using cooperative mobile clouds. In *European Wireless 2012; 18th European Wireless Conference 2012* (April 2012), pp. 1–5.

[40] Keränen, A.; Ott, J.; Kärkkäinen, T. 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, 2009), ICST.

[41] Lee, K.; Lee, J.; Yi, Y.; Rhee, I.; Chong, S. Mobile data offloading: How much can wifi deliver? *IEEE/ACM Transactions on Networking 21*, 2 (April 2013), 536–550.

[42] Li, F.; Wu, J.; Srinivasan, A. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. pp. 2428 – 2436.

[43] Li, Q.; Cao, G. Mitigating routing misbehavior in disruption tolerant networks. *IEEE Transactions on Information Forensics and Security 7*, 2 (April 2012), 664–675.

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

[45] Li, Y.; Su, G.; Hui, P.; Jin, D.; Su, L.; Zeng, L. Multiple mobile data offloading through delay tolerant networks. In *Proceedings of the 6th ACM Workshop on Challenged Networks* (New York, NY, USA, 2011), CHANTS '11, ACM, pp. 43–48.

[46] Li, Y.; Wang, Z.; Jin, D.; Chen, S. Optimal mobile content downloading in device-to-device communication underlaying cellular networks. *IEEE Transactions on Wireless Communications 13*, 7 (July 2014), 3596–3608.

[47] Liu, Z.; Wu, Y.; Deng, S. 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 (2013), 386–390.

[48] Moreira, D. S.; Matthaus, B.; Mota, E.; Carvalho, C. Avaliação experimental da eficácia de um watchdog em redes oportunistas móveis. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos SBRC2018"* (5 2018), p. 14.

[49] Mota, V.; Macedo, D. F.; Ghamri-Doudane, Y.; Nogueira, J. M. MINEIRO: um mecanismo de incentivo para aplicações em redes oportunísticas. In *XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos* (2015).

[50] Mota, V. F. S.; Macedo, D. F.; Ghamri-Doudanez, Y.; Nogueira, J. M. S. Managing the decision-making process for opportunistic mobile data offloading. In *2014 IEEE Network Operations and Management Symposium (NOMS)* (May 2014), pp. 1–8.

[51] Moura, H. d. P.; Camposa, C. A. V. Análise de performance da comunicação ao D2D em redes LTE-A. In *XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais* (2017).

[52] Naves, J. F.; Moraes, I. M. 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* (2014), 105–118.

[53] Naves, J. F.; Moraes, I. M. Mitigating the ACK counterfeiting attack in delay and disruption tolerant networks. In *IEEE Symposium on Computers and Communications (ISCC)* (2017), pp. 1015–1020.

[54] OI. Oi wifi. Disponível em: `http://oiwifi.com.br/`. Acesso em: 10 de outubro de 2018, 2018.

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

[56] Oliveira, T. R.; Nogueira, J. M. S. Certificados sociais para segurança em redes veiculares tolerantes a interrupções. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos SBRC2013* (2013), 835–848.

[57] Pan, Y.; Pan, C.; Zhu, H.; Ahmed, Q. Z.; Chen, M.; Wang, J. Content offloading via d2d communications based on user interests and sharing willingness. In *2017 IEEE International Conference on Communications (ICC)* (May 2017), pp. 1–6.

[58] Panwar, N.; Sharma, S.; Singh, A. K. A survey on 5G: The next generation of mobile communication. *Physical Communication 18* (2016), 64–84.

[59] Peng, W.; Li, F.; Zou, X.; Wu, J. The virtue of patience: Offloading topical cellular content through opportunistic links. In *2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems* (Oct 2013), pp. 402–410.

[60] Pham, T. N. D.; Yeo, C. K. Detecting colluding blackhole and greyhole attacks in delay tolerant networks. *IEEE Transactions on Mobile Computing 15*, 5 (May 2016), 1116–1129.

[61] Phunchongharn, P.; Hossain, E.; Kim, D. I. Resource allocation for device-to-device communications underlaying LTE-advanced networks. *IEEE Wireless Communications 20*, 4 (August 2013), 91–100.

[62] Proulx, B.; Zhang, J. Ameliorating cellular traffic peaks through preloading and P2P communications. In *2013 IEEE Global Communications Conference (GLOBECOM)* (Dec 2013), pp. 4889–4894.

[63] Qu, Y.; Dong, C.; Dai, H.; Wei, Z.; Wu, Q. Maximizing d2d-based offloading efficiency with throughput guarantee and buffer constraint. *IEEE Transactions on Vehicular Technology 68*, 1 (Jan 2019), 832–842.

[64] Ra, M.-R.; Paek, J.; Sharma, A. B.; Govindan, R.; Krieger, M. H.; Neely, M. J. Energy-delay tradeoffs in smartphone applications. In *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services* (New York, NY, USA, 2010), MobiSys '10, ACM, pp. 255–270.

[65] Radu, I. C.; Ciprian, D.; Valentin, C.; Florin, P.; Fatos, X. Sprint-self: Social-based routing and selfish node detection in opportunistic networks. In *Mobile Information Systems* (2015), vol. 2015, p. 12.

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

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

[68] Ristanovic, N.; Boudec, J. L.; Chaintreau, A.; Erramilli, V. Energy efficient offloading of 3G networks. In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems* (Oct 2011), pp. 202–211.

[69] Rolim, C. O. Uso de sensibilidade à situação em redes oportunistas para intensificar a comunicação de dados em aplicações de sensoriamento urbano. Master's thesis, Universidade Federal do Rio Grande do Sul. Instituto de Informática. Programa de Pós-Graduação em Computação., Porto Alegre, 2016.

[70] Sciancalepore, V.; Giustiniano, D.; Banchs, A.; Hossmann-Picu, A. Offloading cellular traffic through opportunistic communications: Analysis and optimization. *IEEE Journal on Selected Areas in Communications 34*, 1 (Jan 2016), 122–137.

[71] Scott, J.; Gass, R.; Crowcroft, J.; Hui, P.; Diot, C.; Chaintreau, A. CRAWDAD dataset cambridge/haggle (v. 2006-09-15). Disponivel em: `https://crawdad.org/cambridge/haggle/20060915/imote`, Sept. 2006. traceset: imote.

[72] Singh, S.; Dhillon, H. S.; Andrews, J. G. Offloading in heterogeneous networks: Modeling, analysis, and design insights. *IEEE Transactions on Wireless Communications 12*, 5 (May 2013), 2484–2497.

[73] Siris, V. A.; Kalyvas, D. Enhancing mobile data offloading with mobility prediction and prefetching. In *Proceedings of the Seventh ACM International Workshop on Mobility in the Evolving Internet Architecture* (New York, NY, USA, 2012), MobiArch '12, ACM, pp. 17–22.

[74] Souza, C. B.; Galvão, L.; Mota, E.; Soares, D. Gerenciamento de buffer baseado em egoísmo para redes tolerantes a atrasos e desconexões. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos SBRC2017"* (5 2017), p. 14.

[75] Stiemerling, M.; Kiesel, S. Cooperative P2P video streaming for mobile peers. In *2010 Proceedings of 19th International Conference on Computer Communications and Networks* (Aug 2010), pp. 1–7.

[76] Teleco. Wi-fi offload: Introdução. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwifioffload/pagina_6.asp. Acesso em: 15 de setembro de 2018, 2018.

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

[78] TIM. Tim wifi. Disponível em: https://www.tim.com.br/rj/para-voce/internet/na-rede/tim-wi-fi-. Acesso em: 10 de outubro de 2018, 2018.

[79] Trestian, I.; Ranjan, S.; Kuzmanovic, A.; Nucci, A. Taming the mobile data deluge with drop zones. *IEEE/ACM Transactions on Networking 20*, 4 (Aug 2012), 1010–1023.

[80] Uddin, M. Y. S.; Godfrey, B.; Abdelzaher, T. Relics: In-network realization of incentives to combat selfishness in dtns. In *The 18th IEEE International Conference on Network Protocols* (Oct 2010), pp. 203–212.

[81] Vigneri, L.; Spyropoulos, T.; Barakat, C. Storage on wheels: Offloading popular contents through a vehicular cloud. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (June 2016), pp. 1–9.

[82] Vukadinović, V.; Karlsson, G. Spectral efficiency of mobility-assisted podcasting in cellular networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking* (New York, NY, USA, 2010), MobiOpp '10, ACM, pp. 51–57.

[83] Wang, W.; Lan, R.; Gu, J.; Huang, A.; Shan, H.; Zhang, Z. Edge caching at base stations with device-to-device offloading. *IEEE Access 5* (2017), 6399–6410.

[84] Wang, W.; Wu, X.; Xie, L.; Lu, S. Joint storage assignment for D2D offloading systems. *Computer Communications 83* (2016), 45 – 55.

[85] Wang, X.; Chen, M.; Han, Z.; Wu, D. O.; Kwon, T. T. Toss: Traffic offloading by social network service-based opportunistic sharing in mobile social networks. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications* (April 2014), pp. 2346–2354.

[86] Wenjie, L.; Galluccio, L.; Bassi, F.; Kieffer, M. Distributed faulty node detection in delay tolerant networks: Design and analysis. *IEEE Transactions on Mobile Computing 17*, 4 (April 2018), 831–844.

[87] Whitbeck, J.; Amorim, M.; Lopez, Y.; Leguay, J.; Conan, V. 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* (June 2011), pp. 1–10.

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

[89] Xu, D.; Li, Y.; Chen, X.; Li, J.; Hui, P.; Chen, S.; Crowcroft, J. A survey of opportunistic offloading. *IEEE Communications Surveys Tutorials 20*, 3 (thirdquarter 2018), 2198–2236.

[90] Yao, H.; Zeng, D.; Huang, H.; Guo, S.; Barnawi, A.; Stojmenovic, I. Opportunistic offloading of deadline-constrained bulk cellular traffic in vehicular dtns. *IEEE Transactions on Computers 64*, 12 (Dec 2015), 3515–3527.

[91] Zhang, D.; Yeo, C. K. Optimal handing-back point in mobile data offloading. In *2012 IEEE Vehicular Networking Conference (VNC)* (Nov 2012), pp. 219–225.

[92] Zhigang, L.; Yan, S.; Shanzh, i. C.; Jingwen, Z. Cellular traffic offloading through opportunistic communications based on human mobility. In *KSII Transactions on Internet and Information Systems* (2015), vol. 9, pp. 872–885.

[93] Zhuo, X.; Gao, W.; Cao, G.; Dai, Y. Win-Coupon: An incentive framework for 3G traffic offloading. In *2011 19th IEEE International Conference on Network Protocols* (Oct 2011), pp. 206–215.

[94] Zhuo, X.; Gao, W.; Cao, G.; Hua, S. An incentive framework for cellular traffic offloading. *IEEE Transactions on Mobile Computing 13*, 3 (March 2014), 541–555.