UNIVERSIDADE FEDERAL FLUMINENSE

**ELY DA SILVA MIRANDA**

# Mecanismos de custódia compartilhada em redes tolerantes a atrasos e desconexões

NITERÓI

2013

UNIVERSIDADE FEDERAL FLUMINENSE

**ELY DA SILVA MIRANDA**

# Mecanismos de custódia compartilhada em redes tolerantes a atrasos e desconexões

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Redes e Sistemas Distribuídos e Paralelos

Orientador:
PEDRO BRACONNOT VELLOSO

Co-orientador:
IGOR MONTEIRO MORAES

NITERÓI

2013

**Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF**

M672 Miranda, Ely da Silva
Mecanismos de custódia compartilhada em redes tolerantes a atrasos e desconexões / Ely da Silva Miranda. – Niterói, RJ : [s.n.], 2013.
90 f.

Dissertação (Mestrado em Ciência da Computação) – Universidade Federal Fluminense, 2013.
Orientadores: Pedro Braconnot Velloso, Igor Monteiro Moraes.

1. Rede de comunicação de computadores. 2. Redes tolerantes a atraso e desconexões. 3. Transferência de custódia (Computação). 4. Confiabilidade (Sistema de computação). I. Título.

CDD 004.6

ELY DA SILVA MIRANDA

Mecanismos de custódia compartilhada em redes tolerantes a atrasos e desconexões

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Redes e Sistemas Distribuídos e Paralelos

Aprovada em agosto de 2013.

BANCA EXAMINADORA

---

Prof. Pedro Braconnot Velloso - Orientador, UFF

---

Prof. Igor Monteiro Moraes - Co-orientador, UFF

---

Prof. Miguel Elias Mitre Campista, UFRJ

---

Prof. Célio Vinicius Neves de Albuquerque, UFF

Niterói

2013

*Dedico este trabalho aos meus pais.*

*"Inexiste orgulho sábio" (Waldo Vieira)*

# Agradecimentos

À causa primária de todas as coisas e a toda a sua legião de servidores fraternos por me permitirem a cada dia, ainda que lentamente, evoluir moral e intelectualmente com base no autoconhecimento e na autopesquisa.

Aos meus amados pais e parentes por sempre acreditarem em meus esforços desde criança e me incentivarem a progredir sempre.

À querida Danielle, por sempre estar disposta a me levar palavras de incentivo e de carinho, bem como entender minhas ausências.

Ao Tribunal de Contas do Estado do Piauí (TCE-PI) por prontamente me liberar de minhas atividades sempre que necessário para realizar atividades relacionadas a esta pós-graduação.

Ao Instituto Federal do Piauí (IFPI) e à Universidade Federal Fluminense (UFF) por viabilizarem a execução deste mestrado interinstitucional.

Aos amigos e servidores do IFPI que estiveram durante o período de quatro meses em Niterói comigo dividindo inúmeros momentos de amadurecimento.

Ao amigo de pesquisas Juliano Naves pelas incontáveis contribuições em discussões sobre este trabalho.

Aos professores Miguel Campista e Célio Albuquerque que gentilmente aceitaram participar da banca examinadora.

Especial agradecimento devo aos Professores Pedro Velloso e Igor Moraes pelos inúmeros ensinamentos e por acreditarem que, mesmo em curto e desafiador período, essa pesquisa poderia render bons frutos.

Finalmente, a todos os que se envolveram e contribuíram de alguma forma para que a realização dessa pesquisa fosse possível, meus sinceros agradecimentos.

# Resumo

A transferência de custódia é um mecanismo proposto para aumentar a confiabilidade em Redes Tolerantes a Atrasos e Desconexões (*Delay/Disruption Tolerant Networks* - DTNs). Com a transferência de custódia, um nó delega a outro a responsabilidade da entrega de um agregado. Essa responsabilidade significa que o nó detentor da custódia de um agregado não pode descartá-lo a menos que seja entregue ou que seu tempo de vida expire, evitando assim que o agregado venha a ser descartado de forma prematura por alguma política de descarte. Este trabalho introduz mecanismos baseados em transferência de custódia para aumentar o desempenho em redes DTN. Para isso, dois mecanismos são propostos. O primeiro, chamado de LJC (*Limited Joint Custody*), propõe o uso da custódia compartilhada e implementa um esquema de replicação controlada para limitar o número de custódias por agregado na rede. O segundo, chamado de FCF (*Forward Custody First*), é uma política de encaminhamento que prioriza os agregados sob custódia. Através de simulações, o desempenho destes mecanismos é avaliado para diferentes protocolos de roteamento em dois cenários distintos baseados em registros reais de mobilidade. Os principais resultados mostram que ambos os mecanismos aumentam a taxa de entrega e também reduzem o atraso nos dois cenários analisados com menor sobrecarga. A combinação dos mecanismos FCF-LJC quando comparada a mecanismos que não usam custódia proporciona um aumento de até 24% na taxa de entrega e reduz em até 40% e 78% o atraso de entrega e sobrecarga de controle, respectivamente. Essa eficiência pode ser observada mesmo em cenários com maior volume de tráfego, onde a combinação FCF-LJC executando sobre um protocolo de replicação probabilística apresenta o melhor desempenho dentre as configurações analisadas.

**Palavras-chave**: Redes Tolerantes a Atraso e Desconexões, transferência de custódia, custódia compartilhada, políticas de encaminhamento.

# Abstract

Custody transfer is a mechanism proposed to increase end-to-end reliability in Delay / Disruption Tolerant Networks (DTNs). With custody transfer, a node delegates to another node the delivery responsibility of a bundle. This responsability means that the node with a bundle in custody can not drop it until it achieves its destination or the TTL expires, thus avoids dropping the bundle prematurely by some dropping policy. This work introduces custody-based mechanisms to improve network performance in DTNs. For this purpose, two mechanisms are proposed. The first one, named LJC (Limited Joint Custody), proposes the use of joint custody and implements a controlled replication scheme to limit the number of custodians per bundle in the network. The second one, named FCF (Forward Custody First), is a forwarding policy that prioritizes bundles in custody. Through simulations, the performance of these mechanisms is evaluated for different routing protocols in two different scenarios based on real traces. Main results show that both mechanisms increase the delivery rate and also reduce the delay in both scenarios with lower overhead. The combination of FCF-LJC mechanisms, compared to implementations with no custody, provides up to 24% higher delivery rate and decreases by 40% and 78% the delivery delay and control overhead, respectively. This efficiency is observed even in scenarios with higher traffic load, where the combination of FCF-LJC running on a probabilistic-replication protocol presents the best performance among all analyzed configurations.

**Keywords**: Delay/Disruption Tolerant Networks, custody transfer, joint custody, forwarding policies.

# Lista de Figuras

# Lista de Tabelas

# Lista de Abreviaturas e Siglas

| | | |
|---|---|---|
| 3G | : | Terceira Geração; |
| BP | : | *Bundle Protocol;* |
| CARNIVORE | : | *Carnivore Adaptive Research Network in Varied Outdoor;* |
| CE | : | Custódia Exclusiva; |
| CBR | : | *Constant Bit Rate;* |
| CHANTS | : | *CHAllenged NeTworkS;* |
| CONDOR | : | *C2 On-the-move Network Digital Over-the-horizon Relay;* |
| DD | : | *Direct Delivery;* |
| DSL | : | *Digital Subscriber Line;* |
| DTN | : | *Delay and Disruption Tolerant Network;* |
| DTNRG | : | *Delay-Tolerant Networking Research Group;* |
| FIFO | : | *First In First Out;* |
| FC | : | Fila de agregados sob Custódia; |
| FCF | : | *Forward Custody First;* |
| FTP | : | *File Transfer Protocol;* |
| FR | : | Fila de agregados Regulares; |
| GPS | : | *Global Positioning System;* |
| IP | : | *Internet Protocol;* |
| IPN | : | *InterPlanetary Network;* |
| IRTF | : | *Internet Research Task Force;* |
| LAN | : | *Local Area Network;* |
| LIFO | : | *Last In First Out;* |
| LJC | : | *Limited Joint Custody;* |
| LRF | : | *Least Recently Forwarded;* |
| MAP | : | *Mobile Access Point;* |
| MULE | : | *Mobile Ubiquitous LAN Extensions;* |
| NECTAR | : | *NEighborhood ConTAct history Routing;* |
| ONE | : | *Opportunistic Network Environment;* |
| ONG | : | Organização Não Governamental; |

| | | |
|---|---|---|
| PDA | : | *Personal Digital Assistant;* |
| PREP | : | *PRiority EPidemc;* |
| PRoPHET | : | *Probabilist Routing Protocol using History of Encounters and Transivity;* |
| PSN | : | *Pocket Switched Networks;* |
| RAPID | : | *Resource Allocation Protocol for Intentional DTN;* |
| RC DESC | : | *Replicated Copies Descending Order;* |
| RFC | : | *Request For Comments;* |
| RR-LRF | : | *Round Robin with Least Recently Forwarded Drop;* |
| RRFS | : | *Round Robin Forwarding Scheduling;* |
| SC | : | Sem Custódia; |
| SeNDT | : | *Sensor Networking with Delay Tolerance;* |
| SFTP | : | *Simple File Transfer Protocol;* |
| SnW | : | *Spray and Wait;* |
| SMTP | : | *Simple Mail Transfer Protocol;* |
| TCP | : | *Transmission Control Protocol;* |
| TMHF | : | *Transmit Max Hop Count First;* |
| TSMF | : | *Transmit Smallest Message First;* |
| TTL | : | *Time To Live;* |
| UDP | : | *User Datagram Protocol;* |

# Sumário

# Capítulo 1

# Introdução

A Internet tornou-se um importante meio de comunicação. Seu alcance é mundial e atualmente é utilizada para realizar diversas atividades relacionadas a ensino, pesquisas, entretenimento e negócios. Em um primeiro momento, os nós das subredes que constituíam a Internet eram predominantemente conectados por fios, formando as chamadas redes cabeadas. Essas redes atualmente apresentam em geral baixas taxas de erro, pequenos atrasos de entrega e altas taxas de entrega devido tanto ao uso eficiente da pilha de protocolos TCP/IP, quanto ao meio em que os dados trafegam. Nelas, presume-se que as taxas de erro sejam baixas devido à baixa atenuação de sinal e também por haver pouca interferência no meio de comunicação e, com isso, minimiza-se a quantidade de retransmissões necessárias para a entrega das mensagens. Esse tipo de rede também apresenta a característica de que seus nós estão a maior parte do tempo conectados. Isso possibilita maiores taxas de entrega e também menores atrasos de comunicação devido à existência de uma conectividade fim-a-fim, ou seja, os nós de origem e de destino estão conectados durante todo o período correspondente às sessões de comunicação.

Entretanto, nos últimos anos houve o aumento da produção e utilização de dispositivos móveis portáteis e o consequente aumento de conexões com a Internet desses dispositivos através de redes sem fios, dentre eles os mais populares são *notebooks/netbooks*, telefones celulares considerados *smartphones* e PDAs (*Personal Digital Assistants*). Além disso, surgiu também a necessidade de levar a conectividade a outros ambientes como zonas rurais [5], campos de batalha [41], redes veiculares [47], redes interplanetárias [4], redes oportunistas [20] e redes de sensores acústicas subaquáticas [44]. Uma característica desses ambientes é a conectividade intermitente, ocasionada pela inexistência ou perda do contato entre os nós devido a fatores como mobilidade, baixa potência do sinal ou mesmo descarregamento de bateria dos nós. Essa intermitência pode causar longos atrasos

e baixas taxas de entrega de mensagens [13]. Como resultado, a tradicional pilha de protocolos TCP/IP é pouco eficiente nesses cenários, pois nela assume-se que há sempre um caminho fim-a-fim entre a origem e o destino. Nesse contexto de ambientes e redes considerados desafiadores, foi definida uma nova categoria de redes denominada Redes Tolerantes a Atrasos e Desconexões (*Delay/Disruption Tolerant Networks* - DTNs) [13].

As Redes Tolerantes a Atrasos e Desconexões ou simplesmente redes DTN adotam como princípio básico o paradigma armazena-carrega-e-encaminha (*store-carry-and-forward*) para lidar com o problema da conectividade intermitente. Nesse paradigma os nós encapsulam as mensagens em agregados e são dotados de *buffers*. Dessa forma, os nós mantêm esses agregados em seu *buffer* durante períodos sem conectividade e tentam encaminhá-los quando um contato é estabelecido com um nó vizinho de acordo com alguma métrica definida pelo protocolo de roteamento. Além disso, encaminhar um agregado significa enviar uma cópia desse agregado e não necessariamente descartá-lo no nó encaminhador. Assim, à medida que os nós mantêm seus agregados encaminhados no *buffer*, mais réplicas trafegam na rede com o objetivo de aumentar as oportunidades de entrega aos nós de destino, bem como diminuir o atraso de entrega desses agregados. Neste contexto, um agregado é removido do *buffer* apenas quando o seu tempo de vida expira, quando ele chega a seu nó de destino ou quando é descartado por políticas de descarte.

Uma consequência do uso do paradigma armazena-carrega-e-encaminha e da replicação de agregados é o transbordamento de *buffers*. Nessa situação, uma política de descarte é acionada quando o *buffer* está cheio ou atinge certo nível de ocupação [37]. Assim, as políticas de descarte são mecanismos que decidem que agregado será descartado do *buffer* para que outro seja recebido mediante a liberação de espaço. Um possível problema nesse contexto é o descarte prematuro, no qual um agregado é descartado em seu nó de origem ou próximo dele. Esse problema tem como consequência direta a redução da taxa de entrega, pois os agregados descartados próximos ao nó de origem não são suficientemente disseminados na rede e, no pior caso, os agregados descartados no próprio nó de origem não possuem qualquer chance de chegar ao nó de destino.

Outra questão importante em redes DTN é a utilização eficiente do tempo de contato entre os nós. Dois nós estabelecem um contato quando um nó está dentro do raio de transmissão de outro nó. A partir desse contato, uma política de encaminhamento é acionada decidindo quais agregados serão encaminhados ao nó vizinho e em que ordem serão enviados. Entretanto, os nós dificilmente transmitem todos os agregados que

desejam encaminhar devido às limitações de largura de banda e de tempo de contato. Portanto, é necessário que as políticas de encaminhamento sejam eficientes por influenciarem diretamente no desempenho da rede.

Muitos mecanismos para redes DTN foram propostos recentemente. Eles abordam diversas questões como protocolos de roteamento [28, 59, 17], políticas de encaminhamento [21, 27, 62] e de descarte [37, 55, 49]. Um mecanismo simples, porém pouco explorado, é a transferência de custódia [15], utilizada neste trabalho para tratar os problemas de descarte prematuro e da utilização eficiente do tempo de contato entre os nós. Basicamente, esse mecanismo consiste em atribuir a custódia de um agregado a um nó específico. O nó detentor da custódia, denominado nó custódio, torna-se responsável pelo agregado e não pode descartá-lo a menos que o mesmo seja entregue ou seu tempo de vida expire. Consequentemente, esse agregado não está sujeito à ação de políticas de descarte. A transferência de custódia é utilizada em redes DTN como uma alternativa para aumentar a confiabilidade da rede, pois com ela é possível garantir que agregados sob custódia trafeguem pela rede sem estarem sujeitos a descartes prematuros. A transferência de custódia também é conhecida como custódia exclusiva e uma variação desse mecanismo é a custódia compartilhada, onde mais de um nó é responsável pela custódia de um agregado.

A literatura de redes DTN, entretanto, não dispõe de trabalhos que proponham e avaliem o uso da transferência de custódia de forma isolada, apenas alguns trabalhos a avaliam de forma combinada com outros mecanismos. Também não há propostas específicas para mecanismos de custódia compartilhada, bem como inexistem estudos direcionados a políticas de encaminhamento associadas a agregados sob custódia. Apenas trabalhos anteriores tentam aumentar a confiabilidade da rede usando mecanismos de custódia exclusiva. Um dos objetivos deste trabalho é então propor mecanismos relacionados à transferência de custódia, particularmente relacionados à custódia compartilhada e às políticas de encaminhamento para agregados sob custódia. Para isso, são propostos o mecanismo *Limited Joint Custody* (LJC) e a política de encaminhamento *Forward Custody First* (FCF). O LJC é um mecanismo de custódia compartilhada cuja ideia é replicar agregados sob custódia na rede com o objetivo de aumentar a probabilidade de entrega desses agregados. Entretanto, o LJC limita o número de custódias por agregado na rede, minimizando o esgotamento prematuro de recursos de armazenamento. Já o mecanismo FCF é uma política de encaminhamento que prioriza o encaminhamento de agregados sob custódia. A ideia da FCF é baseada no fato de que encaminhar primeiro um agregado sob custódia pode acelerar o tempo de entrega. Consequentemente, depois de entregue, os nós

podem remover esse agregado do *buffer*, disponibilizando espaço para novos agregados. Adicionalmente, pode-se aumentar a probabilidade de entrega.

Outro objetivo deste trabalho é avaliar, através de simulações, o ganho de desempenho que pode ser obtido com a transferência de custódia. Para atingir esse objetivo, as simulações foram realizadas com os protocolos *Epidemic* [61], PRoPHET [30] e *Spray and Wait* [58], três protocolos relevantes da literatura, juntamente com registros reais de mobilidade. As análises consideram o desempenho dos mecanismos em relação à taxa de entrega, ao atraso médio de entrega e à sobrecarga de mensagens. Especificamente, o desempenho do mecanismo LJC é comparado ao do mecanismo de custódia exclusiva e também ao desempenho das versões nativas dos protocolos, sem o uso de transferência de custódia. Já a política FCF tem seu desempenho comparado ao desempenho das políticas de encaminhamento nativas dos protocolos analisados. Por fim, é realizada uma combinação dos mecanismos LJC-FCF e seu desempenho é comparado ao de mecanismos que não usam transferência de custódia. Além disso, avaliou-se o impacto dos mecanismos para diferentes volumes de tráfego com o objetivo de verificar o comportamento do uso de mais de um nó custódio por agregado em situações nas quais o transbordamento de *buffer* é mais frequente.

## 1.1 Contribuições

As contribuições deste trabalho são as propostas dos mecanismos de transferência de custódia e a avaliação dos mesmos com protocolos de roteamento parametrizáveis para redes DTN, sendo selecionados os mais relevantes na literatura atual. Especificamente podemos enumerar como contribuições:

- o mecanismo *Limited Joint Custody* (LJC), que implementa o esquema de custódia compartilhada, porém restringe o número de nós custódios por agregado com objetivo de aumentar a probabilidade de entrega dos agregados sob custódia;
- a política de encaminhamento *Forward Custody First* (FCF) e sua variação probabilística, nas quais um nó dá total prioridade aos seus agregados sob custódia, encaminhando-os primeiro em uma oportunidade de contato;
- a avaliação e comparação desses mecanismos com outras propostas da literatura utilizando diferentes protocolos e cenários reais, bem como uma avaliação em um cenário no qual ocorre mais frequentemente o transbordamento de *buffer* devido ao maior volume de tráfego;

- a implementação dessas propostas no simulador *The ONE*.

## 1.2 Organização

Este trabalho está dividido em seis capítulos da seguinte forma. O Capítulo 2 apresenta os cenários desafiadores em que as redes DTN operam. São apresentados ainda seus conceitos básicos e os principais elementos da sua arquitetura. Em seguida, são classificados os tipos de contato e listadas algumas aplicações reais utilizadas como provas de conceito para as redes DTN. Concluindo o capítulo, são discutidas questões de roteamento em redes DTN e os três protocolos utilizados nas simulações deste trabalho são brevemente descritos.

O Capítulo 3 aborda o mecanismo de transferência de custódia e seu uso é discutido como forma de se obter ganhos de desempenho em redes DTN. Primeiramente a custódia exclusiva é apresentada. Posteriormente, o conceito de custódia compartilhada é apresentado como extensão do mecanismo de custódia exclusiva. Por fim, o mecanismo de custódia compartilhada *Limited Joint Custody* (LJC) é introduzido como alternativa para o aumento da taxa de entrega da rede.

O Capítulo 4 define políticas de encaminhamento e discute seu impacto sobre o desempenho geral da rede. Algumas das principais políticas para redes DTN são apresentadas evidenciando-se seus critérios adotados para a escolha e ordenação ao realizar encaminhamentos de agregados. Finalmente, é detalhado o funcionamento da política *Forward Custody First* (FCF), bem como uma variação da mesma para protocolos que utilizam replicação baseada em histórico de contatos.

O Capítulo 5 apresenta a avaliação de desempenho dos mecanismos propostos. Nele são detalhados os registros reais de mobilidade, o ambiente de simulação utilizado, bem como as principais extensões e parametrizações realizadas. Em seguida, as métricas de avaliação de desempenho são brevemente descritas. Por fim, são apresentados e discutidos os resultados das simulações deste trabalho, avaliando-se o impacto dos mecanismos LJC e FCF no desempenho da rede em relação a mecanismos que não utilizam transferência de custódia.

Por fim, no Capítulo 6 são apresentadas as considerações finais sobre a pesquisa realizada. Nele são resumidos os principais pontos e contribuições do trabalho, bem como são recapitulados os principais resultados obtidos. Em seguida, são relacionadas algumas possíveis abordagens para pesquisas futuras.

# Capítulo 2

# Redes tolerantes a atrasos e desconexões

A Internet é um sistema distribuído de abrangência mundial, sendo utilizada como meio de interconexão entre inúmeros tipos de dispositivos e fornecendo acesso à diversas aplicações. Os protocolos definidos pela sua arquitetura foram projetados incialmente para operarem redes cabeadas, nas quais existam premissas como existência de caminhos fim-a-fim entre os nós, baixas taxas de erro e baixos atrasos. Entretanto, há situações em que uma ou mais dessas premissas podem não existir, como por exemplo, em cenários onde os atrasos cheguem a ordem de dias e nos quais ocorram frequentes desconexões devido à mobilidade dos nós. Exemplos de tais cenários são:

- monitoramento ambiental, onde são pesquisados comportamentos da vida animal [24] e também são observados índices de qualidade do ar, água, dentre outros [33];
- comunicações entre dispositivos que possuem restrições de energia, tais como as redes de sensores [53];
- comunicações em áreas de difícil acesso, tais como as redes rurais [5], comunicações em campos de batalha [41] e redes subaquáticas [44];
- redes formadas por pedestres e por veículos em cidades inteligentes, onde a mobilidade dos nós provoca constantes mudanças na topologia da rede [47];
- as comunicações interplanetárias [4] e as comunicações em redes nas quais os nós conseguem se comunicar mesmo que nunca venha a existir um caminho entre eles, as denominadas redes oportunistas [20].

Nesses cenários considerados desafiadores, predominam os longos atrasos e as conexões intermitentes, tornando a pilha de protocolos TCP/IP pouco eficiente. Nos trabalhos de

Demmer *et al.* e Durst *et al.* os autores evidenciam através de simulações que os protocolos TCP (*Transmission Control Protocol*), SMTP (*Simple Mail Transfer Protocol*), FTP (*File Transfer Protocol*) e SFTP (*Simple File Transfer Protocol*) não apresentam bom desempenho nesses cenários [10, 12]. Especificamente no caso do protocolo TCP, falhas nas premissas citadas anteriormente comprometem seu modo de operação, que ocorre em uma sessão de comunicação com três fases distintas [7, 4, 38]. Na primeira fase, estabelecimento de conexão, ocorre o *three-way handshake*, no qual há troca de três mensagens para que a conexão seja estabelecida. Na fase de transferência de dados, o nó receptor deve transmitir ao nó emissor confirmações de recebimentos (ACKs) das mensagens recebidas. Por fim, na fase de encerramento de conexão há a troca de mensagens com o pedido e a confirmação de desconexão. Dessa forma, caso não seja possível determinar um caminho entre dois nós, o protocolo TCP não consegue estabelecer uma conexão e, portanto, não há transmissão de dados. Também é necessário que os atrasos de comunicação sejam pequenos, evitando que ocorram *timeouts* nas transmissões, principalmente nas transmissões de negociação e controle. Por fim, o TCP depende de baixa taxa de erros, pois havendo muitos erros e retransmissões, a sessão de comunicação pode ser encerrada. Possíveis abordagens baseadas no protocolo UDP (*User Datagram Protocol*) resolveriam o problema de estabelecimento da conexão do protocolo TCP, porém também apresentariam falhas quando aplicadas em um contexto de cenários desafiadores. Tais abordagens teriam um baixo desempenho na entrega de agregados por não serem específicas para estes tipos de cenários e por não considerarem os longos períodos sem conexão.

As iniciativas de se especificar alternativas para esses cenários surgiram durante as discussões do projeto da acesso à Internet por meio de Redes Interplanetárias (*InterPlanetary Network* - IPN) [4] devido às semelhanças das soluções desse projeto para problemas de desconexões nas redes terrestres. Assim, surgiram as Redes Tolerantes a Atrasos e Desconexões (*Delay and Disruption Tolerant Networks* - DTNs), que são formadas por redes regionais de arquiteturas tipicamente heterogêneas entre si. A especificação da arquitetura [7] para redes DTN foi então proposta pelo DTNRG (*Delay Tolerant Network Research Group*) com o objetivo de permitir a operação em cenários desafiadores, minimizando os impactos causados pelos longos atrasos e intermitência nas comunicações. As próximas seções apresentam as principais características desses cenários desafiadores e da arquitetura das redes DTN. Em seguida, são classificados os tipos de contato e listadas algumas aplicações reais utilizadas como provas de conceito para as redes DTN. Concluindo o capítulo, são discutidas questões de roteamento em redes DTN e os três protocolos utilizados neste trabalho são brevemente descritos.

## 2.1 Características dos cenários desafiadores

Fall [13] enumera as características das Redes Desafiadoras (*CHAllenged NeTworkS* - CHANTS) que tornam inviáveis as abordagens tradicionais usando a pilha de protocolos TCP/IP. Essas características foram abrangidas nas especificações da arquitetura para redes DTN e são descritas a seguir:

- desconexões: nesse contexto, a mobilidade é uma das causas de desconexão em redes sem fio. Como exemplos, podemos citar o deslocamento dos nós móveis que funcionam como roteadores, tais como um satélite, ônibus ou mesmo uma pessoa com um pequeno dispositivo que sai do alcance de determinada área de cobertura. Há cenários em que as desconexões podem ser mais frequentes do que a existência da conexão. Outras causas de desconexões são os descarregamentos de bateria dos nós, negação de serviços e a utilização de ciclos de trabalho. Nessa última causa, os dispositivos, tipicamente pequenos sensores, definem intervalos nos quais estão ativos e períodos em que estão operando em modo de economia de energia;

- alta latência: o atraso total ou atraso fim-a-fim é influenciado pelo atraso nas filas, atraso de transmissão e atraso de propagação. Já em cenários desafiadores, os atrasos relacionados ao tempo de espera pelo estabelecimento de contatos com os nós da rede [38] possuem grande impacto no atraso total. Nesses cenários, esses atrasos podem variar de segundos a dias devido aos períodos sem estabelecimento de conexão entre os nós;

- baixas taxas de transmissão e assimetria: as redes sem fio possuem como meio de transmissão o ar ou a água. Esses meios possuem taxas de transmissão mais baixas em relação às redes cabeadas pelo fato de suas ondas de transmissão estarem mais sujeitos a ruídos, interferências e atenuações, bem como a obstáculos físicos como árvores e prédios. Outro ponto que influencia as baixas taxas de transmissão é o fato das redes desses cenários serem compostas muitas vezes por dispositivos com baixa potência de transmissão, como é o caso de dispositivos *bluetooth* e sensores. Além disso, alguns dispositivos podem ter taxas assimétricas, priorizando os canais de recepção e reduzindo as taxas de envio;

- interoperabilidade: algumas redes possuem escopo de utilização limitado a problemas específicos e locais, como é o caso das redes de sensores acústicas subaquáticas. Além disso, seus nós podem ter limitações de energia e processamento, levando

a decisões de não implementar pilhas de protocolos complexas, como a pilha de protocolos da arquitetura TCP/IP. Devido a isso, é comum que implementem pilhas de protocolos simplificadas e específicas a um determinado contexto, gerando dificuldades de interoperabilidade com outras redes;

- tempo de vida útil e recursos limitados: redes de emergência, de sensores e militares podem determinar uma curta vida útil aos nós devido à hostilidade do ambiente ou devido à exaustão de recursos de energia. Além disso, nós com limitados recursos de processamento e armazenamento podem estar presentes nas redes citadas. Dessa forma, os protocolos devem utilizar técnicas de gerenciamento de energia e implementar políticas de encaminhamento e gerenciamento de *buffer* que tornem o uso desses recursos eficiente.

## 2.2 Arquitetura de redes DTN

A arquitetura das redes DTN foi proposta como forma de permitir a operação de redes nos cenários considerados desafiadores, minimizando os impactos causados pelos longos atrasos e intermitência nas comunicações. Essa arquitetura está centrada em dois elementos principais: a camada de agregação e o paradigma armazena-carrega-e-encaminha. Um outro elemento importante na arquitetura das redes DTN é a transferência de custódia, no entanto esse mecanismo será abordado em detalhes no Capítulo 3 por ser um ponto central deste trabalho. A seguir são apresentadas as principais características da camada de agregação e do paradigma armazena-carrega-e-encaminha.

### 2.2.1 O paradigma armazena-carrega-e-encaminha

Uma das características dos cenários de aplicação da arquitetura DTN discutidas anteriormente é a conexão intermitente. Isso ocasiona a inexistência de um caminho fim-a-fim, inviabilizando técnicas como a comutação de circuitos. Para amenizar esse problema, as redes DTN fazem uso de comutação de mensagens combinada ao armazenamento persistente. Os nós encapsulam as mensagens em agregados e são dotados de *buffers*. Assim, um agregado ao ser enviado da origem ao destino é armazenado em cada nó intermediário. Os nós mantêm esses agregados em seu *buffer* durante períodos sem conectividade e tentam encaminhá-los quando um contato é estabelecido. Dessa forma, o nó de destino não precisa estar disponível continuamente, pois os nós intermediários armazenam o agregado e o entregam oportunamente. Esse é um princípio básico das redes DTN e é chamado de

paradigma armazena-carrega-e-encaminha (*store-carry-and-forward*).

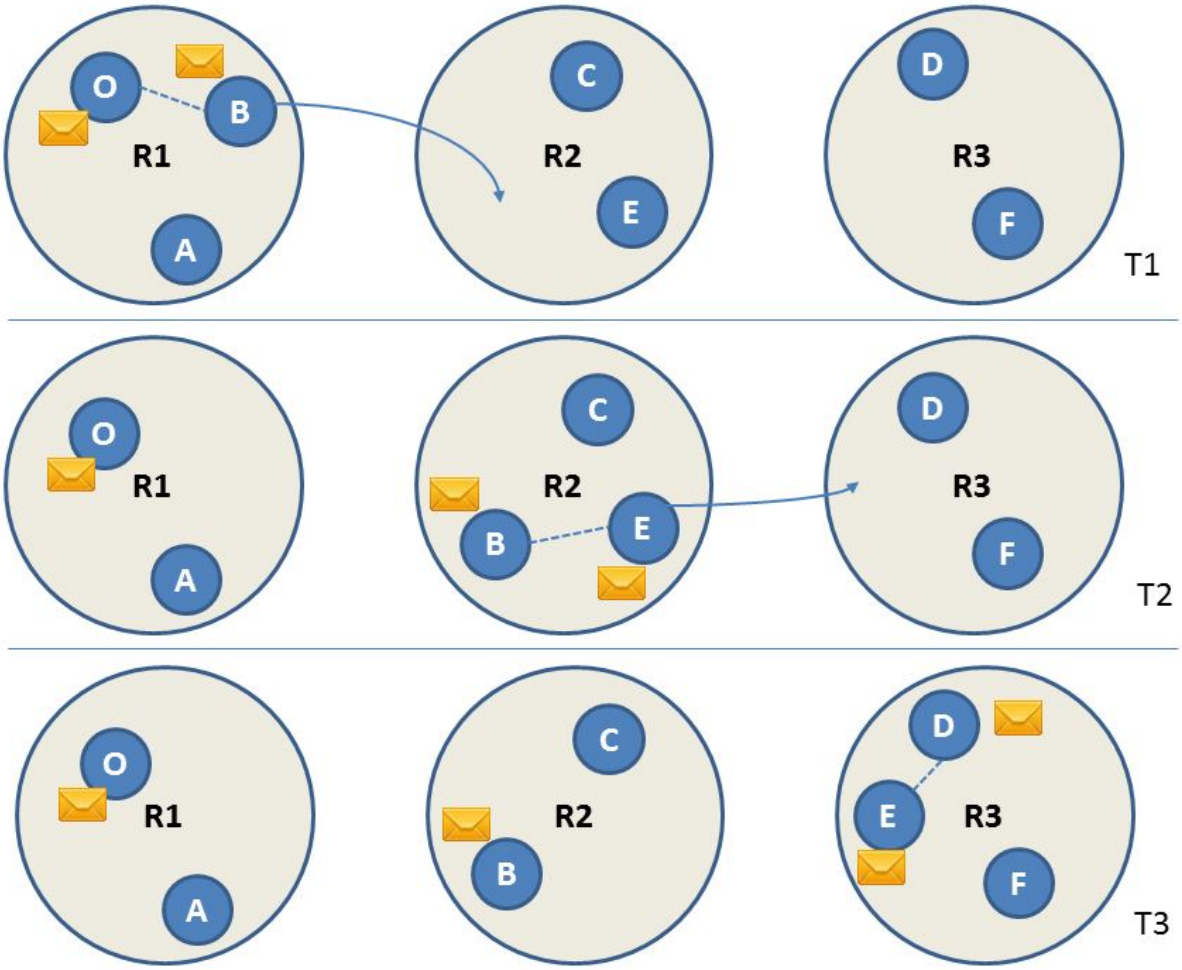



Figura 2.1: Exemplo de operação armazena-carrega-e-encaminha.

A Figura 2.1 ilustra o paradigma armazena-carrega-e-encaminha. Os nós estão representados por círculos azuis e os agregados por ícones de envelopes. Nela há três redes regionais, ou simplismente regiões, representadas por círculos cinzas, e alguns dos nós possuem mobilidade. As setas direcionadas indicam para onde o nó se moverá no próximo instante e as linhas tracejadas indicam o contato entre dois nós. No instante $T1$, um agregado é criado pelo Nó $O$, na região $R1$, com destino ao Nó $D$, que está na região $R3$. Entretanto, não há o caminho fim-a-fim entre eles. O agregado é então replicado para um Nó vizinho $B$. No instante $T2$, o Nó $B$ se desloca para a região $R2$ e replica o agregado para o Nó $E$. Por fim, o Nó $E$ se desloca para a região $R3$ realizando a entrega do agregado ao destinatário no instante $T3$.

### 2.2.2 Camada de agregação

As redes DTN são formadas por redes regionais. Essas regiões representam um agrupamento de nós de uma determinada arquitetura de rede. É possível que alguns dos nós tenham mobilidade e que possam trafegar levando informações para nós de outras regiões com arquiteturas distintas. Esses nós são denominados *gateways* DTN e devem ser capazes de resolver problemas de compatibilidade entre as regiões as quais podem trafegar. A solução proposta pela arquitetura DTN para questões de interoperabilidade entre regiões é a especificação de uma camada denominada camada de agregação (*bundle layer*). Essa camada está situada entre as camadas de aplicação e de transporte e está presente em todos os nós pertencentes a uma rede DTN.

A Figura 2.2 ilustra o posicionamento da camada de agregação em relação à camada de transporte de duas arquiteturas de diferentes regiões. A arquitetura da Região 1 é a TCP/IP e a da Região 2 não é especificada, evidenciando que a camada de agregação deve ser implementada nos *gateways* de modo a interagir com diferentes pilhas de protocolos, de acordo com a tecnologia de cada região.

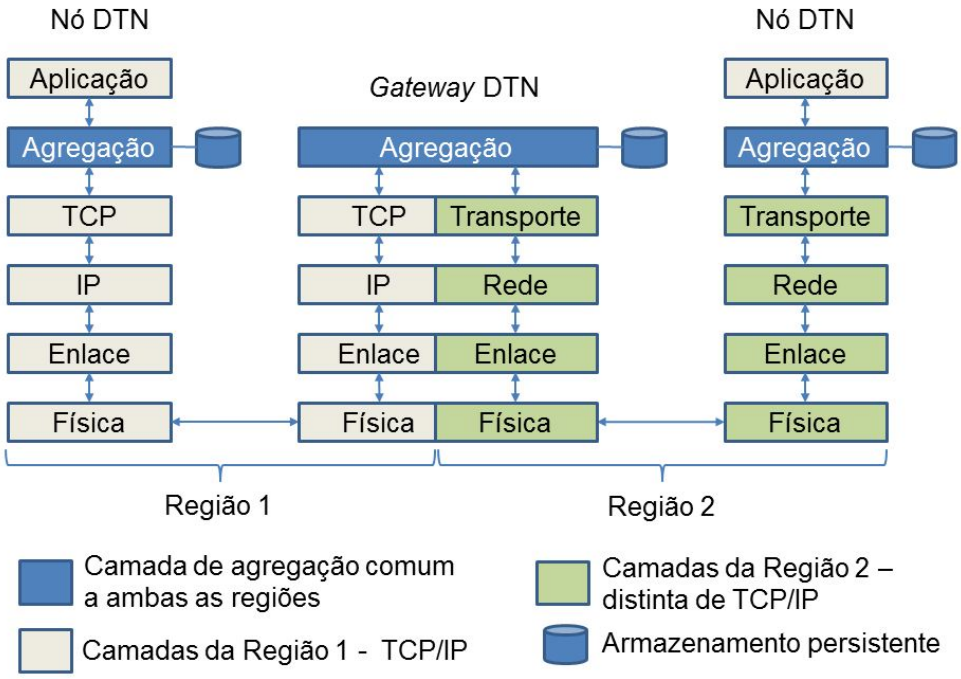



Figura 2.2: A camada de agregação da arquitetura DTN. Baseada em [38].

Além de lidar com questões de interoperabilidade, a camada de agregação tem como função gerenciar a comutação de mensagens e o armazenamento persistente em conformidade com o paradigma armazena-carrega-e-encaminha. Outra função da camada de agregação é criação das unidades de dados da arquitetura DTN, os agregados (*bundles*).

Os agregados são formados por uma sequência de duas ou mais mensagens [51]. Nessa camada há um modelo básico de segurança, que pode ser opcionalmente habilitado, protegendo a infraestrutura da rede de acesso não autorizado. É também na camada de agregação que pode ser implementado o mecanismo de transferência de custódia, objeto de pesquisa deste trabalho.

Na camada de agregação estão definidas as regras do protocolo de agregação (*Bundle Protocol* - BP) [51] e cada nó deve ter uma instância desse protocolo em execução. De forma geral, ele é o responsável por gerenciar os contatos entre os nós. Especificamente, cabe ao protocolo executar operações de fragmentação e reagrupamento de agregados, aplicar políticas de encaminhamento e descarte de agregados, bem como executar mecanismos como autenticação e eventuais confirmações de recebimento dos agregados.

## 2.3 Tipos de contato

Na Internet, assume-se que os nós estão boa parte do tempo ativos e aptos a realizarem transmissões. Isso não ocorre em redes DTN pelas próprias características dos cenários envolvidos. As oportunidades de transmissão ocorrem através de contatos, que tipicamente duram curtos intervalos de tempo [7]. Os contatos podem ser classificados como persistentes, sob demanda, programados, previsíveis e oportunistas. Essa classificação se baseia na previsibilidade das ocorrências de encontro entre os nós e na necessidade de que alguma ação prévia seja executada para que o contato possa existir. Pode ocorrer também mais de um tipo de contato dependendo do cenário. A seguir, as características desses tipos de contatos são detalhadas:

- contatos persistentes: estão sempre disponíveis e não necessitam de nenhuma ação para que fiquem e permaneçam ativados. Exemplos clássicos são as conexões para a Internet como DSL (*Digital Subscriber Line*) ou à cabo.

- contatos sob demanda: são semelhantes aos contatos persistentes, mas necessitam de uma ação prévia para serem iniciados. Ao serem instanciados, se mantêm persistentes até que sejam finalizados. Exemplos de contatos sob demanda são os contatos de linha discada de telefone ou via modem de tecnologia *3G* (Terceira Geração), onde é necessário um pedido de conexão para instanciar o contato. Assim, o contato permanece ativo até que o usuário finalize a conexão.

- contatos programados: são agendados de forma determinística e pré-estabelecida.

Os nós envolvidos devem estabelecer o horário e a duração de cada contato previamente. Para que aconteça esse tipo de contato, é necessária uma sincronização com algum tempo de rede ou estampilha de tempo global. Exemplos de contatos programados são os relacionados a aplicações espaciais, nas quais os nós são estações espaciais, planetas e satélites. Outro exemplo são os contatos agendados em redes de sensores onde em horários pré-estabelecidos os nós são ativados e, após o tempo de contato necessário, voltam a ficar inativos ou em modo de espera para poupar energia de suas baterias.

- contatos previsíveis: nesta categoria os nós são capazes de efetuar estimativas a respeito do horário e da duração dos próximos contatos, baseando-se em históricos de contatos já realizados. Esses contatos se diferenciam dos contatos programados pelo grau de incerteza, ou seja, o contato pode não ocorrer mesmo com uma alta probabilidade com base no histórico. Dependendo do grau de confiabilidade das estimativas, podem ser definidas até mesmo rotas de encaminhamento. Contatos previsíveis ocorrem em linhas de ônibus em grandes centros ou em redes rurais esparsas. Nessas linhas, os ônibus são utilizados como nós e são os responsáveis por disseminar os agregados para estações fixas e para outros veículos. Dessa forma, apesar de existirem horários pré-determinados, há apenas uma estimativa do horário, pois estão sujeitos a tráfego congestionado e a problemas mecânicos.

- contatos oportunistas: ocorrem de forma não programada. São contatos em que os nós se comunicam ao acaso a partir do momento em que os dispositivos estejam em um raio de alcance entre si e deixam de existir quando os nós se afastam. Nessa categoria, os nós não possuem conhecimento prévio da disponibilidade e localização de outros nós. Os nós dessa categoria são representados tipicamente por veículos, pessoas e animais. Um exemplo desse tipo de contato é apresentado por Gerla *et al.* [16], onde os carros de uma rede veicular são utilizados para propagar sinais de emergência e informações sobre tráfego quando outras redes falharem em casos de destastres ambientais. Outro exemplo são os contatos realizados entre os usuários de dispositivos portáteis caracterizados dentro do paradigma das redes oportunistas conhecidas como *Pocket Switched Networks* (PSNs) [20]. Esse paradigma está dentro do contexto de redes DTN e nele são utilizados *Personal Digital Assistants* (PDAs) ou *smartphones* que se comunicam de maneira oportunista. As simulações realizadas neste trabalho utilizam registros reais de mobilidade que foram armazenados através de contatos oportunistas. Esses registros são detalhados na Seção 5.1. A principal justificativa para a escolha dessa categoria para as simulações deste trabalho se deve

ao fato dos contatos oportunistas estarem presentes nos cenários mais desafiadores para redes DTN. Além disso, é uma das categorias mais frequentemente citadas na literatura de redes DTN, tendo também vários protocolos de roteamento, políticas de encaminhamento e de gerenciamento de *buffer* propostos com base em contatos oportunistas.

## 2.4 Projetos e Aplicações

Diversos projetos são utilizados como provas de conceito para as redes DTN em todo o mundo. Esses projetos são desenvolvidos onde não há o acesso convencional e viável à Internet, como nas zonas rurais, e também em centros urbanos onde exista infraestrutura de acesso, porém predominem cenários com conexões intermitentes. Os nós de algumas dessas aplicações são denominados mulas de dados (*Mobile Ubiquitous LAN Extensions*) [53]. As mulas possuem importante papel em redes DTN, pois em muitos casos são os nós responsáveis pelo transporte dos agregados entre as regiões com conectividade intermitente e as regiões com acesso à redes conectadas. Essas mulas são tipicamente humanos, animais ou veículos equipados com dispositivos com algum tipo de sensor ou outro dispositivo de transmissão sem fio. A Figura 2.3 exibe um ônibus funcionando como uma mula de dados entre duas regiões: uma isolada e outra com acesso à Internet. O projetos citados nessa seção são classificados em três categorias: aplicações em áreas remotas, aplicações de monitoramento e aplicações para redes veiculares.

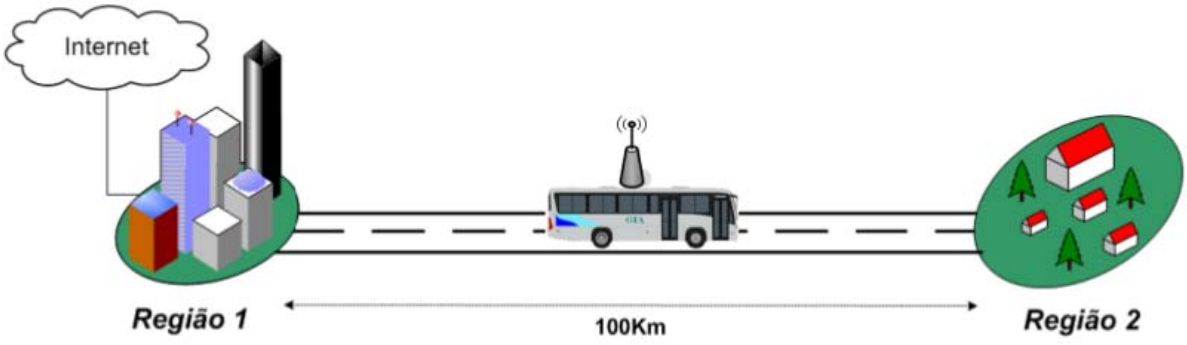



Figura 2.3: Exemplo de mula de dados [38].

### 2.4.1 Aplicações em áreas remotas

Os primeiros projetos criados com redes DTN visam levar conectividade a áreas remotas. Esses projetos estão diretamente relacionados à preocupação social que a exclusão

digital gera. Alguns contam com o incentivo de governos e de ONGs ligadas às causas sociais. Nessas regiões, o acesso à Internet é inviável por questões econômicas ou por características geográficas, tais como, distância, regiões acidentadas, etc. Dois projetos que são descritos neste trabalho são o DakNet e o Kiosknet. Eles possuem finalidade social e têm o objetivo de levar acesso digital para comunidades rurais.

#### 2.4.1.1 DakNet

O projeto DakNet [42] faz uso dos meios de transportes existentes nas regiões para levar acesso à Internet a vilas remotas. Como nessas regiões não é viável tentar transmitir dados por longas distâncias, seja por redes sem fio, por transmissão via satélite ou por meio de estruturas cabeadas , o projeto faz transmissões ponto-a-ponto fazendo uso de quiosques e de Pontos de Acessso Móveis (*Mobile Access Points* - MAPs). Os quiosques são estações fixas de acesso que gerenciam as requisições dos usuários. Já os MAPs funcionam como mulas de dados e são colocados em ônibus, motocicletas ou mesmo bicicletas com pequenos dínamos geradores. Assim, quando os MAPs estabelecem contatos com os quiosques, recebem requisições armazenadas nos quiosques. Posteriormente, já em locais com acesso à Internet, os MAPs enviam as requisições e levam os resultados para a vila conforme ilustra a Figura 2.4. Esse projeto já está implantado em vilarejos da Índia e do Camboja a um custo fracionário do que seria necessário para uma solução tradicional. Apesar de não ser um acesso à Internet em tempo real, a quantidade de dados transmitida é considerável, chegando a superar a quantidade transmitida nas linhas discadas convencionais.

#### 2.4.1.2 KioskNet

O projeto KioskNet [19] é uma iniciativa da Universidade de Waterloo, no Canadá, que tem como objetivo prover acesso à Internet com baixo custo de implantação em quiosques localizados em zonas rurais de países em desenvolvimento. Os quiosques são compostos de um computador reciclado , baterias recarregáveis e painéis solares. Como mulas de dados são usados veículos também equipados com dispositivos controladores que transferem dados para os pontos com acesso à Internet (*gateways*). Até o momento, foram implantados em Anandapuram e Ada, duas vilas da Índia fornecendo acesso a serviços como emissão de certidões de nascimento, óbito, registros de terras e ainda realizar consultas a especialistas relacionadas a problemas de saúde e agricultura. A Figura 2.5 ilustra uma visão dos componentes dos componentes do projeto KioskNet.

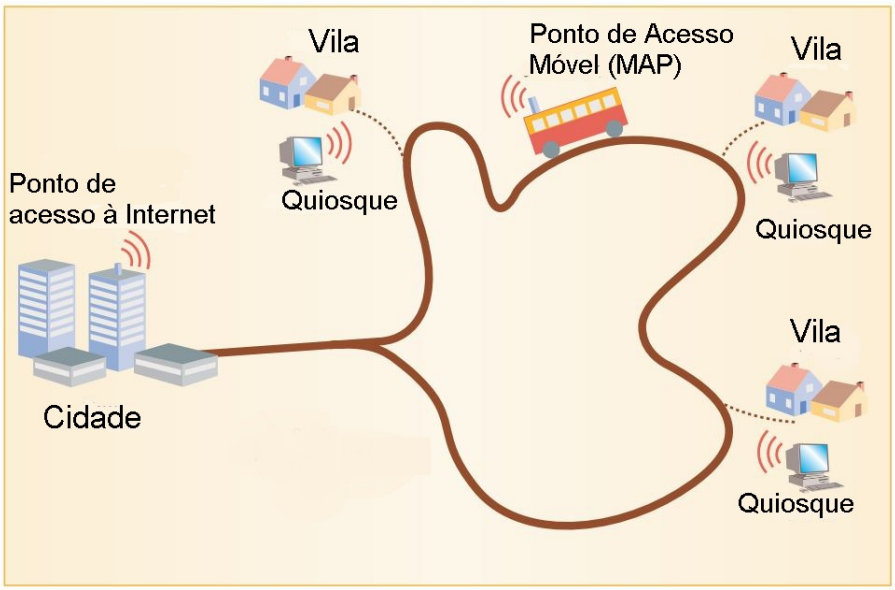



Figura 2.4: Exemplo de funcionamento da DakNet. Adaptada de [42].

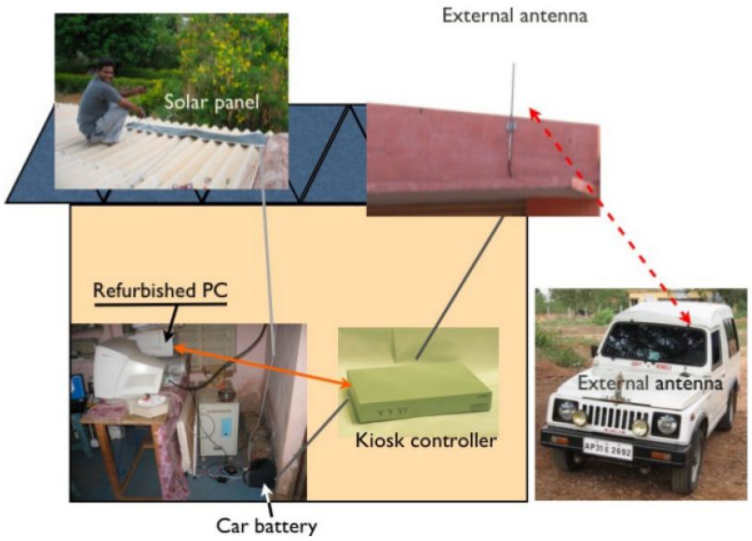



Figura 2.5: Esquema de projeto KioskNet [19].

### 2.4.2 Aplicações de monitoramento

As aplicações de monitoramento relacionadas ao monitoramento da vida animal visam um melhor estudo dos padrões de movimentação e preservação de espécies. Já o monitoramento ambiental e climático tem como objetivo principal analisar níveis de reservatórios, lagos e índices de poluição. O monitoramento realizado com o uso de redes DTN se mostra promissor devido ao fato de que grandes áreas podem ser cobertas com a utilização de nós fixos e nós móveis, usando o conceito de mulas de dados. Alguns exemplos são descritos a seguir.

#### 2.4.2.1 ZebraNet

O ZebraNet [24] é desenvolvido pela Universidade de *Princeton*, nos Estados Unidos, e executado em uma área de preservação no distrito de Laikipia, no Quênia. Um dos objetivos do projeto é monitorar e entender os padrões de migração das zebras no seu território natural. Outro objeto de estudo desse projeto é a relação entre o consumo de energia dos dispositivos utilizados e o protocolo adotado. Para isso, é colocado em cada zebra um colar equipado com um sensor sem fio, memória *flash* e um aparelho GPS (*Global Positioning System*) como ilustrado na Figura 2.6. Os sensores periodicamente coletam e gravam na memória informações sobre a localização e contatos dos animais. Existe ainda uma estação móvel, um veículo que os pesquisadores utilizam para percorrer as áreas por onde as zebras trafegam. Ele tem o papel de mula de dados. Ao entrar no raio de transmissão de um colar, a estação coleta as informações armazenadas nos colares. Como é inviável para os pesquisadores procurarem por todas as zebras monitoradas para obter as informações, o protocolo utilizado no ZebraNet determina que a cada contato oportunista entre zebras, os dados dos seus colares sejam sincronizados. Dessa forma, quando houver um contato entre colar e a estação-base, o maior número possível de informações de diversas zebras será transmitido.

Figura 2.6: Zebra do projeto ZebraNet com um sensor [24].

#### 2.4.2.2 TurtleNet

O projeto TurtleNet [57] foi desenvolvido com o objetivo de estudar o comportamento de uma espécie de tartarugas que tem sua população reduzida no decorrer dos anos. Para

isso, dispositivos foram fixados ao casco de algumas tartarugas e um monitoramento foi realizado durante cinco dias. Os dispositivos eram compostos de um painel de captação de energia solar, uma bateria, um sensor e um GPS. Durante o monitoramento, os dispositivos armazenavam os contatos entre nós vizinhos, coordenadas, o nível e consumo da bateria, bem como dados do ambiente como intensidade da energia solar captada e temperatura. Como o GPS não funcionava quando uma tartaruga submergia, o sensor era utilizado também para registrar esse comportamento e desativar a leitura do GPS, preservando a autonomia do sistema. A Figura 2.7 exibe uma tartaruga equipada com um desses dispositivos.

Figura 2.7: Tartaruga monitorada pelo projeto TurtleNet [57].

#### 2.4.2.3 CARNIVORE

O projeto CARNIVORE (*Carnivore Adaptive Research Network in Varied Outdoor Remote Environments*) [48] possui o mesmo objetivo do ZebraNet e do TurtleNet, que é monitorar o comportamento de animais selvagens em seu habitat natural. Também possui a característica de trabalhar com contatos oportunistas e ter nós fixos e móveis. O diferencial desse projeto é a complexidade do *hardware* utilizado e das informações coletadas sobre os animais. Os colares utilizados no projeto são capazes de coletar 2 GB de dados em cartões de memória comerciais. Os colares de outros projetos possuem no máximo capacidade de armazenamento de 450 KB. O *hardware* do colar conta com um acelerômetro de 3 eixos. Com esses registros é possível aferir situações em que o animal esteja correndo e lutando, dentre outros comportamentos. O colar possui baterias comerciais que dão ao dispositivo autonomia de 50 a 100 dias dependendo do comportamento

do animal monitorado. Um exemplo do colar utilizado no projeto está na Figura 2.8.

Figura 2.8: Colar utilizado no projeto CARNIVORE [48].

Os primeiros experimentos foram realizados com coiotes e atualmente são feitos experimentos com leões. O local das pesquisas atualmente são as montanhas de Santa Cruz, na Califórnia. Apesar do alto custo dos dispositivos, comparados aos demais, os autores da pesquisa evidenciam que o custo/benefício do sistema é viável e muito útil para a pesquisa da vida selvagem.

#### 2.4.2.4 SeNDT

O projeto SeNDT (*Sensor Networking with Delay Tolerance*) [33] foi iniciado em dezembro de 2002 e tem como objetivo auxiliar as autoridades no monitoramento de recursos ambientais. Mais especificamente, visa monitorar os níveis e a qualidade da água de lagos de áreas rurais e a poluição sonora em rodovias na Irlanda.

Para o monitoramento de lagos, o projeto utiliza redes de sensores como os da Figura 2.9 divididos em várias regiões dos lagos. A partir daí são coletados dados sobre temperatura, profundidade, turbidez e minerais. Ainda são utilizadas mulas de dados que trafegam nas regiões coletando informações dos sensores e levando para estações-base. Já para o monitoramento da poluição sonora em rodovias foram instaladas unidades de sensoriamento em veículos com antenas. Então os operadores do sistema trafegavam por

Figura 2.9: Sensor de monitoramento do projeto SeNDT[33].

rodovias coletando informações sobre níveis de poluição sonora que posteriormente são transferidas para estações-base para serem avaliadas.

### 2.4.3 Aplicações para redes veiculares

No contexto das redes DTNs, os veículos podem ser usados apenas como simples mulas de dados ou terem ainda papel mais relevante, como nas aplicações em cidades inteligentes. Nessas cidades, os dados das aplicações veiculares são analisados e utilizados para gerência de tráfego, em pesquisas, para auxiliar na sinalização e para prevenir acidentes. A seguir, dois projetos para redes veiculares são descritos.

#### 2.4.3.1 TrainNet

O projeto TrainNet [65] utiliza trens para transportar por longas distâncias dados que não necessitam ser transferidos em tempo real, como arquivos de áudio e vídeo. Para isso, uma rede ferroviária é utilizada tendo como mulas de dados trens equipados com discos rígidos de alta capacidade para armazenar, transportar e encaminhar os dados para estações. As estações e trens são também equipados com dispositivos de comunicação sem fio para efetuarem as transferências de dados.

A Figura 2.10 mostra um exemplo do uso do projeto TrainNet interligando duas redes $A$ e $B$. Na figura há pontos de acesso, que são locais físicos onde há servidores e roteadores. A rede $A$ está conectada às estações 5, 6 e 7 pelos pontos de acesso $A.1$, $A.2$ e $A.3$. Já a rede $B$ está conectada às estações 5 e 8 pelos pontos de acesso $B.4$ e $B.5$. Como exemplo,

os autores sugerem em [65] que *terabytes* de dados podem ser enviados do ponto de acesso $A.1$ ao ponto $B.5$, via trem, em uma fração de tempo que levaria se os dados trafegassem passando pela estação 5,ponto de acesso $B.4$ e demais nós da rede $B$ até chegar ao destino em $B.5$.

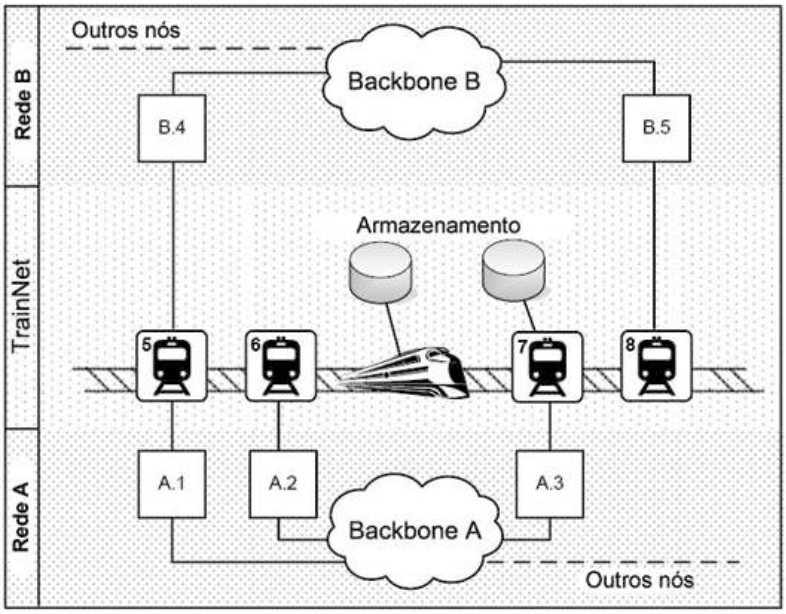



Figura 2.10: Exemplo de utilização do projeto TrainNet interligando duas redes. Os pontos de acesso são representados por $A.1$, $A.2$, $A.3$, $B.4$ e $B.5$ Adaptado de [65].

#### 2.4.3.2 DieselNet

O projeto DieselNet [3] foi desenvolvido pela da Universidade de Massashusetts Amherst, Estados Unidos. Nele, alguns ônibus da cidade de Amherst são equipados com dispositivos de comunicação e, à medida que eles trafegam pela cidade, ocorrem conexões entre os ônibus (nós móveis) e estações-base (nós fixos) em uma área de 150 milhas quadradas da cidade de Amherst. A principal finalidade do projeto é servir como ambiente de experimentação (*testbed*) fornecendo registros reais de mobilidade que são disponibilizados para pesquisas sobre padrões de mobilidade e algoritmos de roteamento. Já para os usuários do projeto, são fornecidos serviços de acesso à redes sociais e busca na *Web*.

Cada ônibus é equipado com uma suíte de equipamentos denominada *diesel bricks* como ilustrado na Figura 2.11. Nessa suíte há um computador rodando Linux e um programa que permite o gerenciamento de aplicações, atualizações e sincronização de informações sobre a mobilidade dos ônibus. Além do computador, há antenas de radio e um dispositivo de GPS. Uma das antenas provê acesso interno aos passageiros. Uma segunda tem a responsabilidade de procurar por outros ônibus, estabelecer contatos e

realizar sincronização de dados entre eles. Uma última antena de longo alcance é a responsável pela comunicação com as estações-base.

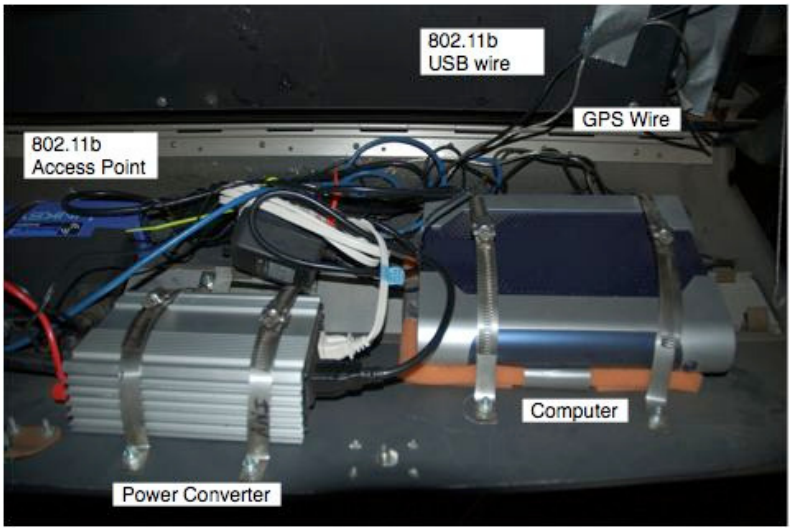



Figura 2.11: Unidade de comunicação dos ônibus do projeto DieselNet [3].

## 2.5 Roteamento em redes DTN

Os protocolos de roteamento para redes de computadores, tradicionalmente, assumem que os nós da rede formam grafos conectados e contam com a existência de pelo menos um caminho fim-a-fim entre quaisquer pares de nós fonte-destino [6]. Além disso, consideram que existem nós ativos e disponíveis a maior parte do tempo, o que faz com que os pacotes permaneçam nos *buffers* dos nós apenas enquanto são encaminhados para outros nós intermediários entre fonte e destino. Já em redes DTN, o roteamento se torna um desafio, pois nelas os protocolos devem ser capazes de lidar com longos atrasos e frequentes desconexões. Além disso, nos cenários de utilização mais desafiadores dessas redes há poucas informações sobre o estado da rede e rotas ativas, bem como sobre a disponibilidade dos nós. No caso específico de roteamento onde predominam contatos oportunistas, o desafio é ainda maior, pois os contatos podem durar pequenos intervalos de tempo e as rotas se modificam durante o tempo de vida da rede. Além disso, um contato oportunista que ocorrera recentemente pode nunca mais acontecer devido à indisponibilidade ocasionada pela mobilidade ou pela falta de energia dos nós [38]. É possível também que dois nós específicos jamais estabeleçam um contato e assim nunca exista um caminho fim-a-fim entre a origem e o destino. Consequentemente, tentar calcular e prever rotas em redes DTN se torna muito complexo e, em alguns casos, até mesmo inviável.

Nos trabalhos de Balasubramanian *et al.* [6] e Spyropoulos *et. al* [59] os protocolos

para redes DTN são classificados em duas categorias distintas: protocolos baseados em encaminhamento e protocolos baseados em replicação. Os protocolos baseados em encaminhamento são caracterizados por manter no máximo uma cópia de cada mensagem na rede, como é o caso do protocolo Direct Delivery (DD) [18], no qual os agregados são encaminhados somente para o destino. Já os protocolos baseados em replicação são caracterizados por criarem várias cópias dos agregados na rede. Com isso, pretende-se atacar o problema da conectividade intermitente da rede, permitindo que os agregados possam trafegar por múltiplos caminhos e, assim, aumentar a probabilidade da entrega e reduzir o atraso dos agregados. Os protocolos baseados em encaminhamento são menos eficientes quando comparados aos baseados em replicação devido ao fato de seus agregados possuírem apenas uma cópia trafegando na rede. Assim, um determinado agregado nessa categoria possui uma única cópia trafegando por uma rota que não necessariamente o levará ao nó de destino. Além disso, em caso de descarte desse agregado, não existirão outras cópias na rede, eliminando assim sua probabilidade de entrega. Dessa forma, os protocolos escolhidos para avaliar as propostas desse trabalho pertencem à categoria de protocolos baseados em replicação por possuírem melhores desempenhos. Foram selecionados os protocolos *Epidemic* [61], PRoPHET [30] e *Spray and Wait* [58], três dos mais citados na literatura para redes DTN e respectivamente os mais relevantes em subcategorias distintas: inundação, replicação probabilística e replicação controlada. A seguir, esses protocolos são apresentados e discutidos brevemente.

### 2.5.1 O protocolo *Epidemic*

O protocolo *Epidemic* [61] é uma das primeiras propostas de protocolos de roteamento para DTNs e se caracteriza por inundar a rede com cópias dos agregados. Assim, quando há um contato entre dois nós, primeiramente, eles trocam informações sobre os agregados armazenados através da troca de vetores de índices (*summary vectors*). Isso é feito para que não sejam transmitidos ao nó vizinho agregados que ele já possua, evitando assim o consumo desnecessário de recursos. Em seguida, cada nó encaminha uma cópia dos agregados que o nó vizinho não possui. Assume-se que, quanto mais cópias de um agregado forem encaminhados na rede, maior será a sua probabilidade de entrega.

A Figura 2.12 ilustra a dinâmica do protocolo *Epidemic* à medida que os nós se movimentam e estabelecem contatos. São representados diferentes instantes de tempo, cada um indicando um estado diferente da rede. Os nós com um ícone de mensagem ao lado estão contaminados, ou seja, possuem uma cópia do agregado. As setas representam

a mobilidade dos nós e mostram para onde eles se movimentarão no próximo instante da figura. No instante $T1$, um agregado é criado pelo Nó $O$ tendo como destino o Nó $D$. À medida que um nó infectado estabelece um contato, o agregado é replicado como ilustrado nos instantes $T2$ e $T3$. Após ser replicado por vários nós intermediários, o agregado é entregue ao nó de destino $D$ no instante $T4$.

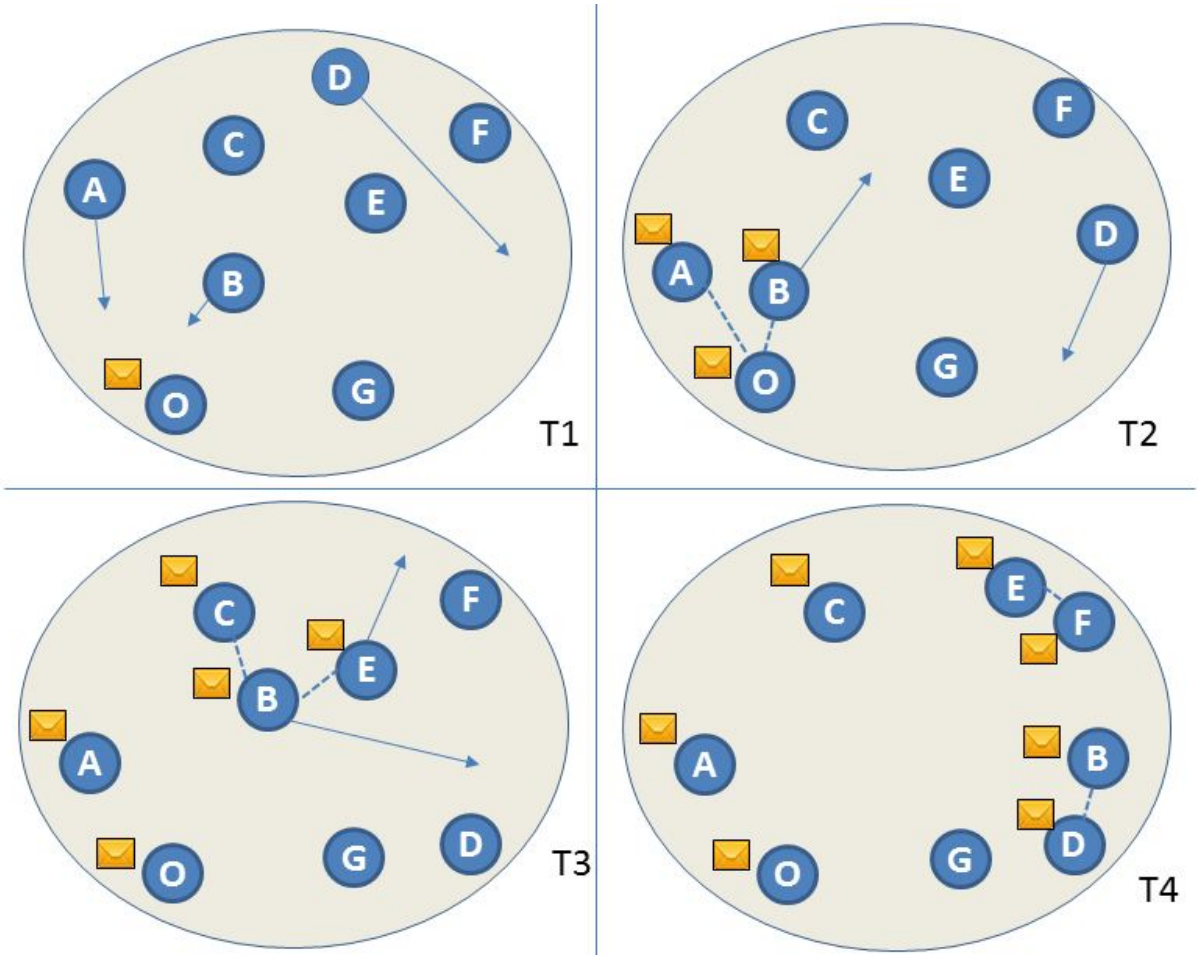



Figura 2.12: Um exemplo de encaminhamento de agregados com o protocolo *Epidemic*. Baseada em [38].

A estratégia de replicação usada pelo *Epidemic* pode aumentar a probabilidade de entrega e reduzir o atraso dos agregados entregues. Para tanto, é necessário que existam recursos suficientes nos nós, como capacidade de armazenamento e largura de banda, além de tempo de contato suficiente para o encaminhamento bilateral dos agregados não comuns. Entretanto, essa escolha da estratégia de replicação do *Epidemic* pode levar à exaustão desses recursos, à medida que o número de nós e de agregados na rede aumente. Nesse caso, observam-se descartes prematuros de agregados que ainda não foram entregues aos seus destinos e maior sobrecarga de controle, o que pode comprometer a escalabilidade do protocolo [45].

Apesar das limitações de escalabilidade, ainda possui relevância na literatura de redes DTN, pois influencia e é base para o projeto de muitos outros protocolos como os protocolos *PRiority EPidemc* (PREP) [45], NECTAR (*Neighborhood Contact History Routing*) [40], MaxProp [3], *Fuzzy-spray* [32], dentre outros relacionados nos trabalhos de Khabbaz *et al.* [26] e Cao *et al.* [6]. Apenas a proposta original do protocolo *Epidemic* é considerada para a avaliação das propostas deste trabalho.

### 2.5.2 O protocolo PRoPHET

O PRoPHET (*Probabilistic Routing using History of Encounters and Transitivity*) é um protocolo de roteamento probabilístico proposto por Lindgren *et al.* [30]. A ideia geral desses protocolos é que os nós não necessariamente realizam encaminhamentos para todos os nós com os quais estabelecem contatos como fazem o *Epidemic* e suas variações. Nessa categoria de roteamento, são realizados cálculos estimando-se a probabilidade dos agregados alcançarem seu destino a partir de determinados nós. Baseando-se nessas estimativas, os nós decidem a quais nós e quando devem realizar encaminhamentos. No caso do ProPHET, são usadas informações sobre históricos de encontros para calcular a probabilidade dos nós se encontrarem novamente. Essa probabilidade é mantida através de uma métrica denominada previsibilidade de entrega (*delivery predictability*), $P_{(a,b)} \in [0,1]$, que é calculada em cada nó $a$ para cada nó $b$ com o qual já se tenha estabelecido contato prévio. A Equação 2.1 detalha $P_{(a,b)}$, onde $P_{init} \in [0,1]$ é uma constante de inicialização:

$$P_{(a,b)} = P_{(a,b)old} + (1 - P_{(a,b)old}) \times P_{init}. \tag{2.1}$$

Dessa forma, ao estabelecer um contato, o nó $a$ envia para $b$ os agregados cujo destino é um nó $d$ apenas se a probabilidade de entrega para $d$ a partir de $b$ for maior que a probabilidade de entrega para $d$ a partir de $a$, $P_{(a,d)} < P_{(b,d)}$.

O valor $P_{(a,b)}$ é influenciado pela quantidade e pela frequência de encontros entre os nós. À medida que $a$ e $b$ se encontram, o valor de $P_{(a,b)}$ aumenta. Porém, se $a$ e $b$ deixam de se encontrar frequentemente, $P_{(a,b)}$ diminui. Isso se deve à aplicação da Equação 2.2, denominada equação de envelhecimento, onde $\gamma \in [0,1]$ é um fator de envelhecimento e $k$ representa o número de unidades de tempo transcorridas desde a última atualização da previsibilidade de entrega.

$$P_{(a,b)} = P_{(a,b)old} \times \gamma^k \tag{2.2}$$

As informações sobre a probabilidade de encontro são calculadas também de forma transitiva. Assim, caso um nó $a$ realize contatos frequentes com um nó $b$ e este por sua vez tenha realizado muitos contatos com um nó $c$, o PRoPHET conclui que encaminhar agregados a partir de $a$ tendo como destino o nó $c$ é uma escolha com alta probabilidade de entrega. Essa propriedade é calculada através da Equação 2.3, onde $\beta \in [0, 1]$ é uma constante que define o impacto que a transitividade deve ter na previsibilidade de entrega.

$$P_{(a,c)} = P_{(a,c)old} + (1 - P_{(a,c)old}) \times P_{(a,b)} \times P_{(b,c)} \times \beta. \tag{2.3}$$

Um exemplo dessa propriedade transitiva é ilustrada na Figura 2.13. Nessa figura, o Nó $O$ possui um agregado a ser entregue ao Nó $D$. Também são exibidas na figura a probabilidade dos nós $O$, $A$ e $B$ encontrarem o Nó $D$. Nos instantes $T1$ e $T2$ o Nó $O$ estabelece contatos respectivamente com os nós $A$ e $B$. Entretanto, apenas o Nó $A$ tem maior probabilidade de entregar o agregado ao Nó $D$ transitivamente. Assim, no instante $T2$, o nó $O$ encaminha uma cópia do agregado para o Nó $A$. No instante $T3$, o agregado é entregue ao Nó $D$ pelo nó $A$ e as probabilidades de novos encontros são atualizadas. No caso de $A$, a probabilidade de encontrar $D$ novamente é aumentada devido ao contato recente. Para os outros dois nós, essa probabilidade é reduzida, por ação da equação de envelhecimento (Equação 2.2).

O PRoPHET utiliza uma política de encaminhamento chamada GRTRMax, que é a responsável pelo mecanismo de encaminhamento utilizando-se dos cálculos apresentados nessa seção. O seu funcionamento é explicado na Seção 4.1. Ainda sobre o protocolo PRoPHET é importante comentar que trata-se de um dos protocolos mais citados na literatura de redes DTN. Devido a essa relevância, está especificado em detalhes na RFC (*Request For Comments*) 6693 [29] (*Probabilistic Routing Protocol for Intermittently Connected Networks*) e possui ainda implementações de referência, como a IBR-DTN [50].

### 2.5.3 O protocolo *Spray and Wait*

Apesar do PRoPHET minimizar os efeitos colaterais do roteamento epidêmico através do roteamento probabilístico, ainda assim não há um controle sobre a quantidade de replicações dos agregados. Os protocolos de replicação controlada, em especial o *Spray and Wait* [58], limitam a quantidade de cópias dos agregados na rede com o objetivo de reduzir a sobrecarga e sem comprometer as taxas de entrega e o atraso dos agregados.

O funcionamento do protocolo *Spray and Wait* consiste em duas etapas. A primeira

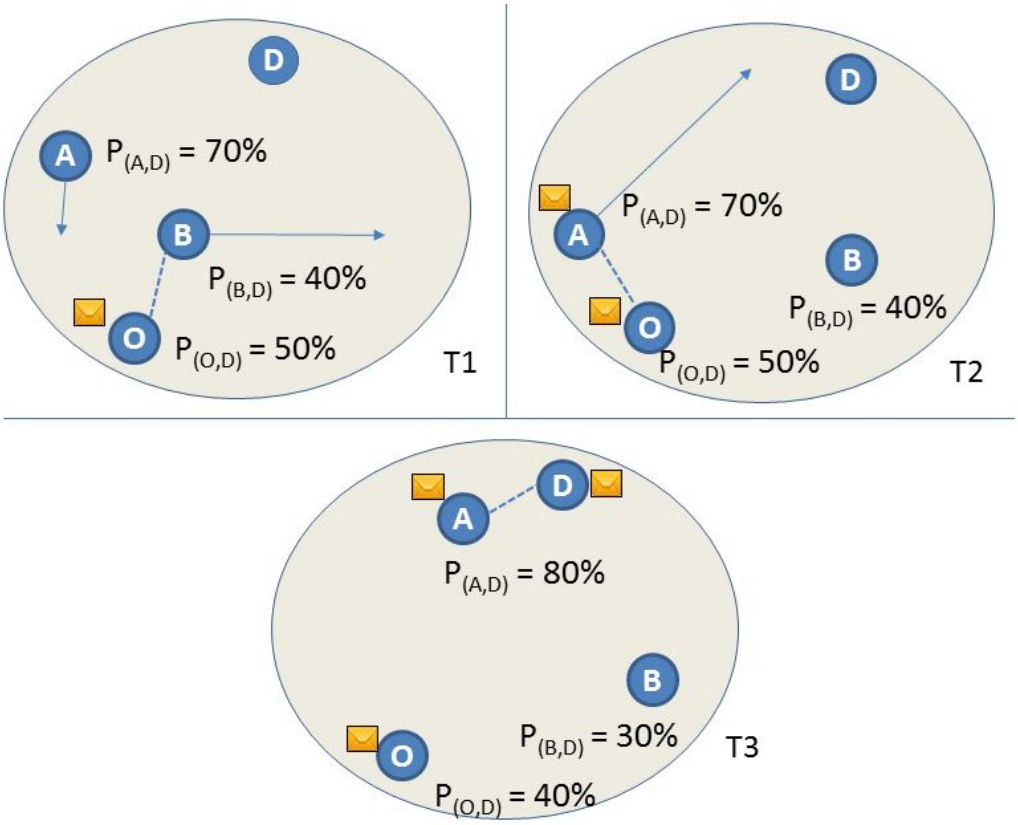
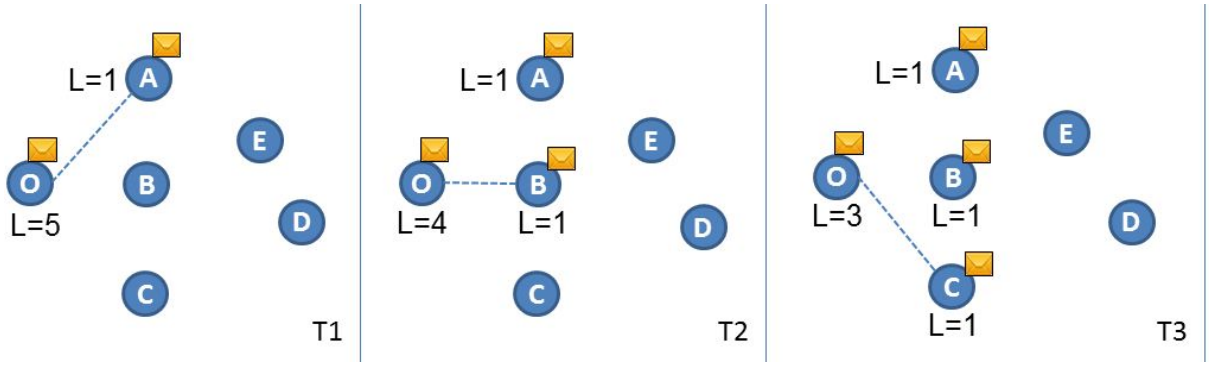



Figura 2.13: A propriedade de transitividade no protocolo PRoPHET.

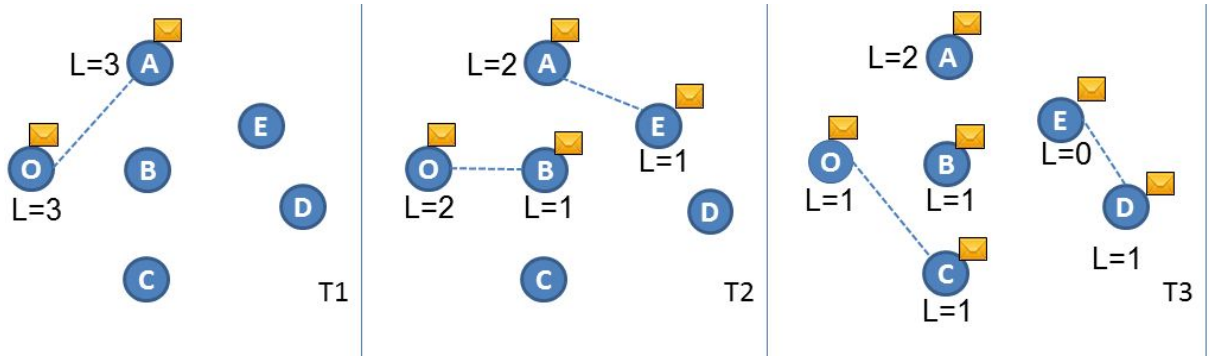
etapa é denominada espalhamento (*spray*) e é baseada em tíquetes de replicação, denotados por uma variável $L$ que é definida no cabeçalho de cada agregado, que representa que um nó pode replicar no máximo $L$ vezes o mesmo agregado. Na segunda etapa, denominada espera (*wait*), a disseminação dos agregados é interrompida, aguardando-se que os nós para os quais foram distribuídas as réplicas da primeira fase realizem a entrega diretamente ao nó de destino, assim como no protocolo *Direct Delivery* (DD) [18].

O protocolo *Spray and Wait* possui dois modos de operação na fase de espalhamento, o *Source Spray* e o *Binary Spray*. A diferença entre os dois modos se dá na forma de distribuição e decremento dos tíquetes de replicação. No primeiro modo, o nó de origem distribui um tíquete de um agregado a cada contato, ficando o nó de origem com $L-1$ tíquetes e o nó vizinho com $L$=1. Nessa forma de distribuição de tíquetes, apenas o nó original é capaz de replicar os agregados e aqueles que possuem $L$=1 podem apenas realizar a entrega direta. Já no modo binário, os tíquetes $L$ são divididos de forma binária entre o nó origem e o nó vizinho. Assim, o nó original mantém $\lceil \frac{n}{2} \rceil$ tíquetes, enquanto o nó vizinho recebe $\lfloor \frac{n}{2} \rfloor$ tíquetes de replicação para o agregado encaminhado. Consequentemente, ambos os nós podem distribuir novas cópias pela rede. Esse modo de operação proporciona uma melhor distribuição de agregados por permitir que vários

nós possam disseminar cópias na rede. Com isso também se evita que a disseminação de agregados seja comprometida devido à falha ou descarregamento de bateria de nós que possuam agregados com muitos tíquetes.




(a) *Source Spray.*




(b) *Binary Spray.*

Figura 2.14: Modos de operação do protocolo *Spray and Wait*. Baseada em [39].

A Figura 2.14 exemplifica os dois modos de operação do protocolo *Spray and Wait*. Nela se considera o envio de um agregado do nó de origem $O$ para o nó de destino $D$ tendo a quantidade inicial de tíquetes de replicação $L = 6$. A Figura 2.14(a) utiliza o modo *source spray*, onde a distribuição é feita apenas pelo nó fonte. Como consequência, apenas os nós vizinhos ao nó fonte recebem réplicas, limitando o espalhamento dos agregados na rede. Nos instantes $T1$, $T2$ e $T3$ o Nó $O$ encaminha um agregado aos seus nós vizinhos. Como os nós vizinhos possuem apenas um tíquete, não podem espalhar cópias do agregado. Consequentemente, o agregado não atinge o seu destino. Já na Figura 2.14(b), o modo binário é utilizado e a replicação é feita tanto pelo nó fonte como pelos nós intermediários, pois os tíquetes $L$ são compartilhados de forma binária. Com isso, no instante $T3$ o agregado é entregue ao destino, pois os agregados tiveram uma melhor distribuição na rede.

# Capítulo 3

# Transferência de custódia

O uso do paradigma armazena-carrega-e-encaminha e da replicação de agregados em redes DTN permitem que os nós mantenham seus agregados no *buffer* mesmo após encaminhá-los. Com isso, mais réplicas passam a trafegar pela rede e aumenta-se a probabilidade de entrega desses agregados aos nós de destino. Neste contexto, um agregado é removido do *buffer* apenas quando o seu tempo de vida expira, quando ele chega a seu nó de destino ou quando é descartado devido ao transbordamento do *buffer*. Nessa situação, uma política de descarte é acionada quando o *buffer* está cheio ou atinge certo nível de ocupação [37]. As políticas de descarte são então mecanismos que decidem que agregado será descartado, liberando espaço para que outro seja recebido. Dependendo do critério de descarte, essas políticas podem realizar descartes prematuros, nos quais os agregados são descartados ainda em seus nós de origem ou próximo deles. Esse problema tem como consequência direta a redução da taxa de entrega. Tal redução acontece, pois agregados descartados próximos ao nó de origem não são suficientemente disseminados na rede e, no pior caso, os agregados descartados no próprio nó de origem não possuem qualquer chance de chegar ao nó de destino.

A transferência de custódia é um mecanismo de uso opcional especificado na camada de agregação que pode ser utilizado para minimizar o problema do descarte prematuro de agregados, aumentando a confiabilidade fim-a-fim [15]. Nela, delega-se a responsabilidade da entrega de um agregado de um nó para outro nó específico, denominado custódio, e dessa forma o nó deve manter em seu *buffer* todo agregado que está sob sua custódia até que os agregados alcancem seu destino ou até que seu TTL expire. Dessa forma, agregados sob custódia não estão sujeitos à ação de políticas de descarte e consequentemente não podem ser descartados prematuramente. Um ponto a ser observado é que apesar do mecanismo de custódia afetar a atuação de políticas de descarte, esses dois mecanismos

não são concorrentes ou excludentes entre si, mas sim complementares conforme ilustra a Figura 3.1. Nela, é representado o contato entre dois nós em que o Nó $A$ precisa transmitir ao Nó $B$ um agregado, destacado com um contorno mais espesso. O Nó $B$ está com o *buffer* cheio e nele são exibidos dois agregados sob custódia, simbolizados com a letra $C$ (custódia), e um agregado sem custódia, denominado neste trabalho como agregado regular. A política de descarte é então acionada como mostra a Figura 3.1(b). Como os dois agregados estão sob custódia e não podem ser descartados pela política, o agregado regular é escolhido para o descarte, liberando espaço para que o novo agregado seja recebido, Figura 3.1(c).

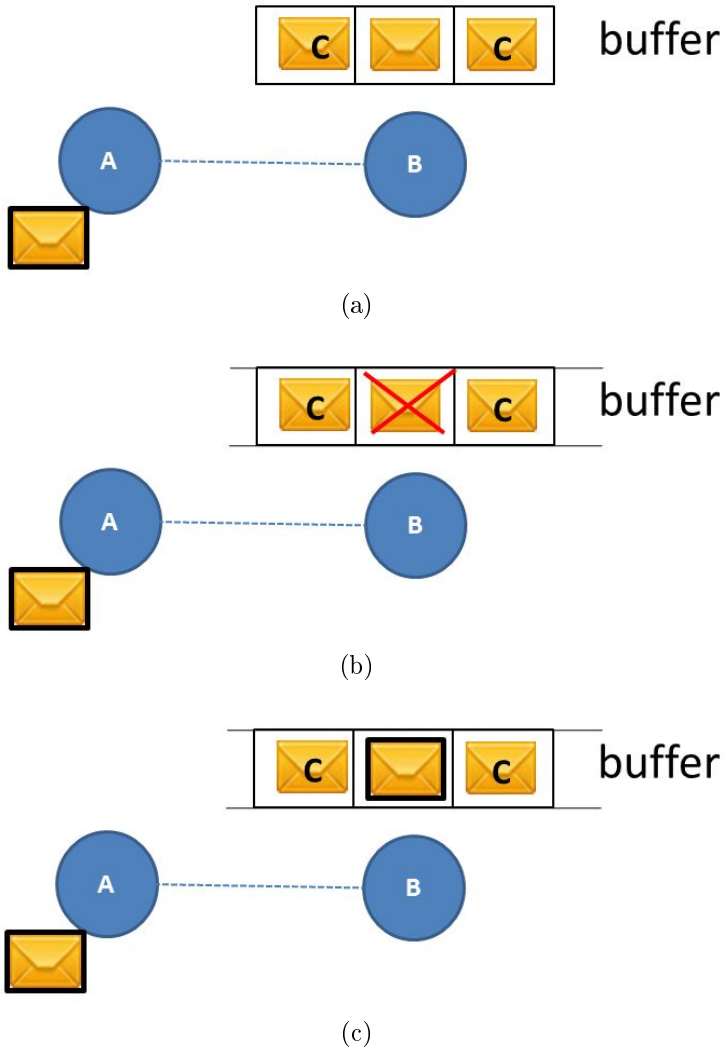



Figura 3.1: Descarte de agregado em um *buffer* quando há agregados sob custódia.

Essa abordagem é também conhecida como custódia exclusiva, na qual a custódia de cada agregado é associada a um único nó. Trata-se de um mecanismo simples, porém pouco explorado. Isso pode ser observado pelos diversos trabalhos propostos recentemente com o objetivo de melhorar o desempenho em redes DTN através de protocolos de rotea-

mento [28, 59, 17], de políticas de encaminhamento [21, 27, 62] e de descarte [37, 55, 49], e, no entanto, são raros os trabalhos que abordam diretamente o uso da transferência de custódia [15, 52, 9, 8].

O foco deste trabalho é o ganho de desempenho que pode ser obtido com a transferência de custódia e, até a conclusão desta pesquisa [34, 35], apenas Chuah *et al.* estudam a transferência de custódia sob essa perspectiva [9, 8]. Mais especificamente, os autores concluem que o uso da transferência de custódia pode aumentar significativamente a taxa de entrega em redes esparsamente conectadas com taxas de sobrecarga aceitáveis. Entretanto, uma comparação com os resultados desses trabalhos não foi possível por diversos fatores. Primeiramente, os autores utilizam registros de mobilidade sintéticos, ao contrario deste trabalho, que considera registros reais de mobilidade. Além disso, os autores não especificam o TTL dos agregados criados nas simulações. Esse parâmetro tem direta influência na avaliação de desempenho da transferência de custódia, pois é o fator que determina o descarte dos agregados sob custódia, caso não atinjam seu destino. Um outro ponto que impossibilita comparações é que nesses trabalhos a transferência de custódia não é avaliada isoladamente, mas combinada com um mecanismo denominado *message ferry*. Por fim, a comparação entre resultados também não foi possível devido a outros parâmetros considerados nas simulações de Chuah *et al.*, como agrupamentos de nós formando redes esparsas e padrão de tráfego CBR (*Constant Bit Rate*), que não são avaliados neste trabalho.

Critérios de escolha para nós custódios não estão especificados na arquitetura das redes DTN [4]. Assim, a definição e escolha de nós custódios são de responsabilidade dos protocolos de roteamento e políticas de encaminhamento. No entanto, alguns requisitos podem ser considerados como ideais ao se avaliar a viabilidade de repassar a custódia de um agregado a um novo nó custódio[26]:

- estar próximo ao destino final do agregado;
- possuir disponibilidade para manter o agregado no *buffer* por um dado intervalo de tempo necessário;
- contar com recursos suficientes de energia de forma a permanecer ativo durante longos períodos;
- possuir meios eficientes de encaminhamento para aproveitar os contatos e aumentar a probabilidade de entrega ao destino final.

Em cenários com contatos oportunistas, foco deste trabalho, o desafio de roteamento é maior que em outros cenários. Dessa forma, a transferência de custódia se torna um importante mecanismo para garantir que os agregados não sejam descartados prematuramente e, além disso, a escolha correta de um nó custódio aumenta as chances de um agregado ser entregue.

Outro ponto relacionado à transferência de custódia é a forma como ela é efetivada. Quando um nó encaminha um agregado sob custódia, ele pode negociar a transferência da custódia para o próximo nó [15]. Quando o nó custódio de um agregado decide transferir a custódia para outro nó, ele envia o agregado e uma solicitação de transferência. Após isso aguarda uma aceitação de custódia. Se o outro nó aceitar o pedido de custódia, envia uma mensagem de reconhecimento (ACK) para o nó de origem do pedido. Caso nenhum reconhecimento seja recebido, o nó emissor pode reenviar a solicitação, no entanto é obrigado a manter o agregado ainda sob custódia. A Figura 3.2 ilustra o mecanismo de transferência de custódia. Nela, são feitas duas solicitações de transferência de custódia ($TC1$ e $TC2$) e os nós intermediários enviam as confirmações de aceitação da custódia ($ACK1$ e $ACK2$). Após algum tempo, o segundo nó intermediário entrega o agregado diretamente ao destino.

A aceitação da transferência de custódia não é obrigatória [4] e a decisão está sujeita a critérios do nó candidato a custódio em função de limitação de recursos [38, 15, 14]. Tais critérios podem envolver a taxa de ocupação no *buffer*, roteamento, prioridade e tamanho dos agregados, dentre outros. Assim, sob determinadas circunstâncias, a aceitação pode estar sujeita a um determinado limiar de ocupação de *buffer* e o nó pode optar por aceitar o agregado, mas não a custódia, bem como aceitar o pedido de custódia apenas para determinadas classes de prioridade. Mecanismos que usam critérios de negociação de custódia ainda são objetos de investigação [26]. Neste trabalho, essa negociação é tratada como uma transferência simples em que, se há espaço no *buffer* do nó que receberá a cópia do agregado, ele aceita o pedido de transferência de custódia.

Uma vez que a transferência é concluída, o agregado original é mantido no *buffer* do nó de origem. Entretanto, torna-se um agregado regular e suscetível a descarte, pois a sua custódia agora é de responsabilidade de outro nó. Uma variação desse mecanismo de custódia exclusiva, a custódia compartilhada é apresentada a seguir. Posteriormente, o mecanismo de custódia compartilhada *Limited Joint Custody* (LJC) é introduzido como alternativa para o aumento da taxa de entrega da rede.

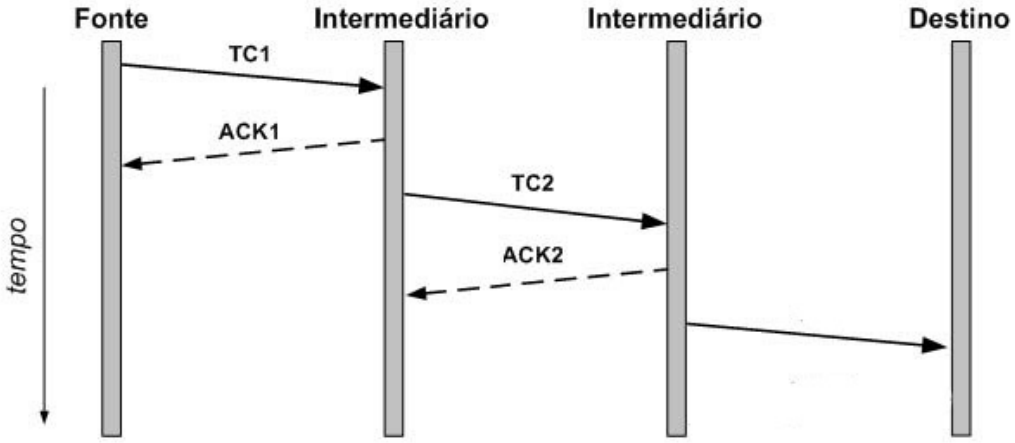



Figura 3.2: O esquema transferência de custódia. Adaptada de [38].

## 3.1 A custódia compartilhada

Mecanismos de custódia compartilhada generalizam o conceito de custódia exclusiva, permitindo que um agregado tenha mais de um nó responsável por sua custódia. Assim, quando um agregado sob custódia é replicado, o nó de origem não transfere, mas mantém a sua custódia e o nó intermediário também se torna custódio da sua réplica. Isto significa que uma determinada quantidade de réplicas de um dado agregado pode estar sob custódia de diferentes nós. Essa proposta é mencionada por Fall *et al.* e Seligman *et al.*, que sugerem seu uso, mas não propõem qualquer mecanismo específico e também não avaliam o impacto do uso de custódia compartilhada no desempenho da rede [15, 52].

Ter múltiplas cópias de um agregado na rede pode aumentar a probabilidade de entrega e reduzir o atraso de entrega [55]. Assim, a ideia principal do uso da custódia compartilhada explorada neste trabalho é aumentar o número de réplicas sob custódia na rede visando aumentar a probabilidade deste agregado ser entregue. Apesar desse aumento de desempenho, em redes DTN essa abordagem de forma não controlada pode levar a problemas de esgotamento de recurso de armazenamento [54, 37]. A custódia compartilhada aumenta o número de agregados na rede que não podem ser descartados pela ação de políticas de descarte. Tal situação pode levar a um congestionamento prematuro da rede, pois os nós apenas liberariam o espaço no *buffer* após a expiração do TTL dos agregados sob custódia ou após a entrega direta desses agregados aos nós de destino. Na Figura 3.3, são exibidos três nós $A$, $B$ e $C$ com os *buffers* cheios de agregados sob custódia. Como as políticas de descarte não podem descartar nenhum desses agregados, não há encaminhamento entre os nós mesmo que estabeleçam contato. A rede fica então congestionada e sairá deste estado apenas quando o TTL dos agregados expirarem ou

caso os nós venham a encontrar os nós de destino dos agregados, quando os mesmos serão entregues diretamente. Diante disso, torna-se essencial o controle de como essas custódias são distribuídas na rede. Assim, um dos objetivos deste trabalho é propor um mecanismo baseado no conceito de custódia compartilhada, limitando o número de nós custódios por agregado. Esse mecanismo é descrito a seguir.

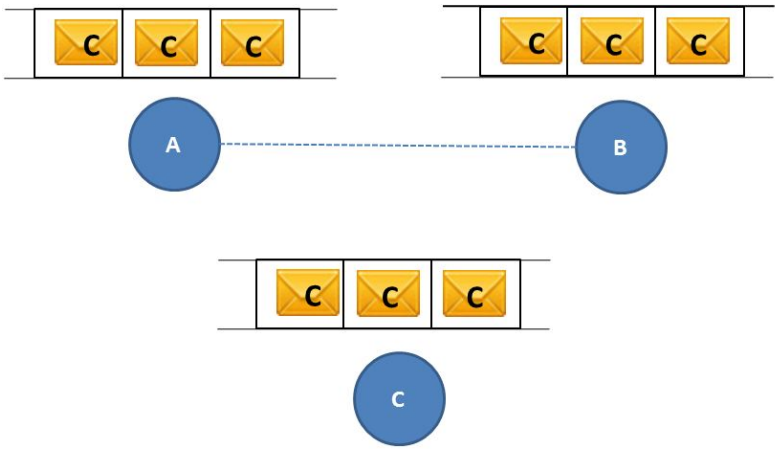



Figura 3.3: Exemplo de nós com *buffers* cheios, impossibilitando que recebam novos agregados por não poderem realizar descartes de agregados sob custódia.

## 3.2 *Limited Joint Custody* (LJC)

O mecanismo *Limited Joint Custody* (LJC) implementa o esquema de custódia compartilhada, porém restringe o número de nós custódios por agregado. O objetivo é aumentar a probabilidade de entrega dos agregados sob custódia, aumentando o número de réplicas que não podem ser descartadas prematuramente por políticas de descarte, mas evitando a propagação fora de controle de agregados sob custódia. Com isso, é possível minimizar congestionamentos nos *buffers*.

O controle de replicação no mecanismo LJC é feito com um esquema baseado em tíquetes. Quando um nó cria um agregado, ele recebe automaticamente a custódia deste agregado. Além disso, uma quantidade determinada de tíquetes está associada a este novo agregado sob custódia em seu cabeçalho. O valor inicial do tíquete define o número máximo de custódias por agregado e sempre que um nó encaminha um pacote sob custódia para um nó vizinho, ele deve compartilhar os tíquetes do agregado original com a nova réplica. Um valor de tíquete igual a 1 representa que a custódia não pode ser compartilhada, apenas transferida. Algumas abordagens possíveis para o compartilhamento de tíquetes de custódia no mecanismo LJC são:

- o nó de origem mantém 1 tíquete de custódia no cabeçalho do agregado original e repassa ao agregado replicado $T-1$ tíquetes, Figura 3.4(a). Dessa forma, apenas o nó vizinho pode compartilhar novamente a custódia do agregado e o nó de origem pode apenas transferir a sua custódia;

- o nó de origem mantém $T-1$ tíquetes no agregado original e repassa ao agregado replicado apenas 1 tíquete, Figura 3.4(b). Com isso, apenas o nó de origem pode compartilhar a custódia em futuros contatos. Já o nó que detém a réplica pode apenas transferir sua a custódia;

- o nó de origem divide o número de tíquetes igualmente entre agregado original e replicado, Figura 3.4(c). Assim, ambos os nós podem compartilhar a custódia do agregado em futuros contatos até que $T = 1$.

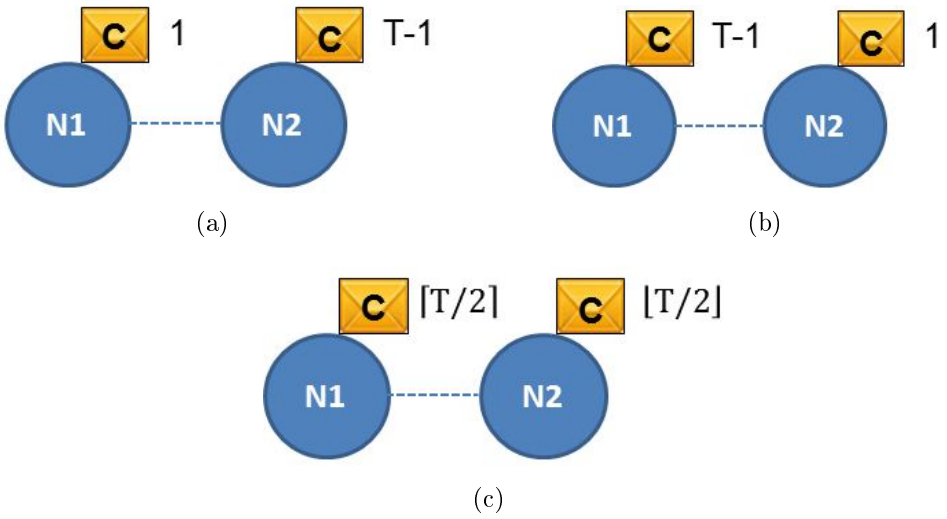



Figura 3.4: Diferentes abordagens para o compartilhamento de tíquetes de custódia no mecanismo LJC.

As duas primeiras abordagens podem comprometer o mecanismo de custódia compartilhada considerando-se que o nó que detém o agregado com maior número de tíquetes pode desconectar-se da rede devido a fatores como mobilidade, descarregamento de bateria ou pela utilização de ciclos de trabalho conforme visto no Capítulo 2. Consequentemente, os agregados desse nó, que poderiam ter suas custódias compartilhadas, não estariam mais disponíveis na rede. Neste trabalho, o LJC utiliza o último esquema de compartilhamento de tíquetes apresentado, pois a divisão binária permite uma melhor distribuição dos agregados sob custódia na rede, não concentrando em apenas um nó a maior parte dos tíquetes de custódia. Essa abordagem é análoga à usada pelo protocolo de roteamento *Spray and Wait* [58] em sua variação binária, como descrito na Seção 2.5.3. Assim, no mecanismo do

LJC, o agregado original mantém $\lceil \frac{T}{2} \rceil$ tíquetes, enquanto o agregado replicado recebe $\lfloor \frac{T}{2} \rfloor$ tíquetes. Quando a réplica de um agregado contém apenas um tíquete, o nó custódio deve transferir a custódia para o próximo contato, e, como consequência, o agregado no nó custódio anterior torna-se regular e a réplica recebida pelo novo custódio possui apenas um tíquete. Desta maneira, a partir do momento em que o número de tíquetes de um pacote sob custódia é igual a 1, o LJC passa a funcionar exatamente como o mecanismo de custódia exclusiva, em que a custódia é transferida a cada contato. Como os tíquetes são distribuídos similarmente ao encontrado no protocolo *Spray and Wait*, o número máximo de vezes que um agregado é replicado com custódia é dado por $log_2 T$, onde $n$ é o número máximo de tíquetes de custódia.

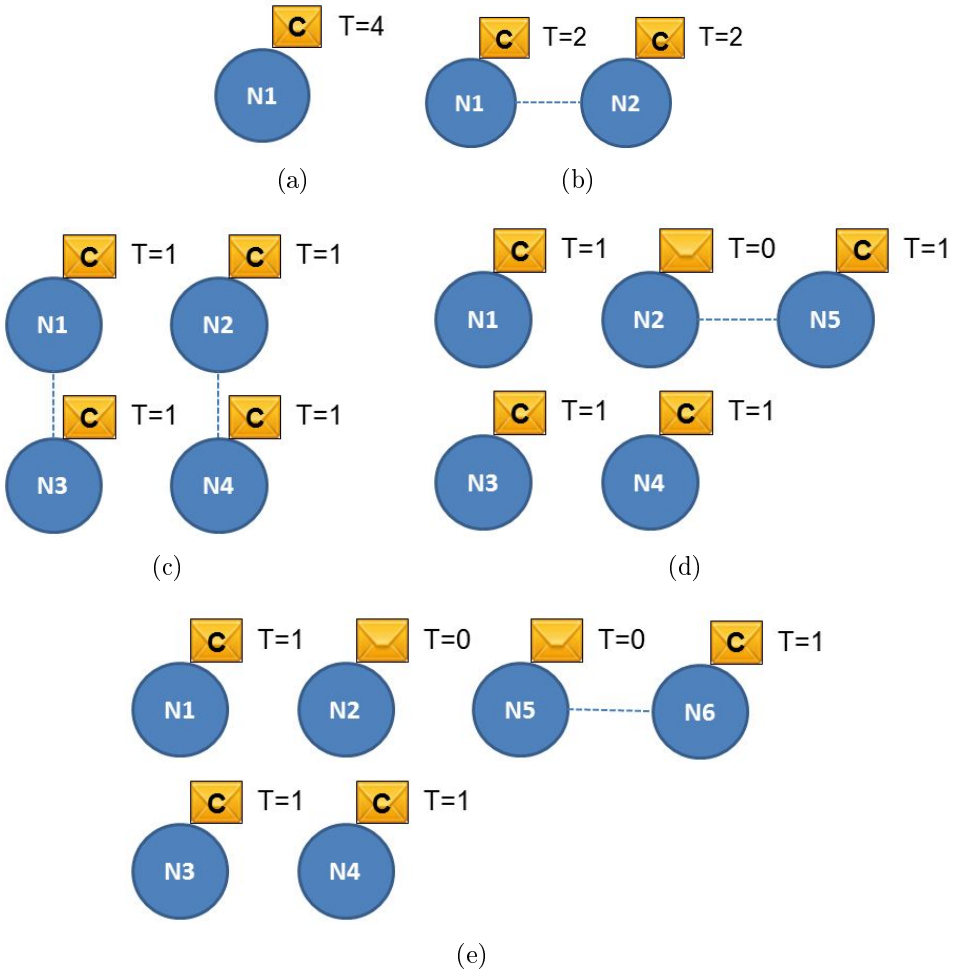



Figura 3.5: Funcionamento da replicação de agregados no mecanismo LJC.

A Figura 3.5 ilustra o funcionamento do LJC com o compartilhamento de tíquetes de custódia binário. Neste exemplo, a quantidade máxima de custódias por agregado é definida pelo nó de origem com o valor 4 e é representada pelo parâmetro $T$. Os agregados que estão sob custódia possuem a letra $C$ (custódia) e possuem $T \geq 1$, enquanto

os agregados regulares possuem $T = 0$. No exemplo, um agregado é criado pelo nó $N1$ (Figura 3.5(a)) e nas figuras seguintes ilustra-se o funcionamento das replicações. No primeiro contato, $N1$ encaminha o agregado ao nó $N2$ que recebe 2 tíquetes (Figura 3.5(b)). Após determinado número de contatos, o nó $N2$ encaminha o agregado e seus tíquetes (Figura 3.5(c)) e transfere a custódia para $N5$ (Figura 3.5(d)). O nó $N5$ faz o mesmo em seu próximo contato (Figura 3.5(e)). Assim, o número máximo de custódias por agregado é assegurado.

O desempenho do mecanismo LJC é avaliado no Capítulo 5 com os protocolos citados na Seção 2.5. Seu desempenho é também comparado ao do mecanismo de custódia exclusiva e das versões nativas dos protocolos, sem o uso de transferência de custódia.

# Capítulo 4

# Políticas de encaminhamento

Muitos protocolos de roteamento em redes DTNs utilizam a replicação de agregados como forma de aumentar a taxa de entrega [6]. As estratégias de replicação são implementadas por políticas de encaminhamento, que são componentes de um protocolo responsáveis por escolher quais agregados serão transmitidos, bem como a ordem de encaminhamento desses agregados durante um contato. Entretanto, mesmo as políticas mais eficientes não necessariamente encaminham todos os agregados disponíveis devido a restrições como largura de banda, conexões que duram curtos intervalos de tempo e interrupções inerentes à própria natureza das redes DTN. Assim, as políticas de encaminhamento tem um grande impacto sobre o desempenho geral da rede [31], pois devem fazer uso eficiente do tempo de contato entre os nós, maximizando a quantidade de agregados transmitidos e minimizando a sobrecarga decorrente dos agregados não transmitidos por completo quando o tempo de contato termina. Além disso, as políticas de encaminhamento devem idealmente escolher agregados de acordo com métricas que aumentem a probabilidade dos mesmos serem entregues.

A seção a seguir apresenta algumas das políticas de encaminhamento mais relevantes existentes na literatura de redes DTN. Em seguida, é apresentada uma proposta de política de encaminhamento chamada *Forward Custody First* (FCF) e uma variação probabilística dessa política.

## 4.1 Estado da arte

Existem diversas políticas de encaminhamento para redes DTN que se diferenciam pelos critérios adotados para a escolha e ordenação dos agregados. Esses critérios vão desde heurísticas simples como a ordem de chegada no *buffer* à critérios mais complexos

que envolvam padrões sociais e a probabilidade de entrega dos agregados com base em históricos de contatos anteriores. A seguir, algumas das principais políticas existentes na literatura são apresentadas e discutidas.

As políticas FIFO (*First In First Out*) e LIFO (*Last In First Out*) ordenam os agregados de acordo com o seu tempo de chegada no *buffer* [11]. Com a FIFO, os agregados mais antigos são encaminhados primeiro. Já com a LIFO, os agregados mais novos são primeiramente encaminhados. A principal vantagem da política LIFO é que os agregados que são entregues em poucos saltos são entregues com baixo atraso, pois estão sempre na cabeça da fila de encaminhamento. Entretanto, ao se encaminhar um agregado em redes DTN, o mesmo não é descartado do *buffer*. Dessa forma, apenas uma parte dos agregados, os primeiros (FIFO) ou os últimos (LIFO) a chegarem no *buffer*, são encaminhados, enquanto os demais correm o risco de sofrer inanição (*starvation*), ou seja, nunca serem encaminhados antes de serem descartados por expiração de TTL ou pela ação de políticas de descarte [23].

A política *Random* escolhe os agregados a serem encaminhados de forma aleatória sem considerar fatores como tempo em que eles estão no *buffer* ou qualquer outra prioridade que influencie o encaminhamento [55]. Uma vantagem dessa política é que todos os agregados possuem teoricamente igual probabilidade de serem encaminhados. Já como principal desvantagem, assim como FIFO e LIFO, tem-se que a escolha aleatória pode encaminhar agregados que já foram bastante replicados na rede. Outra desvantagem dessa política decorre do seu próprio esquema de funcionamento, pois com ela não é possível escolher um agregado específico baseado em alguma outra informação que possa aumentar a probabilidade de entrega.

A política *COIN* utiliza um mecanismo probabilístico para decidir quando um determinado agregado deve ou não ser encaminhado [31]. Assim, a cada oportunidade de encaminhamento é feito um sorteio análogo ao lançamento de uma moeda com 50% de probabilidade do agregado ser encaminhado. Essa política pode ser utilizada junto a protocolos baseados estratégias de inundação, como o *Epidemic*, com o objetivo de limitar o número de replicações.

Ayub *et al.* propõem a política *Transmit Smallest Message First* (TSMF), na qual os agregados de menor tamanho são encaminhados primeiro [1]. Com isso, pretende-se maximizar a quantidade de agregados transmitidos em detrimento dos agregados de maior tamanho. Essa política foi inicialmente proposta como forma de otimizar o protocolo de roteamento *Epidemic* em situações em que os nós se movem em alta velocidade e, por

conseguinte, possuem tempos de contato muito curtos. Uma desvantagem da TSMF é limitar o tamanho máximo dos agregados enviados. Os mesmos autores propõem também a política *Transmit Max Hop Count First* (TMHF) [2], em que são encaminhados primeiramente os agregados com maior número de saltos, ou seja, primeiramente os agregados com maior número de encaminhamentos. Nesse trabalho os autores concluem que encaminhar agregados com vários saltos reduz a sobrecarga de controle, ou seja, reduz-se a quantidade de cópias necessárias de um agregado para se realizar a sua entrega ao nó de destino. Ainda na pesquisa, os autores apresentam resultados em que a política TMHF aumenta a taxa de entrega quando comparada às políticas de encaminhamento FIFO e *Random*.

*Remaining Lifetime DESC* é uma política proposta por Soares *et al.* que tem como critério de ordenação o TTL restante dos agregados [56]. Nela, os agregados com maior TTL são encaminhados primeiro. Os autores concluem que transmitindo mais frequentemente agregados com uma maior vida útil na rede, aumenta-se a probabilidade desses agregados chegarem ao seu destino. Uma desvantagem dessa política é que ela pode penalizar agregados mais antigos, especiamente os agregados criados e enviados durante a inicialização da rede.

A política GRTRMax[1] utiliza estatísticas de contatos para calcular a probabilidade de entrega dos agregados [31]. Nessa política, o encaminhamento é feito apenas para nós que tenham maior probabilidade de contato com o nó destino do que o nó que detém a mensagem. Assim, ao estabelecer um novo contato, um nó encaminhará apenas os agregados que tiverem maior probabilidade de serem entregues ao destino final a partir do nó vizinho. Dessa forma, evitam-se encaminhamentos que dificilmente resultarão na entrega dos agregados, minimizando-se o consumo de recursos de transmissão e de armazenamento. A GRTRMax considera ainda que haja um mecanismo nativo no protocolo de roteamento que viabilize a coleta de estatísticas e realização de cálculos de probabilidades de futuros encontros entre os nós baseados em históricos de contatos. Assim, ela é aplicada apenas a protocolos de roteamento probabilístico como o PRoPHET [30], MaxProp [3], NECTAR [40] e *Predict and Relay* [64]. Uma limitação da política GRTRMax é a inviabilidade de empregá-la em grandes redes formadas por nós com limitações de processamento e de armazenamento, pois tais nós podem ser sobrecarregados com as tarefas de calcular e manter atualizadas as tabelas de estimativas de futuros contatos.

Ip *et al.* [23] propõem a política *Round Robin Forwarding Scheduling* - RRFS, que

[1] Os autores da política observam que GRTR não é uma sigla e sim um mnemônico que deve ser lido como *GREATER*.

se baseia na quantidade de réplicas de cada agregado já disseminadas na rede. Para isso, cada agregado mantém em seu cabeçalho um campo de controle que é incrementado a cada encaminhamento. Então, a cada novo contato, são encaminhados primeiro os agregados com menor número de encaminhamentos. Essa política possui uma abordagem oposta à política TMHF, na qual são encaminhados primeiro os agregados com maior número de encaminhamentos. Com a política RRFS, pretende-se disseminar de forma balanceada os agregados na rede. O trabalho original especifica o uso da política RRFS com uma política de descarte aleatório. Entretanto, o descarte aleatório pode ter o efeito colateral de descartar agregados nunca encaminhados e diminuir o desempenho da rede [37, 31]. Naves [36] propõe uma alteração na política RRFS, criando uma nova denominada RR-LRF (*Round Robin with Least Recently Forwarded Drop*). Nesse trabalho, Naves propõe a substituição do descarte aleatório na política de descarte LRF (*Least Recently Forwarded*), onde são descartados os agregados menos recentemente disseminados na rede. Um ponto a se observar com relação ao trabalho de Naves é que políticas de descarte e políticas de encaminhamento são dois mecanismos distintos e não houve alteração de critérios de encaminhamento na RR-LRF, apenas nos critérios de descarte. Dessa forma, não se considera RR-LRF como uma nova política de encaminhamento. Este trabalho, entretanto possui foco apenas no uso de políticas de encaminhamento e políticas de descarte mais eficientes não estão no escopo desta pesquisa.

A política *Bubble* [21] explora duas métricas sociais e estruturais chamadas centralidade e comunidade. Essas métricas levam em consideração padrões de movimentação e relacionamento humanos observados em redes móveis. A primeira estratégia dessa política considera que os nós, assim como as pessoas, possuem diferentes popularidades. Daí, encaminham-se os agregados para nós mais populares que o nó atual. A segunda parte da estratégia de encaminhamento se baseia no fato de que pessoas formam comunidades com interesses comuns e isso pode ser aplicado aos *clusters*. Então, encaminham-se os agregados para nós centrais em *clusters* que sejam influentes e possam ser usados como replicadores.

Todas as políticas apresentadas nesta seção têm o mesmo objetivo em comum de aumentar a eficiência das redes DTN. Porém, nenhuma delas considera agregados sob custódia e nem são aplicadas com algum mecanismo de custódia compartilhada. Como o foco deste trabalho é o ganho de desempenho que pode ser obtido com a transferência de custódia, especialmente a custódia compartilhada, verificou-se que o uso de uma política de encaminhamento que priorize agregados custódia pode proporcionar ganhos ainda maiores na eficiência da rede. A seção a seguir apresenta uma política de encami-

nhamento proposta que prioriza o encaminhamento de agregados sob custódia e que tem como principais objetivos aumentar a taxa de entrega e reduzir o atraso de entrega.

## 4.2 Política *Forward Custody First* - FCF

A política de encaminhamento *Forward Custody First* (FCF) dá prioridade total aos agregados sob custódia. Nela, um nó encaminha primeiro os agregados que estão sob sua custódia. Os agregados regulares, ou seja, agregados que não estão sob custódia, são encaminhados somente quando não há mais agregados sob custódia. A ideia chave da política FCF é baseada no fato de que agregados sob custódia não podem ser removidos do *buffer* a menos que cheguem ao seu destino ou que o TTL tenha expirado. Já os agregados regulares podem ser descartados prematuramente por políticas de descarte. Assim, encaminhar primeiro um agregado sob custódia pode acelerar o tempo de entrega. Consequentemente, depois de entregue, os nós podem remover esse agregado do *buffer*, disponibilizando espaço para novos agregados. Adicionalmente, pode-se aumentar a probabilidade de entrega.

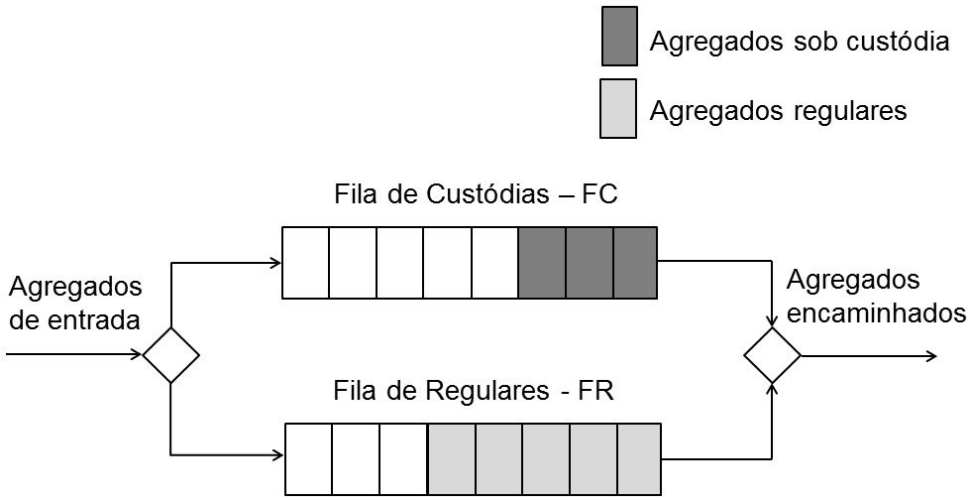



Figura 4.1: O esquema básico de encaminhamento usando a política FCF.

Uma implementação básica dessa política consiste em duas filas isoladas conforme ilustra a Figura 4.1. A primeira fila mantém os agregados sob custódia (Fila de Custódias - FC), que são encaminhados com prioridade. A segunda mantém os agregados regulares (Fila de Regulares - FR), que são encaminhados apenas quando a FC estiver vazia. Em ambas as filas, o critério de ordenação é tempo de chegada no *buffer* usando FIFO. É necessário observar que, em redes DTNs, quando um nó encaminha um agregado para um nó vizinho, o agregado não é removido do *buffer*, e consequentemente não é removido

também da fila de encaminhamento, a menos que o vizinho seja o destino final. Porém, ao se encaminhar um agregado sob custódia para um nó intermediário, realiza-se também a transferência de custódia. Dessa forma, um agregado da FC que fora encaminhado torna-se um regular e sairá dessa fila para a FR.

A política FCF pode ser combinada com o mecanismo de custódia compartilhada LJC, apresentado na Seção 3.2. O comportamento da política permanece o mesmo, encaminhar os agregados sob custódia primeiro. Porém, na FC são encaminhados primeiro os agregados que possuem maior número de tíquetes de custódia. A Figura 4.2 exibe novamente o esquema básico de funcionamento da FCF, porém agora se considera que o mecanismo LJC é utilizado. Dessa forma, os agregados da FC são ordenados em ordem decrescente de tíquetes de custódia, representados na figura por um número vinculado aos agregados. Caso os agregados possuam a mesma quantidade de tíquetes, o critério FIFO é usado como desempate. Encaminhar os agregados com mais tíquetes visa dar à FC um comportamento de fila circular. Dessa forma, a cada encaminhamento, os tíquetes de um agregado são divididos de forma binária, pela própria definição do mecanismo LJC, e isso faz com que os agregados com menos tíquetes possam ir para o início da fila. Já os recém-encaminhados, agora com menos tíquetes, perdem posições ou até mesmo passam para o fim da fila. Com essa divisão e a priorização do encaminhamento dos agregados que possuem mais tíquetes, obtém-se uma melhor distribuição dos agregados sob custódia na rede. Essa estratégia combinada é semelhante à usada na política *Round Robin Forwarding Scheduling* - RRFS [23], na qual os agregados são também disseminados na rede de forma circular conforme comentado na Seção 4.1.

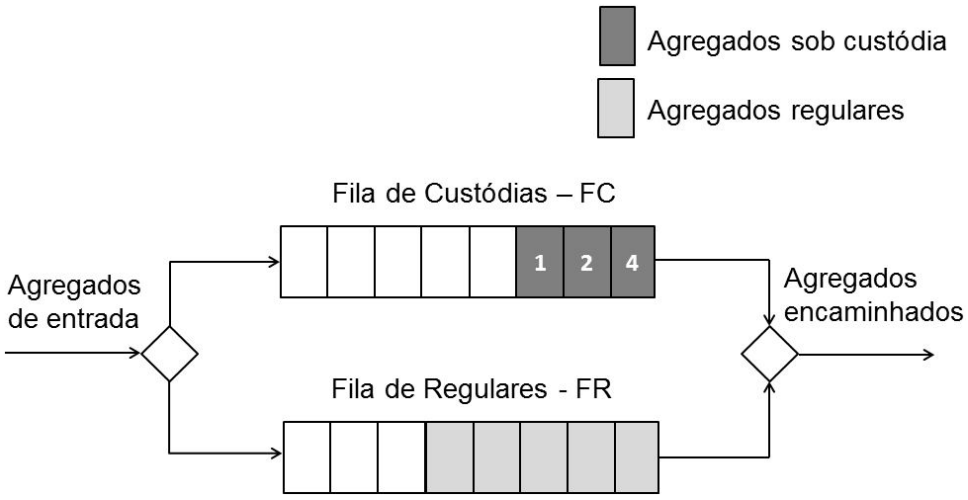



Figura 4.2: O esquema básico de encaminhamento usando a política FCF combinada ao mecanismo LJC.

## 4.3 Variação probabilística da FCF

A priorização de agregados sob custódia realizada pela política proposta neste trabalho não exclui outros critérios de encaminhamento. A política FCF pode ser combinada com outras políticas definindo critérios combinados de encaminhamento. Dessa forma, possiveis variações da política FCF podem encaminhar primeiro agregados sob custódia e ter como critérios de desempate métricas de outras políticas. Como exemplo, critérios de desempate seriam encaminhar agregados com menor tamanho (TSMF), com maior tempo de vida (Remaining Lifetime DESC), com menor número de encaminhamentos (RRFS), dentre outros.

Este trabalho propõe uma variação probabilística da política FCF além da versão padrão. O objetivo principal é combinar a ideia de políticas que utilizam estatísticas de probabilidade de entrega com a priorização de agregados sob custódia da política FCF. A variação probabilística da FCF parte do princípio que exista um mecanismo que calcule a probabilidade de um nó intermediário encontrar o nó de destino de um agregado com base no seu histórico de contatos.

Uma diferença importante entre as versões padrão e a probabilística da FCF se dá na formação das filas de agregados sob custódia (FC) e fila de agregados regulares (FR). Na versão padrão da FCF, as filas são criadas com todos os agregados disponíveis no *buffer* do nó atual. Já na versão probabilística da FCF, as filas são formadas a partir de uma seleção prévia. Nessa seleção, são escolhidos para encaminhamento apenas os agregados que tenham maior probabilidade de entrega a partir do nó vizinho. Aqueles cujo nó atual tem maior probabilidade de contato com o nó de destino, e consequente entrega, não são selecionados para nenhuma das filas. Uma implicação dessa abordagem em relação à FCF padrão é que agregados sob custódia cujo nó atual tem maior probabilidade de entrega não entram na FC. Essa seleção é baseada na que é feita na política GRTRMax [31] apresentada na Seção 4.1 e tem como vantagem minimizar a quantidade de encaminhamentos desnecessários. Consequentemente, menos recursos essenciais como espaço em *buffer* e largura de banda são ocupados com encaminhamentos de agregados que terão pouca probabilidade de serem entregues.

O funcionamento da versão probabilística da política FCF se dá então da seguinte forma. Um nó, ao estabelecer um contato com um nó vizinho, seleciona em seu *buffer* os agregados cuja probabilidade de entrega a partir do nó vizinho seja maior do que a sua própria. Com esses agregados o nó forma as filas FC e FR. Então, são encaminhados

primeiro os agregados sob custódia, fila FC, de maior probabilidade de entrega. Quando a FC estiver vazia, encaminham-se os agregados da FR com maior probabilidade de entrega. Em ambas as filas, em caso de mesma probabilidade, o critério FIFO é utilizado como desempate.

A variação probabilística da FCF também pode ser utilizada com o mecanismo LJC. Após a criação das duas filas como explicado anteriormente, a FCF encaminha primeiro os agregados da FC que possuem mais tíquetes de custódia. Como critério de desempate, são encaminhados os agregados que o nó vizinho possui maior probabilidade de entregar. Em caso de mesma probabilidade, usa-se FIFO como último critério de desempate. A Figura 4.3 exibe o esquema de funcionamento da versão probabilística da política FCF com o LJC. Na figura são também exibidas abaixo dos agregados as probabilidades do nó vizinho entregar os agregados aos nós de destino. Uma observação necessária sobre a figura é que mesmo a FR possuindo um agregado com 40% de chances de ser entregue, ele apenas será encaminhado quando a fila FC estiver vazia. Apesar de parecer uma abordagem contraditória, a ideia é que, mesmo que agregados da FC possuam menor probabilidade de serem entregues que alguns da FR, o LJC potencialize essa probabilidade. No exemplo específico, o LJC garante que os agregados da FC podem ter no mínimo 3 e no máximo 7 réplicas na rede não sujeitas a descartes e, ainda assim, com grandes chances de serem entregues se encaminhados.

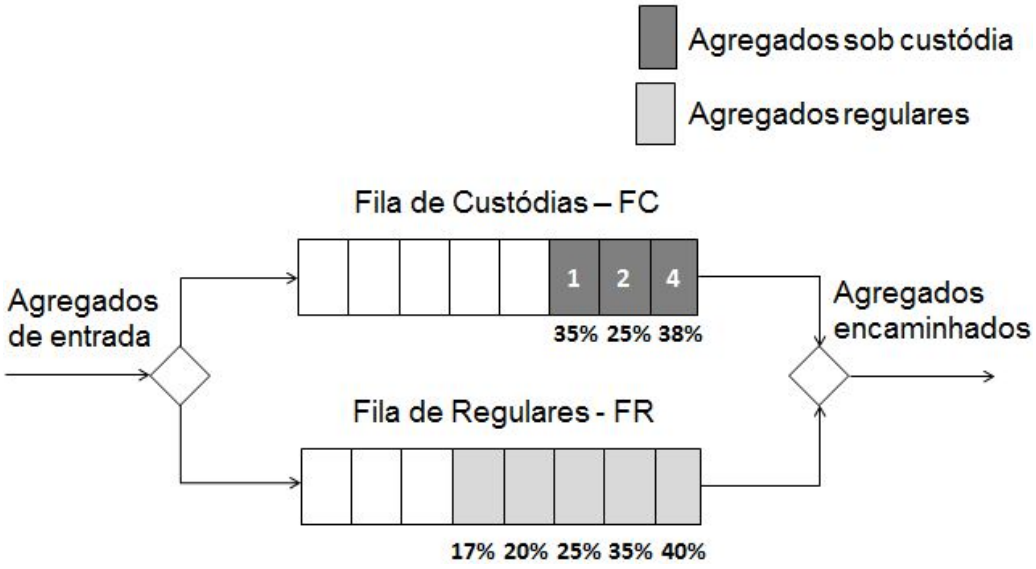



Figura 4.3: O esquema básico da versão probabilística da política FCF combinada ao mecanismo LJC.

Como mencionado, a versão probabilística da política FCF exige que sejam mantidas as estatísticas de contato e que sejam calculadas as probabilidades de entrega entre os

nós mediante o histórico de contatos. Portanto, ela apenas pode ser aplicada a protocolos de roteamento probabilísticos como o PRoPHET [30], MaxProp [3], NECTAR [40] e *Predict and Relay* [64]. Especificamente, uma implementação dessa versão da FCF é implementada e avaliada neste trabalho mediante adaptação da política GRTRMax, nativa do protocolo PRoPHET. A justificativa para essa escolha se deve ao fato desse protocolo já ser um dos protocolos avaliados nesta pesquisa e à política GRTRMax já estar integrada com os meios que o PRoPHET utiliza para gerenciar estatísticas de contato e calcular a probabilidade de encontros futuros.

Neste trabalho, o mecanismo de custódia compartilhada LJC e a política de encaminhamento FCF são avaliados de forma isolada e também combinada, visando analisar o desempenho de ambas as abordagens. No Capítulo 5 os resultados das avaliações desses mecanismos são apresentados e discutidos.

# Capítulo 5

# Resultados

O mecanismo de custódia compartilhada LJC e a política de encaminhamento FCF propostos são implementados e avaliados em três protocolos de roteamento que utilizam diferentes esquemas de replicação de agregados. Nas simulações, é utilizado um simulador específico para redes de contatos oportunistas e são considerados dois conjuntos reais de mobilidade humana coletados através de dispositivos móveis. Com a combinação dos protocolos e os conjuntos de mobilidade, as propostas são avaliadas em seis cenários distintos. Os resultados das simulações são avaliados através de três diferentes métricas e as propostas têm seus desempenhos comparados a outros mecanismos e políticas da literatura para redes DTN. Os cenários de simulação, o simulador DTN e os resultados das simulações são apresentados neste capítulo.

## 5.1 Cenários de simulação

Nas análises, consideram-se dois diferentes registros de mobilidade extraídos de conjuntos de dados reais, denominados Rollernet [60] e Infocom06 [22], como forma de se obter resultados de simulações mais próximos de um ambiente real. Em ambos os conjuntos de dados, que serão referenciados a partir daqui como cenários, os nós armazenam informações sobre todos os seus contatos. Esses contatos são registrados através da distribuição de iMotes, como o exibido na Figura 5.1, para um grupo de pessoas. Os iMotes são pequenos dispositivos que possuem uma interface *Bluetooth* e uma memória auxiliar que registra os contatos com iMote dentro de seu raio de alcance. Especificamente eles armazenam o tempo inicial do contato, a duração e a identificação do iMote pareado.

As informações de contato do cenário Rollernet foram coletadas durante um circuito de patinação realizado em 2006 em Paris. Foram distribuídos 62 iMotes para voluntários

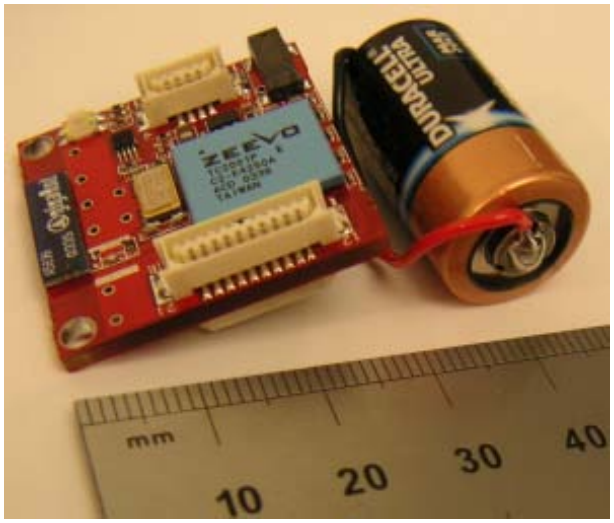



Figura 5.1: Exemplo de um iMote [20].

participantes. Os iMotes foram configurados para procurar outros nós a cada 15 s e durante 5 s. No total, o tempo de coleta de informações durou aproximadamente 3 horas. Os dados do cenário Infocom06 foram coletados na conferência IEEE Infocom em 2006 em Barcelona. Durante a coleta, os iMotes foram configurados para procurar por outros dispositivos em intervalos de 120 segundos. O tempo total do experimento durou aproximadamente 4 dias.

Esses dois cenários foram escolhidos por apresentarem diferentes padrões de mobilidade, os quais são indicados pela média de contatos por hora e o tempo de duração desses contatos, exibidos na Tabela 5.1. Assim, os mecanismos foram avaliados em um cenário onde os nós se encontram com mais frequência, mas os contatos têm curta duração, Rollernet, e também em um cenário onde os nós se encontram menos frequentemente, mas os tempos de contato têm maior duração, Infocom06. O objetivo é investigar o desempenho dos mecanismos LJC e FCF em cenários com diferentes características de modo a identificar o impacto do número e tempo de contatos no comportamento de cada um deles.

## 5.2 O ambiente de simulação

Os mecanismos propostos são avaliados através de simulações utilizando o simulador *The ONE* (Opportunistic Network Environment) [25]. O *The ONE é* um simulador amplamente utilizado para a validar diversos experimentos em redes de contatos oportunistas e aplicações de redes DTN [34, 46, 55, 2, 1, 37, 40].

A escolha desse simulador também se deve à sua facilidade de extensão. De forma simples, é possível incluir novos protocolos e políticas, como os mecanismos de transferência de custódia e custódia compartilhada avaliados e propostos neste trabalho. O simulador conta ainda com um conjunto de relatórios que permitem observar o comportamento de diversas métricas, tais como a taxa de entrega, quantidade de agregados encaminhados e descartados, a latência média dos agregados entregues e a sobrecarga de mensagens. Com o *The ONE* também é trivial a vinculação dos cenários escolhidos a partir de arquivos de entrada disponíveis no repositório CRAWDAD [63]. O projeto CRAWDAD mantém um repositório com registros reais de mobilidade disponíveis para a avaliação e validação de pesquisas. O projeto ainda disponibiliza metadados sobre os registros, tais como a topologia da rede, a quantidade e tipo dos usuários/dispositivos envolvidos, bem como informações sobre a metodologia de coleta dos dados.

### 5.2.1 Extensões implementadas

O *The ONE* não suporta de forma nativa a transferência de custódia e o mecanismo de custódia compartilhada. Assim, o simulador foi estendido para suportá-los. Basicamente, assume-se que os agregados sob custódia são removidos do *buffer* somente quando o seu TTL expira. Ou seja, os critérios das políticas de descarte não são aplicados a esses agregados. Além disso, não é considerado o uso de *ACKs* enviados pelo nó destino para informar o recebimento de agregados e, assim, remover cópias desses agregados entregues dos *buffers*.

As mensagens tratadas no simulador são modificadas para conter informações no cabeçalho indicando se o agregado está ou não sob custódia. Um campo adicional também é introduzido no cabeçalho das mensagens para informar a quantidade de tíquetes de custódia que o nó custódio da mensagem pode ainda distribuir de acordo com as definições do mecanismo LJC na Seção 3.2. Os trechos de código responsáveis pela transferência e replicação de mensagens são também alterados para tratar a distribuição de tíquetes entre os agregados originais e os agregados encaminhados.

Mecanismos de prioridade de filas utilizados pela política FCF conforme detalhado na Seção 4.2 também são introduzidos no simulador. Assim, quando se utiliza a FCF nos protocolos *Epidemic* e *Spray and Wait*, primeiro são encaminhados os agregados sob custódia com mais tíquetes e posteriormente os mais antigos no *buffer* (FIFO). No caso específico do protocolo PRoPHET, a política FCF em sua variação probabilística é combinada com a política de encaminhamento GRTRMax, nativa do protocolo, conforme

explicado na Seção 4.3. Na política GRTRMax, o encaminhamento é feito apenas para nós que tenham maior probabilidade de contato com o nó destino dos agregados do que o nó que detém a mensagem. Altera-se então seu comportamento para que, dentre os agregados mais prováveis de chegar ao destino a partir do contato atual, sejam encaminhados primeiramente os agregados sob custódia.

### 5.2.2 Configurações das simulações

Os parâmetros das simulações são definidos baseados em características específicas dos cenários e dos protocolos utilizados. Ao todo, são considerados seis cenários de avaliação: dois registros de mobilidade para cada um dos três protocolos avaliados.

As diferentes durações dos experimentos apresentados por cada cenário implicam valores distintos de TTL, carga de tráfego e tamanhos de *buffer*, como indicado na Tabela 5.1. O TTL é definido baseado nos resultados apresentados por Naves *et al.* [37]. Nesse trabalho, com os valores de TTL considerados, aproximadamente 90% dos agregados chegam ao seu destino usando o protocolo *Epidemic* em ambos os cenários. Durante cada rodada de simulação, os pares fonte-destino de cada agregado são escolhidos aleatoriamente, com distribuição uniforme. Para o conjunto Rollernet e Infocom06 são geradas respectivamente 500 e 5000 mensagens. Especificamente para o protocolo *Spray and Wait* são definidas maiores cargas de tráfego, 2000 e 20000 mensagens, visando saturar a rede e analisar principalmente o comportamento do uso de várias custódias em situações na qual o transbordamento de *buffer* é mais frequente.

Assume-se também um limite de tempo para a criação de novos agregados. A ideia é permitir que o tempo de simulação não influencie as métricas de desempenho. Por exemplo, se um agregado é criado no último segundo da simulação, ele dificilmente será encaminhado e chegará ao seu destino antes do término da simulação. Assim, os agregados são criados apenas nas duas primeiras horas de simulação para o cenário Rollernet. Já para o Infocom06, os agregados são criados até que faltem 12 horas para o fim da simulação.

O tamanho configurado para as mensagens é de 1,0 MB, visto que redes DTN trabalham com agregados que podem conter várias mensagens. Ainda para o protocolo *Spray and Wait*, o parâmetro $L$ do protocolo, que representa o número máximo de replicações para cada agregado, foi definido considerando-se a metade do número de nós.

Tabela 5.1: Parâmetros das simulações e dos cenários.

| Parâmetros/Cenário | Rollernet | Infocom06 |
|---|---|---|
| Duração (≈) | 3 horas | 4 dias |
| Número de dispositivos | 62 | 98 |
| Número de contatos | 15.803 | 74.224 |
| Média de contatos por hora | 5.704,96 | 796,21 |
| Tempo de contato médio (s) | 21,75 | 408 |
| Tempo de contato máximo(s) | 488 | 40.550 |
| Tempo de contato mínimo(s) | 1 | 1 |
| TTL (minutos) | 60 | 2014 |
| Número de agregados Epidemic e PRoPHET | 500 | 5000 |
| Número de agregados SnW | 2000 | 20000 |
| Parâmetro L do SnW | 32 | 44 |
| Tamanho dos agregados (MB) | 1 | 1 |
| Tamanho do *Buffer* (MB) | 10-50 | 100-500 |

## 5.3 Métricas avaliadas

Neste trabalho, o mecanismo LJC e a política FCF propostos são avaliados considerando-se três métricas distintas. As escolhidas foram a taxa de entrega, o atraso de entrega e a sobrecarga. Essas métricas são brevemente descritas a seguir:

- a taxa de entrega é a razão entre o número de agregados que atingem seu nó de destino e o número de agregados enviados pelos nós de origem. Múltiplas cópias do mesmo agregado que tenham sido recebidos pelo nó destino não são computadas. Dessa forma, a taxa de entrega $t_e$ é definida pela fórmula $t_e = \frac{a_e \times 100}{a_c}$, onde $a_e$ é o número de agregados entregues e $a_c$ é o número de agregados criados durante a simulação;.

- o atraso de entrega dos agregados é dado pelo intervalo entre o momento em que o agregado é enviado pelo nó de origem até o momento em que atinge seu destino;.

- a sobrecarga $S$ é calculada de acordo com a seguinte equação: $S = \frac{a_r - a_e}{a_e}$, onde $a_r$ é o número de agregados retransmitidos e $a_e$ é o número de agregados entregues. Cópias não são computadas. Portanto, a sobrecarga indica quantas ações de encaminhamento em média são necessárias para entregar um agregado.

## 5.4 Avaliação dos resultados

Esta seção apresenta os resultados da avaliação de desempenho do mecanismo LJC e da política de encaminhamento FCF. O principal objetivo é analisar o impacto da custódia compartilhada e da política de encaminhamento no desempenho da rede em termos das três métricas definidas anteriormente: taxa de entrega, sobrecarga e atraso de entrega. A FCF também é comparada a outras políticas de encaminhamento. Compara-se a política proposta com a FIFO para os protocolos *Epidemic* e *Spray and Wait*. Já a variação probabilística da FCF é comparada com a GRTRMax para o protocolo PRoPHET, protocolo este que fornece à política proposta estatísticas e cálculos de probabilidades de futuros encontros entre os nós baseados em históricos de contatos. A escolha das políticas de encaminhamento FIFO e GRTRMax para as comparações com a FCF deve-se ao fato delas serem as políticas implementadas nativamente por esses protocolos.

Primeiramente, são analisados os mecanismos de custódia exclusiva e compartilhada. Assim, consideram-se os três protocolos de roteamento avaliados sem o uso de custódias (FIFO-SC e GRTRMax-SC), com custódia exclusiva (FIFO-CE e GRTRMax-CE), e com o mecanismo proposto LJC utilizando $i$ agregados sob custódia (GRTRMax-LJC$_i$ e FIFO-LJC$_i$). Em seguida, é avaliado o impacto de priorizar os agregados sob custódia exclusiva usando a política de encaminhamento proposta FCF no lugar da FIFO para os protocolos *Epidemic* e *Spray and Wait* e da GRTRMax para o protocolo PRoPHET (FCF-CE). Finalmente, as propostas LJC e FCF são incorporadas aos três protocolos de roteamento (FCF-LJC$_i$) visando avaliar a custódia compartilhada e a priorização de agregados sob custódia operando simultaneamente. Em todas as configurações mencionadas anteriormente, os agregados regulares são descartados dos *buffers* de acordo com a política FIFO.

Os resultados apresentados nesta seção são obtidos através do cálculo da média de dez rodadas de simulação distintas. Usa-se um intervalo de confiança de 95% nos resultados e barras de erro são exibidas como linhas verticais em cada ponto dos gráficos.

### 5.4.1 Taxa de entrega

As Figuras 5.2, 5.3 e 5.4 mostram como o tamanho do *buffer* afeta a taxa de entrega para todos os mecanismos em ambos os cenários - Rollernet e Infocom06. Dois aspectos podem ser claramente observados. Primeiro, quanto maior o tamanho do *buffer*, maior é a taxa de entrega para todos as configurações de mecanismos e protocolos. Esse resultado

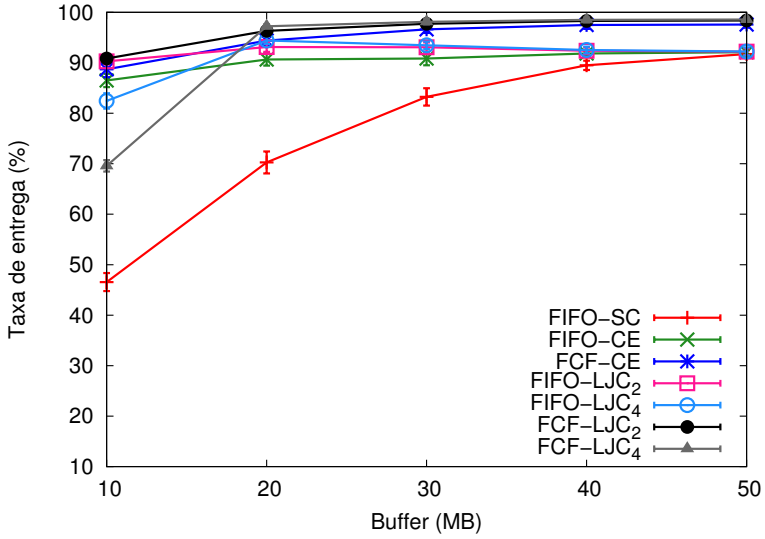
se deve à redução do número de mensagens descartadas e também pelo fato de que os nós carregam mais agregados e aumentam a probabilidade da troca de mensagens a cada contato. Segundo, o uso dos mecanismos de custódia – exclusiva ou compartilhada – aumenta a taxa de entrega. Na verdade, os mecanismos de custódia garantem pelo menos uma cópia de cada agregado na rede e que essa cópia é descartada apenas se seu TTL expirar. Agregados regulares, ao contrário, podem ser descartados prematuramente por políticas de descarte. Assim, a quantidade de agregados sob custódia aumenta e, consequentemente, a probabilidade de um agregado chegar ao seu destino também aumenta.

A Figura 5.2 exibe os resultados para o protocolo *Epidemic* nos cenários Rollernet e Infocom06, respectivamente. O mecanismo proposto FCF-LJC$_i$ obtém a maior taxa de entrega em relação a todos os outros mecanismos, inclusive maior que os de custódia exclusiva (FIFO-CE e FCF-CE) em ambos os cenários. Especificamente, o mecanismo FCF-LJC$_4$, com 4 custódias por agregado, apresenta o melhor desempenho e atinge nos cenários Rollernet e Infocom06 as taxas de entrega de aproximadamente 98% e 85% para os tamanhos de *buffer* de 50 MB e 500 MB, representando desempenho 8% e 18% superiores em relação ao mecanismo sem custódia usando FIFO (FIFO-SC).

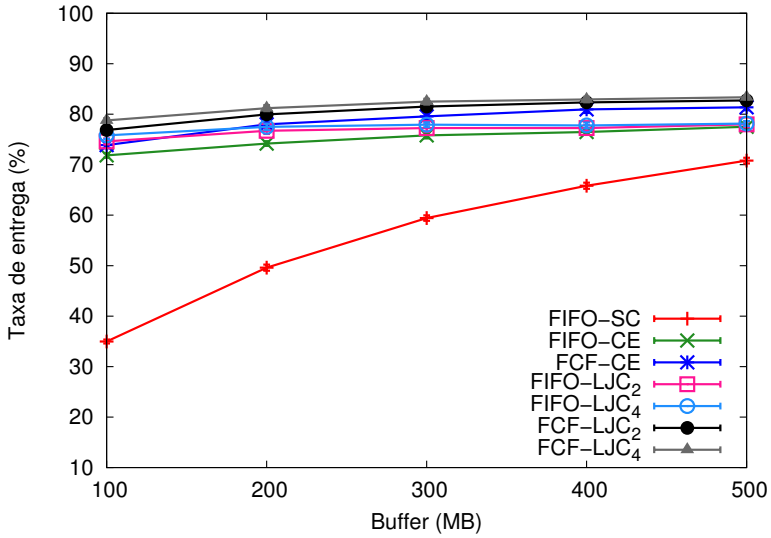
A Figura 5.3 mostra os resultados para o protocolo PRoPHET nos dois cenários analisados. Novamente, o mecanismo proposto FCF-LJC$_i$ obtém a maior taxa de entrega. Especificamente, o mecanismo FCF-LJC$_4$ apresenta melhor desempenho e atinge nos cenários Rollernet e Infocom06 as taxas de entrega de aproximadamente 98% e 85% para os maiores tamanhos de *buffer*, representando desempenhos 15% e 24% superiores em relação ao mecanismo sem custódia usando GRTRMax (GRTRMax-SC).

Os resultados para protocolo *Spray and Wait* são exibidos na Figura 5.4. A configuração FCF-LJC$_2$ obtém as maiores taxas de entrega atingindo aproximadamente 85% e 78% para os cenários Rollernet e Infocom06 em seus maiores tamanhos de *buffer*, representando ganhos de desempenho de 16% e 7% em relação ao mecanismo sem custódia usando FIFO (FIFO-SC).

Em geral, o uso da cústodia compartilhada, representada pelo mecanismo LJC, supera a custódia exclusiva porque incrementa o número de replicas dos agregados sob custódia pela rede e assim incrementa a probabilidade de entrega. Além do mais, com a política FCF, também se garante que os agregados sob custódia sejam encaminhados mais frequentemente que os regulares devido à maior prioridade de encaminhamento. Com a combinação de LJC e FCF, temos mais agregados com prioridade e com uma melhor distribuição na rede e, assim, os mecanismos analisados atingem maiores taxas de entrega.



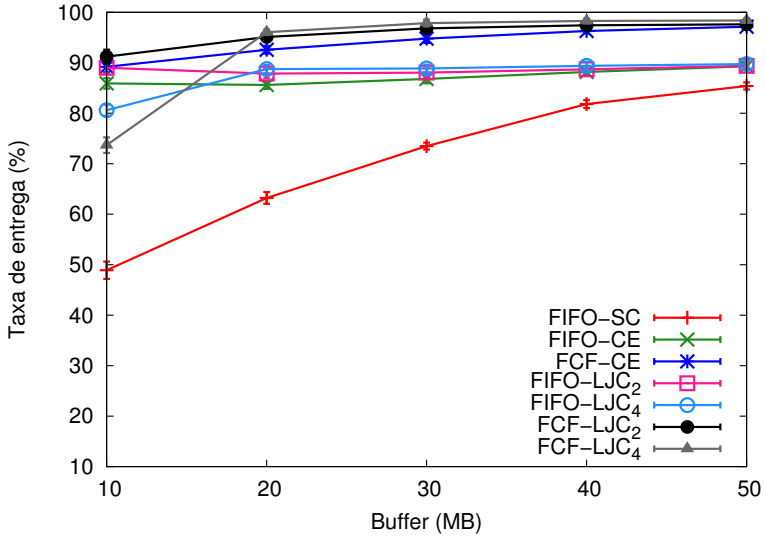

(a) Rollernet.



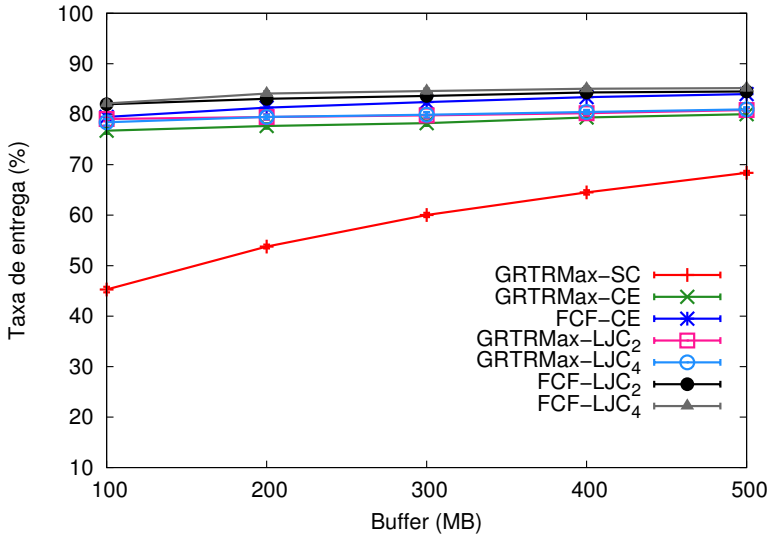

(b) Infocom06.

Figura 5.2: Taxa de entrega com o protocolo *Epidemic*.

É importante também evidenciar que a política de encaminhamento FCF tem o maior impacto na taxa de entrega que o mecanismo LJC para todos os protocolos. Esse resultado se deve à priorização, que aumenta a disponibilidade dos agregados sob custódia. Adicionalmente, a FCF supera a FIFO porque a política proposta não sofre do problema conhecido como cabeça de linha (*head-of-line problem*) [23]. Com FIFO, os agregados mais antigos no *buffer* são encaminhados primeiro durante um contato. Consequentemente, os agregados nas primeiras posições da fila são frequentemente encaminhados enquanto os que estão no fim da mesma raramente o são. Por outro lado, FCF não prioriza os mesmos agregados a cada contato. A cada encaminhamento o valor dos tíquetes de custódia é dividido e, nesse caso, um determinado agregado será encaminhado com prioridade apenas




(a) Rollernet.

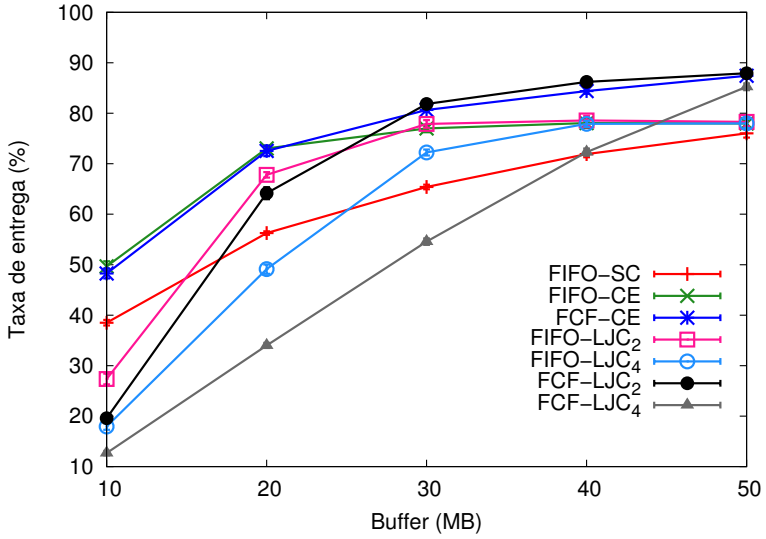



(b) Infocom06.

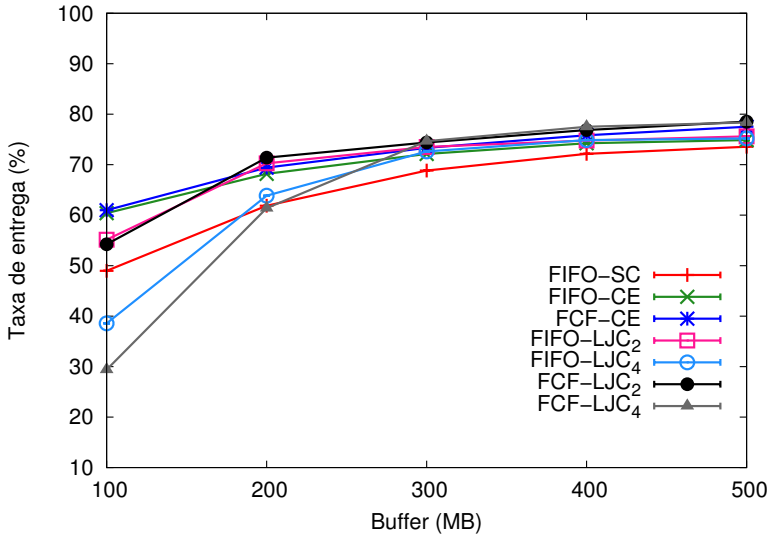
Figura 5.3: Taxa de entrega com o protocolo PRoPHET.

enquanto sua quantidade de tíquetes for maior que a quantidade dos agregados posteriores a ele na fila. Também, quando o valor do tíquete de custódia atinge 1, o próximo encaminhamento ocasionará uma transferência de custódia e o agregado será movido para a fila de agregados regulares. Em resumo, a política FCF aumenta a diversidade de agregados na rede e diminui a saturação do *buffer* por agregados sob custódia.

Apesar dos ganhos apresentados, deve-se observar que o uso de custódia compartilhada, especialmente com 4 réplicas por agregado, em alguns casos é ineficiente para os tamanhos de *buffers* reduzidos. Nos casos dos protocolos *Epidemic* e PRoPHET, esse baixo desempenho ocorre devido à inundação da rede, pois no cenário Rollernet há mui-




(a) Rollernet.




(b) Infocom06.

Figura 5.4: Taxa de entrega com o protocolo *Spray and Wait*.

tos contatos em um curto período e ambos os protocolos favorecem a replicação sem controle, por isso os *buffers* ficam congestionados com agregados sob custódia, e os nós impedidos de realizarem descartes. No caso específico do protocolo *Spray and Wait* isso é justificado pela ação do mecanismo de replicação inerente ao protocolo limitar a propagação dos agregados. Com isso, ocorrem menos encaminhamentos, fazendo com que os tíquetes de custódia não sejam distribuídos. Consequentemente, os nós com *buffers* de tamanho reduzido ficam congestionados com agregados sob custódia, por não poderem realizar descartes. Em todos os casos, esse congestionamento impede que novos agregados sejam recebidos e, consequentemente, a distribuição desses agregados na rede fica comprometida, tendo como principal consequência a redução da taxa de entrega. O mesmo não

ocorre com a custódia exclusiva, pois a cada encaminhamento, ocorre a transferência de custódia, deixando os agregados recém-encaminhados no nó de origem sujeitos a descartes caso o *buffer* chegue ao seu limite.

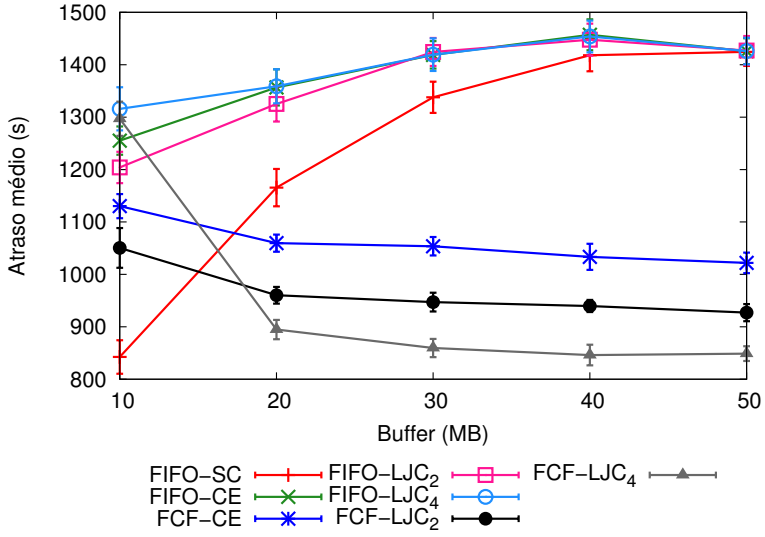
Portanto, conclui-se que os mecanismos analisados aumentam a taxa de entrega para esses dois cenários distintos, em termos de tempo de contato e conectividade, para os protocolos *Epidemic*, PRoPHET e *Spray and Wait* quando comparados às configurações com custódia exclusiva e também sem o uso de mecanismos de custódia.

### 5.4.2 Atraso médio

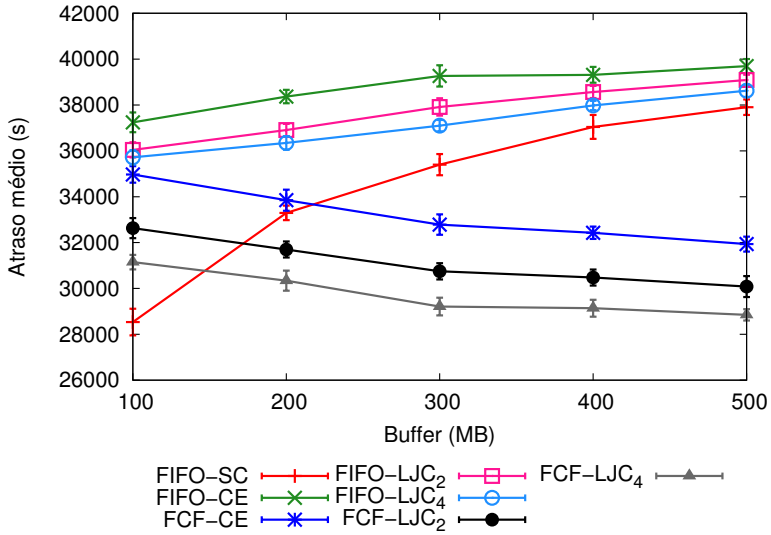
As Figuras 5.5, 5.6 e 5.7 exibem o atraso médio de todos os agregados entregues nos cenários Rollernet e Infocom06. Pode-se concluir que a maioria dos resultados ratificam a ideia de que a política FCF reduz o atraso por priorizar os agregados sob custódia.

Na Figura 5.5 são apresentados os resultados para os cenários Rollernet e Infocom06 para o protocolo *Epidemic*. O mecanismo FCF-LJC$_i$ obtém o menor atraso médio em relação a todos os outros mecanismos em ambos os cenários. Especificamente, o mecanismo FCF-LJC$_4$, apresenta nos cenários Rollernet e Infocom06 atrasos aproximadamente 40% e 24% menores em relação ao mecanismo sem custódia usando FIFO (FIFO-SC) para os tamanhos de *buffer* de 50 MB e 500 MB.

A Figura 5.6 exibe os resultados para os cenários Rollernet e Infocom06 para o protocolo PRoPHET. Novamente, o mecanismo FCF-LJC$_i$ obtém o menor atraso médio. Especificamente, o mecanismo FCF-LJC$_4$, apresenta no cenário Rollernet atraso aproximadamente 23% menor em relação ao mecanismo sem custódia usando GRTRMax (GRTRMAX-SC) para o *buffer* de tamanho 50 MB. Um ponto a ser observado é que no cenário Infocom06 o comportamento do atraso médio é distinto dos demais. O mecanismo sem custódia (GRTRMax-SC) possui o menor atraso para a maioria dos tamanhos de *buffer*. Isso se deve à atuação mais frequente da política GRTRMax, pois o cenário Infocom06 possui um número de contatos muito superior ao do Rollernet como mostra a Tabela 5.1. Também deve ser observado que o cenário foi coletado em uma conferência com duração de quatro dias e, nesse período, os nós se reencontram com maior frequência que no cenário Rollernet. Assim, quanto mais contatos e reencontros entre os nós, mais efetivamente são mantidas as probabilidades de futuros encontros, ocasionando encaminhamentos para nós com maior probabilidade de entrega, gerando menos atraso. Já os mecanismos GRTRMax-LJC$_i$ possuem maiores atrasos em relação à GRTRMax-SC por atingirem maiores taxas de entrega (Figura 5.3(b)) e, por consequência, entregar também




(a) Rollernet.

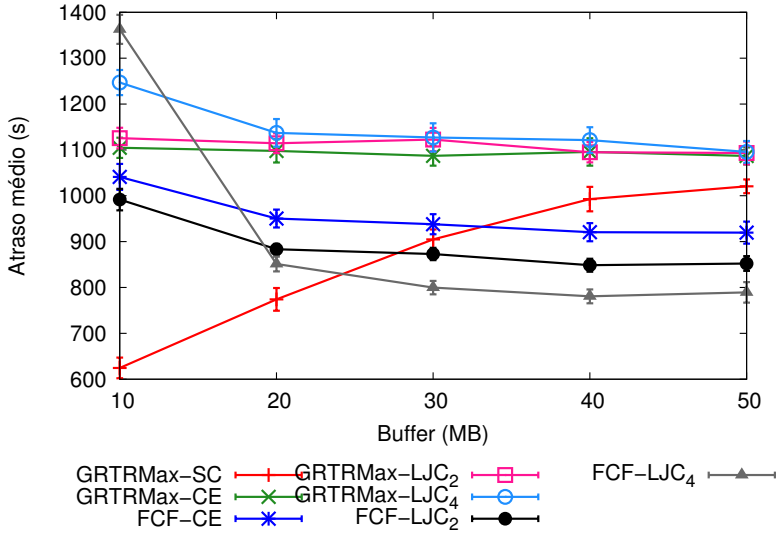



(b) Infocom06.

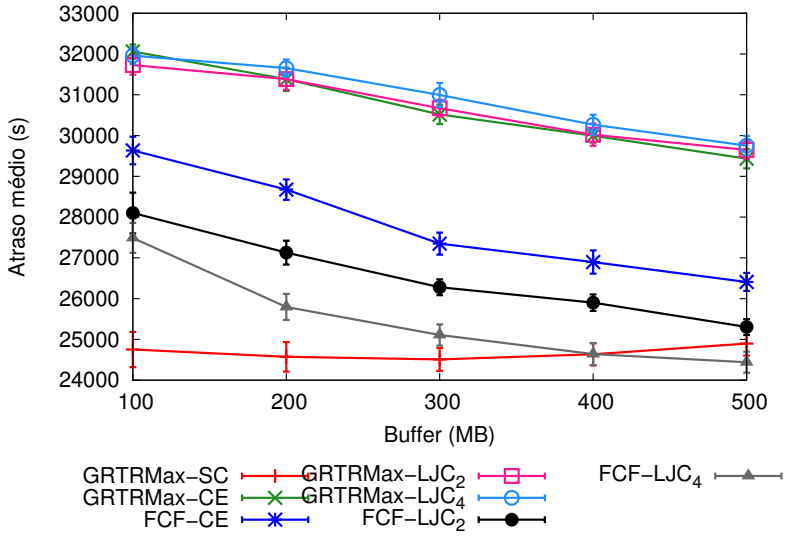
Figura 5.5: Atraso médio para o protocolo *Epidemic*.

agregados que estão a mais tempo na rede. Por fim, os mecanismos FCF-LJC$_i$ ocupam posição intermediária devido à política FCF ser híbrida nesse protocolo: primeiro os agregados sob custódia são encaminhados e, como critério de desempate, a probabilidade de entrega utilizada. Ainda assim, percebe-se a tendência dos mecanismos que utilizam a FCF serem mais eficientes que a configuração sem custódia, pois com valores de *buffers* a partir de 400 MB, o esquema FCF-LJC$_4$ passa a ter atraso inferior ao do mecanismo GRTRMax-SC.

Os resultados do atraso médio para os cenários Rollernet e Infocom06 com o protocolo *Spray and Wait* são apresentados na Figura 5.7. A combinação FCF-LJC$_4$ reduz em 22%




(a) Rollernet.

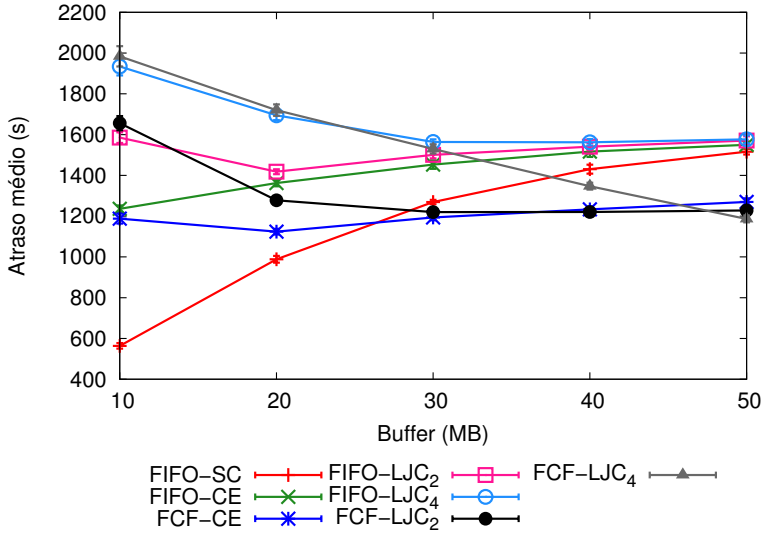



(b) Infocom06.

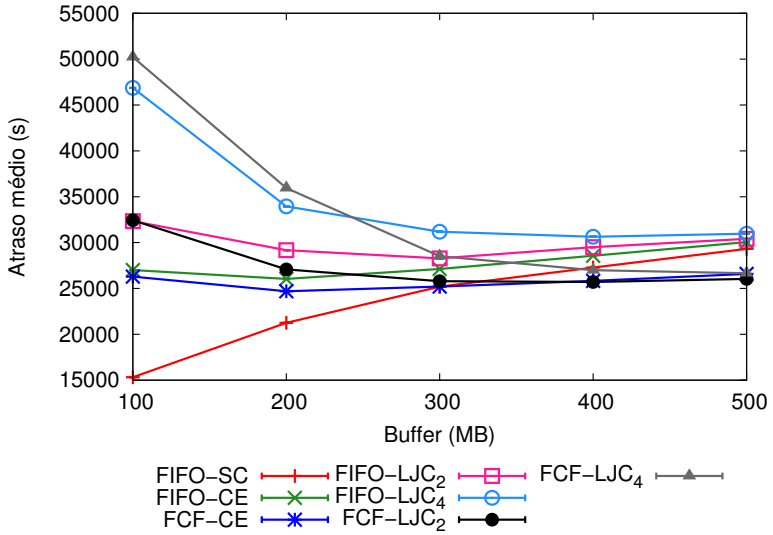
Figura 5.6: Atraso médio para o protocolo PRoPHET.

o atraso no cenário Rollernet para o *buffer* de tamanho 50 MB. Para o tamanho de *buffer* igual a 500 MB no cenário Infocom06, o mecanismo FCF-LJC$_2$ reduz em aproximadamente 11% o atraso de entrega. Ambas as reduções de atraso de entrega são relativas às implementações sem custódia usando FIFO (FIFO-SC).

Com os protocolos *Epidemic* e *Spray and Wait*, também se observa que quanto maior o tamanho do *buffer* com FCF, menor é o atraso de entrega. Com FIFO, ao contrário, quanto maior o tamanho do *buffer*, maior é o atraso. Isso é explicado pelo fato da política FCF reduzir o tempo de entrega e assim permitir que os nós removam os agregados entregues do buffer, liberando espaço para novos agregados. Desse modo, a disponibilidade




(a) Rollernet.




(b) Infocom06.

Figura 5.7: Atraso médio para o protocolo *Spray and Wait*.

dos agregados aumenta e consequentemente a probabilidade de entrega também, o que é corroborado pelos resultados apresentados na Seção 5.4.1.

A política FCF garante que um agregado com tíquetes restantes será encaminhado pelo menos uma vez pelo seu nó receptor antes que seja movido para a fila de regulares. Assim, esse agregado pode ser encaminhado mais rapidamente, pois tem prioridade. Por outro lado, o problema denominado cabeça de linha experimentado pela política de encaminhamento FIFO aumenta o tempo de entrega dos agregados. Sem priorização, os agregados recebidos recentemente por um nó, devem esperar nos *buffers* até ficarem antigos suficiente para alcançar o início da fila. Uma vez no início da fila, o agregado é

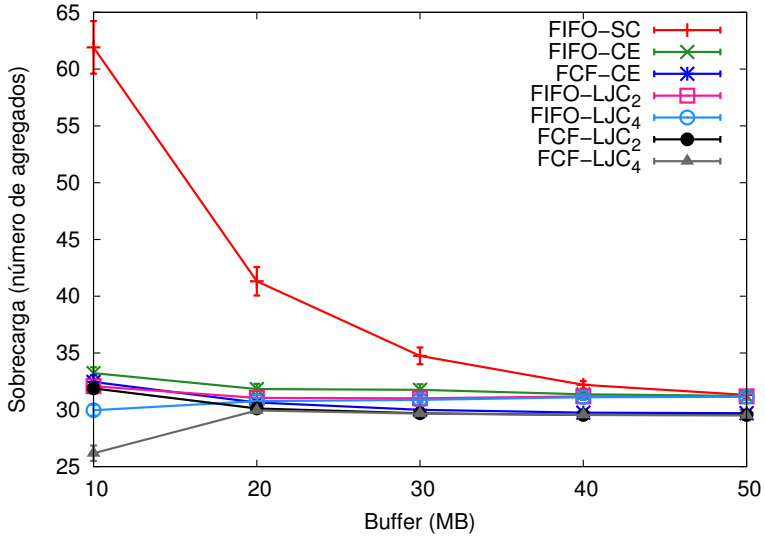
encaminhado. Esse atraso pelo qual os agregados passam depende tanto do tamanho do *buffer* quanto da dinâmica entre os contatos. Assim, quanto maior o tamanho do *buffer*, mais demorado é o tempo de espera por um encaminhamento. Os agregados também podem ser descartados por uma política de descarte durante esse período de espera, o que reduz a taxa de entrega.

Particularmente, o problema cabeça de linha também explica o baixo atraso de entrega provido pelo mecanismo FIFO-SC quando comparada a todos os outros mecanismos baseados em FIFO nos dois cenários. De fato, a FIFO-SC apenas entrega os agregados enviados durante a inicialização da rede, como observado por Lindgren e Phanse [31], o que é corroborado pelo baixo desempenho do mecanismo FIFO-SC em termos de taxa de entrega. Os primeiros agregados enviados pela rede experimentam baixo tempo de atraso porque os *buffers* estão quase vazios. Portanto, o atraso médio é baixo, uma vez que são levados em conta apenas os agregados entregues para calcular essa métrica.

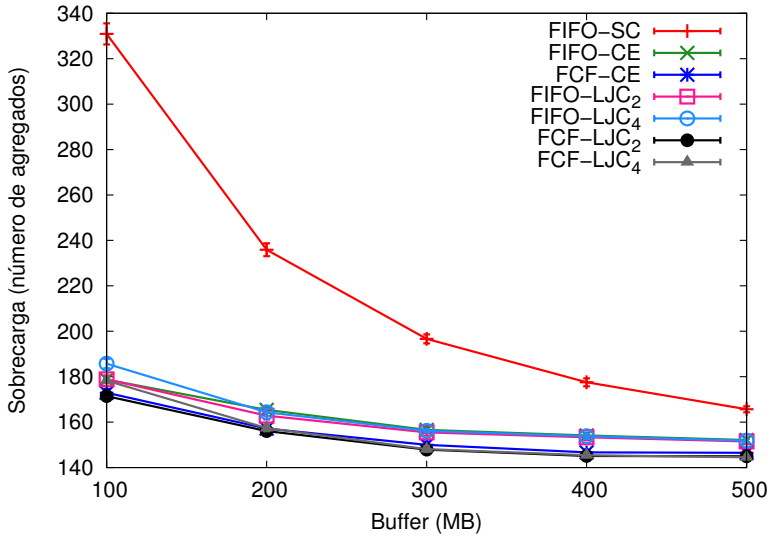
### 5.4.3 Sobrecarga

A sobrecarga para ambos os cenários é exibida nas Figuras 5.8, 5.9 e 5.10. Claramente, o uso de custódia reduz a sobrecarga. Nesse caso, os agregados sob custódia não são descartados por políticas de descarte e assim os nós tendem a carregá-los por um período de tempo maior. Consequentemente, mais cópias desses agregados são encaminhadas e, como resultado, mais agregados atingem seus destinos, o que reduz a sobrecarga por agregado entregue.

Os mecanismos que utilizam FCF, em geral, obtêm menor sobrecarga que os mecanismos que utilizam FIFO porque eles atingem maiores taxas de entrega em ambos os cenários Rollernet, e Infocom06. Todas as configurações FCF-LJC$_i$ superam as demais configurações em ambos os protocolos analisados. Isso é evidenciado para o tamanho de *buffer* igual a 10 MB, o mais restrito e no qual ocorre o maior número de descartes. Para esse tamanho, a configuração FCF-LJC$_4$ com o protocolo *Epidemic* obteve na Figura 5.8 reduções na sobrecarga de aproximadamente 58% e 46% para os cenários Rollernet e Infocom06 quando comparada à configuração sem o uso de custódia (FIFO-SC). Já com o protocolo *Spray and Wait* na Figura 5.10, a FCF-CE obtém uma redução de aproximadamente 47% para o cenário Rollernet e de aproximadamente 78% para o cenário Infocom06 em relação à FIFO-SC. Para o protocolo PRoPHET esse melhor desempenho é ainda mais evidente em ambos os cenários, chegando a configuração FCF-LJC$_4$ a obter 73% e 61% de redução da sobrecarga quando comparada à FIFO-SC como ilustra a Figura 5.9.




(a) Rollernet.

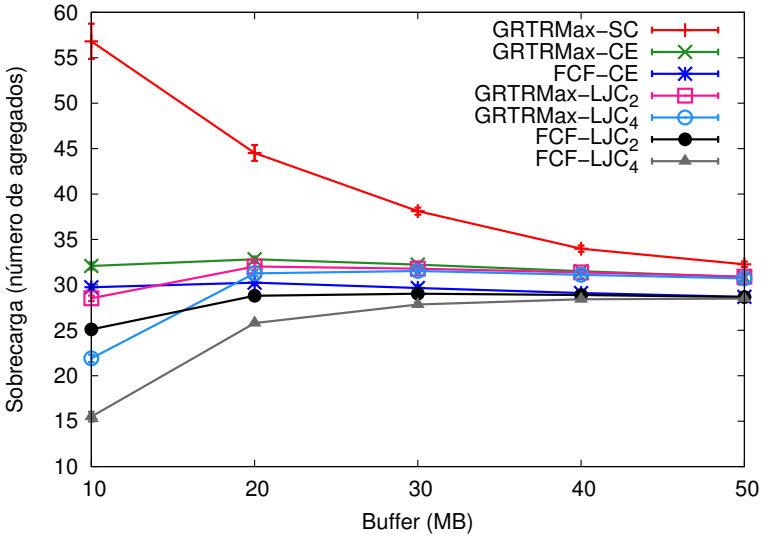



(b) Infocom06.

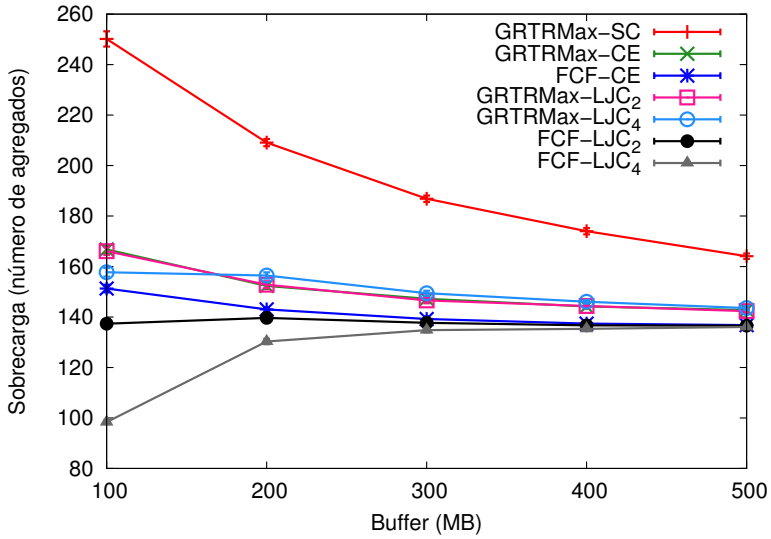
Figura 5.8: Sobrecarga para o protocolo *Epidemic*.

### 5.4.4 Uma alternativa ao *Spray and Wait*

Assim como neste trabalho, diversas pesquisas na literatura de redes DTN avaliam suas propostas com os protocolos *Epidemic*, PRoPHET e *Spray and Wait*. Como exemplo, podem ser citadas propostas de novos mecanismos de fragmentação de agregados [43], políticas de descarte [49], políticas de encaminhamento [27], bem como propostas de novos protocolos de roteamento [17, 58]. Nas avaliações de desempenho realizadas nesses trabalhos citados, o protocolo *Spray and Wait* possui desempenho superior em relação aos protocolos *Epidemic* e PRoPHET. Diante disso, nessa seção é realizada uma comparação do mecanismo combinado FCF-LJC nos protocolos *Epidemic* e PRoPHET com a versão




(a) Rollernet.

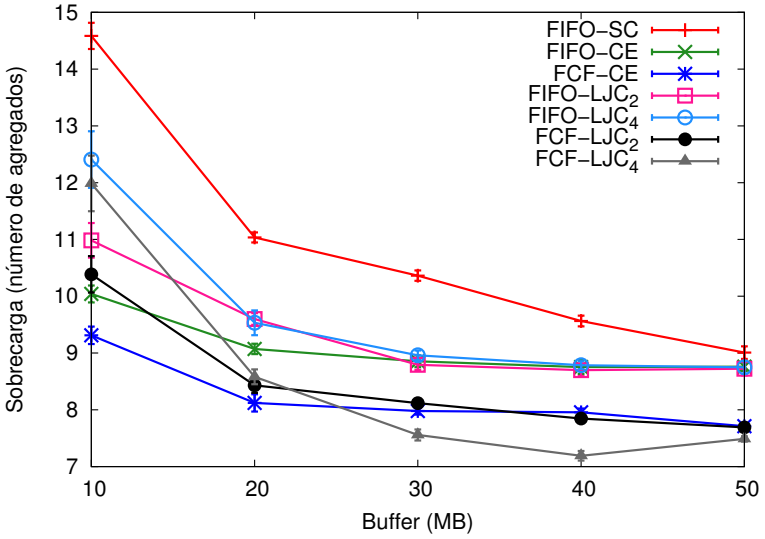



(b) Infocom06.

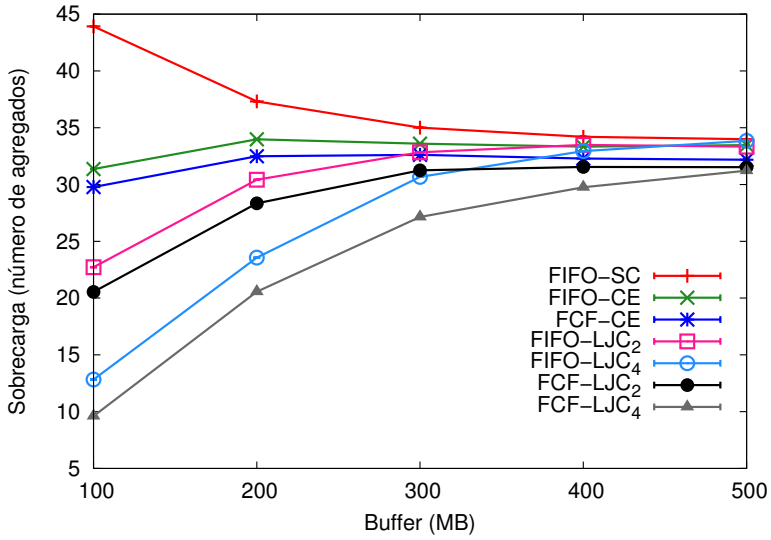
Figura 5.9: Sobrecarga para o protocolo PRoPHET.

sem o uso de custódia do *Spray and Wait*. O intuito é mostrar que é possível proporcionar uma taxa de entrega maior que o *Spray and Wait*, com uma sobrecarga menor e com atraso mais baixo em um cenário com um maior volume de tráfego, no qual o transbordamento de *buffer* é mais frequente. A Figura 5.11 exibe o desempenho dos protocolos *Epidemic*, PRoPHET e *Spray and Wait* sem o uso de custódias, na qual é possível verificar o melhor desempenho deste último. A figura ainda exibe os protocolos *Epidemic* e PRoPHET utilizando a configuração FCF-LJC$_2$, escolhida por apresentar melhor desempenho geral com o uso de 2000 agregados para o cenário Rollernet. As seguintes considerações são relacionadas ao tamanho de *buffer* de 50 MB.

Os resultados mostram que o mecanismo FCF-LJC combinado a ambos os protocolos



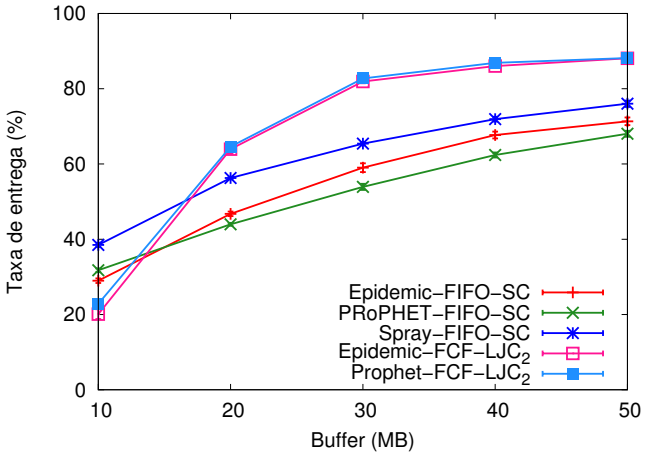

(a) Rollernet.



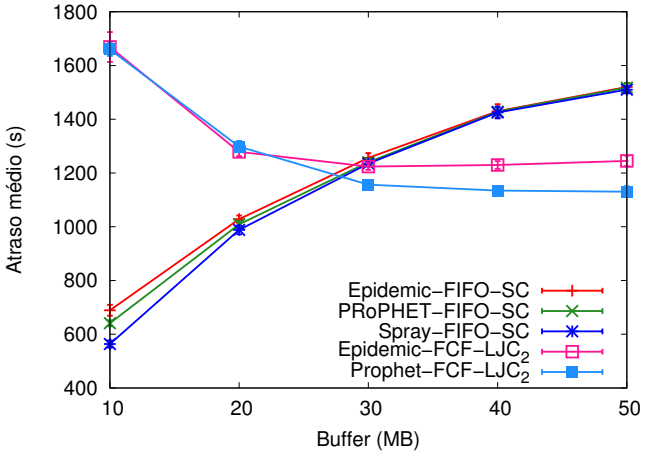

(b) Infocom06.

Figura 5.10: Sobrecarga para o protocolo *Spray and Wait*.

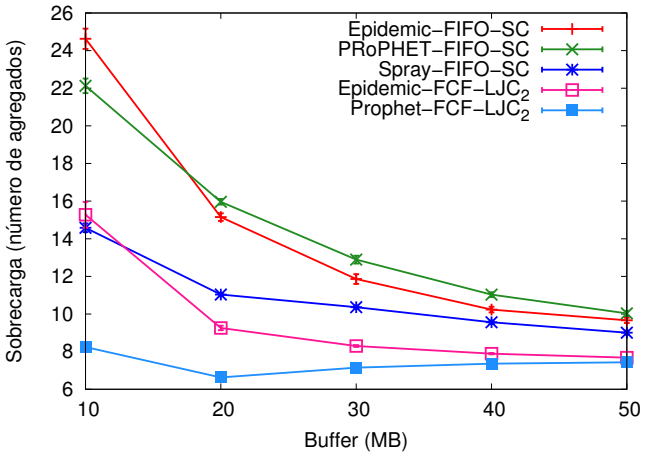
proporcionou desempenhos superiores aos do protocolo*Spray and Wait*. Os protocolos PRoPHET e *Epidemic* apresentam uma taxa de entrega aproximadamente 12% maior. Verifica-se também que com o PRoPHET e *Epidemic* os atrasos médios de entrega são aproximadamente 26% e 18% menores, respectivamente. Por fim, o mecanismo FCF-LJC$_2$ com os protocolos PRoPHET e *Epidemic* obtêm sobrecargas aproximadamente 18% e 15% menores que a apresentada pelo protocolo *Spray and Wait*. Conclui-se, portanto, que as propostas desse trabalho aumentam o desempenho da rede em termos de taxa de entrega, de sobrecarga e do atraso. Pode-se concluir ainda que um protocolo híbrido baseado em replicação probabilística e com replicação controlada, como o mecanismo FCF-LJC$_2$ sobre o protocolo PRoPHET, se comporta como a melhor configuração possível dentre as




(a) Taxa de entrega.




(b) Atraso médio




(c) Sobrecarga

Figura 5.11: Comparação no cenário Rollernet entre os Protocolos *Epidemic* e PRoPHET com o uso de custódia e o *Spray and Wait* em sua versão padrão.

analisadas e se destaca como uma alternativa ao protocolo de replicação controlada *Spray and Wait* em cenários com maior volume de tráfego.

# Capítulo 6

# Conclusões

As redes DTN se apresentam como importante alternativa para viabilizar a conectividade em cenários nos quais não há garantias de caminhos fim-a-fim entre os nós e em que hajam frequentes desconexões e longos atrasos nas transmissões. Nestes cenários, conhecidos como cenários desafiadores, diversas aplicações e projetos são desenvolvidos em situações nas quais pilhas de protocolos tradicionais como a TCP/IP são ineficientes. Tais aplicações vão desde o monitoramento da vida animal, onde não há o acesso convencional e viável à Internet, a projetos em centros urbanos onde exista infraestrutura de acesso, porém predominem as conexões intermitentes entre os nós.

Um dos problemas abordados neste trabalho relacionado às aplicações com redes DTN foi o descarte prematuro de agregados, no qual um agregado é descartado do *buffer* ainda em seu nó de origem ou próximo dele sem que seja suficientemente disseminado na rede. Tal problema tem como consequência direta a redução da taxa de entrega, pois agregados descartados prematuramente não possuem chances de atingirem seus nós de destino. Outro problema tratado nesta pesquisa foi a utilização do tempo de contato para transmissão entre os nós através do uso de políticas de encaminhamento. A oportunidade de contato entre os nós quando não utilizada de forma eficiente influi diretamente no desempenho da rede, pois os nós dificilmente transmitem todos os agregados que desejam encaminhar devido às limitações de largura de banda e de tempo de contato.

O objeto de estudo desta pesquisa utilizado para tratar os dois problemas citados foi a transferência de custódia, um mecanismo simples, porém pouco explorado em pesquisas. A transferência de custódia, também conhecida como custódia exclusiva, foi inicialmente proposta na literatura de redes DTN com a finalidade de aumentar a confiabilidade da rede. Mais especificamente, este trabalho abordou o uso da transferência de custódia, especialmente a custódia compartilhada, como forma de aumentar desempenho da rede,

evitando descartes prematuros de agregados e também utilizando de forma eficiente o tempo de contato entre os nós. Para isso, foram propostos e avaliados os mecanismos *Limited Joint Custody* (LJC) e *Forward Custody First* (FCF). O LJC emprega a custódia compartilhada, permitindo que um agregado sob custódia tenha várias replicas na rede. Porém, o LJC limita essa replicação evitando o esgotamento de recursos de armazenamento. A FCF é uma política de encaminhamento que prioriza agregados sob custódia. Assim, havendo no *buffer* de um nó agregados regulares e agregados sob custódia, os sob custódia são encaminhados primeiro.

O desempenho das propostas LJC e FCF foi avaliado através de simulações utilizando-se as métricas taxa de entrega, atraso de entrega e sobrecarga. Para essas simulações foram escolhidos três protocolos de roteamento dentre os mais citados na literatura de redes DTN: um protocolo baseado em inundação, o *Epidemic*, um protocolo de replicação probabilística, representado pelo PRoPHET, e outro de replicação controlada, representado pelo *Spray and Wait* [58]. Os registros reais de mobilidade Rollernet e Infocom06 foram utilizados com o objetivo de produzir nas simulações resultados mais próximos de um ambiente real. O desempenho do mecanismo LJC foi comparado ao do mecanismo de custódia exclusiva e também ao desempenho das versões nativas dos protocolos, sem o uso de transferência de custódia. Já a política FCF teve seu desempenho comparado ao desempenho das políticas nativas dos protocolos analisados. Por fim, a combinação dos mecanismos LJC-FCF teve seu desempenho comparado ao de mecanismos que não usam transferência de custódia.

Os principais resultados mostram que a combinação de LJC e FCF proporciona um aumento significativo de desempenho em termos da taxa de entrega, atraso e sobrecarga nos dois cenários analisados com menor sobrecarga. A explicação para tais ganhos é a seguinte. O LJC aumenta o número de réplicas de agregados sob custódia na rede. A FCF, por sua vez, dá total prioridade aos agregados sob custódia e, assim, encaminha esses agregados primeiro e mais frequentemente que os agregados regulares. Assim, a combinação FCF-LJC obtém mais agregados com prioridade na rede atingindo maiores taxas de entrega e menores atrasos. A combinação dos mecanismos FCF-LJC quando comparada a mecanismos que não usam custódia proporciona um aumento de até 24% na taxa de entrega e reduz em até 40% e 78% o atraso de entrega e sobrecarga de controle, respectivamente.

Outra conclusão importante foi obtida pela comparação direta entre os três protocolos analisados em um cenário com maior volume de tráfego, no qual o transbordamento de

*buffer* é mais frequente. Diversas pesquisas apontam o protocolo *Spray and Wait* como tendo desempenho superior ao dos protocolos *Epidemic* e PRoPHET. Com base nisso, foi realizada uma avaliação em que os mecanismos FCF-LJC nos protocolos *Epidemic* e PRoPHET foram comparados à versão sem o uso de custódia do *Spray and Wait*. Os resultados mostraram que o mecanismo LJC-FCF combinado a ambos os protocolos proporcionou desempenhos superiores aos do protocolo *Spray and Wait*. Especificamente, o protocolo de replicação probabilística PRoPHET apresentou-se como uma alternativa mais eficiente. A combinação dos mecanismos FCF-LJC com o PRoPHET quando comparada ao *Spray and Wait* proporcionou uma taxa de entrega 12% maior e atraso de entrega e sobrecarga de controle 26% e 18% menores, respectivamente. Também se verificou nesses cenários que não há melhoria no desempenho com o uso de mais de duas custódias por agregado.

## 6.1 Trabalhos futuros

Os trabalhos futuros incluem implementar diferentes mecanismos de transferência de custódia. Além disso, seriam consideradas estratégias de negociação, concessão e revogação de custódia como os mencionados a seguir:

- concessão de custódia de forma probabilística: nessa abordagem, um nó vizinho aceita a custódia dos agregados apenas se ele tiver grande probabilidade de encontro com o nó de destino. Ainda relacionada a essa proposta, pode-se definir limites de valores de probabilidade de encontro entre os nós a partir dos quais os agregados podem ser encaminhados, mas sem a transferência de custódia. Com essa proposta, pretende-se avaliar o impacto de apenas os agregados com grandes chances de serem entregues trafegarem sob custódia na rede;

- custódia baseada no número de saltos: nessa proposta, a custódia é concedida aos agregados que possuem um determinado limiar de saltos. Com isso, pretende-se avaliar o impacto dos agregados com maior número de encaminhamentos não serem descartados por políticas de gerenciamento de *buffer*. Esforços também seriam necessários para determinar o limiar ideal de saltos de acordo com as características dos cenários;

- custódia baseada em métricas sociais: nessa abordagem, os nós mais populares de acordo métricas sociais como centralidade e comunidade obtém a custódia de seus

agregados. Um desafio dessa abordagem é definir limiares de popularidade dos nós a partir dos quais as custódias de seus agregados seriam revogadas;

- custódia baseada em ocupação de *buffer*: com essa abordagem, pretende-se definir percentuais de ocupação de *buffer* a partir dos quais agregados sob custódia não são aceitos ou sua aceitação é condicionada à revogação da custódia de outros agregados. A ideia dessa proposta é evitar que *buffers* de menor capacidade fiquem congestionados com agregados que não podem ser descartados por estarem sob custódia. Uma variação dessa ideia é aceitar os agregados, mas não aceitar a transferência de custódia;

Com relação a políticas de encaminhamento envolvendo custódias, algumas abordagens podem ser propostas relacionadas. A seguir, seguem alternativas de trabalhos futuros envolvendo variações da política FCF:

- encaminhamento probabilístico com o protocolo *Spray and Wait*: essa ideia visa criar uma política de encaminhamento probabilístico com custódias e aplicá-lo ao protocolo *Spray and Wait*. Com isso, pretende-se adotar uma abordagem híbrida com um protocolo de replicação controlada, mas utilizando uma política de encaminhamento probabilística. Assim, na fase de espalhamento, o protocolo encaminharia primeiro os agregados para nó que tiverem maior probabilidade de encontro com os nós de destino dos agregados;

- FCF com métricas sociais: uma outra possibilidade é criar uma política de encaminhamento que relacione a FCF com métricas sociais. Assim, os agregados sob custódia que possuírem mais relevância ou popularidade são encaminhados primeiro;

- FCF relacionada ao tempo de vida: nessa proposta, a política FCF levaria em consideração o tempo de vida dos agregados sob custódia. Assim, pretende-se observar o impacto de encaminhar primeiro os agregados sob custódia que têm maior tempo de vida, partindo-se do princípio que os que possuem menor TTL serão logo descartados e terão menor probabilidade de atingir seu destino.

# Referências


[1] Ayub, Q.; Rashid, S.; Zahid, M. Optimization of epidemic router by new forwarding queue mode TSMF. *International Journal of Computer Applications* (Outubro 2010), 5–8.

[2] Ayub, Q.; Rashid, S.; Zahid, M. S. M. TMHF: Transmit max hop first forwarding strategy to optimize the performance of epidemic routing protocol. *International Journal of Computer Applications* (Março 2011), 40–45.

[3] Burgess, J.; Gallagher, B.; Jensen, D.; Levine, B. N. MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks. Em *IEEE INFOCOM* (Abril 2006), pp. 1–11.

[4] Burleigh, S.; Hooke, A.; Torgerson, L.; Fall, K.; Cerf, V.; Durst, B.; Scott, K.; Weiss, H. Delay-tolerant networking: an approach to interplanetary Internet. *IEEE Communications Magazine* (Junho 2003), 128–136.

[5] Campista, M.; Moraes, I.; Esposito, P.; Amodei, A.; de O Cunha, D.; Costa, L.; Duarte, O. The ad hoc return channel: a low-cost solution for Brazilian interactive digital TV. *IEEE Communications Magazine* (Janeiro 2007), 136–143.

[6] Cao, Y.; Sun, Z. Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges. *IEEE Communications Surveys & Tutorials* (Maio 2012), 1–24.

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

[8] Chuah, M. C.; Yang, P.; Davison, B. D.; Cheng, L. Performance comparison of unicast routing schemes in DTNs. Relatório técnico, Dept. of Computer Science and Engineering, Lehigh University, 2006.

[9] Chuah, M.-C.; Yang, P.; Davison, B. D.; Cheng, L. Store-and-forward performance in a DTN. Em *IEEE VTC'06* (Maio 2006), pp. 187–191.

[10] Demmer, M.; Brewer, E.; Fall, K.; Ho, M.; Patra, R.; Demmer, M.; Brewer, E.; Fall, K.; Jain, S.; Ho, M.; Patra, R. Implementing delay tolerant networking. Relatório técnico, 2003.

[11] Doering, M.; Wolf, L. Work in progress: Evaluation of generic bundle transmission scheduling strategies in vehicular disruption tolerant networks. Em *ExtremeCom* (Março 2012), pp. 1–11.

[12] Durst, R. C.; Feighery, P. D.; Scott, K. L. Why not use the standard internet suite for the interplanetary internet. Em *Interplanetary Internet Study Seminar, California Institute of Technology* (1999).

[13] Fall, K. A delay-tolerant network architecture for challenged Internets. Em *ACM SIGCOMM* (Agosto 2003), pp. 27–34.

[14] Fall, K.; Farrell, S. DTN: an architectural retrospective. *IEEE JSAC* (Maio 2008), 828–836.

[15] Fall, K.; Hong, W.; Madden, S. Custody transfer for reliable delivery in delay tolerant networks. Relatório técnico, Intel Research, Berkeley, California, Julho 2003.

[16] Gerla, M.; Kleinrock, L. Vehicular networks and the future of the mobile Internet. *Computer Networks* (Fevereiro 2011), 457–469.

[17] Grasic, S.; Davies, E.; Lindgren, A.; Doria, A. The evolution of a DTN routing protocol - PRoPHETv2. Em *ACM CHANTS* (Junho 2011), pp. 27–30.

[18] Grossglauser, M.; Tse, D. N. C. Mobility increases the capacity of ad hoc wireless networks. *IEEE/ACM Transactions on Networking.* (Agosto 2002), 477–486.

[19] Guo, S.; Falaki, M.; Oliver, E.; Ur Rahman, S.; Seth, A.; Zaharia, M.; Ismail, U.; Keshav, S. Design and implementation of the KioskNet system. Em *ICTD* (Dezembro 2007), pp. 1–10.

[20] Hui, P.; Chaintreau, A.; Scott, J.; Gass, R.; Crowcroft, J.; Diot, C. Pocket switched networks and human mobility in conference environments. Em *ACM SIGCOMM workshop on Delay-tolerant networking* (Agosto 2005), pp. 244–251.

[21] Hui, P.; Crowcroft, J.; Yoneki, E. Bubble rap: Social-based forwarding in delay-tolerant networks. *IEEE Transactions on Mobile Computing* (Novembro 2011), 1576–1589.

[22] Hui, P.; Lindgren, A. Phase transition of opportunistic communications. Em *ACM Workshop on Challenged networks* (Setembro 2008), pp. 73–80.

[23] Ip, Y.-K.; Lau, W.-C.; Yue, O.-C. Forwarding and replication strategies for DTN with resource constraints. Em *IEEE VTC* (Abril 2007), pp. 1260–1264.

[24] Juang, P.; Oki, H.; Wang, Y.; Martonosi, M.; Peh, L. S.; Rubenstein, D. Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet. *ACM SIGPLAN Noticies* (Outubro 2002), 96–107.

[25] Keränen, A.; Ott, J.; Kärkkäinen, T. The ONE simulator for DTN protocol evaluation. Em *SIMUTools* (Março 2009), pp. 55:1–55:10.

[26] Khabbaz, M. J.; Assi, C. M.; Fawaz, W. F. Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges. *IEEE Communications Surveys & Tutorials* (2012), 607–640.

[27] Khalid, O.; Khan, S. U.; Kolodziej, J.; Zhang, L.; Li, J.; Hayat, K.; Madani, S. A.; Wang, L.; Chen, D. A checkpoint based message forwarding approach for opportunistic communication. Em *European Conference on Modelling and Simulation - ECMS* (Maio 2012), pp. 512–518.

[28] Li, Q.; Zhu, S.; Cao, G. Routing in socially selfish delay tolerant networks. Em *IEEE INFOCOM* (Março 2010), pp. 1–9.

[29] Lindgren, A.; Doria, A.; Davies, E.; Grasic, S. Probabilistic Routing Protocol for Intermittently Connected Networks. RFC 6693 (Experimental), Agosto 2012.

[30] Lindgren, A.; Doria, A.; Schelén, O. Probabilistic routing in intermittently connected networks. *ACM SIGMOBILE Mobile Computing and Communications Review* (Julho 2003), 19–26.

[31] Lindgren, A.; Phanse, K. S. Evaluation of queueing policies and forwarding strategies for routing in intermittently connected networks. Em *COMSWARE* (Agosto 2006), pp. 1–10.

[32] Mathurapoj, A.; Pornavalai, C.; Chakraborty, G. Fuzzy-spray: efficient routing in delay tolerant ad-hoc network based on fuzzy decision mechanism. Em *International conference on Fuzzy Systems* (Dezembro 2009), pp. 104–109.

[33] McDonald, P.; Geraghty, D.; Humphreys, I.; Farrell, S.; Cahill, V. Sensor Network with Delay Tolerance (SeNDT). Em *ICCCN* (Agosto 2007), pp. 1333–1338.

[34] Miranda, E.; Naves, J. F.; Moraes, I. M.; Velloso, P. B. A joint custody-based forwarding policy for delay-tolerant networks. Em *IEEE GIIS* (Dezembro 2012), pp. 1–6.

[35] Miranda, E.; Naves, J. F.; Moraes, I. M.; Velloso, P. B. Uma avaliação do uso de mecanismos de custódia compartilhada em redes tolerantes a atrasos e desconexões. Em *Simpósio Brasileiro de Redes de Computadores* (Maio 2013), pp. 687–700.

[36] Naves, J. Dissertação de mestrado: Políticas de encaminhamento de mensagens e de gerenciamento de buffer para redes tolerantes a atrasos e desconexões, Agosto 2012. Disponível em http://www.ic.uff.br/PosGraduacao/Dissertacoes/547.pdf.

[37] Naves, J. F.; Moraes, I. M.; de Albuquerque, C. V. N. LPS and LRF: Efficient buffer management policies for delay and disruption tolerant networks. Em *IEEE LCN* (Outubro 2012), pp. 368–375.

[38] 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. Em *Minicursos do Simpósio Brasileiro de Redes de Computadores* (Maio 2007), pp. 203–256.

[39] Oliveira, E. C. R. *Roteamento Adaptativo a Contextos para Redes Tolerantes a Atrasos e Desconexões*. Tese de Doutorado, Instituto de Computação, Universidade Federal Fluminense, Niterói, RJ, Brasil, Setembro 2011.

[40] Oliveira, E. C. R.; de Albuquerque, C. V. N. NECTAR: a DTN routing protocol based on neighborhood contact history. Em *Proceedings of the ACM symposium on Applied Computing* (Maio 2009), pp. 40–46.

[41] Parikh, S.; Durst, R. Disruption tolerant networking for Marine Corps CONDOR. Em *IEEE Military Communications Conference* (Outubro 2005), pp. 325–330 Vol. 1.

[42] Pentland, A.; Fletcher, R.; Hasson, A. DakNet: rethinking connectivity in developing nations. *IEEE Computer* (Janeiro 2004), 78–83.

[43] Pitkanen, M.; Keranen, A.; Ott, J. Message fragmentation in opportunistic DTNs. Em *WOWMOM* (Junho 2008), pp. 1–7.

[44] Pompili, D.; Akyildiz, I. F. Overview of networking protocols for underwater wireless communications. *IEEE Communications Magazine* (Janeiro 2009), 97–102.

[45] Ramanathan, R.; Hansen, R.; Basu, P.; Rosales-Hain, R.; Krishnan, R. Prioritized epidemic routing for opportunistic networks. Em *ACM MobiOpp* (Março 2007), pp. 62–66.

[46] Ribeiro, F. J. L.; Pedroza, A. C. P.; Costa, L. H. M. K. Deepwater monitoring system in underwater delay/disruption tolerant network. *IEEE Latin America Transactions* (Janeiro 2012), 1324–1331.

[47] Rubinstein, M. G.; Abdesslem, F. B.; Cavalcanti, S. R.; Campista, M. E. M. C.; Alves, R. S.; Costa, L. H. M. K.; Amorim, M. D.; Duarte, O. C. M. B. Measuring the capacity of in-car to in-car vehicular networks. *IEEE Communications Magazine* (Novembro 2009), 128–136.

[48] Rutishauser, M.; Petkov, V.; Boice, J.; Obraczka, K.; Mantey, P.; Williams, T. M.; Wilmers, C. C. Carnivore: a disruption-tolerant system for studying wildlife. *EURASIP Journal on Wireless Communications and Networking* (Janeiro 2011), 10:1–10:14.

[49] Sathita, K.; Ochiai, H.; Esaki, H. Message deletion and mobility patterns for efficient message delivery in DTNs. Em *PerCom Workshops* (Março 2010), pp. 760–763.

[50] Schildt, S.; Morgenroth, J.; Pöttner, W.-B.; Wolf, L. IBR-DTN: A lightweight, modular and highly portable bundle protocol implementation. *Electronic Communications of the EASST* (Janeiro 2011), 1–11.

[51] Scott, K.; Burleigh, S. Bundle Protocol Specification. RFC 5050 (Experimental), Novembro 2007.

[52] Seligman, M. Storage usage of custody transfer in delay tolerant networks with intermittent connectivity. Em *ICWN* (Junho 2006), pp. 386–392.

[53] Shah, R.; Roy, S.; Jain, S.; Brunette, W. Data mules: modeling a three-tier architecture for sparse sensor networks. Em *IEEE SNPA* (Maio 2003), pp. 30–41.

[54] Soares, V. N. G. J.; Farahmand, F.; Rodrigues, J. J. P. C. Evaluating the impact of storage capacity constraints on vehicular delay-tolerant networks. Em *IEEE CTRQ* (Julho 2009), pp. 75–80.

[55] Soares, V. N. G. J.; Farahmand, F. F.; Rodrigues, J. R. Performance analysis of scheduling and dropping policies in vehicular delay-tolerant networks. *International Journal on Advances in Internet Technology* (Julho 2010), 137–145.

[56] Soares, V. N. G. J.; Rodrigues, J. J. P. C.; Ferreira, P. S.; Nogueira, A. M. D. Improvement of messages delivery time on vehicular delay-tolerant networks. Em *ICPP Workshops* (Setembro 2009), pp. 344–349.

[57] Sorber, J.; Kostadinov, A.; Garber, M.; Brennan, M.; Corner, M. D.; Berger, E. D. Eon: A language and runtime system for perpetual systems. Em *ACM Conference on Embedded Networked Sensor Systems* (Novembro 2007), pp. 161–174.

[58] Spyropoulos, T.; Psounis, K.; Raghavendra, C. S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks. Em *ACM SIGCOMM Workshop on Delay-tolerant networking* (Agosto 2005), pp. 252–259.

[59] Spyropoulos, T.; Rais, R. N. B.; Turletti, T.; Obraczka, K.; Vasilakos, A. Routing for disruption tolerant networks: taxonomy and design. *Wireless Networks* (Setembro 2010), 2349–2370.

[60] Tournoux, P.-U.; Leguay, J.; Benbadis, F.; Conan, V.; de Amorim, M. D.; Whitbeck, J. The accordion phenomenon: Analysis, characterization, and impact on DTN routing. Em *IEEE INFOCOM* (Abril 2009), pp. 1116–1124.

[61] Vahdat, A.; Becker, D. Epidemic routing for partially-connected ad hoc networks. Relatório técnico, Duke University, Julho 2000.

[62] Wang, Y.; Wu, J.; Jiang, Z.; Li, F. A joint replication-migration-based routing in delay tolerant networks. Em *IEEE ICC* (Junho 2012), pp. 73–77.

[63] Yeo, J.; Kotz, D.; Henderson, T. CRAWDAD: a community resource for archiving wireless data at Dartmouth. *SIGCOMM Computer Communication Review* (Abril 2006), 21–22.

[64] Yuan, Q.; Cardei, I.; Wu, J. Predict and relay: an efficient routing in disruption-tolerant networks. Em *ACM MobiHoc* (Maio 2009), pp. 95–104.

[65] Zarafshan-Araki, M.; Chin, K.-W. TrainNet: A transport system for delivering non real-time data. *Computer Communications* (Setembro 2010), 1850–1863.