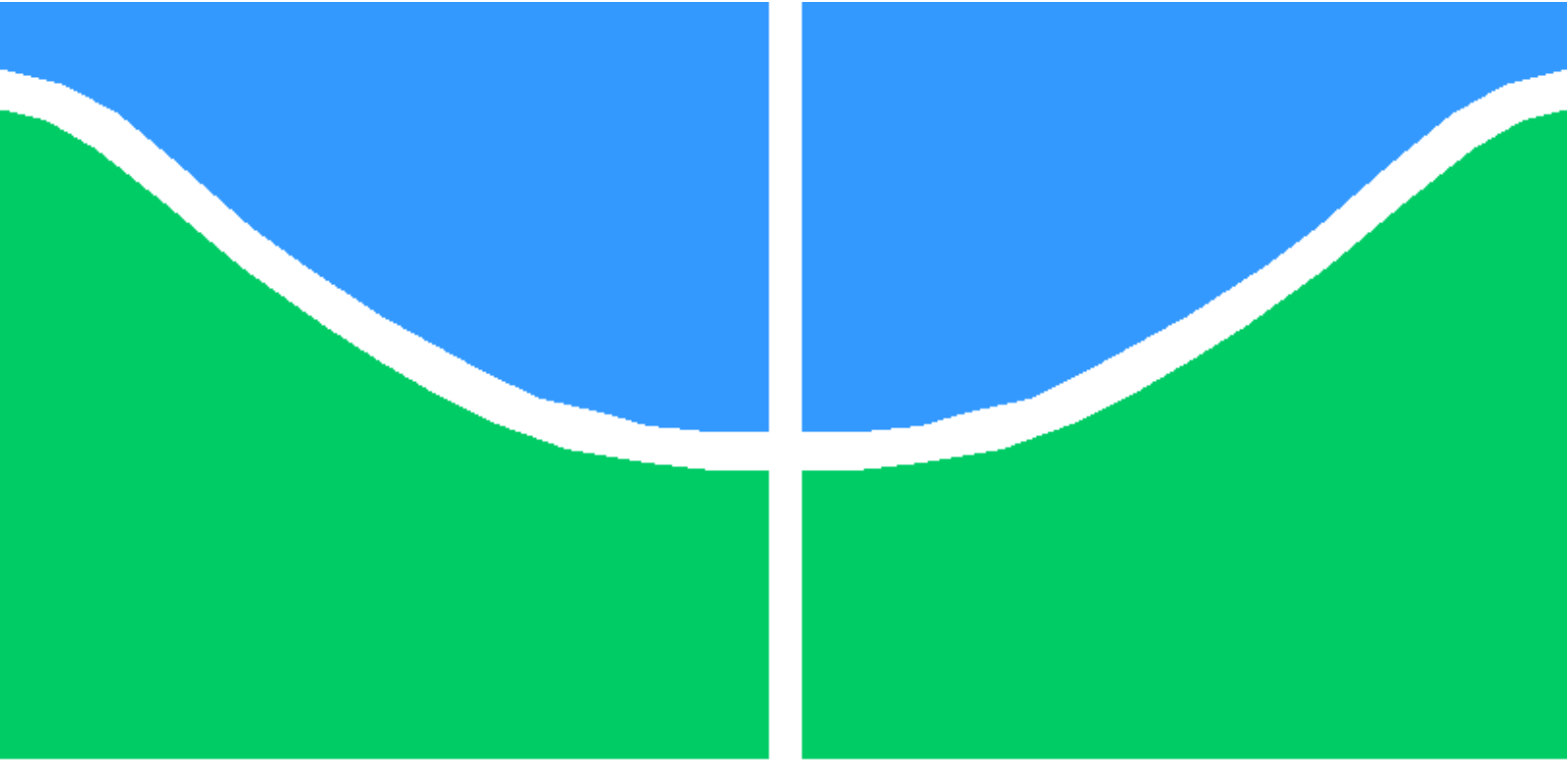

TRABALHO DE GRADUAÇÃO

DESEMPENHO DE ESTRATÉGIAS DE ESCOAMENTO DE TRÁFEGO SOBRE REDES *AD HOC* BASEADAS NO SISTEMA OPERACIONAL ANDROID

Everton Augusto de Lima Andrade

Brasília, julho de 2015

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

DESEMPENHO DE ESTRATÉGIAS DE ESCOAMENTO DE TRÁFEGO SOBRE REDES *AD HOC* BASEADAS NO SISTEMA OPERACIONAL ANDROID

Everton Augusto de Lima Andrade

Relatório submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Marcelo Menezes de Carvalho, ENE/UnB _____
Orientador

Prof. Paulo Roberto de Lira Gondim, ENE/UnB _____
Examinador Interno

Prof. Jacir Luiz Bordim, CIC/UnB _____
Examinador Interno

Dedicatória

A todas as mentes que não se fecham ao pensamento da sociedade.

Everton Augusto de Lima Andrade

Agradecimentos

Agradeço a todos que me ajudaram de algum modo, até mesmo você que que pode ter me emprestado uma simples caneta que salvou a minha vida. Agradeço à minha família, por sempre acreditar no meu potencial e por sempre estar presente na minha vida; à toda a equipe do GPDS, por mostrarem que existe uma luz no fim do túnel; ao Lucas Soares, por ter me ajudado a entender todo o funcionamento da estratégia e por compartilhar do mesmo sofrimento; ao Fadhil Firyaguna, que se deixou levar pelo lado negro da força mas sempre esteve presente nos momentos de PIBIC e de sofrimento com o ns-3; à Ana Carolina, por automatizar muitos processos; à Thayane Viana, por esquecer seus pacotes de chá na minha sala; ao Moacir Balestrini, por compartilhar a planta baixa do SG-11, a todos os meus amigos que me ajudaram com a realização dos experimentos, amigos capazes de irem à faculdade em um domingo de manhã ou em um feriado nacional apenas para ajudarem um amigo necessitado, Evandro Costa, Márcia Manuela, Sávio Neves e Rodrigo Rozário; ao professor Marcelo, por me permitir fazer parte da equipe NERds durante todos esses anos; à toda a equipe que participou do Maniac Challenge, obrigado por comentarem o código. Por fim, agradeço ao café, por ter me mantido acordado por longas e longas horas durante todos esses anos de engenharia.

Everton Augusto de Lima Andrade

RESUMO

Este trabalho apresenta uma avaliação de desempenho de duas estratégias diferentes de escoamento de dados sobre redes *ad hoc*. As estratégias estudadas trabalham sobre um esquema de leilões recursivos, onde cada mensagem é transmitida para o dispositivo seguinte da rede à partir das ofertas recebidas de cada nó vizinho. A primeira estratégia estudada, chamada "estratégia do aperto", é capaz de realizar uma análise da rede para a definição do valor de oferta de um pacote leiloado à partir da tabela de roteamento gerada pelo protocolo OLSR, essa avaliação considera a vantagem, ou desvantagem, de sua posição na rede até o destino final em relação a todos os outros nós próximos. Essa mesma estratégia, utiliza uma função de preferência para a definição do vencedor de um leilão, o valor da preferência é determinado à partir do valor de oferta recebido e o aperto relativo do nó em questão para a entrega bem sucedida do pacote ao destino final. A segunda estratégia estudada, chamada de "estratégia aleatória", não realiza nenhum tipo de análise da rede antes de definir o valor de oferta para um leilão gerado, sempre que é recebido uma requisição de oferta a estratégia gera um valor aleatório limitado pelo valor máximo de oferta. Em relação a definição de um vencedor de um leilão, a "estratégia aleatória" utiliza como base apenas o valor recebido, escolhendo como vencedor o nó que oferecer o menor valor. Ambas estratégias foram avaliadas em termos de taxa de sucesso de transmissão, número de saltos necessários para que a transmissão ocorra com sucesso e saldo médio final dos tablets. Toda a arquitetura montada para a realização dos experimentos utilizou como base o código fonte disponibilizado pelos desenvolvedores da competição Maniac (*Mobile Ad Hoc Networking Interoperability and Cooperation*) realizada na Alemanhã em 2013. A montagem da arquitetura foi realizada no prédio SG-11 da Universidade de Brasília, onde foram utilizados dois roteadores de backbone controlados por um computador central e 9 tablets habilitados com o sistema operacional Android. Os resultados obtidos apresentam significativa vantagem da utilização da "estratégia do aperto" em termos de número de saltos e saldo médio final.

ABSTRACT

This work presents a performance evaluation of two different data offloading strategies operating over an *ad hoc* network. The studied strategies are based on recursive auctions scheme where each message is transmitted to the next device based on the received bid of each neighbour. The first studied strategy, called “Tightness Strategy”, is able to perform a network analysis to define a bidding value of a auctioned packet using the routing table created by the OLSR protocol, this analysis consider the advantage, or disadvantage, of each node based on its location with respect to the final destination. This same strategy uses a preference function to define an auction winner, the preference value is calculated based on the received bidding value and the relative tightness of each node for successful packet delivery to final destination. The second strategy, called "Random Strategy", do not perform any kind of network analysis to define the bidding value for an auctioned packet, when a *request for bid* is received the strategy generate a random value limited by the maximum bid accepted value. With respect to the auction winner decision, the “Random Strategy” uses only the received bidding values, always choosing the lowest received value. Both strategies were evaluated in terms of successful transmission rate, number of hops needed to sucessfully complete the transmission, and average final balance. The whole architecture built to perform the experiments was developed using the source code available from the Maniac (*Mobile Ad Hoc Networking Interoperability and Cooperation*) Challenge, 2013. The architecture assembly and configuration was carried out inside the SG-11 building at University of Brasilia, where were used two backbone routers controlled by a central computer and nine Android enabled tablets. The results show significant advantage of using the “Tightness Strategy” in terms of number of hops and average final balance.

SUMÁRIO

1 Introdução 1
1.1 Contextualização 1
1.2 Definição do problema 4
1.3 Objetivos do projeto 5
1.4 Contribuições do Projeto 5
1.5 Apresentação do manuscrito 6

2 Fundamentação Teórica 7
2.1 Introdução 7
2.2 Redes Locais Sem Fio (WLANs) 7
2.2.1 Camada Física 9
2.2.2 Subcamada de Controle de Acesso ao Meio 10
2.2.2.1 Função de Coordenação Distribuida 10
2.3 Redes *Ad Hoc* 12
2.4 Protocolos de Roteamento para redes *Ad Hoc* 13
2.4.1 OLSR - *Optimized Link State Routing Protocol* 14
2.5 A Plataforma Android 15
2.5.1 Arquitetura Android 16

3 A competição *MANIAC* 18
3.1 Introdução 18
3.2 Regras e Arquitetura Geral da Rede 18
3.2.1 Mestre 20
3.2.2 Roteadores de Backbone 21
3.2.3 ManiacLib 22

4 Estratégias 25
4.1 Introdução 25
4.2 Estratégia do Aperto 25
4.3 Estratégia Aleatória 28

5 Configuração dos Experimentos 30
5.1 Introdução 30
5.2 Local dos Experimentos 30

5.3 Canal de operação da rede 30
5.4 Configuração dos Tablets 32
5.5 Configuração das máquinas de backbone e mestre 34

6 Avaliação de Desempenho 38
6.1 Introdução 38
6.2 Configuração dos Experimentos 38
6.3 Resultados dos Experimentos 40

7 Conclusões 46
7.1 Trabalhos Futuros 47

REFERÊNCIAS BIBLIOGRÁFICAS 51

Anexos 54

I Ambiente de Realização dos Experimentos 55

II Equipamentos Utilizados para Realização dos Experimentos 57

LISTA DE FIGURAS

1.1 Estratégia tradicional de conexão, todos os dispositivos estão diretamente conectados com um ponto de acesso principal 2
1.2 Estratégia de escoamento de informações por meio de repasse de mensagens entre dispositivos móveis 3

2.1 Exemplo de rede WLAN 8
2.2 Espalhamento espectral por sequência direta (DSSS) 9
2.3 Formato de quadro do padrão IEEE 802.11 10
2.4 Modo de contenção sem uso de RTS/CTS, o período de conteção NAV é definido pelo tamanho das mensagens de dados recebidas de outras estações 11
2.5 Modo de transmissão utilizando RTS/CTS, o tamanho do período de contenção NAV é atualizado toda vez que uma informação de RTS ou CTS é recebida 12
2.6 Exemplo de Rede *Ad Hoc* aplicado a dispositivos móveis e aplicado a comunicação militar 13
2.7 Funcionamento da técnica de múltiplos pontos de retransmissão (MPR) 15
2.8 Distribuição da utilização das versões do sistema operacional Android 16
2.9 Arquitetura em camadas do sistema operacional Android 17

3.1 Arquitetura da Rede durante a Competição *MANIAC* 20

4.1 Exemplo de curva de oferta O_{c_n} para diferentes valores de a_n quando $B_u = 200$ e $F_u = 80$ 27
4.2 Exemplo da função de preferência para valores de $B_n = 20$, $c_{max} = 3$, $k_1 = 2$ e $k_2 = 3$ 28

5.1 Planta do andar térreo do prédio SG11. 31
5.2 Planta do primeiro andar do prédio SG11. 31
5.3 Ocupação dos canais de rede na faixa de 2.4GHz medido à partir do ponto A. 32
5.4 Ocupação dos canais de rede na faixa de 2.4GHz medido à partir do ponto B. 32
5.5 Ocupação dos canais na faixa de 5GHz 33
5.6 Aplicação Manet Manager utilizada para iniciar a rede *ad hoc* e habilitar o protocolo OLSR. 34
5.7 Aplicação ManiacLib utilizada para a execução do repasse de informações e execução da estratégia utilizada 35
5.8 Planta baixa do andar térreo do prédio SG11 com a disposição do roteador de backbone e dos tablets utilizados 36

5.9 Planta baixa do primeiro andar do prédio SG11 com a disposição do roteador de backbone e dos tablets utilizados 36

6.1 Taxa de Sucesso de transmissão utilizando a estratégia do aperto e a estratégia aleatória 40
6.2 Ocorrência de número de saltos para todas as transmissões realizadas com sucesso com a estratégia do aperto 41
6.3 Taxa de entrega de pacotes com sucesso como função do número de saltos necessários para entrega com sucesso com a estratégia aleatória 42
6.4 Taxa de Sucesso de transmissão utilizando a estratégia do aperto e a estratégia aleatória para um limite de 4 saltos 43
6.5 Taxa de Sucesso de transmissão utilizando a estratégia do aperto e a estratégia aleatória para um limite de 2 saltos 43
6.6 Pontuação média de cada tablet utilizando a estratégia do aperto 44
6.7 Pontuação média de cada tablet utilizando a estratégia aleatória..... 44
6.8 Saldo médio final, por tablet participante em cada rodada de experimento, para ambas as estratégias do aperto e aleatória 45

I.1 Área inferior do prédio SG11 com os tablets posicionados durante a realização dos experimentos 55
I.2 Área superior do prédio SG11 utilizada para a realização dos experimentos 56

II.1 Computadores utilizados como backbones da rede e tablets utilizados para a instalação da aplicação ManiacLib durante a realização dos Experimentos..... 57

LISTA DE TABELAS

5.1 Endereços IPs configurados em cada tablet e a versão da plataforma Android utilizada 34
5.2 Endereços IPs configurados em cada uma das maquinas de backbone para se comunicarem via rede LAN 37
5.3 Endereços IPs configurados em cada uma das maquinas de backbone para se conectarem à rede *ad hoc* 37

6.1 Valores utilizados em cada parâmetro do protocolo de roteamento OLSR..... 39

LISTA DE ABREVIATURAS

Acrônimos

ACK	Acknowledgment
AODV	Ad Hoc On-Demand Distance Vector
AP	Access Point
CFP	Contention-free Period
CP	Contention Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DCF	Distributed Coordination Function
DIFS	Distributed Interframe Space
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
DVM	Dalvin Virtual Machine
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Eletrical and Eletronic Engineers
IFS	Interframe Space
IR	Infra-Red
ISM	Industrial, Scientific and Medical
JVM	Java Virtual Machine
LAN	Local Area Network
MAC	Medium Access Control
MPR	Multipoint Relay
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing Protocol
OSPF	Open Shortest Path First
PHY	Physical Layer
RIP	Routing Information Protocol
SIFS	Short Interframe Space
STAR	Source Tree Adaptative Routing
TBRPF	Topology Dissemination Based on Reverse-Path Forwarding
TCP	Transport Contro Protocol

TORA	Temporally Ordered Routing Algorithm
UDP	User Datagram Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

Abreviaturas

c_n	Aperto relativo do no n
Δ_i	Aperto do nó i
$\overline{\Delta}$	Aperto medio
MANIAC	Mobile Ad Hoc Networking Interoperability and Cooperation
RFB	Request For Bid
H_0	Número máximo de Saltos a partir do backbone de origem
p_u	Número de saltos até o backbone final a partir do nó u

Capítulo 1

Introdução

1.1 Contextualização

A utilização de dispositivos móveis capazes de se conectarem a redes sem fio já é uma realidade para grande parte da sociedade mundial, e sua utilização cresce cada dia mais em um ritmo acelerado. Atualmente, a quantidade de dispositivos móveis ativos chega a superar a população mundial [1]. Tudo ao nosso redor está se conectando à Internet para oferecer melhores serviços aos usuários: os nossos celulares, computadores, tablets, relógios e até mesmo os nossos carros.

Pouco tempo atrás, utilizávamos nosso celulares principalmente para a realização de ligações e o envio e recebimento de mensagens de texto, preferíamos utilizar o acesso à Internet por computadores pessoais via redes Wi-Fi, por representar um custo menor e uma maior praticidade de uso. Com a evolução da tecnologia, a redução do custo de serviços móveis e a necessidade da sociedade de poder contar com meios mais práticos e rápidos para resolver problemas diários, os *smartphones*, que são celulares inteligentes capazes de substituirem um computador pessoal em muitas atividades, passaram a fazer parte do nosso dia a dia. Para muitos, é praticamente impossível trabalhar sem um *smartphone*. Toda comunicação, agendamento e realização de atividades é feita por meio desse tipo de aparelho. Utilizamos esses equipamentos diariamente para todos os tipos de atividades, uma simples verifição de email, um envio de mensagens, uma leitura de notícias do dia ou até mesmo para assistir a filmes, escutar músicas por *streaming* e baixar arquivos da internet.

Muitas das aplicações que os aparelhos móveis possuem atualmente exigem conexão constante com a Internet para atualização de estado, serviços populares como Whatsapp, Instagram, Facebook, Twitter e LinkedIn ou serviços de email, necessitam que o aparelho esteja conectado com a Internet para que possam notificar o usuário de qualquer evento ocorrido. Além disso, por uma simples mudança de comportamento da sociedade, estamos constantemente verificando atualizações em redes sociais ou mesmo conversando com alguém, gastamos grande parte do nosso tempo livre utilizando nossos aparelhos pessoais para nos mantermos atualizados.

Todos esses fatores citados acarretaram um crescimento exponencial na utilização da Internet por meio de aparelhos móveis nos últimos anos. Apenas no ano de 2014, o volume de dados

trafegados via redes móveis foi aproximadamente 30 vezes maior que o volume de dados gerados por todos os meios de comunicação no ano de 2000 e, além disso, nesse mesmo ano foi registrado um aumento de 497 milhões de dispositivos móveis no mundo todo. A utilização de serviços de *streaming* representam o agravante da situação das tecnologias móveis atuais. Esses serviços, além de exigirem altas taxas de transmissão, exigem que a taxa de transmissão permaneça constante durante boa parte da execução do serviço, para que não haja interrupção na transmissão do vídeo e/ou áudio. Aproximadamente 55% de todo o trafego de dados de dispositivos móveis é decorrente da transmissão de vídeo. Até o ano de 2019, é esperado que o volume de dados gerados a partir de dispositivos móveis seja 10 vezes maior que o registrado em 2014.

Devido a essa crescente utilização de serviços móveis e à rápida popularização desse tipo de dispositivo, estruturas cada vez mais robustas para suportarem o volume de acessos e de dados trafegados na rede estão sendo exigidas das operadoras. Assim, mesmo com investimentos cada vez maiores em novas tecnologias e novos equipamentos, é difícil garantir que todos os usuários consigam utilizar os serviços como gostariam. Lidamos frequentemente com situações onde as redes 3G ou 4G de operadoras estão congestionadas, ou seja, as antenas não estão suportando o volume de solicitações de acesso simultâneas, tornando impossível a utilização de muitos serviços oferecidos pelos aparelhos.

Durante a ultima década, diversos avanços tecnológicos na área de redes sem fio foram feitos, permitindo, principalmente, maiores taxas de transmissão. Porém, grande parte desses avanços mantiveram a mesma ideia central aplicada desde o início da comunicação sem fio que consiste na existencia de um ponto principal na rede onde todos os dispositivos podem se conectar, como mostrado na Figura 1.1. Redes Wi-fi e redes celulares aplicam essa mesma ideia atualmente, ou seja, todos os dispositivos que desejam utilizar a Internet devem se conectar a um ponto de acesso (AP, do inglês *access point*). Porém, esses pontos de acesso possuem limitada capacidade de usuários simultâneos, que varia de acordo com a tecnologia utilizada. Assim, durante eventos de grante porte, onde uma grande quantidade de usuários deseja utilizar a Internet ao mesmo tempo, como em shows, concertos e jogos em estádios, o uso de técnicas tradicionais torna-se ineficaz.

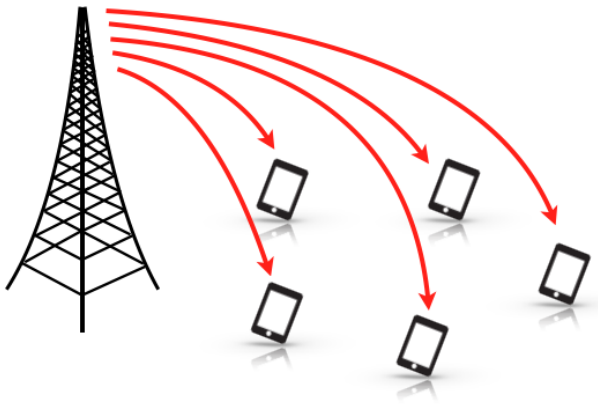

Figura 1.1: Estratégia tradicional de conexão, todos os dispositivos estão diretamente conectados com um ponto de acesso principal

Atualmente, para contornar esse problema, as provedoras de serviço disponibilizam pontos de acesso adicionais para garantir o funcionamento do sistema. Como exemplo de situação real, durante a Copa do Mundo do Brasil em 2014 foram instaladas 4738 antenas nos 12 estadios para garantir que todo o público presente (cerca de 53591 pessoas, em média [2]) conseguisse utilizar seus aparelhos celulares durante os jogos, ao custo para as operadoras de 101.6 milhões de dólares. Segundo as operadoras, nenhum retorno a curto prazo desse investimento é esperado [3]. Então, apesar da disponibilização de pontos de acesso adicionais reduzir o congestionamento da rede e permitir um melhor escoamento dos dados, o custo para esse tipo de alternativa é exorbitante, e não se justifica pelo período que a estrutura permanecerá ativa.

Como solução para esse tipo de situação, algumas propostas estão sendo analisadas e estudadas pela academia e indústria [4]. Uma dessas estratégias, propõe a utilização de pequenos *hubs* para o escoamento do tráfego para redes móveis. Assim, ao invés de todos os usuários se conectarem a pontos de acesso, apenas uma limitada quantidade de usuários se conectariam a esses pontos. Todos os outros usuários se conectariam, de algum modo, a usuários já conectados aos pontos de acesso. Assim, um dispositivo poderia ser utilizado para trafegar informações de outros usuários. Expandindo essa ideia, se um usuário B pode se conectar a um usuário A já conectado a um ponto de acesso, nada impede que um usuário C possa se conectar ao usuário B. Desse modo, uma rede *ad hoc* onde apenas poucos usuários estariam conectados a pontos de acesso para escoamento do trafego poderia ser implementada. Essa situação está representada na Figura 1.2.

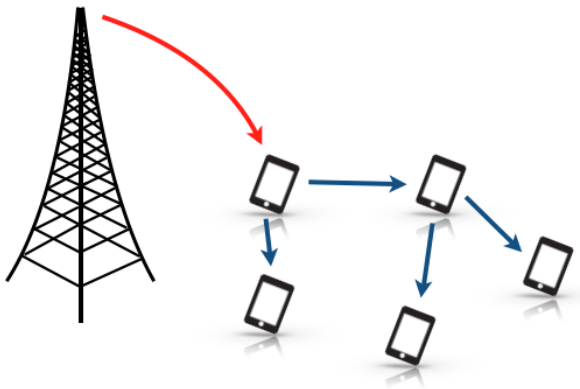

Figura 1.2: Estratégia de escoamento de informações por meio de repasse de mensagens entre dispositivos móveis

Esta estratégia representa uma possível solução para desafogar a atual situação das redes móveis, além de representar um custo muito baixo em infraestrutura quando comparado com as técnicas atualmente utilizadas. Ao invés de investir em infraestrutura fixa, os próprios aparelhos móveis do local seriam utilizados para o repasse de informações. Essa solução também é útil em caso de rompimento de fibra entre dois pontos da rede, pois caso esse problema ocorra, seria possível escoar parte da informação gerada por meio dos dispositivos móveis do local. Como a transmissão sem fio não consegue atingir taxas tão altas como a transmissão cabeada, pacotes prioritarios poderiam utilizar a alternativa enquanto que pacotes menos importantes aguardariam o reestabelecimento da conexão.

Uma possível abordagem é incentivar a participação de dispositivos móveis dos usuários para complementação da infraestrutura de distribuição de tráfego. Neste contexto, tem-se discutido o uso de "leilões recursivos", nos quais a operadora solicita ofertas para o trabalho de repasse de pacotes pelos seus usuários, oferecendo uma recompensa para quem participar da rede e entregar os pacotes. Nesta abordagem, os usuários participam do leilão de acordo com sua própria estratégia individual. Para estudar este problema foi realizada uma competição na Alemanhã em 2013 chamada Maniac Challenge onde diversas equipes puderam desenvolver estratégias próprias para o repasse de informações dentro de uma mesma rede *ad hoc*. A competição tinha como objetivo a colaboração entre as estratégias para o repasse de informações. Ao utilizar estratégias diferentes, era impossível prever o comportamento dos outros dispositivos participantes da rede.

Diferentemente da competição realizada na alemanhã, o projeto desenvolvido explora essa abordagem de escoamento de tráfego baseada em leilões recursivos sobre uma rede ad hoc utilizando unicamente uma estratégia por vez. Esse tipo de abordagem foi escolhido por permitir uma melhor avaliação do desempenho individual de cada estratégia estudada. Dentre as estratégias utilizadas durante a competição, a estratégia escolhida para a avaliação neste trabalho é a “estratégia do aperto” desenvolvida pela equipe da Universidade de Brasília. Para comparação de desempenho, uma segunda estratégia, mais simples que a primeira, foi analisada. Essa segunda estratégia é chamada "Estratégia Aleatória".

Toda a arquitetura de rede desenvolvida para a realização dos experimentos utilizou o mesmo código fonte utilizado na competição Maniac, disponível publicamente na página da competição [21]. Para isso, foi necessário o estudo de toda a arquitetura da rede desenvolvida para a competição para que a mesma pudesse ser reproduzida no ambiente escolhido para a realização dos experimentos.

1.2 Definição do problema

Apesar do repasse de informações ser uma alternativa para o escoamento de dados, utilizar seu dispositivo para trafegar informações alheias pode representar uma queda na durabilidade das bateiras que, em dispositivos modernos, dificilmente duram mais que 1 dia. Assim, medidas que estimulem a contribuição para esse tipo de escoamento de tráfego devem ser implementadas, essas medidas poderiam ser simples descontos na conta do usuário, ou acúmulo de pontos para troca por benefícios, de modo semelhante ao acúmulo de milhas.

Para garantir que a recompensa recebida pela contribuição no repasse de mensagens seja justa, estratégias de repasse que otimizem o desempenho geral da rede devem ser utilizadas. Essas estratégias devem levar em consideração a eficiênca de entrega com sucesso das mensagens ao destino final, ao mesmo tempo que permite que o dispositivo avalie o estado geral da rede para otimizar o seu desempenho. Apesar do interesse individual por parte dos usuários em relação ao ganho de benefícios provenientes da contribuição no repasse de informações, a estratégia implementada deve sempre buscar o melhor desempenho da rede, mesmo que isso signifique a contribuição de apenas um pequeno grupo. Nenhum usuário da rede deve ser capaz de utilizar uma estratégia de repasse

que beneficie apenas a si próprio, pois esse tipo de atitude poderia comprometer a eficiência geral da rede.

A definição da melhor rota para o repasse de informação deve ser levada em consideração na estratégia implementada, pois a utilização de um número desnecessário de dispositivos para o repasse de um determinado pacote pode significar o comprometimento de outros repasses. Ao manter dispositivos ocupados por um período muito maior que o necessário outras transmissões podem ser impedidas de ocorrerem.

Transitar informações alheias pode acarretar problemas de segurança, um usuário mal intencionado poderia coletar as informações trafegadas para descobrir senhas e/ou modificar o conteúdo trafegado. Para isso, sistemas de segurança capazes de evitar esse tipo de atitude devem ser implementados e usuários mal intencionados devem ser excluidos da rede. Apesar da abordagem de segurança ser um ponto crítico nesse tipo de sistema, o trabalho exclui essa abordagem e explora apenas a parte de repasse de informações, todos os usuários do sistema são considerados bem intencionados.

1.3 Objetivos do projeto

Este projeto tem como objetivo comparar o desempenho de duas estratégias diferentes de escoamento de dados em redes *ad hoc*. A primeira estratégia avaliada é capaz de analisar o estado da rede para definir o melhor caminho a ser tomado por um pacote até o destino final, a partir da tabela de repasse gerada pelo protocolo OLSR. A segunda estratégia analisada não verifica o estado da rede antes de realizar suas ações. As estratégias em questão foram implementadas em uma arquitetura de rede que faz uso de leilões para definir o proxímo nó que receberá o pacote na rede. Essas avaliações consideram pontos como taxa de sucesso de transmissão para cada uma das estratégias analisadas, ocorrência de número de saltos para as transmissões realizadas com sucesso, taxa de sucesso de transmissão para diferentes limites de saltos e saldo médio final, por tablet participante em cada rodada de experimento, para ambas as estratégias estudadas

1.4 Contribuições do Projeto

As contribuições que podem ser destacadas deste trabalho são:

- Avaliação de desempenho de estratégia de repasse de informação capaz de avaliar o estado da rede antes de definir o valor de lance para um leilão realizado por um nó vizinho, e antes de realizar o repasse de pacotes para nós adjacentes;
- Avaliação de desempenho de estratégia que utiliza valores de oferta aleatórios toda vez que um leilão é realizado por um nó vizinho;
- Correção de falhas encontradas na aplicação utilizada nos dispositivos Android e na estratégia implementada;

- Validação dos resultados obtidos a partir da realização de experimentos em campo;
- Tradução para o inglês da aplicação utilizada nos dispositivos Android, originalmente feita em Alemão;
- Analise de ocupação dos canais de rede do prédio SG11 para a faixa de frequência de 2.4GHz e 5GHz;
- Documentação do funcionamento dos compotenes da arquitetura de rede utilizada para a realização dos experimentos, essa documentação foi feita de modo a permitir sua utilização para a realização de futuros trabalhos na área.

1.5 Apresentação do manuscrito

A organização do trabalho segue a seguinte ordem: no Capítulo 2 são apresentadas as principais fundamentações teóricas necessárias para o entendimento e o desenvolvimento do projeto. No Capítulo 3 são explicadas as regras e a arquitetura geral da rede implantada durante a competição MANIAC em 2013. É explicado individualmente o funcionamente de cada parte integrante da arquitetura da rede, roteadores de backbone, mestre e a aplicação Android. No Capítulo 4 é explicado detalhadamente o funcionamento da *estratégia do aperto* desenvolvida para a competição MANIAC e, além disso, é apresentado o funcionamento de uma estratégia que não faz nenhum tipo de análise da rede para o repasse de informações. No Capítulo 5 é detalhado o modo como a arquitetura da rede foi configurada, os parâmetros utilizados durante os testes, o ambiente onde os testes foram realizados com a disposição dos equipamentos e os dispositivos utilizados. No Capítulo 6 é feita uma análise de todos os resultados obtidos durantes os testes realizados e possíveis soluções para o aperfeiçoamento da estratégia. No Capítulo 7 são apresentadas as principais considerações em relação ao trabalho desenvolvido e as possíveis áreas para desenvolvimento de trabalhos futuros. Por último, os anexos possuem imagens do ambiente e dos equipamentos utilizados para a realização dos testes.

Capítulo 2

Fundamentação Teórica

2.1 Introdução

Neste capítulo são apresentados os principais conceitos e tecnologias utilizadas para o desenvolvimento do projeto. Na Seção 2.2 é apresentado o funcionamento de redes sem fio no padrão IEEE 802.11, sua arquitetura, especificações e formato de quadros, na camada física (PHY) e na camada de controle de acesso ao meio (MAC). Na Seção 2.3 é explicado o funcionamento de redes *ad hoc*, suas principais vantagens e desvantagens e sua diferença em relação a redes infra estruturadas. Na Seção 2.4 são apresentadas as caracteristicas de protocolos de roteamento desenvolvidos para redes *ad hoc* e a diferença entre protocolos proativos e reativos. Na Seção 2.5 é explicado as principais características da plataforma Android e sua arquitetura.

2.2 Redes Locais Sem Fio (WLANs)

Durante os anos 90, a utilização de sistemas que permitissem a comunicação com a internet via rede sem fio se popularizou mundialmente, mas sem uma padronização do serviço, o usuário ficava limitado aos equipamentos de uma mesma fabricante por serem incompativeis com os padrões utilizados pelas outras. Em decorrência disso, o IEEE (*Institute of Eletrical and Eletronic Engineers*) definiou o padrão a ser seguido em redes locais sem fio (WLANs, do ingles *Wireless Local Area Networks*), conhecido com IEEE 802.11 [5].

O padrão IEEE 802.11 define o conjunto de regras a serem seguidas em cada camada para que haja compatibilidade entre os diversos fabricantes de equipamentos, como modo de acesso ao meio, formato de quadros, divisão de canais, frequências que devem ser utilizadas e sinalização de camada física. É definido pelo IEEE 802.11 o conjunto de regras utilizadas tanto no modo infra-estrutura, onde há um ponto central de acesso na rede, e no modo *ad hoc*, que não não faz uso de pontos de acesso centrais.

Idealmente, usuários de redes sem fio desejam que o serviço ofereça as mesmas experiências, em temos de velocidade e estabilidade, que as redes cabeadas oferecem. Porém, transmissões sem

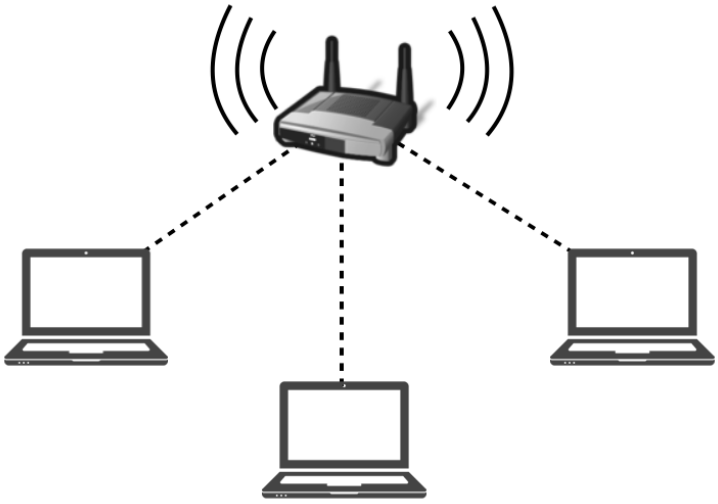

Figura 2.1: Exemplo de rede WLAN

fio devem considerar fatores que não interferem, ou são levados em menor consideração, em redes cabeadas, por exemplo: alocação de frequência, interferência, segurança, consumo de energia e mobilidade.

Para que os aparelhos possam se comunicar, é necessário que uma mesma faixa de frequência esteja sendo utilizada por todos os equipamentos participantes da rede, mas ao contrário de redes cabeadas, onde o ambiente propagante é limitado e o cabo é proprietário, em redes sem fio o uso de faixas de espectro para a propagação de sinais eletromagnéticos deve ser previamente aprovada por uma entidade reguladora, esse processo é necessário para que não haja interferência entre serviços fornecidos via rede sem fio. Quando dois ou mais dispositivos transmitem informações na mesma faixa de frenquência, os sinais podem se interferir e, consequentemente, causar falhas de transmissão e queda na qualidade do serviço.

Redes cabeadas possuem um ambiente controlado de propagação do sinal, toda mensagem enviada propaga por dentro do cabo utilizado, essa particularidade permite uma maior segurança da informação trafegada. Em redes sem fio, é mais difícil garantir segurança da informação pois as mensagens são propagadas livremente pelo ar. Para garantir segurança, as mensagens propagadas são criptografadas. Porém, tal processo acarreta um aumento de custo e uma queda no desempenho da rede.

O uso eficiente de energia é crucial em redes sem fio, pois esse tipo de rede normalmente é composta de dispositivos móveis que possuem uma reserva limitada de bateria, e que necessitam operar sem a necessidade de recarga durante longos períodos. Por isso, algorítimos desenvolvidos para aplicações móveis devem otimizar seu serviço sem comprometer a durabilidade da bateria.

Em relação a mobilidade, usuários de redes cabeadas nao têm a possibilidade de se locomoverem e manterem a conexão ativa nos dispositivos. Em um ambiente empresarial, a rede cabeada é previamente planejada e os pontos de acesso geralmente são estabelecidos próximos ao local de trabalho de cada possível usuário. Assim, os usuários desse tipo de serviço estão limitados ao

alcance do cabo utilizado. Em relação a redes WLAN, a área de atuação da rede está limitada pelo raio de alcance dos equipamentos Wi-Fi utilizados, isso permite que o usuário possa se deslocar juntamente com sua ferramenta de trabalho sem perder a conexão com a rede.

2.2.1 Camada Física

A camada física da Padrão IEEE 802.11 original estipula 3 tipos diferentes de implementações, utilizando espalhamento espectral por sequência direta (DSSS, do inglês *direct sequence spread spectrum*), utilizando espalhamento espectral por saltos de frequência (FHSS, do inglês *frequency hopping spread spectrum*) e utilizando infra vermelho (IR, do inglês *infrared*). DSSS e FHSS utilizam a banda de 2,4 GHz (2,4000 - 2,4835 GHz), faixa de frequência reservada para o uso industral, científico e médico (ISM, do inglês *Industrial, Scientific and Medical*). Assim, o padrão original IEEE 802.11 era capaz de prover velocidades de transmissão de 1Mbps e 2Mbps.

Com a demanda de taxas de transmissão cada vez mais altas, diferentes versões do IEEE 802.11 foram disponibilizadas, as mais conhecidas são IEEE 802.11a/b/g/n. O padrão IEEE 802.11a, diferentemente de todas as outras três, utiliza a frequência de 5GHz para a transmissão de informações e utiliza esquema de multiplexação por divisão ortogonal de frequências (OFDM, do inglês *Orthogonal Frequency Division Multiplexing*), essas diferenças permitem que esse padrão atinja taxas de transmissão de até 54Mbps. Já a versão IEEE 802.11b, assim como o IEEE 802.11 original, utiliza espalhamento espectral por sequencia direta (DSSS) mas garante taxas de transmissão de até 11Mbps. Enquanto que a versão IEEE 802.11b utiliza apenas DSSS, o padrão IEEE 802.11g permite o uso de DSSS, OFDM, ou ambos, na frequência de 2.4GHz, garantindo uma taxa de até 54Mbps [6]. Por ultimo, o padrão IEEE 802.11n faz uso de múltiplas antenas para garantir altas taxas de transmissão, que podem chegar a até 600Mbps [7].

No DSSS, o espalhamento espectral é feito dividindo a faixa de espectro reservada em 13 canais com 22Mhz cada, onde cada canal é espaçado do canal adjacente em 5MHz. Assim, é possível ter no máximo 3 canais operando na mesma região simultaneamente com interferência nula, conforme demonstrado na Figura (2.2). Por questão de compatibilidade de uso entre tecnologias, padrões 802.11 que utilizam OFDM também fazem uso da mesma organização de canais, havendo diferença apenas no modo como o sinal é tratado em cada canal.

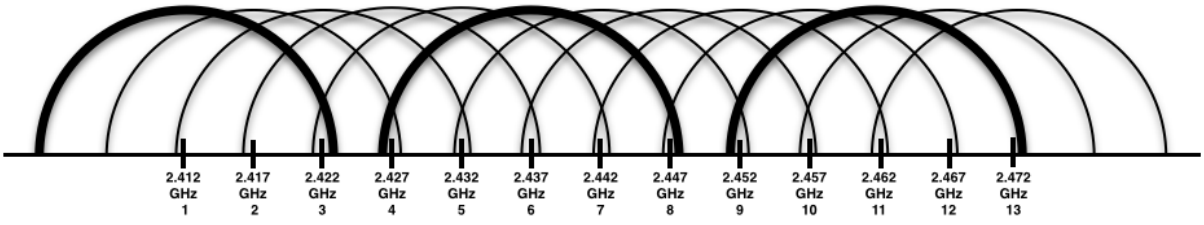

Figura 2.2: Espalhamento espectral por sequência direta (DSSS)

2.2.2 Subcamada de Controle de Acesso ao Meio

A Subcamada de controle de acesso ao meio, ou subcamada MAC (do inglês, *Medium Access Control*), é responsável, dentre outras atribuições, pela alocação de canal, formatação de quadro, checagem de erros e fragmentação. A camada MAC pode operar exclusivamente no modo de contenção, exigindo que todas as estações disputam o canal toda vez que tiverem algum pacote para enviar, ou pode operar alternando entre períodos de contenção (CP, do inglês *contention period*) e períodos livres de contenção (CFP, do inglês *contention-free period (CFP)*)

Três categorias principais de quadros são suportados pelo IEEE 802.11, quadros de gerência, dados e controle. Quadros de gerência são utilizados para associação e desassociação de pontos de acesso, sincronização e autenticação. Quadros de controle são responsáveis pelo estabelecimento da conexão (*handshake*), pelo envio de confirmação de recebimento de pacotes (ACK, *acknowledgments*) durante período de contenção e pela finalização do período livre de contenção (CFP).

O formato de quadro segundo o padrão IEEE 802.11 é como mostrado na Figura 2.3, possui um tamanho que pode variar entre 34 e 2346 bytes e contem informações de versão de protocolo, tipo de criptografia utilizada para autenticação de usuários e tempo que o canal permanecerá ocupado até que a mensagem seja transmitida com sucesso.

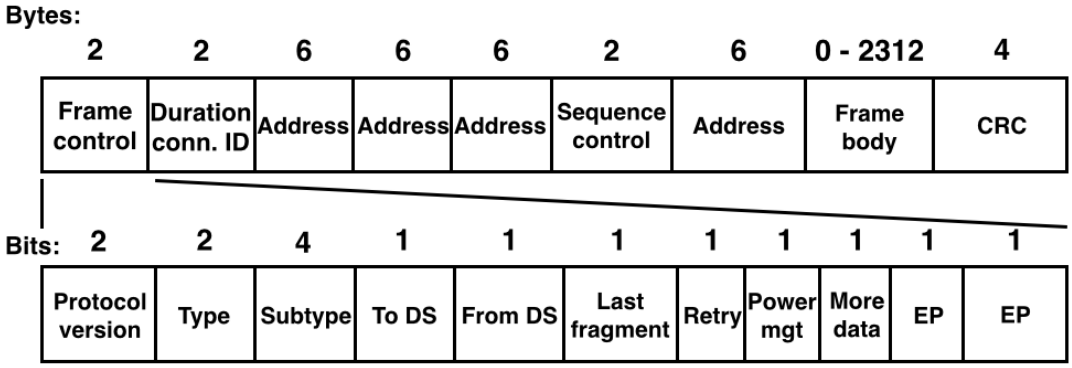

Figura 2.3: Formato de quadro do padrão IEEE 802.11

2.2.2.1 Função de Coordenação Distribuida

A função de coordenação distribuida (DCF, do inglês *Distributed Coordination Function*) é utilizada para suportar transferência de dados em modo assíncrono com base no melhor esforço, é baseada em acesso múltiplo com detecção de portadora e prevenção de colisão (CSMA/CA, do inglês *carrier sensing multiple access with collision avoidance*). Não é utilizado o acesso múltiplo com deteção de portadora e deteção de colisão (CSMA/CD, do inglês *carrier sensing multiple access with collision detection*) pois, ao contrario de redes cabeadas, não há um meio físico que possa ser analisado periodicamente.

O controle do acesso ao meio é feito por meio do uso de intervalos de tempo de espaçamento entre quadros (IFS, do inglês *interframe space*), esses intervalos são períodos obrigatórios sem que haja transmissões. Na função de coordenação distribuida (DCF), são definidos dois tipos

diferentes de IFS's, *short* IFS (SIFS) e DCF-IFS (DIFS). Quando uma estação tem algo a enviar e percebe que o canal está livre, aguarda um período DIFS e analisa o canal novamente, caso o canal ainda esteja livre o pacote é enviado. Quando o pacote é recebido, é feito uma checagem de erros (*checksum*) para verificar se houve algum erro no processo de transmissão, caso o pacote tenha sido corretamente recebido, um período SIFS é aguardado antes de enviar um pacote de confirmação de recebimento (*acknowledge*) para o estação de origem. Quando um quadro de dados é enviado, a informação de duração do frame contida no cabecalho do pacote é utilizado para informar todas as estações próximas sobre o tempo que o canal permanecerá ocupado, todas as estaçoes que recebem essa informação utilizam o tempo informado para atualizar o período NAV(*Network Allocation Vector*) que contém, além da duração do pacote de dados, o tempo SIFS e o de tempo de confirmação de recebimento (ACK). Esse processo é apresentado na Figura 2.4

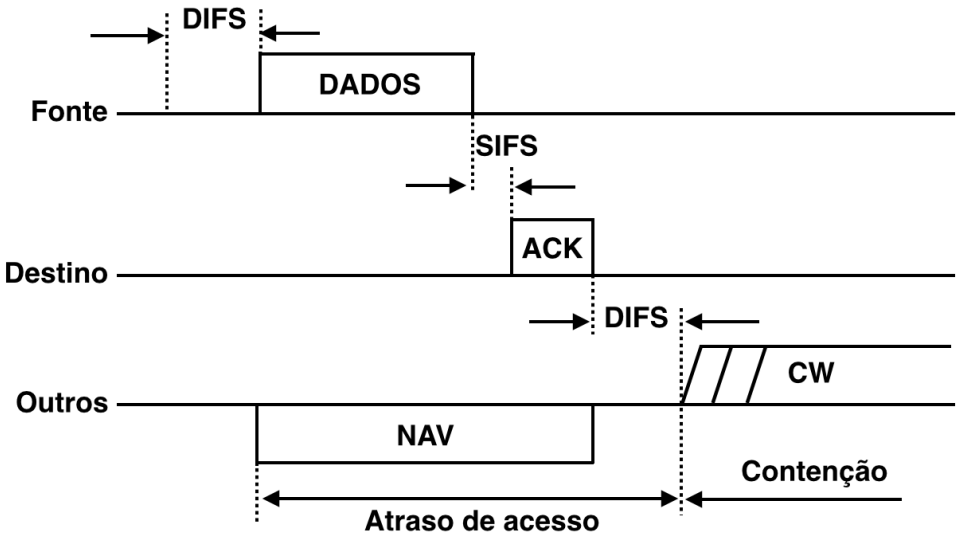

Figura 2.4: Modo de contenção sem uso de RTS/CTS, o período de conteção NAV é definido pelo tamanho das mensagens de dados recebidas de outras estações

Utilizando essa técnica, caso ocorra uma colisão durante uma transmissão, o sistema não é capaz de identificar tal acontecimento e continua transmitindo o pacote até o fim. Esse tempo gasto transmitindo uma informação que provavelmente não poderá ser corretamente recebida pelo destino final, representa uma considerável queda de desempenho do sistema. Para contornar esse problema, a função de coordenação distribuída permite o uso de mensagens de controle de requisição de envio de mensagem (RTS, do inglês *Request To Send*) e de confirmação de canal livre (CTS, do inglês *Clear To Send*). As mensagens de RTS e CTS são utilizadas para reservar o canal toda vez que uma estação quiser enviar uma mensagem, reduzindo as colisões que podem ocorrer durante uma transmissão. Quando uma estação quer transmitir uma informação, ela necessariamente aguarda o período de contenção e, após esse período, envia uma mensagem de requisição de envio de dados (RTS) para o destino do pacote. Todas as estações próximas que escutarem essa mensagem atualização seu tempo NAV de acordo com o tempo da mensagem indicado no RTS. Quando o destino final recebe a mensagem de RTS, responde à estação de origem com uma mensagem CTS após um período SIFS de contenção. Novamente, todas as estação próximas que escutarem a

mensagem CTS, atualizarão seu tempo NAV a partir do tempo da mensagem de dados indicado. Quando a estação de origem do RTS recebe a mensagem de CTS, é assumido que o canal está livre para o envio do quadro de dados. Então, após um período SIFS de contenção, o quadro é finalmente enviado. Como as mensagens de controle RTS e CTS são muito pequenas (20 bytes e 14 bytes, respectivamente), mesmo que haja uma colisão durante a transmissão, o tempo perdido é muito menor se comparado com a transmissão sem uso de RTS/CTS.

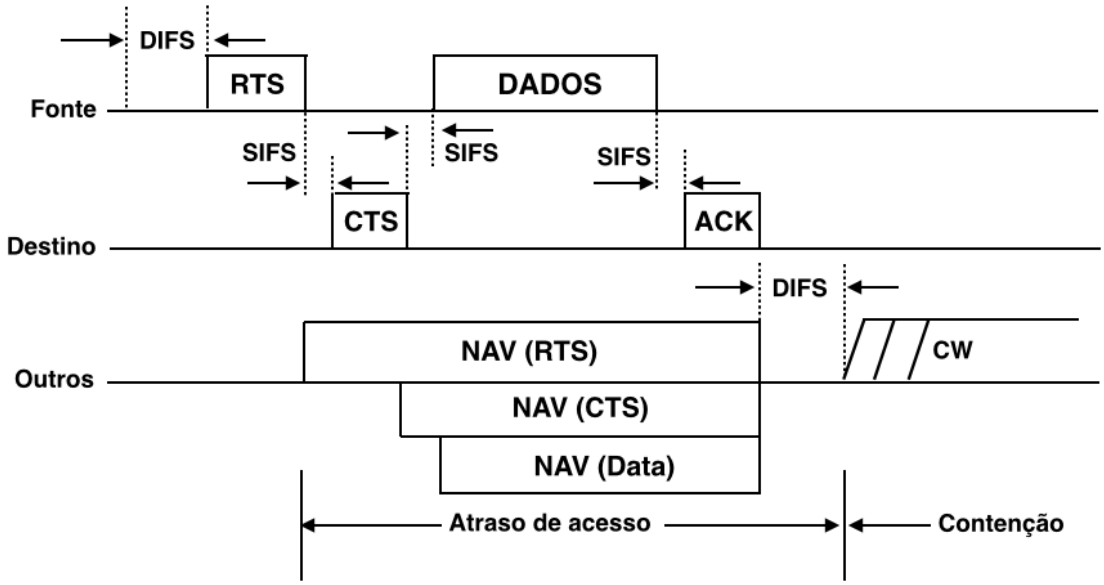

Figura 2.5: Modo de transmissão utilizando RTS/CTS, o tamanho do período de contenção NAV é atualizado toda vez que uma informação de RTS ou CTS é recebida

2.3 Redes *Ad Hoc*

Redes *Ad Hoc* são redes que não necessitam de uma arquitetura central, ou um ponto de acesso central, para que existam. Todos os dispositivos na rede participam igualmente e são responsáveis pelo seu bom funcionamento, bem como pelo repasse de mensagens para os elementos adjacentes. Esse tipo de rede possui a vantagem de ser de fácil e baixo custo de implementação, além de poder ser deslocada com facilidade e poder ser rapidamente configurada.

Redes *ad hoc* são úteis em ambientes de desastre natural onde a comunicação entre as equipes de resgate é fundamental e, em muitos casos, a estrutura de rede celular está comprometida e impossibilitada de ser utilizada no momento. É utilizada, também, em ambientes de guerra onde as tropas e os soldados precisam se comunicar e, ao mesmo tempo, a rede deve garantir que que a comunicação chegue apenas até os membros da tropa aliada e que possa ser movida na mesma velocidade que a tropa avança.

Apesar dos exemplos citados, redes *ad hoc* também podem ser utilizadas nos próprios centros urbanos no nosso dia a dia, como na comunicação entre veículos para a prevenção de acidentes e compartilhamento de informações que possam ajudar o motorista de moto geral [8].

Redes *ad hoc* também são amplamente utilizadas em redes sensores, como no caso de localização de animais cadastrados dentro de uma floresta para estudo de comportamento, e prevenção de invasão de ambientes urbanos por parte desses animais.

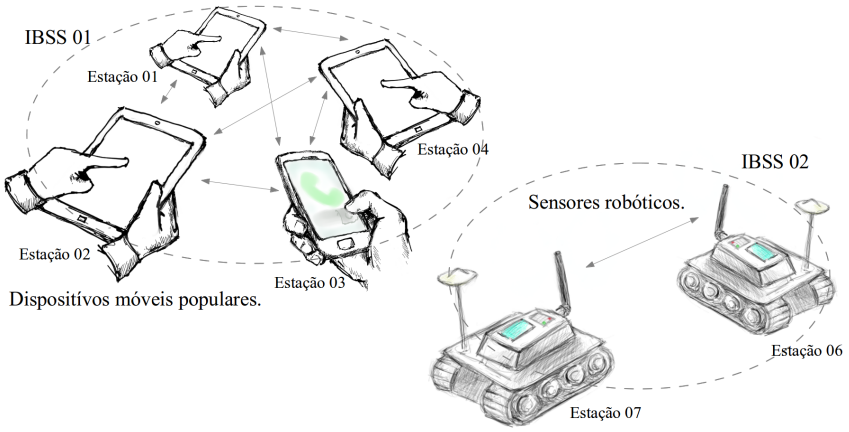

Figura 2.6: Exemplo de Rede *Ad Hoc* aplicado a dispositivos móveis e aplicado a comunicação militar

A principal diferença entre redes *ad hoc* e redes estruturadas é justamente a ausência de uma infraestrutura centralizada. Em rede celulares, por exemplo, todos os aparelhos se conectam a uma estação base, e esse ponto de acesso se conecta a um *backbone*. Então, não há a presença de comunicação dispositivo a dispositivo nesse tipo de rede, mesmo que dois aparelhos dentro de uma mesma célula tentem se comunicar, a comunicação será feita por intermédio da estação base. Assim, as estações base e o backbone de redes celulares são responsáveis por todas as funções de controle da rede, como roteamento de ligações e autenticação de dispositivos [9]. Grande parte das redes locais sem fio possuem esse tipo de abordagem centralizada onde todos os aparelhos se conectam a um ponto cental. No caso de redes *ad hoc*, a comunicação é feita dispositivo a dispositivo e as funções de roteamento são executadas pelos proprios aparelhos. Caso algum dispositivo deixe de fazer parte da rede, a rede *ad hoc* é capaz de se reestruturar, o que a torna tão atrativa.

Um grande desafio encontrado em redes *ad hoc*, principalmente quando tratamos de dispositivos móveis, é o consumo de bateria. Projetos de roteamente em redes *ad hoc* devem levar esse ponto em consideração, pois roteamentos que exigem um grande processamento acarretam um impacto na durabilidade da bateria dos dispositivos, o que torna tal estratégia inviável.

2.4 Protocolos de Roteamento para redes *Ad Hoc*

Devido a mudança contante de topologia, tempo de atraso e taxa de perda de pacotes em redes *ad hoc*, protocolos de roteamento tradicionais, como OSPF ou RIP, não conseguem lidar com esse tipo de rede do mesmo modo que lidam com redes cabeadas. Para redes *ad hoc*, protocolos específicos devem ser utilizados, esse protocolos devem ser capazes de lidar com as particularidades da rede e não podem depender de um operador central, tendo em mente que redes *ad hoc* possuem um funcionamento distribuído. Duas abordagens principais são utilizadas nos protocolos projetados

para esse tipo de rede: protocolos reativos e protocolos proativos.

Protocolos reativos são protocolos que não tomam a iniciativa de encontrar uma rota até o destino final até que seja solicitado, sendo também chamados de protocolos sob-demanda. Sempre que uma requisição de rota é recebida, o protocolo inunda a rede com mensagens de *broadcast* para encontrar um rota até o destino solicitado. Esse tipo de protocolo reduz a quantidade de mensagens de controle na rede por não manter uma tabela de rota atualizada mas, em contrapartida, possuem um tempo de latência elevado. São exemplos desse tipo de roteamento os protocolos AODV[10], DSR[11] e TORA[12].

Protocolos proativos fazem uso da troca constante de mensagens de controle para manterem atualizadas as tabelas de roteamento. Assim, sempre que solicitado esse tipo de protocolo proverá imediatamente a rota até o destino final. Protocolos proativos necessitam de uma maior largura de banda devido ao envio periódico de mensagens de controle, mas possuem uma latência menor quando comparados com protocolos reativos. São exemplos desse tipo de roteamento os protocolos OLSR[13], STAR[14], TBRPF[15] e DSDV[16].

Ainda é possível utilizar um terceiro tipo de protocolo que mescla ideias aplicadas em protocolos reativos e ideias aplicadas em protocolos proativos, esses protocolos são conhecidos como protocolos híbridos.

2.4.1 OLSR - *Optimized Link State Routing Protocol*

Desenvolvido especialmente para redes móveis sem fio, o roteamento otimizado por estado de enlace (OLSR) faz uso do envio periódico de mensagens de atualização para todos os nós da rede para que, sempre que um nó necessitar enviar algum pacote, ele já saiba o destino a ser utilizado baseado na tabela de roteamente fornecida pelo protocolo.

O OLSR foi desenvolvido para operar em redes completamente descentralizadas e apresenta um roteamento de saltos, cada nó utiliza a informação mais recente em sua tabela de roteamento para o repasse de um pacote. Portanto, mesmo que o destino esteja se movendo é possível entregar o pacote com sucesso, desde que esse destino esteja dentro do raio de alcance de algum nó da rede.

Para reduzir a inundação de mensagens de controle na rede, o OLSR faz uso da técnica de múltiplos pontos de retransmissão (MPR, do inglês *multipoint relay*), que reduz retransmissões na mesma região. Cada nó da rede escolhe um grupo de nós em sua vizinhança que retransmitirão seus pacotes, esse grupo é chamado de pontos de retransmissão (MPRs) do nó em questão. Assim, os vizinhos de um nó N que não façam parte do MPR desse mesmo nó irão ler e processar o pacote recebido, mas não irão retransmiti-lo. Os nós escolhidos para fazerem parte do MPR do nó N podem mudar de tempos em tempos através da seleção de nós feita pela troca de mensagens HELLO. A seleção de nós para o grupo MPR é feita de modo arbitrário, mas são escolhidos de modo que todos os nós a dois saltos de distância possam ser alcançados através de algum nó escolhido para o grupo.

A partir dos pontos de retransmissão escolhidos na rede, o OLSR utiliza essas informações para calcular as rotas possíveis para todos os nós da rede. Para que isso ocorra, todos os nós

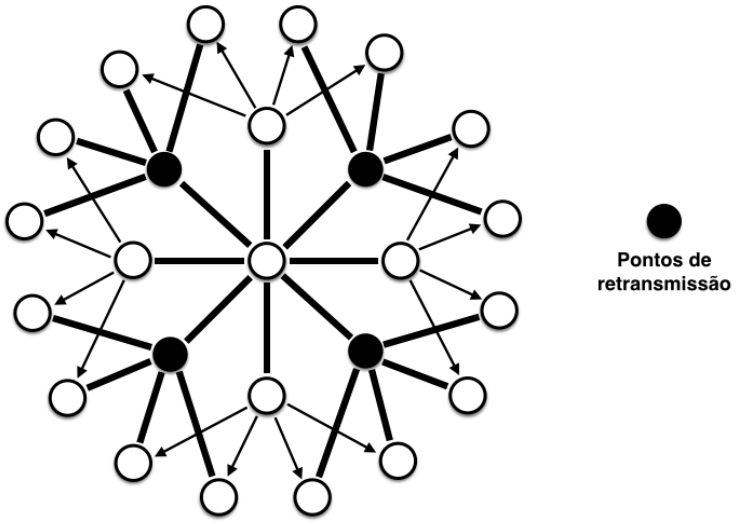

Figura 2.7: Funcionamento da técnica de múltiplos pontos de retransmissão (MPR)

compartilham informações periódicas sobre seus vizinhos diretos (vizinhos a apenas um salto de distância) pertencentes ao grupo MPR. Quando essas informações sobre os vizizinhos são recebidas, cada nó calcula e atualiza suas rotas para todo nó conhecido. Assim, as rotas formadas no OLSR são sequências de saltos passando por múltiplos pontos de retransmissão (MPRs).

2.5 A Plataforma Android

Anunciado em Setembro de 2006 e lançado, em versão beta, em novembro de 2007, o Android é um sistema operacional desenvolvido pela Google para operar, inicialmente, em smartphone e tablets. É um sistema operacional baseado no kernel do Linux mas com modificações que otimizam a utilização de bateria e permitem o uso de funcionalidades exclusivas desse tipo de aparelho, como GPS, giroscópio, NFC, envio e recebimento de ligações e mensagens.

O Android é o sistema operacional móvel mais utilizado no mundo e isso se deve, principalmente, ao modo de licenciamento empregado pela Google, qualquer fabricante de celular no mundo pode solicitar o uso da plataforma em seus celulares. Assim, é possível encontrar disponível no mercado hoje uma infinidade de modelos de smartphones que utilizam Android como sistema operacional.

Desde que foi lançado, as versões do Android seguem uma ordem alfabética com nomes de sobremesas em inglês [17], a primeira versão comercial lançada foi batizada de *Cupcake* (versão 1.5) seguido pelas versões *Donut* (1.6), *Eclair* (2.0), *Froyo* (2.2), *Gingerbread* (2.3), *Honeycomb* (3.0), *Ice Cream Sandwich* (4.0), *Jelly Bean* (4.1), *Kit Kat* (4.4) e *Lollipop* (5.0). A cada nova versão lançada, novas funcionalidades são acrescentadas para acompanharem as tendências e necessidades do mercado.

Android permite que qualquer pessoa possa desenvolver aplicações para os diversos tipos de equipamentos que fazem uso do sistema operacional e permite, também, que os desenvolvedores vendam ou distribuam gratuitamente suas aplicações através da loja online Google Play.

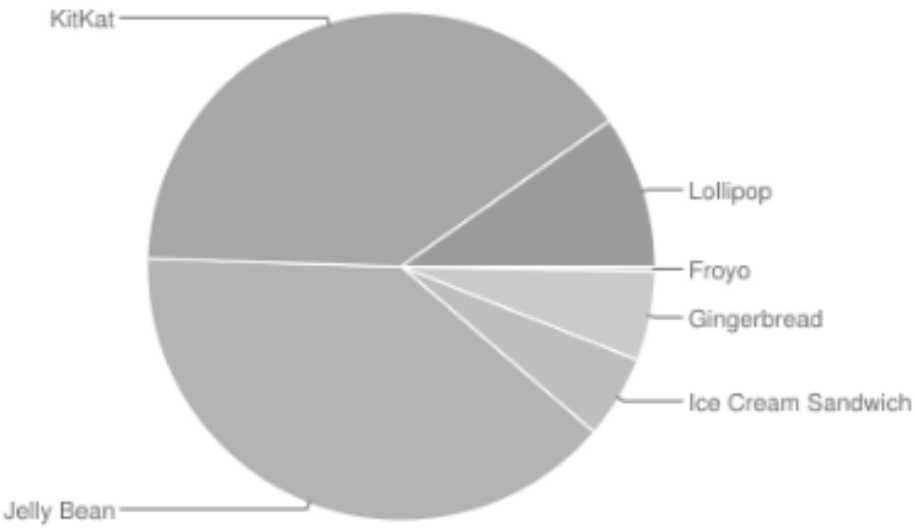

Figura 2.8: Distribuição da utilização das versões do sistema operacional Android

Atualmente, o Android é utilizado em smartphones, tablets, smartwatches, televisores e carros e é utilizado em centenas de milhões de dispositivos em mais de 190 paises. Devido o sistema operacional ser disponibilizado para uma grande variedade de dispositivos com diferentes capacidades de processamento e diferentes funcionalidades, apenas uma pequena parcela dos equipamentos utiliza a última versão da plataforma. Atualmente, cerca de 12.4% dos dispositivos em uso utilizam a versão *Lollipop* como sistema operacional, como mostrado na Figura 2.8 [18]. Esta particularidade impossiblita que desenvolvedores desenvolvam aplicações que possam ser instaladas e utilizadas em todos os aparelhos Android disponíveis no mercado atualmente.

2.5.1 Arquitetura Android

A arquitetura principal do sistema operacional Android pode ser divida em quatro camadas, *Linux Kernel*, *Libraries*, *Application Framework* e *Applications*, conforme mostrado na Figura 2.9.

A primeira camada, Linux Kernel, foi desenvolvida com base na versão 2.6 do Kernel do Linux, é responsavel pelo gerenciamento de memoria, processos e energia, e provê configurações de segurança e drivers necessários para a utilização de recursos como NFC, GPS e demais componentes do aparelho.

A camada seguinte, *Libraries* (Bibliotecas), é implementada em C/C++ e permite que o aparelho lide com diferentes tipos de informações, por exemplo, a biblioteca SQLite é responsável por armazenar informações em seu banco de dados local, o WebKit é responsável pela exibição de conteúdo HTML e o OpenGL é responsável pela renderização de conteúdos 2D e 3D, amplamente utilizado para a produção de jogos e conteúdos que fazem uso de vetorização.

Ainda na mesma camada, encontramos a subcamada Android *Runtime* (tempo de execução) que possui as bibliotecas de núcleo e a maquina virtual Dalvik. Apesar do sistema operacional Android ser desenvolvido em java, o DVM (*Dalvik Virtual Machine*) é utilizado em substituição ao

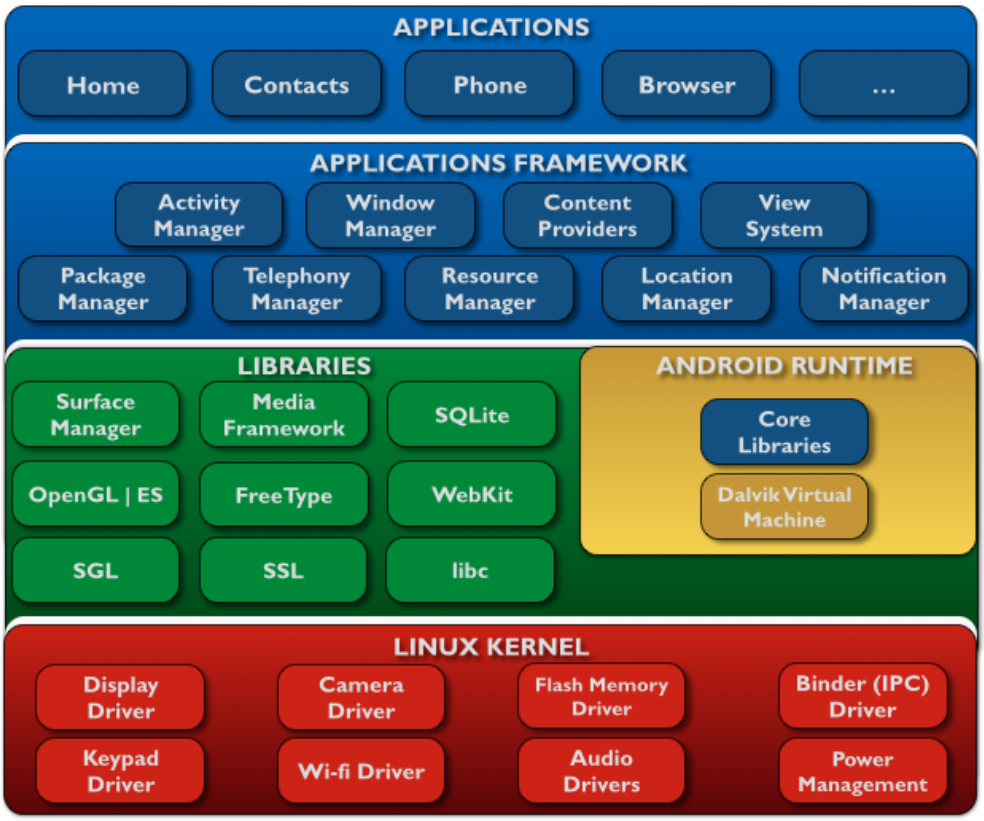

Figura 2.9: Arquitetura em camadas do sistema operacional Android

JVM (*Java Virtual Machine*) pois o DVM foi desenvolvido para operar em dispositivos pequenos com limitada quantidade de memória. O DVM compila o arquivo fonte java em bytecodes (.class) que em seguida são convertidos para o formato executável .dex (*Dalvik Executable*). Após esse processo, todos os arquivos .dex são armazenados dentro de um unico arquivo .apk (*Android package*) o qual contem todas as informações necessárias para a instalação da aplicação nos disposivitos.

A camada de *Application Framework* é a camada diretamente acessada pela aplicação e provê todos os recursos necessários para a aplicação. Fornece, por exemplo, recursos para criação de interface gráfica nas aplicações, notificação de usuário por meio de alertas, gerência as funções básicas do aparelho como compartilhamento de dados entre aplicações, e permite utilizar o sistema de localização instalado no aparelho.

A camada *Applications* (Aplicações) inclui, como o próprio nome diz, as aplicações presentes no dispositivo, como navegadores, calendarios e clientes de email. Essas aplicações consideram tanto as aplicações presentes originalmente presentes no Android como aplicações desenvolvidas para terceiros desenvolvidas para Android são feitas em JAVA

Capítulo 3

A competição *MANIAC*

3.1 Introdução

Organizado pelo grupo *Computer Systems and Telematics* da Universidade Livre de Berlim (*Freie Universität Berlin*, em Alemão) e pelo grupo *Internet Technologies* da Universidade de Ciências Aplicadas de Hamburg (*Hochschule für Angewandte Wissenschaften Hamburg*, em Alemão), a competição *MANIAC (Mobile Ad Hoc Networking Interoperability and Cooperation)*[19] foi uma competição realizada com o intuito de avaliar o desempenho de diferentes estratégias de escoamento de dados dentro de uma mesma rede *Ad Hoc* no ambito de cooperação entre essas estratégias.

Este capítulo apresenta o todo o funcionamento da rede utilizada durante a competição. Na Seção 3.2 é explicado o funcionamento geral da arquitetura da rede e todas as regras aplicadas durante a competição, em seguida é explicado separadamente cada parte da arquitetura da rede, roteadores de backbone, computador mestre e aplicação ManiacLib.

3.2 Regras e Arquitetura Geral da Rede

Para a realização da competição, diversos pontos de acesso (AP) foram instalados por 2 andares do prédio onde a competição ocorreu, todos os pontos de acesso estavam conectados entre si pela rede local cabeada (LAN) e eram gerenciados por um computador principal (mestre). A parte móvel da competição ficava por parte dos tablets distribuídos entre as equipes, esses tablets se conectavam entre si e com os diversos pontos de acesso da rede via rede *ad hoc*, e o roteamento entre esses dispositivos e os pontos de acesso era feito via protocolo OLSR.

A competição era baseada em múltiplas rodadas de lançamento de pacotes em que os participantes tinham a possibilidade de aperfeiçoar suas estratégias após cada rodada. Cada lançamento de pacote por parte de um ponto de acesso era iniciado com uma requisição de oferta (RFB, do inglês *Request For Bid*) de todos os nós ao alcance do ponto de acesso, essa requisição informava o valor máximo a ser pago pelo roteador de backbone em caso de sucesso de transmissão (B), o valor de multa em caso de falha de transmissão (F) e o número máximo de saltos permitidos até

o destino final (H_0). O ponto de acesso escolhia o nó que receberia o pacote baseado no valor de oferta recebido.

Toda equipe era livre para desenvolver sua estratégia conforme julgasse necessário, mas uma série de regras obrigatórias deveriam ser seguidas por todas as equipes participantes. Para garantir que nenhuma equipe estivesse trapaceando na competição, os organizadores monitoravam os pacotes trafegados e analisavam estatísticas para identificar qualquer irregularidade.

As regras gerais da competição para as requisições de oferta (RFB), valores de oferta anunciados, repasse de pacotes e demais pontos importante seguiam os seguintes pontos [20]:

- Cada nova rodada é iniciada com a geração de uma requisição de oferta (RFB) a partir de um roteador de backbone da rede;
- A escolha do nó seguinte que receberá o pacote é feita por meio de requisições de oferta (RFB) recursivas, aquele que estiver com o pacote deverá sempre fazer uma RFB antes de encaminhar o pacote para o nó seguinte;
- O ponto de acesso que gerar uma RFB irá anunciar sempre um valor máximo de oferta (B), um valor de multa (F) e um número máximo de saltos (H_0);
- O nó da rede que gerar uma RFB deve informar na mensagem o seu valor máximo de oferta (B), seu valor de multa (F) e o número máximo de saltos restantes a partir do nó de origem da RFB (H_0 - saltos já realizados);
- Todo nó da rede que escutar uma RFB deverá responder com uma oferta menor ou igual ao valor máximo anunciado;
- O roteador de backbone sempre escolherá como vencedor da RFB aquele que oferecer o menor valor;
- Os nós da rede escolhem o nó vencedor de suas RFBs com base na própria estratégia implementada;
- Um nó não pode participar de uma mesma transação mais de uma vez;
- O valor de multa anunciado por um nó deve ser menor ou igual ao valor de multa recebido do nó anterior;
- Um nó pagará ao nó vencedor o valor acertado apenas se esse nó conseguir entregar o pacote ao rotador de backbone final com sucesso;
- Se um nó não conseguir entregar um pacote ao roteador de backbone final esse nó deverá pagar o valor anunciado pelo nó anterior que gerou a RFB;
- Os valores inicias de multa, máximo valor a ser pago e número máximo de saltos são definidos diretamente no computador mestre;

- Em todas as RFBs, o valor da multa anunciado deve ser menor ou igual ao valor máximo a ser pago;
- O saldo de um nó participante pode ser negativo ou positivo dependendo de seu desempenho;

A Figura 3.1 apresenta a estrutura geral da rede durante a competição. As linhas mas grossas representam a conexão cabeada na rede entre os roteadores de backbone, enquanto que as linhas mais finas representam as possíveis rotas que um pacote poderia seguir partindo sempre de um roteador de backbone inicial. As setas representam um possível caminho que um pacote poderia percorrer para chegar até um roteador de backbone final.

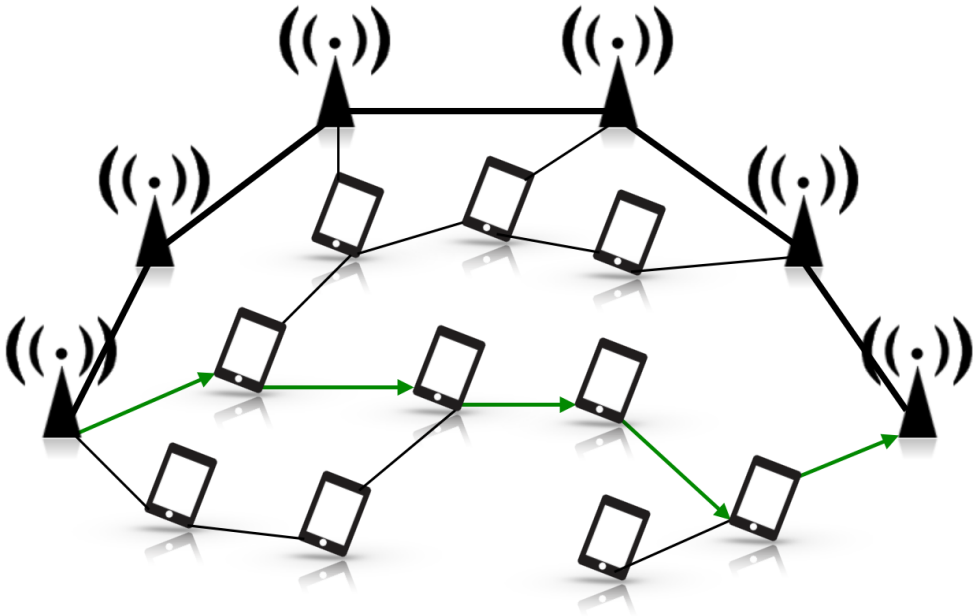

Figura 3.1: Arquitetura da Rede durante a Competição *MANIAC*

A arquitetura principal da rede era dividida em 3 partes principais: computador mestre, roteadores de backbone e aplicação *ManiacLib*. Cada uma das partes está detalhada abaixo para melhor compreensão de seu funcionamento e importância para o funcionamento do sistema. Todo o código utilizado durante a competição está disponível online na plataforma GitHub [21].

3.2.1 Mestre

Utilizando Go[22], MongoDB[23] e JavaScript, o mestre é responsável por controlar a geração de pacotes em todos os roteadores de backbone da rede. Sempre que solicitado o envio de um pacote pelo moderador, o mestre escolhe aleatoriamente um roteador de backbone da rede como sendo o ponto de origem e outro roteador como sendo o destino final. Por isso, é necessário que um mínimo de 2 roteadores de backbone estejam conectados ao mestre para que o sistema funcione corretamente.

Todas as informações sobre transações em andamento e conluídas, recebidas dos roteadores de

backbone, são repassadas para o banco de dados em MongoDB o qual armazena todos os passos percorridos por cada pacote na rede em diferentes documentos.

Para automatização do processo de geração de pacotes, o mestre permite que um documento com todas as informações sobre os pacotes a serem gerados seja criado, esse documento pode conter os seguintes parâmetros:

- ***Round*:** Determina que uma nova rodada de pacotes será iniciada, os *rounds* são identificados pela data e hora configurada no computador mestre;
- ***Send*:** Agenda o envio de um pacote na rede, quando esse modo é utilizado o mestre envia imediatamente o comando para que um roteador de backbone envie um pacote na rede;
- ***Mode <milisegundos>*:** Agenda o envio automático de pacotes na rede, o parâmetro <milisegundos> determina o intervalo entre a geração de cada pacote;
- ***Sleep <segundos>*:** Informa ao mestre que nenhuma outra ação será tomada dentro de <segundos>, essa função é usada principalmente para estabelecer o tempo que a rodada de envio de pacote permanecerá ativa;
- ***Print <mensagem>*:** Imprime a <mensagem> digitada, usada pelo moderador para controlar quanto tempo resta até o fim da rodada de geração de pacotes, ou pra informar que um determinado pacote foi enviado;
- ***Ceil*:** Configura o valor máximo a ser pago ao tablet vencedor do leilão do pacote caso haja sucesso de transmissão até o roteador de backbone destino. Se esse parametro não for configurado, o computador mestre utilizará o valor pré estabelecido, 40;
- ***Fine*:** Configura o valor que deve ser pago de multa pelo tablet vencedor do leilão caso a transmissão não seja bem sucedida, ou seja, caso o pacote não seja entregue ao roteador de backbone final. Se esse parâmetro não configurado, o roteaodr mestre utilizará o valor pré estebelecido, 20;
- ***Hops*:** Configura o número máximo de saltos que um pacote poderá efetuar entre o roteador de backbone de origem e o roteador de backbone final. Caso esse valor não seja configurado, o mestre utilizará o valor pré estabelecido, 10 saltos;

3.2.2 Roteadores de Backbone

Os roteadores de backbone são os pontos de acesso (AP) da rede, são resposáveis por transmitir e receber os pacotes enviados aos tablets participantes dos leilões. O roteador de backbone recebe do mestre a informação de que um pacote deve ser transmitido, essa informação recebida já inclui todos os parâmetros que o pacote deve ter, ou seja:

Ceil

Valor máximo a ser pago ao tablet vencedor do leilão do pacote caso haja sucesso de transmissão até o roteador de backbone destino;

Fine

Valor que deve ser pago de multa pelo tablet vencedor do leilão caso a transmissão não seja bem sucedida, ou seja, caso o pacote não seja entregue ao roteador de backbone final;

Hops

Número máximo de saltos que um pacote pode efetuar entre o roteador de backbone de origem e o roteador de backbone final;

Os roteadores de backbone são responsáveis, também, por notificar o mestre de tudo que acontece durante as transmissões. Todas as mensagens recebidas pelos roteadores de backbone, provenientes dos tablets participantes da rede, são repassadas para o mestre.

Os roteadores de backbone mantêm 3 ou mais conexões ativas simultaneamente:

- *TCP Connection*: Conexão mantida com o computaodr mestre para recebimento de solicitação de envio de pacotes ou para envio de resultados de transações;
- *UDP Socket*: Escuta por todo tráfego proveniente da rede WLAN para repasse de informações para o mestre pela rede LAN;
- *TCP ServerSocket*: Escuta por conexões de nós da rede WLAN;
- *TCP Socket*: Usado para envio periódico de mensagens de *check* para os tablets contendo informações de saldos e de ganhos nos últimos 5 segundos, é usado também para recebimento de mensagens de *BidWin* propagadas pelos tablets.

É necessário configurar corretamente nos roteadores de backbone os endereços para a rede local cabeada (LAN) que os conectam ao mestre, e os endereços para a rede local sem fio (WLAN) que os conectam aos tablets participantes da competição.

Toda transferência de pacotes entre os nós da rede é feita via UDP, mas os tablets esteleciam conexão TCP com os roteadores de backbone para garantir que cada tablet estivesse conectado a apenas um ponto de acesso, isso fazia com que qualquer transmissão de pacote passasse por pelo menos 2 tablets da rede. Assim, mesmo que um nó considerasse possível entregar um pacote ao destino final com base na tabela gerada pelo protocolo OLSR, se sua conexão TCP estivesse estabelecida com outro ponto de acesso, a mensagem não era enviada diretamente para o destino final.

3.2.3 ManiacLib

O ManiacLib é a aplicação desenvolvida pelos organizadores do evento que permite que os desenvolvedores possam implementar a estratégia desejada. Essa aplicação foi desenvolvida especialmente para dispositivos que utilizam a plataforma Android como sistema operacional e, durante a competição, foi instalada em todos os Tablets Nexus 7 utilizados.

Para que o ManiacLib possa funcionar corretamente, é necessário que a aplicação MANET manager [24] esteja funcionando, essa aplicação é responsavel por estabelecer a rede *ad hoc* entre os dispositivos e o protocolo OLSR.

O ManiacLib é responsável por todo o repasse de informações até o destino final, quando o tablet recebe uma requisição de oferta, o ManiacLib analisa se o dispositivo já participou daquela transação anteriormente, caso não tenha participado a estratégia implementada no dispositivo é acionada.

A aplicação possui uma classe específica para os desenvolvedores implementarem suas estratégias, onde seguintes métodos estão disponíveis para uso:

public Long onRcvAdvert(Advert adv)

Método utilizado para definir o tempo que a estratégia aguardará até responder a requisição de oferta, esse tempo pode variar entre 0 e 3 segundos (tempo máximo que o anúncio fica aberto aguardando respostas);

public Integer sendBid(Advert adv)

Usado para determinar o valor de oferta toda vez que uma RFB for recebida de um roteador de backbone ou de um outro nó da rede;

public void onRcvBid(Bid bid)

Permite que a estratégia utilize a informação das ofertas anuncias pelos outros tablets, essa informação pode ser utilizada, por exemplo, para verificar um padrão entre os valores anunciados pela equipe concorrente, ou mesmo utilizar essas informações para anunciar um valor mais baixo que os outros participantes;

public void onRcvBidWin(BidWin bidwin)

Método chamado toda vez que o dispositivo recebe uma mensagem sobre o vencedor de uma transação, que pode ser o próprio dispositivo ou qualquer outro dispositivo próximo. Essa informação permite que a estratégia faça uso do valor de oferta do dispositivo vencedor para definição dos seus próximos valores de oferta;

public AuctionParameters onRcvData(Data packet)

Usado para definir os valores da próxima RFB toda vez que o dispositivo ganhar um leilão, mesmo que os desenvolvedores tentem burlar a relação em que o valor máximo de oferta é maior ou igual ao valor de multa, a aplicação muda os valores de modo a não permitir tal ação;

public Bid selectWinner(List<Bid> bids)

Usado para definir o vencedor da RFB anunciada a partir dos valores de oferta recebidos. A implementação permite que o vencedor seja escolhido a partir do menor valor de oferta recebido ou utilizando qualquer outra estratégia escolhida pelas equipes;

public void onException(ManiacException ex, boolean fatal)

Utilizada para tratar qualquer tipo de exceção que possa ocorrer durante a execução da estratégia;

public boolean dropPacketBefore(Data buffer_ data)

Permite que a estratégia possa descartar um pacote recebido antes de realizar um novo leilão;

Essa classe onde as equipes desenvolviam suas estratégias é a única parte do código que era permitido modificar, todo o resto do sistema deveria permanecer intocável.

Para que a aplicação pudesse diferenciar os tablets da rede e os roteadores de backbone, apenas observando a tabela OLSR, um arquivo de texto era mantido dentro do aparelho com o endereço IP de todos os roteadores de backbone da rede. Esse arquivo era constantemente lido pela aplicação para identificar se as novas conexões em sua tablea OLSR representavam conexões com tablets ou com um novo roteador de backbone.

Capítulo 4

Estratégias

4.1 Introdução

Para a competição MANIAC, diferentes estratégias foram propostas pelas equipes participantes, onde cada estratégia seguia ideias próprias das equipes mas sempre seguindo as regras gerais estabelecidas para a competição. Na Seção 4.2 é detalhado a estratégia proposta pela equipe da Universidade de Brasília [25] que considera o "aperto" do nó até o destino final para conseguir entregar o pacote com sucesso. Na Seção 4.3 é apresentado uma estratégia simples que não faz nenhum tipo de avaliação da rede para determinar os valores gerados, utiliza apenas valores aleatoriamente escolhidos.

4.2 Estratégia do Aperto

Essa estratégia verifica o quão "apertado" o nó está para entregar o pacote com sucesso ao destino final. Para isso, quando uma requisição de oferta (RFB, do inglês *request for bid*) é recebida, a estratégia calcula o aperto para a entrega do pacote a partir da seguinte equação

$$\Delta_i = (H_0 - p_u - 1) - hc_i, \ \forall_i \in \mathcal{N}(u), \tag{4.1}$$

onde $\mathcal{N}$ é o conjunto de todos os nós que conseguem ouvir a RFB do nó u, ou seja, todos os vizinhos do nó u. H_0 é número máximo de saltos que o pacote está autorizado a atravessar. Após alcançar este máximo, o pacote não pode mais ser entregue, e todos os tablets particiantes da transação são obrigados a pagarem multa. p_u é o número de saltos que o pacote já efetuou, subtraído de um, pois já considera o próprio salto, e hc_i é o número de saltos necessários para chegar ao destino final, à partir do nó que recebeu a RFB, calculado pelo caminho de menor custo, via algorítmo de Dijkstra. Logo, quanto menor hc_i (para um dado valor de H_0 e p_u), maior o delta, e maior a folga para conseguir entregar o pacote ao destino final. Assim, caso Δ_i seja menor que 0, o número de saltos para se chegar ao destino final é maior que o número de saltos que o pacote pode efetuar. Caso Δ_i seja igual a 0, o número de saltos necessários para entregar o pacote ao destino final pelo menor caminho é igual ao número de saltos que o pacote ainda pode efetuar, essa condição define a

situação de "aperto" onde uma única mudança de topologia ou mudança de rota no caminho pode significar a perda do pacote. Quando Δ_i é maior que 0, o pacote pois uma grande chance de ser entregue com sucesso pois mesmo que haja uma mudança de topologia ou de rota, o pacote ainda poderá ser entregue ao roteador de backbone final com sucesso.

Quando uma RFB é recebida, o nó precisa calcular não apenas o seu Δ, mas também o Δ de todos os outros nós que também receberam a RFB, ou seja, todos os nós pertencentes o conjunto $\mathcal{N}(u)$, esses nós represtam todos os outros nós que disputarão o pacote. Assim, é necessário definir um subconjunto $\mathcal{S}(u)$ pertencente ao conjunto $\mathcal{N}(u)$ ($\mathcal{S}(u) \subseteq \mathcal{N}(u)$) que contém todos os nós que em que $\Delta_i \geq 0$, ou seja, todos os nós que estão aptos a entregar o pacote ao destino final dentro do limite máximo de saltos.

A partir da determinação do conjunto $\mathcal{S}(u)$, a estratégia busca definir topologicamente o quão competitivo estamos em relação aos outros nós da rede. Assim, usando a equação de aperto, definimos quão apertado estamos em relação ao aperto médio $\overline{\Delta}$ dos nós contidos em $\mathcal{S}(u)$, definido por

$$\begin{aligned} \overline{\Delta} &= \frac{1}{|\mathcal{S}(u)|} \sum_{i \in \mathcal{S}(u)} (H_0 - p_u - 1) - hc_i \\ &= (H_0 - p_u - 1) - \overline{hc}, \end{aligned} \tag{4.2}$$

onde $|\mathcal{S}(u)|$ é a cardinalidade de $\mathcal{S}$ e $\overline{hc}$ é a média de saltos de todos os nós $i \in \mathcal{S}(u)$. A partir da definição de $\overline{\Delta}$, podemos calcular o valor do aperto relativo em relação a $\overline{\Delta}$ com a seguinte equação

$$c_n = \frac{\Delta_n}{\overline{\Delta}} = \frac{(H_0 - p_u - 1) - hc_n}{(H_0 - p_u - 1) - \overline{hc}} \tag{4.3}$$

onde o índice n representa o tablet onde o cálculo está sendo realizado.

E importante notar que a Equação (4.3) é válida apenas se $\Delta_n > 0$ e $|\mathcal{S}(u)| > 0$, caso $\Delta_n \leq 0$ a estratégia responde à RFB com um valor de oferta igual ao valor de leilão (B_u). Do mesmo modo, caso $|\mathcal{S}(u)| = 0$ não há competidores para o pacote leiloado e o valor de oferta será o maior possível, ou seja, será igual ao valor de (B_u).

Caso $c_n < 1$ e $\Delta_n > 0$, os competidores estão, na média, melhor posicionados que nós em relação ao número de saltos até o destino final e, portanto, assume-se que os competidores serão agressivos no valor da oferta devido a grande possibilidade de entrega do pacote com sucesso ao destino. Assim, caso $c_n < 1$ a estratégia responde à RFB com um valor próximo ao B_u pois a condição é desfavorável para o nó. Caso $c_n \approx 1$ o nó está, em média, na mesma situação que todos os outros nós pertencentes a $\mathcal{S}(u)$, nessa situação o nó deve tentar ganhar o leilão oferecendo um valor inferior ao da situação anterior, mas superior ao valor de multa F_u. Por último, caso o valor de $c_n > 1$ estamos melhor posicionados que todos os outros nós e, portanto, devemos ser agressivos no valor da oferta, oferecendo um valor próximo ao F_u.

Comparando Δ_n com o maior valor de Δ_i para todo $i \in \mathcal{S}(u)$, encontramos o valor de a_n, que compara o nosso valor de aperto com o melhor valor de aparto de $\mathcal{S}(u)$, definido por

$$a_n = \frac{\Delta_n}{\Delta_{max}}. \tag{4.4}$$

Tendo conhecimento do valor do leilão (B_u) e o valor da multa (F_n), e sabendo que $B_n \geq F_n$, o valor de oferta O_{c_n} será definido pela expressão

$$O(c_n) = (B_u - F_u)\left[1 - \frac{1}{1 + e^{-a_n(c_n - 1)}}\right] + F_u, \tag{4.5}$$

onde $F_u \leq O_{c_n} \leq B_u$, a função é centrada em $c_n = 1$ e a declividade é controlada por a_n.

A Figura 4.1 apresenta o comportamento do valor de oferta quando variado o valor do aperto relativo c_n, observamos que quanto maior o valor do aperto relativo do nó, mais proximo do valor da multa será a oferta indicada. Por outro lado, caso o valor do aperto relativo seja baixo, o valor de oferta será próximo do valor máximo B_n

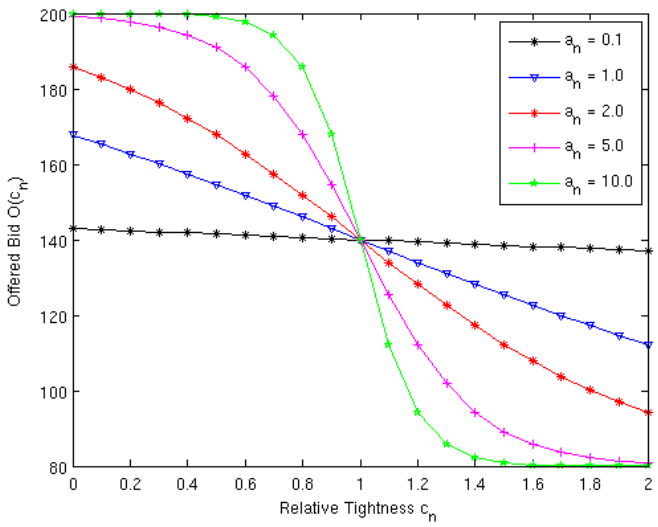

Figura 4.1: Exemplo de curva de oferta O_{c_n} para diferentes valores de a_n quando $B_u = 200$ e $F_u = 80$

Quando um leilão é ganho pelo nó, a estratégia utiliza uma condição fixa para determinar os valores a serem estabelecidos na próxima RFB, ou seja, os valores de leilão (B_n) e o valor de multa (F_n). Assim, os valores para esses parâmetros são determinados por

$$\begin{aligned} B_n &= 0.6 \times O^* \\ F_n &= 0.9 \times B_n \end{aligned} \tag{4.6}$$

A escolha do vencedor de uma RFB leva em consideração, além do valor oferecido, o aperto relativo de cada nó i vizinho ao nó de origem da RFB, ou seja, o aperto relativo de todos os nós que receberam a requisição de oferta. A escolha do nó vencedor é feita a partir de uma função de preferência $P(c_i, op_i)$ que determina o melhor nó a partir do valor do aperto relativo, segundo a Eq.

(4.3), e do valor de oferta recebido op_i. Para a definição da função de preferência, é considerado o maior valor de oferta que pode ser recebido, que no caso é o próprio valor B_n indicado no anuncio da RFB, e o maior aperto relativo c_{max}, que corresponde ao nó vizinho melhor posicionado em relação ao roteador de backbone final. Objetivando o melhor desempenho possível da rede, a estratégia da preferência ao valor do aperto médio e considera menos importante o valor de oferta oferecido. Assim, a preferência mais baixa será dada ao nó em que $c_i = 0$ e $op_i = B_n$ e a prefência mais alta será dada ao nó em que $c_i = c_{max}$ e $op_i = 0$. A situação em que $P_n(0, 0)$ representa a situação de aperto em relação ao roteador de backbone final mas que o valor de oferta recebido do nó vizinho é igual a zero. Por outro lado, a situação em que $P_n(B_n, c_{max})$ representa a condição em que um nó ofereceu o maior valor de oferta possível e está melhor posicionado que todos os outros nós. Assim, se $P_n(0, 0) = k_1$ e $P_n(B_n, c_{max}) = k_2$, a prêferencia entre k_1 e k_2 que reflete a tendência de favorecer a entrega do pacote, e não o ganho de dinheiro, pode ser dada por $k_2 > k_1 > 0$. Assim, a função de preferência é dada como um plano definido por

$$P(c_i, op_i) = k_1 - \left(\frac{k_1}{B_n}\right) op_i + \left(\frac{k_2}{c_{max}}\right) c_i \tag{4.7}$$

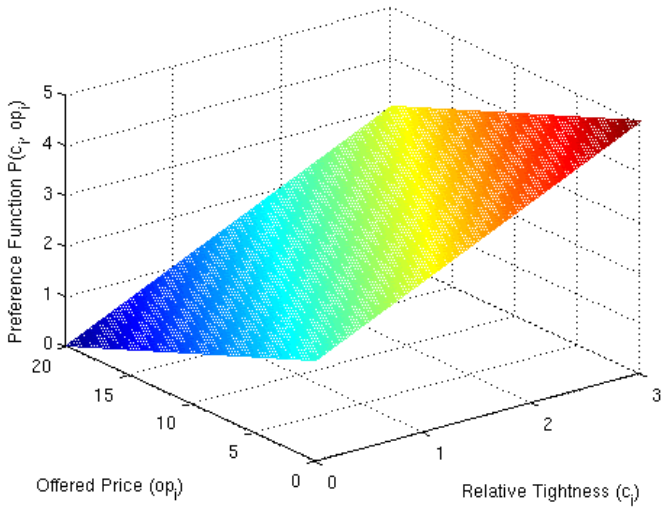

Figura 4.2: Exemplo da função de preferência para valores de $B_n = 20$, $c_{max} = 3$, $k_1 = 2$ e $k_2 = 3$

A partir da definição dos valores de k_1 e k_2 que representam a tendência a ser seguida na definição do nó vencedor, o nó que receberá o pacote será aquele que apresentar o maior valor de preferência.

4.3 Estratégia Aleatória

Essa estratégia foi desenvolvida para repesentar a condição aleatória da rede, quando nenhum tipo de "inteligência" é utilizada para a escolha do caminho até o roteador de backbone final. Durante o seu funcionamento, nenhum tipo de avaliação da rede é feito para a determinação dos valores aplicados. Quando uma RFB é recebida de um roteador de backbone ou de outro nó da

rede, a estratégia calcula um valor aleatório entre 1 e B_n, e não leva em consideração nem mesmo o valor de multa indicado na RFB. Assim, essa estratégia pode oferecer valores maiores ou menores que o valor de multa F_n.

Caso o nó ganhe um leilão, os valores utilizados para a nova RFB são os mesmo utilizados pelo nó anterior, modificando apenas o número de saltos já ocorridos. Assim, caso uma rede seja composta por nós utilizando apenas essa essa estratégia, todos os nós da rede lançarão RFBs com o mesmo valor anunciado pelo roteador de backbone de origem.

A determinação do vencedor de uma RFB utiliza, apenas, o valor de oferta como parâmetro. Assim, o pacote é repassado ao nó que oferecer a menor oferta pelo pacote.

Por não utilizar nenhum tipo de inteligência, essa estratégia pode ficar com saldo negativo nas transmissões mesmo que consiga realizá-las com sucesso, pois seu valor de oferta pode ser menor que o valor de oferta do nó seguinte. Além disso, devido a sua aleatoriedade, associada ao fato de um mesmo nó não poder participar de uma mesma transação mais de uma vez, um pacote pode ficar "preso" em uma região da topologia por eliminar das transações os possíveis caminhos até o roteador de backbone final.

Capítulo 5

Configuração dos Experimentos

5.1 Introdução

Nesta capítulo é apresentado o modo como a arquitetura da rede foi montada para a realização dos experimentos, e todos os equipamentos e sofwares utilizados. São apresentados também o modo como os testes foram feitos, a avaliação do ambiente utilizado, assim como as condições impostas sobre os experimentos. Na Seção 5.2 são apresentadas as principais características do local escolhido para realização dos testes, juntamente com a planta baixa do ambiente onde os testes foram realizados. Na Seção 5.3 são apresentadas as avaliações feitas para a escolha do melhor canal de transmissão. Na Seção 5.4 é explicado todo o procedimento feito para viabilizar a execução da aplicação ManiacLib nos tablets utilizados. Por último, na Seção 5.5, é explicado o processo de implementação e configuração das máquinas que atuam no backbone da rede e a máquina "mestre".

5.2 Local dos Experimentos

O ambiente escolhido para a realização dos testes foi o prédio SG11 da Universidade de Brasília. A escolha do local foi feita levando em consideração a presença de locais seguros em que os equipamentos pudessem ser mantidos, e a presença de uma rede cabeada abrangendo todo o edifício para fins de uso do backbone da rede. Os dois andares do prédio foram utilizados para os experimentos. As Figuras 5.1 e 5.2 apresentam as plantas baixas dos andares térreo e primeiro andar do prédio em questão. Além de possuir locais seguros para a montagem do backbone da rede, o prédio possui longos corredores e diversos locais para posicionamento dos dispositivos móveis da rede.

5.3 Canal de operação da rede

Diversas redes Wi-Fi operam no prédio onde os testes foram realizados. Além das próprias redes Wi-Fi mantidas pela universidade (UNBWireless, UNBWireless Suporte e eduroam) muitas outras

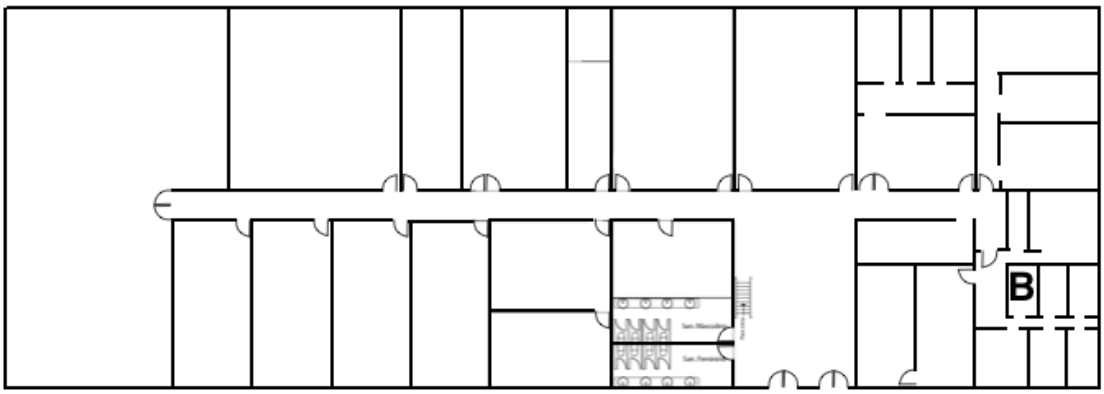

Figura 5.1: Planta do andar térreo do prédio SG11.

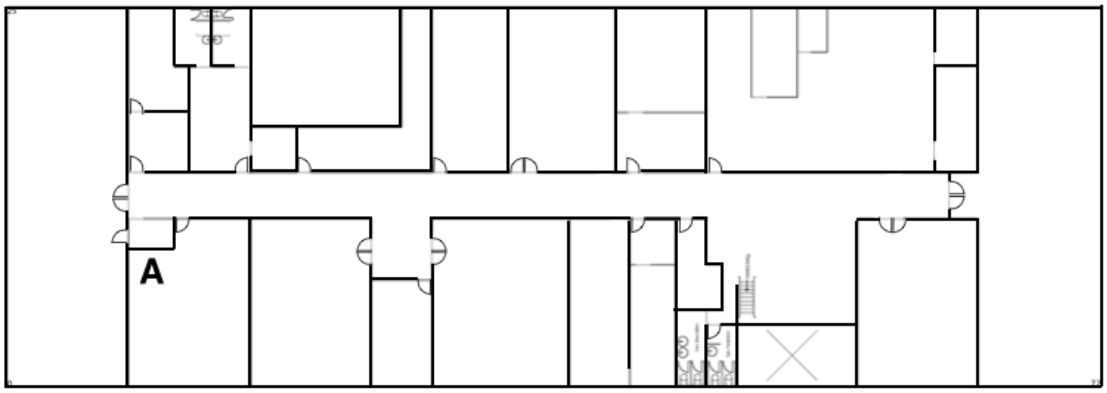

Figura 5.2: Planta do primeiro andar do prédio SG11.

salas e laboratórios mantêm suas próprias redes Wi-Fi. Como mostrado no Capítulo 2, apenas 3 canais podem coexistir sem que haja interferência co-canal, desde que os canais utilizados sejam 1, 6 e 11. Porém, devido ao grande volume de redes no local, não há uma frequência na faixa de 2.4GHz que esteja livre de interferência. Para a escolha do melhor canal a ser utilizado, o ambiente foi analisado utilizado o aplicativo Wifi Analizer [26]. Tal aplicativo permite visualizar a ocupação dos canais e a potência recebida de cada um dos pontos de acesso.

As Figuras 5.3 e 5.4 mostram a ocupação dos canais nas duas extremidades do prédio, identificado nas Figuras 5.1 e 5.2 pelas letras A e B. Essas localizações representam a posição de cada roteador de backbone da rede. Apesar do espectro estar totalmente ocupado, o canal 3 apresenta a menor quantidade de canais interferentes. Por esse motivo, esse canal foi escolhido como sendo o canal de nossa rede *ad hoc*. Assim, a frequência central utilizada ficou em 2422MHz, ocupando a faixa de 2411MHz até 2433MHz. É importante ressaltar que, no dia da realização dos experimentos, a rede NMI-Alunos não estava ocupando o canal 4, essa rede foi criada dias após a realização dos experimentos. Todas as outras redes não tiveram seus canais modificados.

Apesar da faixa de 2.4GHz estar totalmente ocupada, a faixa de 5GHz possui apenas 3 redes funcionando atualmente, sendo todas elas redes oferecidas pela própria universidade e utilizando o mesmo canal de rede, o canal 100. Assim, utilizar essa faixa de frequência poderia representar uma grande vantagem em relação à faixa de 2.4GHz, seria possível escolher uma faixa de frequência

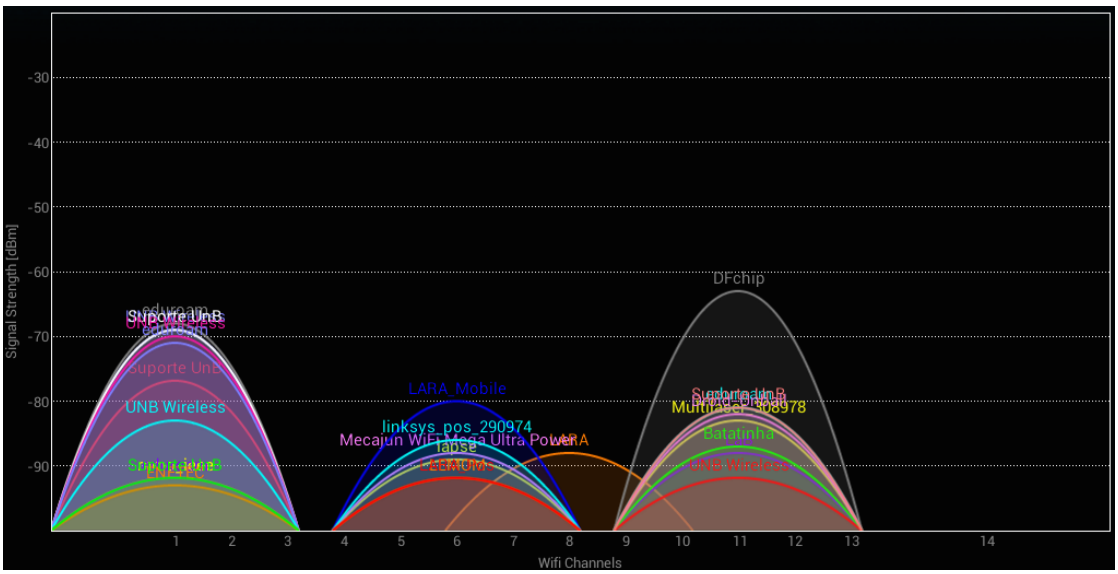

Figura 5.3: Ocupação dos canais de rede na faixa de 2.4GHz medido à partir do ponto A.

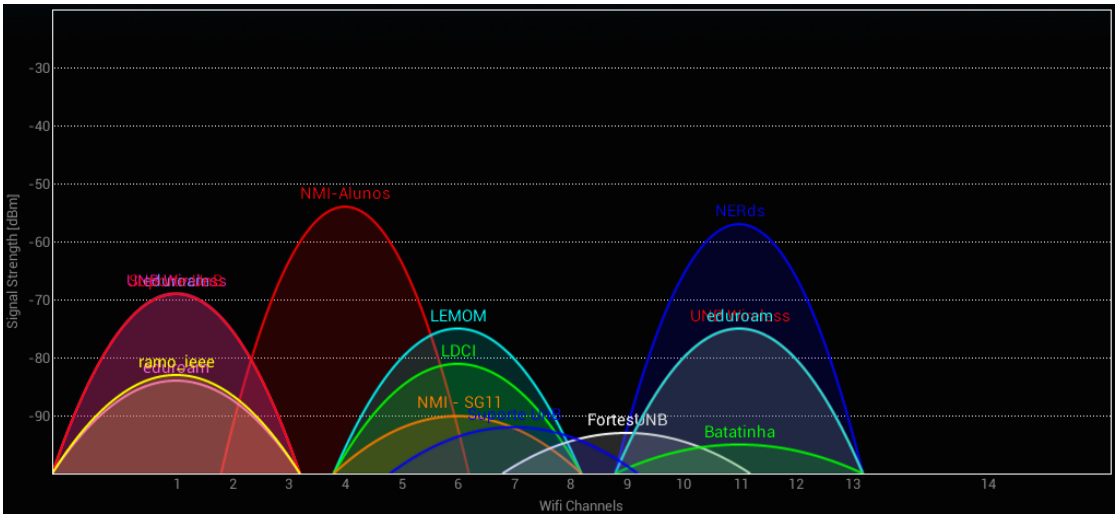

Figura 5.4: Ocupação dos canais de rede na faixa de 2.4GHz medido à partir do ponto B.

onde não houvesse nenhuma estação interferente. Infelizmente, essa faixa não pôde ser utilizada pois um dos roteadores de backbones da rede possui uma placa de rede capaz de operar apenas nos padrões IEEE 802.11b/g, ou seja, apenas na faixa de 2.4GHz.

5.4 Configuração dos Tablets

Foram utilizados nove tablets Samsung Galaxy Tab 3. Esse modelo de dispositivo foi escolhido por possuir uma placa de rede que permite o uso em modo *ad hoc* e por possuir uma grande quantidade de documentação disponível online.

Infelizmente, a plataforma Android não possui nenhuma API que permite que o usuário habilite o modo *ad hoc* no dispositivo. Para que essa função seja liberada, é necessário realizar um

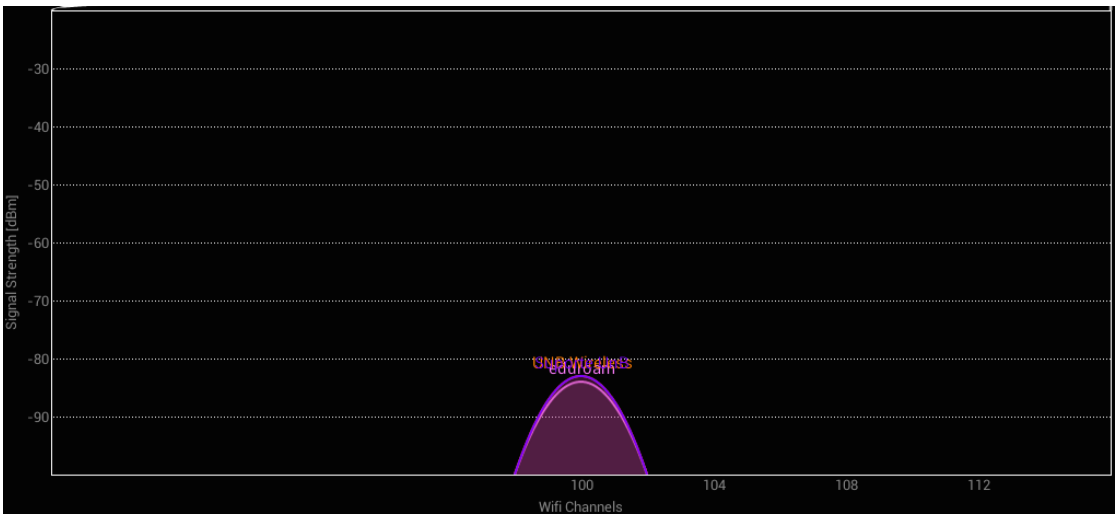

Figura 5.5: Ocupação dos canais na faixa de 5GHz

procedimento que libera acesso em nível de super usuário (su, do inglês *super user*) ao dispositivo. Por não ser um processo fornecido pela fabricante ou liberado pela Google, toda a garantia do equipamento é perdida após a realização desse processo.

Após realizar esse procedimento, que varia bastante de um modelo para outro, podemos dar prosseguimento à configuração dos tablets. Para estabelecer a rede *ad hoc* e o protocolo de roteamento OLSR, foi instalado o aplicativo Manet Manager [24] em cada um dos tablets. Tal aplicativo permite que seja escolhido o tipo de protocolo de roteamento da rede (AODV ou OLSR) e também permite que o endereço IP do equipamento seja configurado. A Figura 5.6 apresenta a tela principal da aplicação citada.

O Samsung Galaxy Tab 3 possui a vantagem de não necessitar de modificação do *kernel* (ou núcleo) do sistema operacional Android, ao contrário do modelo de tablet utilizado na competição MANIAC Challenge na Alemanha, o Google Nexus 7. Para que a aplicação Manet Manager possa funcionar corretamente em um tablet Google Nexus 7, é necessário que uma versão modificada do Android seja instalada. Esta versão modificada, conhecida como CyanogenMod [27], permite que o usuário faça qualquer tipo de modificação no sistema operacional original, incluindo modificações no próprio *kernel* do sistema. Felizmente, apenas o processo para acesso em nivel de super usuário ao sistema é necessário para que a aplicação Manet Manager funcione em um tablet Samsung Galaxy Tab 3.

Todos os tablets foram configurados com a mesma versão do sistema operacional Android, a versão 4.1.2 (“Jelly Bean”). Todos os dispositivos foram numerados sequencialmente de 1 a 9 para fácil identificação na tabela de roteamendo OLSR e fácil identifição de problemas na rede, como mostrado na Tabela 5.4. Utilizando esses endereços, a identificação do tablet na rede pode ser facilmente feita observando-se unicamente o último digito do endereço IP.

Após esse processo, a aplicação ManiacLib pôde finalmente ser instalada e executada. A aplicação para de funcionar abruptamente caso o maniacLib seja executado sem que o processo anterior seja feito. Na tela da aplicação é possivel verificar se todas as APIs estão funcionando

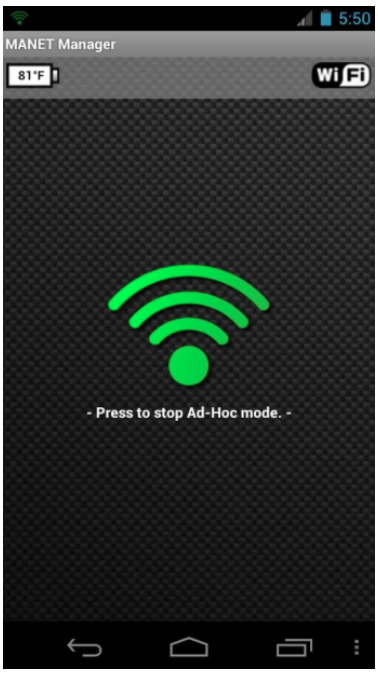

Figura 5.6: Aplicação Manet Manager utilizada para iniciar a rede *ad hoc* e habilitar o protocolo OLSR.

Tablet	Versão do Android	Endereço IP	Máscara de rede
1	4.1.2	192.168.17.101	255.255.255.0
2	4.1.2	192.168.17.102	255.255.255.0
3	4.1.2	192.168.17.103	255.255.255.0
4	4.1.2	192.168.17.104	255.255.255.0
5	4.1.2	192.168.17.105	255.255.255.0
6	4.1.2	192.168.17.106	255.255.255.0
7	4.1.2	192.168.17.107	255.255.255.0
8	4.1.2	192.168.17.108	255.255.255.0
9	4.1.2	192.168.17.109	255.255.255.0

Tabela 5.1: Endereços IPs configurados em cada tablet e a versão da plataforma Android utilizada

corretamente e consultar toda a tabela OLSR. A Figura 5.7 apresenta a tela da aplicação ManiacLib com a tabela de roteamento gerada pelo protocolo OLSR.

5.5 Configuração das máquinas de backbone e mestre

Para controlar toda a geração de pacotes e contabilizar os pontos de cada dispositivo, o computador mestre foi configurado no mesmo computador em que uma das máquinas do backbone foi instalada. Para a configuração do dispositivo mestre fez-se necessária apenas a instalação dos programas necessários para o seu funcionamento. Apesar da competição original fazer uso de dezenas

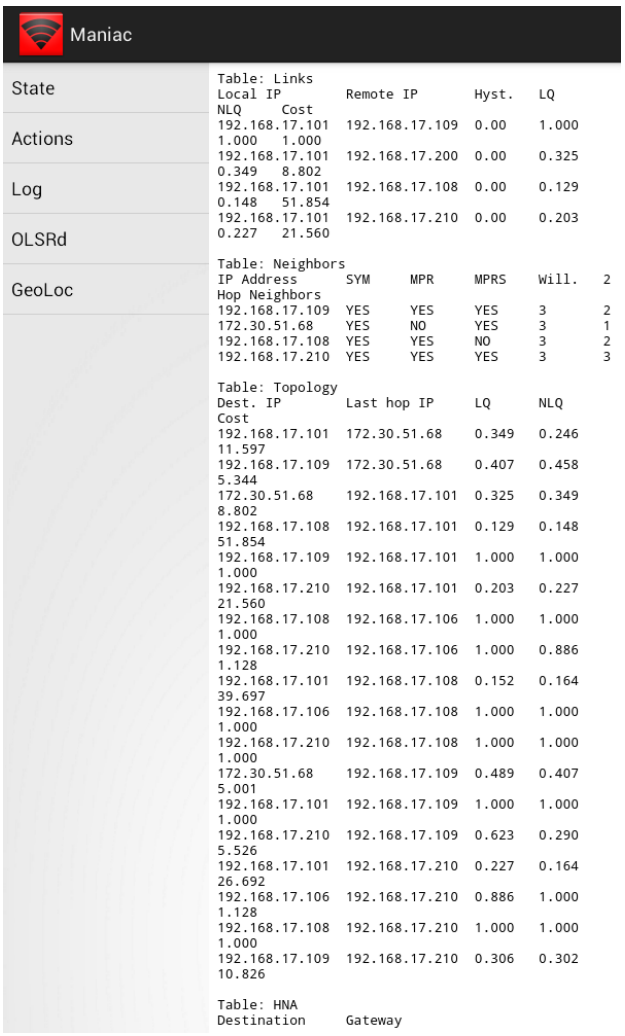

Figura 5.7: Aplicação ManiacLib utilizada para a execução do repasse de informações e execução da estratégia utilizada

de máquinas de backbone, utilizamos apenas dois *laptops* como roteadores de backbone em nossos experimentos devido à indisponibilidade de outros computadores e a área limitada do ambiente utilizado. O uso de um maior número de roteadores de backbone implicaria na necessidade de uma área maior de cobertura para garantir a existência de múltiplos saltos nas rotas para os vários roteadores de backbone, algo necessário para realização dos experimentos e teste das estratégias.

Para a configuração dos roteadores de backbone, cada um dos computadores foi posicionado em uma extremidade do prédio SG11, permanecendo o primeiro dentro do laboratorio do Grupo de Processamento de Sinais Digitais (GPDS), no andar térreo, e o segundo na sala de suporte TI do SG-11, no primeiro andar. Esse locais foram escolhidos para que os dois computadores permanecessem a uma distância suficientemente grande, de modo que não pudessem estar ao alcance um do outro pela pela rede sem fio, e também para aproveitar a extensão do prédio ao máximo. Para que os dois computadores pudessem se comunicar e, consequentemente, comunicarem-se com o mestre, a rede cabeada do prédio foi configurada de modo que os dois computadores permanecessem dentro de uma mesma subrede.

Todos os 9 tables foram espalhados pelos 2 andares do prédio SG11, conforme mostrado nas Figuras 5.8 e 5.9. Assim, 5 tablets permaneceram no andar térreo e 4 tablets foram posicionados no primeiro andar. A disposição dos tablets foi feita de modo a garantir concorrência entre diversos tablets para todos os leilões gerados.

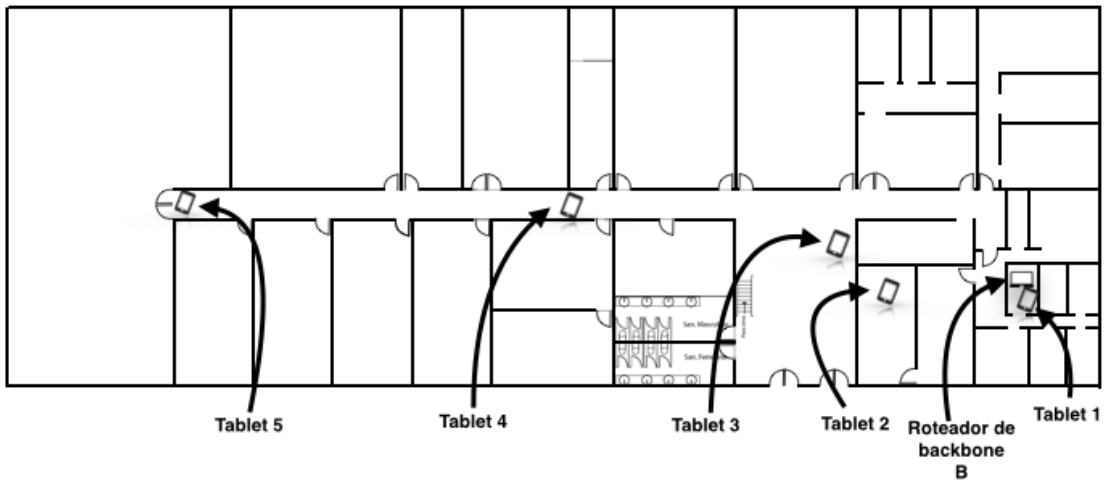

Figura 5.8: Planta baixa do andar térreo do prédio SG11 com a disposição do roteador de backbone e dos tablets utilizados

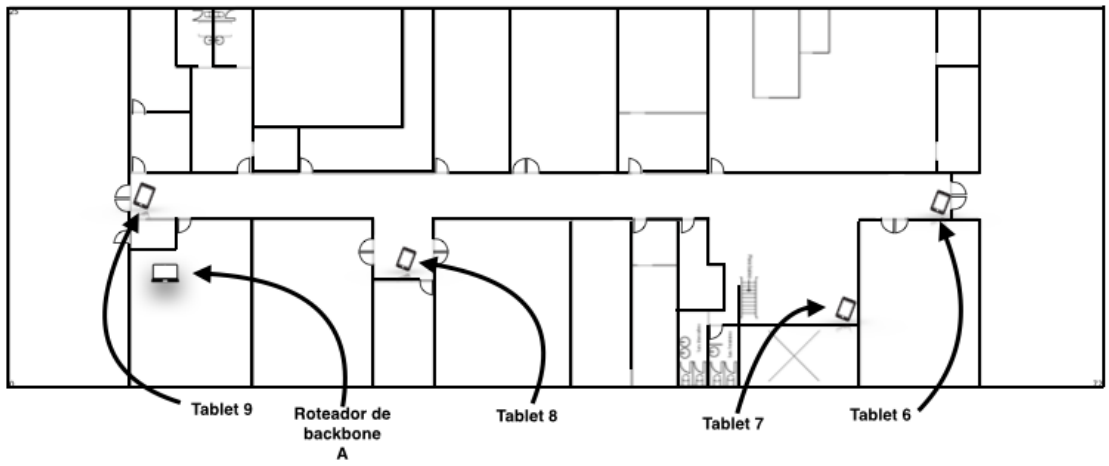

Figura 5.9: Planta baixa do primeiro andar do prédio SG11 com a disposição do roteador de backbone e dos tablets utilizados

Para uma fácil identificação dos roteadores de backbone, seus indereços IPs para a rede cabeada (rede entre os dois backbones) foram configurados como mostrado na Tabela 5.2, enquanto que os endereços configurados para a rede sem fio foram configurados como mostrado na Tabela 5.3. Assim, ao consultar a tabela gerada pelo OLSR, todos os endereços IP terminados em 200 ou 210 identificavam os roteadores de backbone na rede.

Como foi dito, o computador mestre foi configurado no mesmo computador que um dos roteadores de backbone operava. No caso, foi utilizado o computador Dell de endereço 172.16.17.200 como computador mestre da rede. Assim, o roteador de backbone do computador 172.16.17.200

Computador	Identificação	Endereço IP	Máscara de rede
Dell	A	172.16.17.200	255.255.255.0
Mac	B	172.16.17.210	255.255.255.0

Tabela 5.2: Endereços IPs configurados em cada uma das maquinas de backbone para se comunicarem via rede LAN

Computador	Identificação	Endereço IP	Máscara de rede
Dell	A	192.168.17.200	255.255.255.0
Mac	B	192.168.17.210	255.255.255.0

Tabela 5.3: Endereços IPs configurados em cada uma das maquinas de backbone para se conectarem à rede *ad hoc*

foi configurado para localizar o computador mestre utilizando o endereço 127.0.0.1 (*localhost*). Após todos esses processos realizados, a rede estava finalmente pronta para realizar experimentos e validações.

Capítulo 6

Avaliação de Desempenho

6.1 Introdução

Esta seção apresenta os resultados obtidos a partir dos experimentos realizados utilizando a "estratégia do aperto" e a "estratégia aleatória". Na Seção 6.2 são explicados os parâmetros utilizados durante as experimentos e na Seção 6.3 são apresentados e analisados os resultados obtidos a partir dos experimentos realizados.

6.2 Configuração dos Experimentos

Com o objetivo de obter um maior número de saltos entre os roteadores de backbone de origem e destino, todos os tablets foram configurados para operarem com a menor potência de transmissão permitida pelo equipamento (8dBm). Durante os experimentos, os tablets permaneceram na posição horizontal, pois foi observado que, nesta posição, o raio de alcance dos tablets diminui ainda mais. Essas medidas foram necessárias pois o ambiente utilizado para os experimentos não possui barreiras suficientes para impedir a propagação do sinal. Assim como os Tablets, o roteador de backbone A também foi configurado para operar em 8dBm, e o roteador de backbone B permaneceu com a tela abaixada durante toda a realização dos experimentos.

Todos os roteadores de backbone e os tablets utilizados foram configurados para operarem no canal 3, pelos motivos citados na Seção 5.3 do capítulo anterior. Como a topologia utilizada consistia de apenas 2 roteadores de backbone, os fluxos de dados eram sempre gerados a partir do ponto A ou do ponto B, escolhidos aleatoriamente.

A geração de pacotes em cada roteador de backbone aconteceu à taxa de 1 pacote a cada 15 segundos. Esta taxa baixa de geração de pacotes se deve ao fato do estudo não explorar o comportamento da rede em situações de alto tráfego. O objetivo dos experimentos é avaliar o desempenho de cada estratégia implementada, observando-se a taxa de entrega de pacotes, o número médio de saltos necessários até o destino, e o saldo médio obtido por cada partipante da rede. Além disso, a utilização da baixa taxa de geração de pacotes evita que a rede fique

sobrecarregada de leilões, tendo em vista que a aplicação utilizada não é capaz de lidar com múltiplos leilões simultaneamente. Cada leilão individual ocorre durante um período de 3 segundos. Utilizando uma taxa de geração de pacotes de 1 pacote a cada 15 segundos, garantimos que nenhum outro pacote esteja em leilão durante um período de até 5 saltos.

Os pacotes de dados gerados enviam as informações de valor máximo a ser pago, valor de multa e número de saltos restantes no próprio corpo da mensagem e todos os pacotes de dados possuem tamanho fixo de 86 bytes. As mensagens de anuncio de vencedor de leilão possuem 69 bytes, as mensagens de requisição de oferta possuem 75 bytes e as mensagens de anuncio de oferta possuem tamanho de 50 bytes.

Os valores utilizados para o protocolo OLSR nos roteadores de backbone não foram modificados, todos os valores utilizados seguiram o mesmo valor obtido diretamente da aplicação instalada, esse valores estão apresentados na Tabela 6.1.

Parâmetro	Tempo(s)
HelloInterval	6.0
HelloValidityTime	600.0
TcInterval	0.5
TcValidityTime	300.0
MidInterval	10.0
MidValidityTime	300.0
HnaInterval	10.0
HnaValidityTime	300.0

Tabela 6.1: Valores utilizados em cada parâmetro do protocolo de roteamento OLSR

Os valores iniciais de leilão foram configurados de modo que o valor máximo de oferta fosse sempre 400, o valor de multa igual a 200 e o número máximo de saltos igual a 10. Para os valores de k_1 e k_2 da função de preferência, os valores utilizados foram $k_1 = 2$ e $k_2 = 3$, dando preferência à entrega do pacote, e não ao ganho de pontos.

Todos os experimentos foram realizados em 10 rodadas com duração de 16 minutos cada para garantir uma maior confiabilidade dos resultados obtidos. Esse processo foi necessário para considerar variações temporais do canal de rádio e consequentes ações dos protocolos das camadas MAC (IEEE 802.11) e roteamento OLSR.

Durante toda a realização dos experimentos não houve mudança na posição dos tablets utilizados, os experimentos foram realizados sem mobilidade e não houve mudança no posicionamento deles entre realização de experimentos.

6.3 Resultados dos Experimentos

A Figura 6.3 apresenta os resultados para a taxa de entrega de pacotes com sucesso de ambas as estratégias. De acordo com os resultados, a taxa de sucesso de transmissão entre a estratégia do aperto e a estratégia aleatória ficou praticamente empatada, cerca de 65% de sucesso. Os outros 35% perdidos são consequências das falhas de transmissão decorrentess da sobregarga de mensagens de controle provenientes do protocolo OLSR, dos diversos pontos de acesso presentes no ambiente e as mensagens de controle enviadas pelos roteadores de backbone. Além disso, é importante lembrar que um mesmo nó não participa de uma mesma transmissão mais de uma vez. Então, principalmente na estratégia aleatória, um pacote pode ficar "preso" em uma determina região por eliminar todas as possíveis rotas até o destino final.

A estratégia do aperto tentará sempre chegar ao destino final pelo melhor caminho, para essa escolha do caminho a estratégia utiliza como fator de decisão o valor de oferta recebido e o aperto relativo de cada nó. Como o valor de $k_1 = 2$ e $k_2 = 3$, a estratégia tende a preferir os caminhos de menor aperto, segundo a função de preferência. Por outro lado, a estratégia não avalia a qualidade desses enlaces e acaba gerando falhas de transissão por escolher nós que estão muito distantes. A estratégia do aperto define o repasse de um pacote baseando-se no resultado a função de preferência, e a estratégia aleatória ficará passando o pacote aleatoriamente entre os tablets até que ocorra o encontro com o backbone final. Durante os experimentos, o número máximo de saltos estipulado para as transações foi maior do que o número de tablets participantes na rede. Com isso, o número de saltos nunca foi um limitante para a rede, pois mesmo que o pacote passasse por todos os tablets presentes, esse limite não seria excedido.

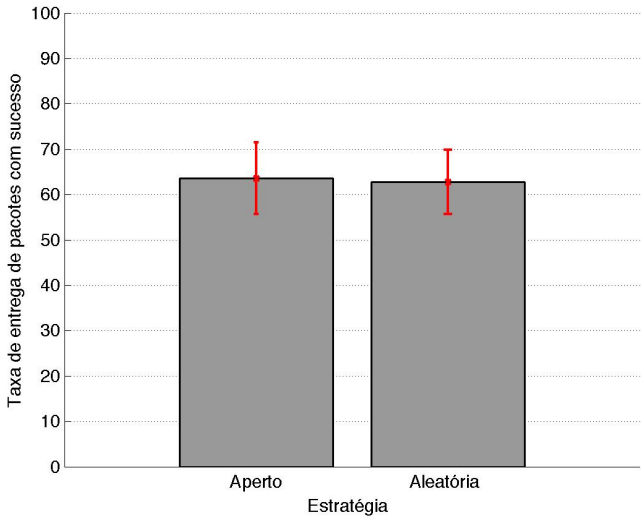

Figura 6.1: Taxa de Sucesso de transmissão utilizando a estratégia do aperto e a estratégia aleatória

Analisando os pacotes da estratégia do aperto em que houve falha de transmissão, foi identificado que essas transmissões não foram concluídas com sucesso puramente por falha na transmissão. Isso signifia que ao tentar otimizar ao máximo o melhor caminho até o roteador de backbone final, a estratégia não leva em consideração a qualidade dos enlaces entre os tablets. Então, ao invés

de escolher um caminho em que a qualidade dos enlaces entre os tablets estivesse acima de um determinado patamar, a estratégia preferiu seguir sempre pelo caminho de menor custo na rede. Além da interferência proveniente dos diversos pontos de acesso presentes no local, outra possível causa de falhas de transmissão é o envio periódico de mensagens de controle por parte do OLSR.

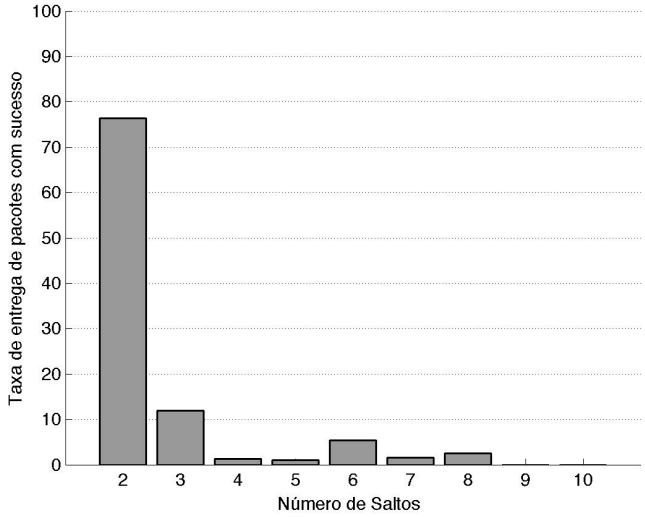

Figura 6.2: Ocorrência de número de saltos para todas as transmissões realizadas com sucesso com a estratégia do aperto

Podemos ver na Figura 6.2 que aproximadamente 77% das transmissões com sucesso utilizando a estratégia do aperto ocorreram com apenas 2 saltos, e pouco mais de 10% das transmissões ocorreram com 3 saltos. Isso ocorreu pois a estratégia tenta otimizar ao máximo o caminho até o destino final. Enquanto que na estratégia aleatória menos de 15% das transmissões ocorrem com apenas 2 saltos, a maior parte das transmissões com sucesso nessa estratégia ocorreram com 3 saltos, cerca de 44%, conforme mostrado na Figura 6.3.

É importante citar que as ocorrências de transmissões bem sucedidas com um número elevado de saltos utilizando a "estratégia do aperto" é consequência de falhas na própria aplicação Android. Por algum motivo que não pude identificar claramente, a aplicação parava de funcionar em momentos aleatórios, após um determinado período de correto funcionamento. Aparentemente, a falha tem relação com o modo como a tabela gerada pelo OLSR é passada para o ManiacLib, acarretando a quebra da aplicação, pois ao tentar consultar a rota até um determinado destino, nenhum valor é retornado. Esse mesmo problema não acontece em transmissões utilizando a "estratégia aleatória", pois não é feita nenhuma consulta a tabela gerada pelo OLSR por essa estratégia. Essa falha tem origem nos próprios roteadores de backbone acarretando a falha em alguns dos dispositivos diretamente conectados. Quando essa falha ocorre, os tablets que estão transmitindo um determinado pacote são obrigados a escolherem uma nova rota. A opção de não reiniciar as rodadas onde essa falha foi identificada se deu pelo fato da rede estar constantemente sendo monitorada e, sempre que a falha era identificada em algum tablet, a aplicação era imediatamente reiniciada, essa mesma falha ocorria em tempos aleatórios não estando presente em todas as rodadas geradas. Além disso, a falha pode ser vista como uma mudança forçada de rota por parte dos dispositivos

onde determinados participantes da rede deixam de participar das transações por alguns segundos e a estratégia era forçada a escolher um outro caminho, que poderia necessitar de mais saltos para chegar ao destino final.

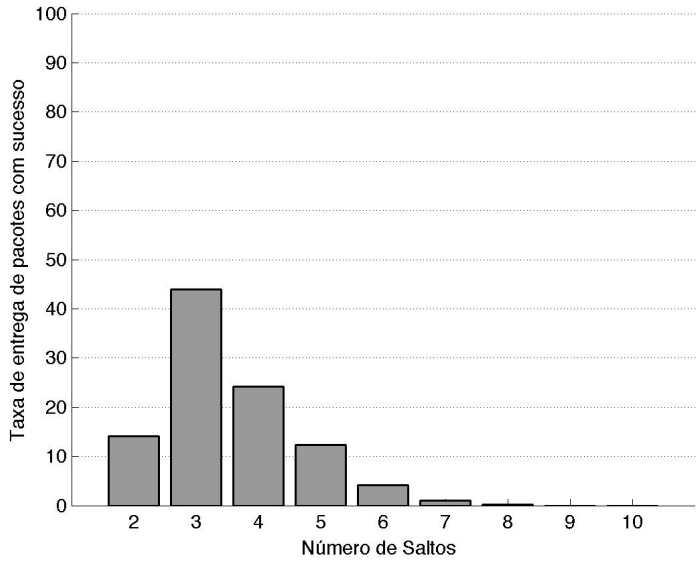

Figura 6.3: Taxa de entrega de pacotes com sucesso como função do número de saltos necessários para entrega com sucesso com a estratégia aleatória

Caso sejam consideradas apenas as transmissões com sucesso feitas até um número máximo de saltos, a estratégia do aperto começa a mostrar suas vantagens em relação à estratégia aleatória. Para um limite de até 4 saltos, conforme mostra a Figura 6.4, a estratégia do aperto se mostrou cerca de 8% melhor que a estratégia aleatória. Este resultado pode ser visto na Figura 6.3 anterior, onde a soma das transmissões ocorridas com 5 ou mais saltos representa pouco menos de 20% das transmissões totais.

Se agora analisarmos a taxa de entrega de pacotes com sucesso para os casos em que até um máximo de 2 saltos foram necessários — caso mínimo, em que há a participação de um único tablet da rede ad hoc — identificamos claramente a diferença entre as duas estratégias implementadas: a estratégia do aperto mostra-se, nesta situação, cerca de 5 vezes mais eficiente que a estratégia aleatória. Os resultados referentes a este caso estão mostrados na Figura 6.5.

Apesar da transmissão envolvendo apenas alguns tablets apresentar um tempo de entrega menor e um melhor uso da rede, essa atitude beneficia apenas os tablets envolvidos nessas transmissões enquanto que todos os outros tablets na rede não conseguem participar das transações e, consequentemente, acumular pontos.

Se analisarmos a pontuação média de cada tablet utilizando a estratégia do aperto, percebemos que as maiores pontuações estão centradas em 3 tablets principais, os tablets 5, 6 e 9, conforme mostrado na Figura 6.6. Se retornamos às imagens das plantas baixas do prédio utilizado para os experimentos, Figuras 5.8 e 5.9, percebemos que os Tables 6 e 9 estavam posicionados nas extremidades do primeiro andar, o que mostra que mesmo reduzindo a potência de transmissão

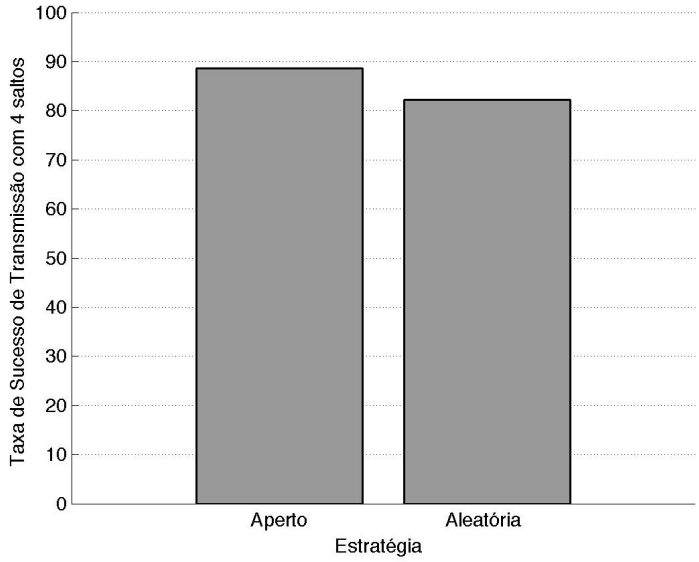

Figura 6.4: Taxa de Sucesso de transmissão utilizando a estratégia do aperto e a estratégia aleatória para um limite de 4 saltos

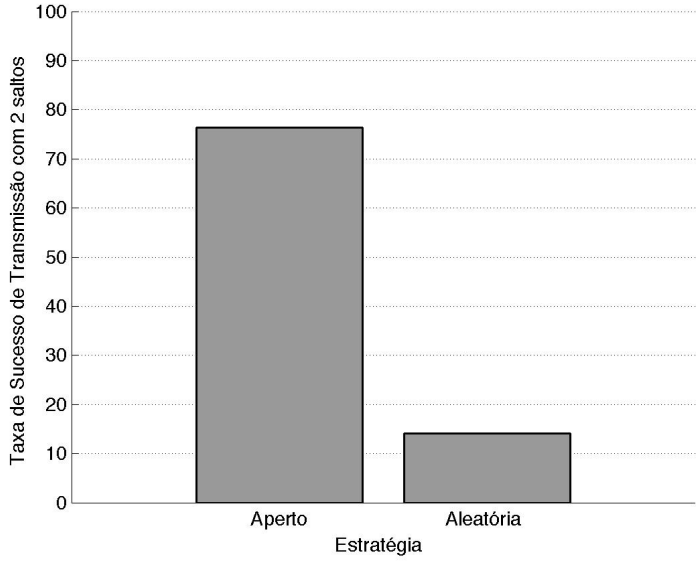

Figura 6.5: Taxa de Sucesso de transmissão utilizando a estratégia do aperto e a estratégia aleatória para um limite de 2 saltos

ao máximo, o alcance dos tablets continuou cobrindo o prédio quase todo. O Tablet 5 estava posicionado no andar térreo próximo ao Tablet 9 e ao roteador de backbone A localizado no andar superior.

Em relação à estratégia aleatória, vemos que a pontuação média de cada tablet variou muito entre cada realização de experimento. Isso já era esperado, pois os valores de oferta anunciados pelos tablets durante a execução da estratégia são gerados aleatoriamente e a estratégia sempre

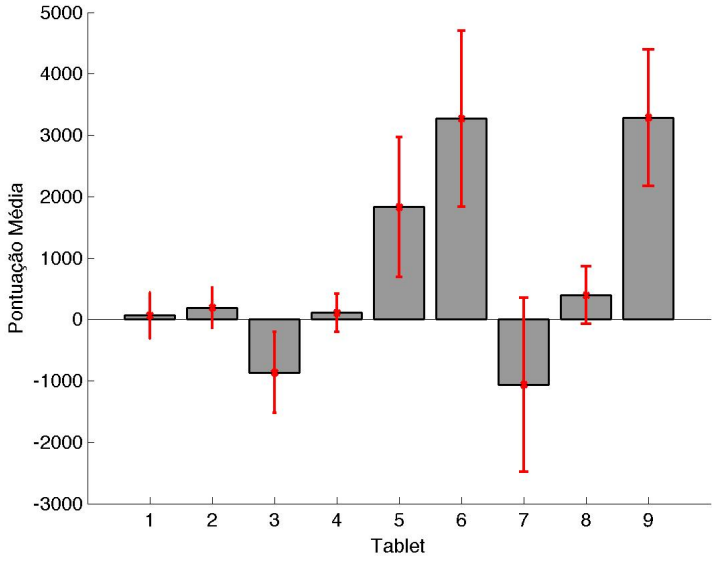

Figura 6.6: Pontuação média de cada tablet utilizando a estratégia do aperto

seleciona o tablet com menor valor ofertado. Apesar de alguns tablets apresentarem uma média de pontos relativamente alta, como é o caso do tablet 4, é difícil inferir qualquer resultado a partir do gráfico pois, ao gerar um valor aleatório de oferta para um determinado leilão, o tablet pode sair em prejuizo mesmo que a transmissão ocorra com sucesso.

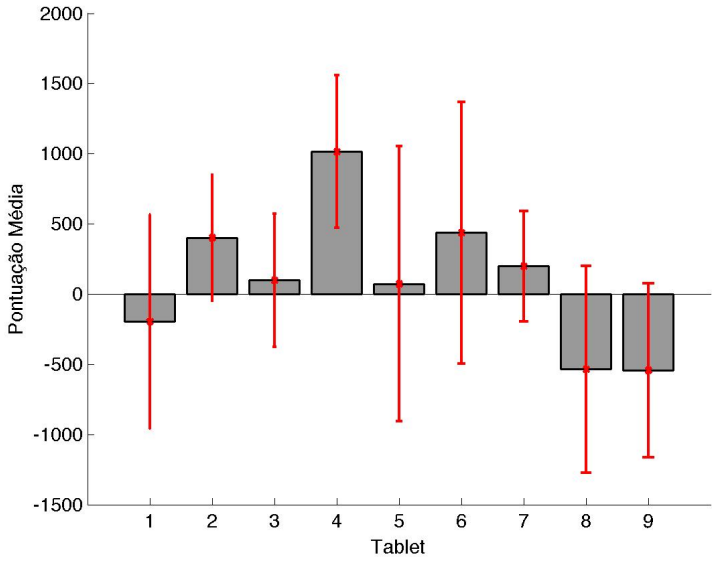

Figura 6.7: Pontuação média de cada tablet utilizando a estratégia aleatória

Se considerarmos a soma das pontuações de cada tablet divido pelo número de tablets participantes, ou seja, que tiveram ao menos um pacote repassado durante todo o experimento, obtemos a pontuação média geral para cada uma das estratégias. Nesse caso, conforme mostra a Figura 6.8, a pontuação média geral para a estratégia do aperto se mostrou 8 vezes superior, demonstrando

um ganho considerável em relação à estratégia aleatória. Isto significa que o valor inicial oferecido pelo roteador de backbone não foi fragmentado entre diversos tablets, com consequente atraso na entrega do pacote. Observa-se que o saldo médio acumulado ao final dos experimentos, dos tablets participantes é praticamente o dobro do valor oferecido pelo roteador de backbone para cada pacote.

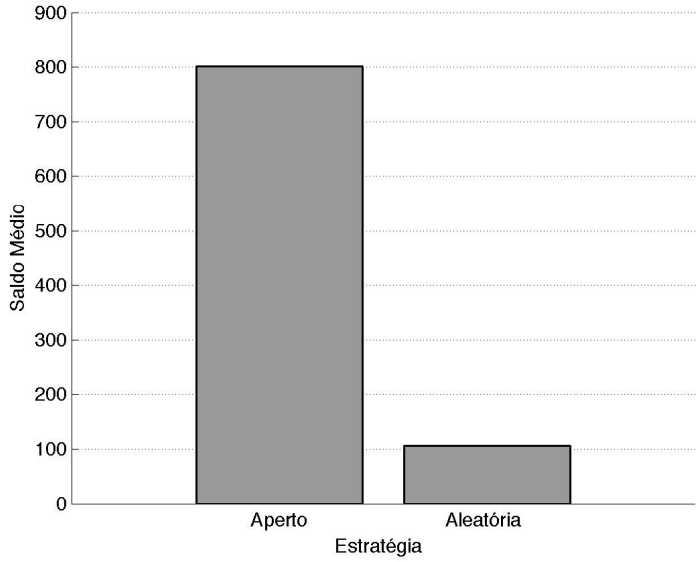

Figura 6.8: Saldo médio final, por tablet participante em cada rodada de experimento, para ambas as estratégias do aperto e aleatória

Assim, a partir das informações apresentadas, podemos afirmar que a utilização da estratégia do aperto permite um melhor uso da rede em termos de número de saltos e saldo médio por tablet. Ao fazer um melhor uso da rede, em termo de número de saltos, a estratégia evita a ocupação desnecessária da rede por um período maior que o período realmente necessário para a transmissão e, consequentemente, reduz o atraso nas transmissões.

A estratégia se mostrou falha em relação à robustez das transmissões, pois falhas de transmissão que poderiam ser evitadas, comumente acontecem devido à estratégia não avaliar a qualidade do enlace entre os tablets participantes antes de realizar um repasse de pacote.

Capítulo 7

Conclusões

Este trabalho apresentou uma avaliação de desempenho comparativa de duas estratégias de escoamento de tráfego de redes celulares para redes oportunistas do tipo *ad hoc*, que baseiam-se no uso de leilões recursivos para a definição do repasse do pacote até o destino final. Particularmente, este trabalho reproduziu o ambiente de experimentação real, utilizado durante a competição MANIAC Challenge em 2013, a partir do uso da implantação do código disponível publicamente para avaliação de desempenho da "estratégia do aperto". Diferentemente da competição, o objetivo deste trabalho foi avaliar o desempenho do escoamento quando todos os nós da rede utilizam a mesma estratégia de escoamento. Ou seja, todos eles utilizam as mesmas funções para participação dos leilões, definição de valores para leilão de pacotes, e como decidem o ganhador de um leilão. Para entender o desempenho desta estratégia específica, uma segunda estratégia foi utilizada na qual os valores das ofertas anunciadas pelos participantes são valores aleatórios uniformemente distribuídos. No entanto, nesta estratégia simplificada, o vencedor do leilão é sempre o nó que apresenta o menor valor. Assim, comparamos as estratégias citadas em termos de taxa de sucesso de transmissão, ocorrência de número de saltos para as transmissões realizadas com sucesso, taxa de sucesso de transmissão para diferentes limites de saltos e saldo médio final, por tablet participante em cada rodada de experimento, para ambas as estratégias estudadas.

Os resultados obtidos com a realização dos experimentos mostraram que, para a topologia imposta, a taxa média sucesso de transmissão entre a estratégia aleatória e a estretégia do aperto permaneceram praticamente iguais. Isso ocoreu pois o limite de saltos imposto para as simulações ultrapassa o limite de dispositivos móveis utilizados no ambiente, isso permite que um pacote fique passando de um tablet para outro até encontrar algum que esteja conectado ao destino final. Por outro lado, a estratégia do aperto apresentou um melhor desempenho em relação ao número de saltos até o destino final, enquanto que a estratégia do aperto realizou aproximadamente 77% das transmissões utilizando apenas 2 saltos, ou seja, utilizando apenas um tablet da rede, a estratégia aleatória realizou menos de 15% de suas transmissões utilizando a mesma quantidade de saltos. Assim, a estratégia do aperto se mostra mais eficiente quando há um limite de saltos imposto para a transmissão, de modo que o pacote não possa ficar passando de tablet em tablet “procurando” o destino final.

Como a estratégia aleatória pode gerar saldo negativo para um tablet mesmo que a transmissão ocorra com sucesso, a estratégia do aperto se mostrou bastante eficiente quando avaliada a média geral de pontos por tablet. Nesse aspecto, a estratégia se mostrou 5 vezes melhor pois, para toda transmissão bem sucedida, todos os tablets participantes recebem valores positivos por nunca oferecerem um valor de oferta abaixo do valor e multa e por gerar o leilão seguinte pagando no máximo 90% do valor acertado com o nó anterior.

Quando utilizado esquema de leilões de pacotes para definição do repasse de mensagens entre dispositivos móveis, a utilização de estratégias que garantam um melhor aproveitamento da rede se mostra necessária em muitos aspectos. O primeiro deles é a recompensa justa pela participação no bom funcionamento da rede, o valor pago deve representar o quanto aquela contribuição significou para o funcionamento geral da rede. O segundo deles é a possibilidade de avaliação geral da rede por parte dos dispositivos móveis para definição de melhores caminhos até o destino final. Nesse ponto, a estratégia se mostrou realmente eficiente, por tentar sempre utilizar o melhor caminho com as melhores ofertas até o destino final.

Infelizmente, o ambiente utilizado impossibilitou a realização de experimentos capazes de avaliar a estratégia do aperto de modo mais profundo. Seria necessário um ambiente maior que permitisse a instalação de uma maior quantidade de roteadores de backbone e possibilitasse uma maior quantidade de saltos entre os dispositivos. Mesmo tomando medidas para reduzir ao máximo o raio de transmissão dos dispositivos, grande parte das transmissões ocorreram com apenas 2 saltos.

A ocupação dos canais de rede representa um grande problema para esse tipo de aplicação, pois ao utilizar todo o prédio para a realização dos experimentos, a rede sofre interferência de vários pontos de acesso. Como a potência de transmissão é reduzida de modo a permitir um maior número de saltos, a rede se torna mais propensa à falhas de transmissão decorrentes dos sinais provenientes dos outros pontos de acesso próximos, que geralmente possuem potência de transmissão muito superior a 8dBm.

7.1 Trabalhos Futuros

A partir da contribuição do trabalho apresentado, diversas linhas de estudo podem ser exploradas e diversas melhorias podem ser feitas na própria estratégia estudada para melhorar o seu desempenho. Melhorias em relação à taxa de transmissão, atraso, mobilidade e mudança de parâmetros utilizados são alguns dos pontos que podem ser explorados, mas muitos outros aspectos podem ser estudados para tornar o repasse de informações entre dispositivos móveis atrativo para os usuários e operadoras.

Durante a competição realizada na Alemanha, diferentes estratégias eram utilizadas pelas equipes participantes, e não era possível saber o funcionamento da estratégia alheia para identificar o melhor modo de ação. No trabalho desenvolvido, a realização dos testes envolvia apenas uma estratégia, ou a estratégia do aperto ou a estratégia aleatória, mantendo a rede homogênea, esse tipo de abordagem permite que o comportamento do nó adjacente possa ser previsto. O estudo em

redes herogêngeas, onde há o uso de mais de uma estratégia simultaneamente, torna a competição pelos pacotes imprevisível, pois é complicado determinar o comportamento de outras estratégias sem conhecimento prévio de seu funcionamento. Utilizando esse tipo de abordagem, é possível que uma análise da contribuição da estratégia para o funcionamento geral da rede possa ser feito e, além disso, é possível avaliar o grau de participação da estratégia no repasse geral de pacotes da rede.

A taxa de transmissão utilizada durante os experimentos não representa uma transmissão de informação real. A escolha da transmissão de apenas um pacote a cada 15 segundos levou em consideração dois aspectos principais: o foco principal do estudo, que era avaliar o caminho percorrido pelos pacotes até o caminho final da rede (e não o desempenho da rede em altas taxas de transmissão) e o fato da aplicação utilizada não ser capaz de lidar com múltiplos leilões simultaneamente. De fato, apesar da aplicação ser capaz de enviar ofertas para múltiplas RFBs, ela não é capaz de efetuar múltiplos leilões simultaneamente, e nem de responder a uma RFB quando está efetuando um leilão. Para que o estudo se aproxime do encontrado nas transmissões reais, o sistema deve ser avaliado em situações de altas taxas de transmissão, onde todos os elementos de rede são capazes de lidar com múltiplas transmissões simultaneamente.

O estudo feito não analisou o impacto da variação dos fatores k_1 e k_2 da função de prefêrencia para o repasse de informações. Durante todos os testes realizados, os valores permaneceram em $k_1 = 2$ e $k_2 = 3$. Para um estudo mais aprofundado dessa estratégia, a variação desse fator poderia representar uma variação na vazão média da rede, tendo em vista que tal variação representa uma mudança de comportamento, frente aos valores recebidos após uma RFB.

Para a definição dos valores na realização de uma nova RFB, a estratégia do aperto utiliza porcentagens fixas dos valores recebidos na RFB anterior. Sempre que um nó precisa realizar uma nova RFB o valor máximo de oferta é definido como 60% do valor decidido com o nó anterior, e o valor de multa é sempre 90% do valor de multa anterior, como pode ser visto nas Equações 4.6. Um estudo capaz de identificar o melhor valor para esses parâmetros permitiria que o ganho individual por transmissão bem sucedida pudesse ser otimizado, além disso, permitiria que o ganho de cada dispositivo após uma transmissão bem sucedida representasse fielmente a importância desse dispositivo em relação a sua posição geográfica.

Grande parte das falhas de transmissão utilizando a estratégia do aperto ocorreram, unicamente, devido a erros de canal. Ao tentar otimizar ao máximo a transmissão da informação, a estratégia não leva em consideração a qualidade do enlace utilizado e, em muitos casos, tenta transmitir a informação para um dispositivo que está muito longe, e que dificilmente é capaz de receber o que está sendo transmitido. É importante lembrar que o ambiente utilizado para as transmissões possui uma grande quantidade de redes Wi-Fi disponíveis e, consequentemente, um elevado nível de interferência, sendo esse, um dos fatores responsáveis pelas falhas na transmissão. Para tentar garantir um aumento na taxa de transmissão com sucesso, é interessante implementar na própria estratégia um limiar de qualidade que define o quão confiável/robusta é a transmissão neste caminho, em termos de estado de canal, essa avaliação poderia ser feita juntamente com a definição de valores de oferta para RFBs e na definição do melhor destino do pacote no cálculo da

função de preferência.

Apesar da estratégia implementada e a arquitetura utilizada permitirem que haja mobilidade dos nós da rede, o estudo do impacto da mobilidade não pôde ser realizada a tempo. Esse tipo de estudo é importante para avaliar o comportamento da estratégia quando a topologia é constantemente modificada. É importante, também, para evitar que o mesmo caminho seja utilizado na maior parte do tempo, como aconteceu nos testes realizados.

Por questão de disponibilidade de espaço e equipamentos, todos os experimentos realizados foram feitos utilizando apenas 2 roteadores de backbone e 9 tablets. Seria interessante que a mesma avaliação pudesse ser feita utilizando uma maior quantidade de dispositivos na rede. Uma maior quantidade de roteadores de backbone evitaria a situação encontrada em que apenas 3 tablets participavam majoritariamente das transmissões, tendo em vista que os caminhos percorridos dependiam mais da localização dos dos roteadores de backbone de origem e destino. Além disso, uma maior concentração de tablets acarretaria maiores competições por um mesmo pacote, e uma combinação maior de possíveis caminhos que um pacote poderia percorrer.

Para avaliar o desempenho da rede em situações extremas, com grandes quantidades de dispositivos móveis e grandes quantidades de roteadores de backbone, simulações computacionais devem ser feitas explorando esse tipo de rede. A realização de simulações computacionais, além de reduzir os custos com equipamentos por necessitar apenas de um computador capaz de processar todas as informações, permite que situações específicas possam ser estudadas, situações que sejam difíceis de serem reproduzidas em ambiente real mas que possam representar problemas sérios no desempenho da rede. Além disso, simulações computacionais permitem que testes longos possam ser feitos sem que haja a necessidade de alguém gerenciando todos os equipamentos.

Apesar do esquema de leilões de pacotes representar uma solução para o escoamento de informações pelo melhor caminho, a realização de leilões por parte dos dispositivos móveis representa um atraso na transmissão das informações. No caso estudado, todo leilão realizado durava 3 segundos, então para o caso de 5 dispositivos móveis participantes de uma transmissão, o tempo mínimo para que a informação pudesse ser transmitida com sucesso é de 15 segundos. Esse tempo representa um atraso muito grande para qualquer tipo de aplicação web, e impossibilita a execução de muitas dessas aplicações, principalmente aplicações de transmissão de áudio e/ou vídeo em tempo real. Para um estudo mais aprofundado desse tipo de repasse de informações, a questão de leilões poderia ter um tempo reduzido ou mesmo ser extinta. A tomada de decisões do caminho a ser percorrido poderia ser definido pelos próprios roteadores de backbone na rede, tornando os dispositivos móveis participantes apenas repassadores de informações, não sendo capazes de definirem nenhum tipo de rota. Utilizando essa abordagem de definição de rotas a partir dos roteadores de backbones, a definição da melhor rota na rede poderia levar em consideração a quantidade de vezes que um determinado nó já tenha contribuído para a rede. Isto poderia ser utilizado para a definição de estratégias que considerassem uma melhor distribuição de participações, buscando uma melhor distribuição dos pontos na rede.

A definição de rotas a partir dos roteadores de backbone poderia significar um menor risco de dispositivos móveis mal intencionados na rede, pois nenhum dispositivo seria capaz de definir

rotas e, caso ainda houvesse algum dispositivo móvel atrapalhando o bom funcionamento da rede, os roteadores de backbone seriam capazes de excluí-lo facilmente das opções da caminhos a serem tomados.

Ainda sobre a ideia de utilizar os roteadores de backbone como pontos ativos da rede e os dispositivos móveis como pontos passivos, essa estratégia poderia representar uma redução de processamento dos elementos da rede, pois a retirada da obrigação de cálculo da rede e definição de rotas por parte dos dispositivos móveis representaria uma menor exigência de processamento dos aparelhos e, consequentemente, um melhor aproveitamento das baterias, reduzindo o impacto da contribuição no repasse de informações na vida útil delas.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] CISCO Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014-2019 White Paper. Feb 2015. Disponível em: <http://goo.gl/pzfCse>. Acesso em: 14 Jun. 2015.

[2] REIS, R. *Final iguala recorde, e Copa-2014 tem segunda maior média de público da história.* Jul 2014. Disponível em: <http://goo.gl/ZH7LPV>. Acesso em: 14 Jun. 2015.

[3] LATAM: World Cup network use broke records; Oi/PT merger hit by funding problems. Disponível em: <http://goo.gl/M0Sl03>. Acesso em: 14 Jun. 2015.

[4] REBECCHI, F.; AMORIM, M. Dias de; CONAN, V.; PASSARELLA, A.; BRUNO, R.; CONTI, M. Data offloading techniques in cellular networks: A survey. IEEE, 2014.

[5] CROW, B. P.; WIDJAJA, I.; KIM, J. G.; SAKAI, P. t. Ieee 802.11 wireless local area networks. *IEEE Communications Magazine*, v. 35, n. 9, p. 116–126, set. 1997.

[6] VASSIS, D.; KORMENTZAS, G.; ROUSKAS, A.; MAGLOGIANNIS, I. The ieee 802.11 g standard for high data rate wlans. *Network, IEEE*, IEEE, v. 19, n. 3, p. 21–26, 2005.

[7] PAUL, T.; OGUNFUNMI, T. Wireless lan comes of age: Understanding the ieee 802.11n amendment. *IEEE Circuits and Systems Magazine*, v. 8, 2008.

[8] WANG, Y.; LI, F. Vehicular ad hoc networks. In: *Guide to wireless ad hoc networks.* [S.l.]: Springer, 2009. p. 503–525.

[9] MOLISCH, A. F. *Wireless Communications.* 2. ed. [S.l.]: John Wiley & Sons Ltd, 2011.

[10] PERKINS, C. E.; ROYER, E. M. Ad hoc on-demand distance vector routing. In: *In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99).* [S.l.: s.n.], 1999. p. 90–100.

[11] JOHNSON, D. B.; MALTZ, D. A. Dynamic source routing in ad hoc wireless networks. In: *Mobile computing.* [S.l.]: Springer, 1996. p. 153–181.

[12] PARK, V. D.; CORSON, M. S. A highly adaptive distributed routing algorithm for mobile wireless networks. In: IEEE. *INFOCOM'97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE.* [S.l.], 1997. v. 3, p. 1405–1413.

[13] JACQUET, P.; MUHLETHALER, P.; CLAUSEN, T.; LAOUITI, A.; QAYYUM, A.; VIENNT, L. Optimized link state routing protocol for ad hoc networks. In: *In Proc. IEEE INMIC 01. Technology for the 21st Century.* [S.l.: s.n.], 2001. p. 62–68.

[14] GARCIA-LUNA-ACEVES, J. J.; SPOHN, M. Source-tree routing in wireless networks. In: IEEE. *Network Protocols, 1999.(ICNP'99) Proceedings. Seventh International Conference on.* [S.l.], 1999. p. 273–282.

[15] OGIER, R. G. Efficient routing protocols for packet-radio networks based on tree sharing. In: IEEE. *Mobile Multimedia Communications, 1999.(MoMuC'99) 1999 IEEE International Workshop on.* [S.l.], 1999. p. 104–113.

[16] PERKINS, C. E.; BHAGWAT, P. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In: ACM. *ACM SIGCOMM computer communication review.* [S.l.], 1994. v. 24, n. 4, p. 234–244.

[17] A Evolução da plataforma Android. Disponível em: <https://www.android.com/history/>. Acesso em: 9 Jun. 2015.

[18] A Distribuição do uso das diferentes versões do sistema operacional Android. Disponível em: <https://goo.gl/1FIDwX>. Acesso em: 2 Jun. 2015.

[19] A PÃągina Web da competiÃğÃčo Maniac Challenge de 2013. Disponível em: <http://2013.maniacchallenge.org/>. Acesso em: 14 Jun. 2015.

[20] AS Regras gerais e arquitetura geral da rede da Competição MANIAC de 2013. Disponível em: <http://2013.maniacchallenge.org/rules-setup/>. Acesso em: 15 Jun. 2015.

[21] REPOSITÓRIO com todo o todo o código fonte disponibilizado da competição Maniac. Disponível em: <https://github.com/maniacchallenge>. Acesso em: 14 Jun. 2015.

[22] A Linguagem de programação GO. Disponível em: <https://golang.org/>. Acesso em: 14 Jun. 2015.

[23] O Banco de Dados MongoDB. Disponível em: <https://www.mongodb.org/>. Acesso em: 14 Jun. 2015.

[24] O Repositório do GitHub contendo todo o código fonte da aplicação Manet Manager. Disponível em: <https://github.com/ProjectSPAN/android-manet-manager>. Acesso em: 15 Jun. 2015.

[25] KALEIJAIYE, G. B. T.; RONDINA, J. A. S. R.; ALBUQUERQUE, L. V. V.; PEREIRA, T. L.; CAMPOS, L. F. O.; MELO, R. A. S.; MASCARENHAS, D. S.; CARVALHO, M. M. *Mobile Offloading in Wireless Ad Hoc Networks.* Aug 2013. Disponível em: <https://goo.gl/R5EZvO>. Acesso em: 14 Jun. 2015.

[26] A Aplicação Wifi Analyzer utilizada para verificação de ocupação de canais. Disponível em: <https://goo.gl/amHN5V>. Acesso em: 16 Jun. 2015.

[27] O CyanogenMod, versão modificada do sistema operacioal Android. Disponível em: <http://www.cyanogenmod.org>. Acesso em: 18 Jun. 2015.

ANEXOS

I. AMBIENTE DE REALIZAÇÃO DOS EXPERIMENTOS

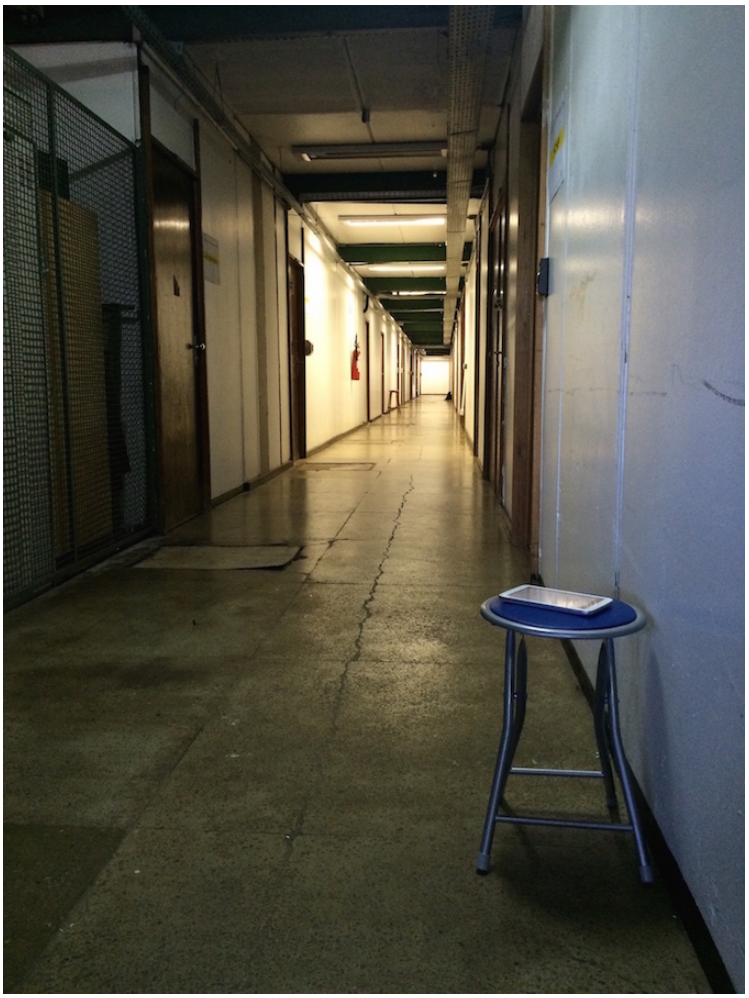

Figura I.1: Área inferior do prédio SG11 com os tablets posicionados durante a realização dos experimentos

Figura I.2: Área superior do prédio SG11 utilizada para a realização dos experimentos

II. EQUIPAMENTOS UTILIZADOS PARA REALIZAÇÃO DOS EXPERIMENTOS

Figura II.1: Computadores utilizados como backbones da rede e tablets utilizados para a instalação da aplicação ManiacLib durante a realização dos Experimentos