UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

RÔMULO PINTO DE ALBUQUERQUE

FHDRA: UMA PROPOSTA PARA REDUÇÃO DA LATÊNCIA DE HANDOFF EM REDES SEM FIO DE MÚLTIPLOS SALTOS

BELÉM-PA

Novembro / 2013

RÔMULO PINTO DE ALBUQUERQUE

FHDRA: UMA PROPOSTA PARA REDUÇÃO DA LATÊNCIA DE HANDOFF EM REDES SEM FIO DE MÚLTIPLOS SALTOS

Dissertação submetida à banca examinadora do Programa de Pós-Graduação em Ciência da Computação da UFPA para obtenção do grau de Mestre em Ciência da Computação

Orientador: Dr. Antônio Jorge Gomes Abelém

BELÉM-PA

Novembro / 2013

RÔMULO PINTO DE ALBUQUERQUE

FHDRA: UMA PROPOSTA PARA REDUÇÃO DA LATÊNCIA DE HANDOFF EM REDES SEM FIO DE MÚLTIPLOS SALTOS

Dissertação submetida à banca examinadora do Programa de Pós-Graduação em Ciência da Computação da UFPA para obtenção do grau de Mestre em Ciência da Computação

Aprovada em: __/__/____

BANCA EXAMINADORA

Prof. Dr. Antônio Jorge Gomes Abelém
Universidade Federal do Pará
Orientador

Prof. Dr. Agostinho Luiz da Silva Castro
Universidade Federal do Pará / FCT

Prof. Dr. Raimundo Viégas Junior
Universidade Federal do Pará / FACOMP

À minha esposa e à minha filha, Juliana e Ágata.

Agradecimentos

Inicialmente a Deus por ter me permitido chegar até aqui.

À minha esposa, por ter me dado um sentido maior para avançar e chegar até aqui, que foi a nossa filha. Pelo amor, incentivo, além é claro, de toda compreensão nos momentos de ausência.

A todos os meus familiares, tios, tias, primos e primas, mas em especial aos meus avós que me educaram e me orientaram, fornecendo condições favoráveis para trilhar este caminho.

Ao professor Antônio Abelém, meu orientador, por ter acreditado em mim, confiando essa laboriosa tarefa.

Ao GERCOM, não somente pela ajuda acadêmica, mas também pelas amizades construídas.

Ao apoio da FAPESPA, que me suportou financeiramente, permitindo que eu pudesse me dedicar melhor aos estudos.

Resumo

Resumo da Dissertação apresentada à UFPA como parte dos requisitos necessários para obtenção do grau de Mestre em Ciência da Computação.

FHDRA: Uma Proposta para Redução da Latência de Handoff em Redes Sem Fio de Múltiplos Saltos

Orientador: Dr. Antônio Jorge Gomes Abelém
Palavras-chave: Mobilidade; Redes sem fio de múltiplos saltos; Handoff; DHCP; Agente DHCP relay

As redes sem fio se consolidaram como um dos principais meios de comunicação da atualidade e são uma alternativa viável de acesso a Internet para a última milha. Uma das suas principais linhas de pesquisa é o estudo da mobilidade. Sempre houve um expressivo esforço em prol de soluções de mobilidade para as redes sem fio mais tradicionais, tais como redes celulares e as redes IEEE 802.11. Outro tipo de rede sem fio que tem se destacado mais recentemente são as de múltiplos saltos. Porém a questão da mobilidade neste tipo de rede não é uma simples extensão das redes sem fio tradicionais. Por isso são necessárias soluções de mobilidade específicas que atendam aos requisitos das redes sem fio de múltiplos saltos.

O DHCP, por exemplo, embora seja amplamente utilizado em redes sem fio, é um protocolo que foi projetado para redes cabeadas e portanto não atende adequadamente cenários de alta mobilidade onde os clientes móveis necessitam de rápida configuração e que mantenham suas conexões ativas após o handoff.

Com o objetivo de minimizar a latência do processo de handoff em redes sem fio de múltiplos saltos, o presente trabalho propõe uma adaptação ao DHCP. A proposta intitulada FHDRA (Fast Handoff DHCP Relay Agent) adiciona inteligência ao agente DHCP relay, tornando-o capaz de acelerar o processo de aquisição de IP durante o handoff. Em testes realizados em uma rede sem fio de múltiplos saltos, a proposta FHDRA obteve

um desempenho superior ao DHCP tradicional, demonstrando ser indicada para suportar aplicações com restrição de tempo.

Abstract

Abstract of Dissertation presented to UFPA as a partial fulfillment of the requirements for the degree of Master in Computer Science.

FHDRA: A Proposal to Reduce Handoff Latency in Wireless Multihop Networks

Advisor: Dr. Antônio Jorge Gomes Abelém
Co-advisor:
Key words: Mobility; Wireless multihop networks; Handoff; DHCP; DHCP relay agent.

Wireless networks have become a widely deployed medium and a great alternative for last mile Internet access. Mobility has been a very explored research area from wireless network. Mobility solutions have always had much effort towards traditional wireless networks such as cellular and IEEE 802.11. Recently, a especial kind of wireless network has received attention by multihop communication attribute. However, mobility in wireless multihop networks is not a simple extension from traditional wireless networks. Therefore, to fulfill wireless multihop networks requirements, specific solution must be developed.

Even though DHCP is widely used in wireless network, this protocol has been designed for wired networks, that is why it does not fit high mobility scenarios where mobile clients need fast configuration and need to maintain alive connections after handoff.

In order to mitigate the latency of handoff process in wireless multihop networks, this thesis proposes an adaptation of DHCP. The proposal entitled FHDRA (Fast Handoff DHCP Relay Agent) accelerate DHCP IP acquisition during handoff by adding capabilities to DHCP relay agents to understand handoff process. During tests in a wireless multihop network, FHDRA proposal obtained lower delays comparing to traditional DHCP protocol which demonstrate FHDRA has conditions to support time constrained applications over handoff.

Sumário

Lista de Abreviaturas

WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
MANETs	Mobile Ad Hoc Networks
WMNs	Wireless Mesh Networks
WSNs	Wireless Sensor Networks
IEEE	Institute of Electrical and Electronics Enginieers
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
QoS	Quality of Service
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
RFCs	Request For Comments
NS-3	Network Simulator
FHDRA	Fast Handoff DHCP Relay Agent
VoIP	Voice over IP
RSSI	Received Signal Strenght Indicator
AP	Access Point
WEP	Wired Equivalent Privacy
DS	Distribution System
IAPP	Inter Access Point Protocol
WLANs	Wireless Local Area Networks
MAC	Media Access Control
UDP	User Datagram Protocol
DRCP	Dynamic Registration and Configuration Protocol
IETF	International Enginnering Task Force
FHO	Fast Handoff Optimization

RTT	Round Trip Time
SDN	Software Defined Network

Lista de Figuras

Lista de Tabelas

CAPÍTULO 1

Introdução

1.1 Visão geral

As redes sem fio já se consolidaram como um dos principais meios de comunicação. O uso destas redes compreende um domínio que vai das redes pessoais (WPAN – *Wireless Personal Area Networks*) às redes de longa distância (WWAN – *Wireless Wide Area Networks*). Dentro desse contexto um tipo especial de rede sem fio se destaca pela capacidade de seus nós estabelecerem caminhos formados por nós intermediários através de enlaces sem fio. Esse tipo de rede é conhecida na literatura acadêmica como rede sem fio de múltiplos saltos e sua adoção reduz ou elimina a necessidade de infraestrutura cabeada, diminuindo os custos com implantação, sendo por isso frequentemente escolhida como alternativa viável para cobrir áreas de grande extensão e/ou difícil acesso.

As principais representantes das redes sem fio de múltiplos saltos são as MANETs (*Mobile Ad Hoc Networks*), WMNs (*Wireless Mesh Networks*) e WSNs (*Wireless Sensor Networks*). Segundo Akyildiz e Wang [1], as WMNs desempenharam um papel importante dentro da Internet de nova geração, pois possuem a capacidade de autoconfiguração, possibilitando fácil manutenção, poder de resiliência e aumento da área de cobertura através do enlace sem fio, sem o custo da infraestrutura cabeada. Por isso diversas tecnologias sem fio, tais como IEEE (*Institute of Electrical and Electronics Enginieers*) 802.11, IEEE 802.15 e IEEE 802.16, têm manifestado esforço para incluir o modo *mesh* em suas especificações.

O desenvolvimento das tecnologias sem fio contribuiu para o barateamento e popularização dos dispositivos móveis. Junto com o crescimento da Internet as redes sem fio se estabeleceram como rede de acesso à primeira milha, o que propiciou conectividade de diversos dispositivos a qualquer tempo e em qualquer lugar, culminando no que se denomina por ubiquidade. Dados recentes da ITU-T (*International Telecommunication*

Union - Telecommunication Standardization Sector) [2] revelam que houve um aumento global desde 2005 de 96% no número de assinaturas de celulares e que o número de assinaturas de celular está quase superando o número de habitantes no mundo. Nesse terreno fértil a mobilidade é uma área de pesquisa bastante explorada, e ainda repleta de desafios. Os autores Zhu e Wakikawa [3] oferecem uma rica pesquisa a respeito da mobilidade na Internet nas últimas décadas.

1.2 Motivação

Com o aumento do número de dispositivos móveis novas aplicações ganharam espaço nesse meio. Tablets, PDAs e *smart phones* oferecem interação com aplicativos de voz e vídeo através da Internet. Na outra ponta os usuários estão mais exigentes e os provedores de acesso, por sua vez, já chegaram a parametrizar os recursos da rede a fim de prover QoS (*Quality of Service*) para seus clientes.

Nesse contexto, a manutenção da latência e do *jitter* para aplicações sensíveis ao atraso pode ser um fator crítico. A transparência de mobilidade exige que durante o *handoff* os parâmetros da rede sejam mantidos e assim oferecer ao usuário a percepção de continuidade dos serviços correntes. Sabe-se, porém, que o processo de *handoff* causa uma latência que pode chegar a ordem dos segundos, fato que pode inviabilizar o uso de aplicações multimídia e tempo real. Segundo a norma G.114 [4], as aplicações de voz sobre IP podem tolerar atrasos de até 150 milissegundos, enquanto aquelas de tempo real podem ser afetadas por atrasos abaixo de 100 milissegundos. Logo, são necessários mecanismos que atenuem ao máximo os atrasos e perdas gerados durante o *handoff*.

Apesar de terem sido propostas muitas soluções para gerência de mobilidade como é o caso do bem conhecido Mobile IP [5], muitas redes sem fio adotam apenas o DHCP (*Dynamic Host Configuration Protocol*) [6]. É o caso, por exemplo, das redes sem fio locais de múltiplos saltos, frequentemente empregadas para aumentar a área de cobertura como alternativa às redes sem fio infraestruturadas. Nesse tipo de cenário, usa-se geralmente uma única sub-rede para atender todos os clientes e apenas um servidor DHCP para centralizar a alocação de endereços IP (*Internet Protocol*). Ou seja, o deslocamento dos clientes entre os roteadores gera apenas mobilidade intradomínio.

Mesmo quando os nós se movimentam dentro do mesmo domínio, o cliente DHCP será executado, desencadeando o processo de aquisição de IP. O processo de aquisição de IP realizado pelo DHCP é apontado por Hsieh e Kao [7] com uma das fases que mais consomem tempo durante todo o *handoff* e Forte [8] afirma que o tempo requerido para o DHCP realizar esse processo pode chegar a ordem de segundos. O tempo gasto no processo de aquisição de IP pode ser ainda mais custoso em redes sem fio de múltiplos saltos, já que o servidor DHCP pode estar vários saltos distante do cliente.

Além disso, o DHCP foi projetado para redes cabeadas, onde os hosts estão fixos e o tráfego de mensagens DHCP não compromete a capacidade da rede. Ainda assim, o DHCP é bastante empregado em redes sem fio, embora não atenda alguns requisitos para

esse cenário. McAuley [9] aponta alguns desses requisitos necessários ao DHCP para se adequar a novos cenários.

Apesar de muitos trabalhos terem sido propostos para redução da latência de *handoff*, poucos têm se ocupado com a redução do tempo de aquisição de IP realizado pelo DHCP. E durante a pesquisa não foram encontradas propostas para melhorar o tempo de aquisição do DHCP durante o processo de *handoff* que fossem aplicadas especificamente às redes sem fio de múltiplos saltos.

1.3 Objetivos

O presente trabalho propõe o *Fast Handoff DHCP Relay Agent* (FHDRA) que tem como objetivo reduzir a latência de aquisição de IP durante o *handoff* em redes sem fio de múltiplos saltos. Para isso foram feitas modificações no agente DHCP *relay*, agregando neste inteligência para reconhecer um evento de *handoff* e rapidamente efetuar a configuração do cliente móvel sem a necessidade de repassar a requisição para o servidor DHCP que pode estar situado a vários saltos de distância do cliente requisitante. A proposta foi implementada em ambiente real utilizando roteadores sem fio IEEE 802.11 com a distribuição Linux OpenWRT [10] e analisada em *testbed*.

Além do objetivo principal deste trabalho que é o projeto e implementação da proposta FHDRA, outros objetivos mais específicos foram alcançados, tais como:

- **Estudo sobre mobilidade:** foram analisadas as principais soluções para mobilidade em redes sem fio infraestruturadas e redes sem fio de múltiplos saltos; foram identificados os componentes do atraso gerados durante o processo de *handoff*;
- **Estudo sobre o DHCP:** foram analisadas as principais RFCs (*Request For Comments*) referentes ao DHCP, a partir desse estudo concluiu-se a viabilidade de modificação do protocolo para adequação da proposta;
- **Definição da proposta e implementação:** foram definidas a lógica de programação da proposta, assim como os componentes e estruturas envolvidos. Foi realizado um estudo para definir a implementação da proposta, onde analisou-se os principais simuladores gratuitos amplamente utilizados, NS-3 (*Network Simulator*) [11] e OMNET++[12], assim como a possibilidade de implementação em ambiente real. Com esse estudo concluiu-se a viabilidade de implementação da proposta em ambiente real através de uma solução de baixo custo, utilizando roteadores Wifi com o *software* Openwrt;
- **Estudo do Openwrt:** foram realizados estudos e testes sobre o *software* livre para dispositivos embarcados Openwrt com o objetivo de dominar esta solução para o desenvolvimento da proposta;
- **Validação da proposta:** foram realizados testes tanto em ambiente *indoor* quanto em *testbed outdoor* a fim de verificar o comportamento e desempenho da proposta.

1.4 Organização do Texto

Este trabalho está estruturado da seguinte forma: a seção 2 expõe o referencial teórico necessário para a visualização do problema e entendimento da proposta. Neste capítulo será realizada uma explanação sobre o processo de *handoff*, explicando os componentes de atraso nas camadas de enlace e de rede, assim como o atraso gerado durante o procedimento de aquisição de IP e seu impacto em redes sem fio de múltiplos saltos. Será realizado também um breve estudo sobre o DHCP, mostrando o funcionamento das máquinas de estado cliente e servidor, as mensagens trocadas por ambas, bem como o funcionamento dos agentes DHCP *relay*.

A seção 3 apresenta os trabalhos relacionados ao tema da dissertação. Os trabalhos abordados nesta seção são aqueles que tratam sobre o protocolo DHCP, o processo de aquisição de IP e processo de *handoff*.

Na seção 4 será apresentada a proposta FHDRA (*Fast Handoff DHCP Relay Agent*), onde será descrito em detalhes o seu funcionamento. Neste capítulo também será discutido a arquitetura de rede em que a proposta foi implantada.

A seção 5 apresenta a avaliação de desempenho da proposta. Neste capítulo será detalhado o cenário utilizado, bem como os testes efetuados. Serão detalhadas também as métricas utilizadas para avaliação da proposta e por fim será discutida a análise dos resultados.

A seção 6 apresenta uma síntese do trabalho desenvolvido. O autor expõe suas considerações e cita as contribuições do trabalho. Concluindo, o autor apresenta a sinalização de futuros trabalhos que possam aprimorar a proposta em tese.

CAPÍTULO 2

Referencial Teórico

2.1 Handoff e Aquisição de IP

Handoff é um dos elementos centrais dentro do estudo da mobilidade, sendo uma questão crítica para aplicações com restrição de tempo, tais como VoIP (*Voice over IP*), teleconferência, entre outras. O processo de *handoff* é caracterizado pela mudança de conectividade de um cliente móvel entre pontos de acesso diferentes. Quando os pontos de acesso estão no mesmo domínio, diz-se que ocorreu mobilidade intra domínio ou micro mobilidade. No caso de os pontos de acesso estarem em domínios distintos, a mobilidade é inter domínio também dita macro mobilidade. Em ambos os casos os clientes móveis que executam DHCP realizarão o processo de aquisição de IP.

2.1.1 Handoff da Camada de Enlace

O processo de *handoff* pode ser divido de acordo com as camadas de enlace e de rede da pilha de protocolos TCP/IP. No caso do padrão IEEE 802.11, de acordo com [13], o processo de *handoff* da camada de enlace compreende as fases descoberta e reautenticação como podem ser vistas na Figura 1.

Descoberta: Devido a capacidade de mobilidade dos clientes, a intensidade do sinal recebido, RSSI (*Received Signal Strenght Indicator*) do seu AP (*Access Point*) atualmente conectado, pode diminuir a ponto de ocorrer uma desassociação. É nesse momento que se inicia o processo de *handoff*, onde o cliente móvel tentará se conectar a outro AP dentro do seu raio de alcance. Para isso o cliente móvel executa o procedimento de *scan* que consiste na verificação de todos os canais disponíveis a fim de detectar a presença de APs vizinhos. O padrão IEEE 802.11 define dois tipos de *scan*, o passivo que indica que o cliente móvel deve apenas escutar temporariamente em cada um dos canais

a presença de *beacons* dos APs, assim como o *scan* ativo que permite que o cliente móvel envie quadros de pedido (*probe request*) solicitando associação com os APs encontrados.

Reautenticação: Após o *scan*, o cliente móvel poderá ter uma lista de APs oferecendo condição de conexão. O cliente móvel, entretanto, deverá se conectar com apenas um dos APs, cujo critério de prioridade pode variar, mas usualmente é o RSSI. A fase de reautenticação envolve dois serviços especificados pelo padrão IEEE 802.11 que são a **autenticação** e a **reassociação**, nesta sequência.

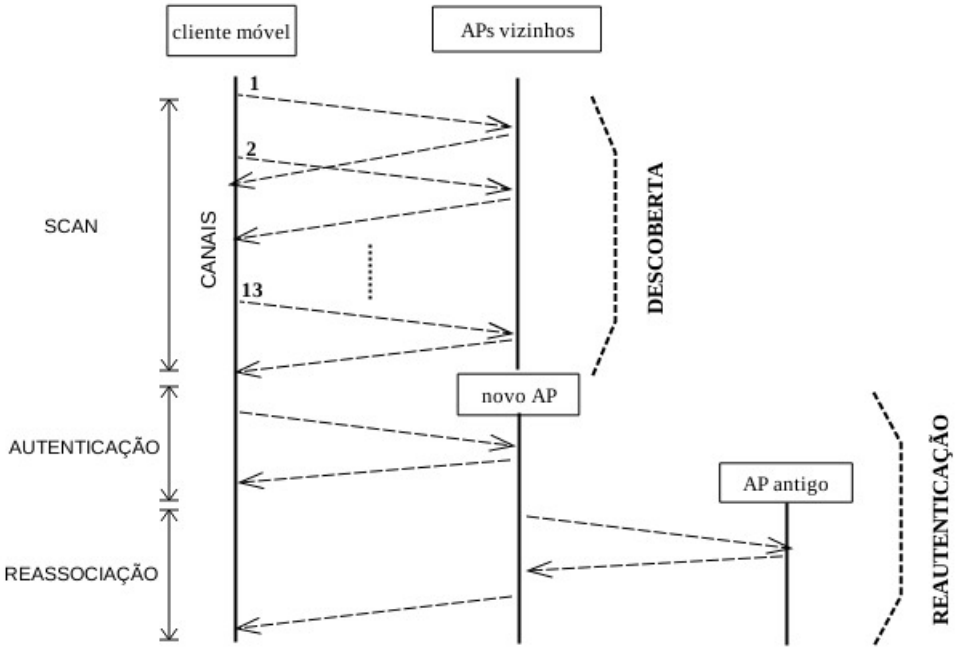

Figura 1: Handoff da camada de enlace IEEE 802.11 [13].

Mishra [13] cita ainda que o processo total de *handoff* da camada de enlace é influenciado por três componentes de atraso: **atraso de *probe***, **atraso de autenticação** e **atraso de reassociação**.

Atraso de *probe*: Este atraso é dependente do tipo de *scan* realizado pelo cliente móvel. No *scan* passivo, o atraso médio é dado em função do número de canais disponíveis e o parâmetro `MaxChannelTime` que indica o tempo máximo que a estação deve permanecer escutando em cada canal do espectro. Tomando como exemplo um intervalo de transmissão de *beacons* de 100ms, então, o atraso médio de uma rede IEEE 802.11b/g utilizando 13 canais seria de 1300ms. Já no *scan* ativo, o atraso médio é expresso em função do número de canais disponíveis mais os valores `MinChannelTime` e `MaxChannelTime` que representam, respectivamente, o tempo mínimo e máximo que o cliente móvel deve esperar por uma resposta (*probe response*) em cada um dos canais rastreados.

Atraso de autenticação: Assim como o atraso de *probe*, o atraso de autenticação não é um valor fixo e varia de acordo com o tipo de autenticação realizada. Três

tipos de autenticação podem ser encontradas. A mais simples é a do tipo aberta (*open-system*), na qual o AP selecionado aceita instantaneamente o cliente móvel após a fase de *scan*. O segundo tipo é a autenticação por chave pré-compartilhada, através do protocolo WEP (*Wired Equivalent Privacy*), onde cliente móvel e AP trocam quatro mensagens de acordo com [14].

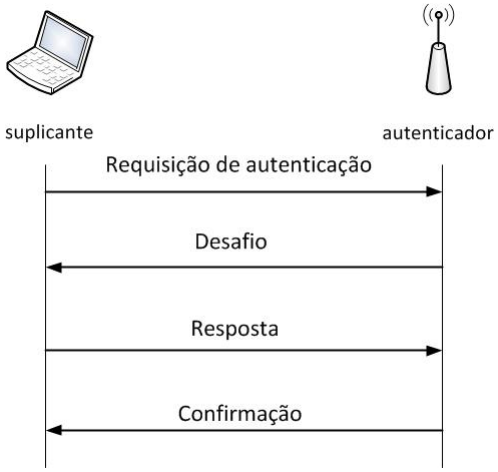

Figura 2: Processo de autenticação WEP.

O terceiro tipo de autenticação é o mais seguro, porém mais dispendioso em termos de atraso. Trata-se da emenda IEEE 802.11i [15] que implementa o *framework* 802.1X e visa corrigir as vulnerabilidades de segurança encontradas no protocolo WEP. Redes sem fio que adotam o padrão IEEE 802.11i podem utilizar um terceiro elemento, servidores de autenticação dedicados, o que aumenta ainda mais o número de mensagens trocadas e consequentemente o atraso gerado durante a fase de autenticação como pode ser visto na Figura 3.

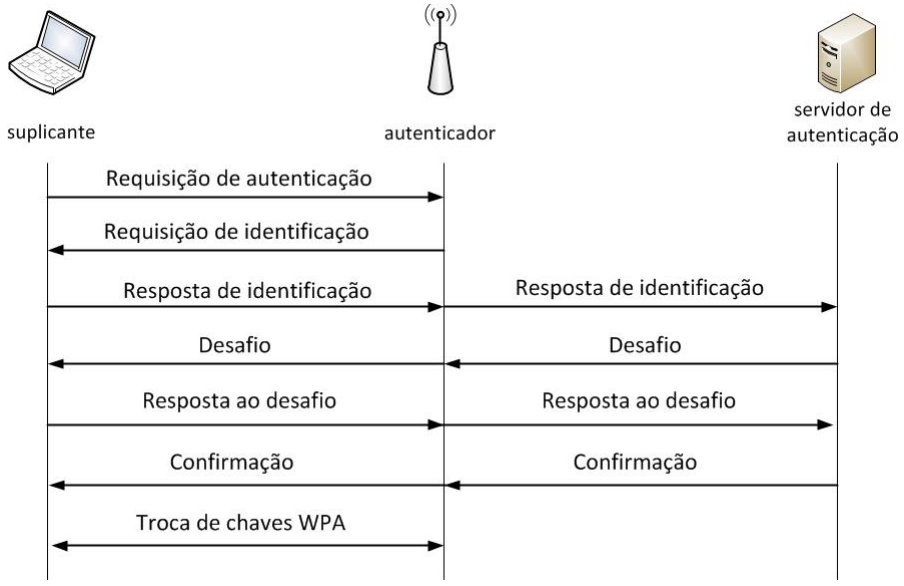

Figura 3: Processo de autenticação com protocolo IEEE 802.11i

Atraso de reassociação: Reassociação é um serviço provido pela especificação

IEEE 802.11 para que a rede mantenha a localização correta dos clientes móveis dentro do sistema de distribuição (DS – *Distribution System*). Sendo assim, após a desassociação do cliente móvel com seu antigo AP, o cliente móvel deverá solicitar a reassociação com o DS enviando uma mensagem de reassociação para o novo AP selecionado, contendo a informação do antigo AP. O novo AP deverá contatar o antigo AP através do protocolo IAPP (*Inter Access Point Protocol*) ou via um protocolo proprietário para verificar a veracidade da informação, e caso positivo, o novo AP deve informá-lo de que aquele cliente móvel agora possui nova associação. Além disso, o Antigo AP também pode encaminhar pacotes que foram armazenados durante o *handoff* do cliente móvel para o novo AP. A Figura 4 mostra o processo de reassociação em redes IEEE 802.11.

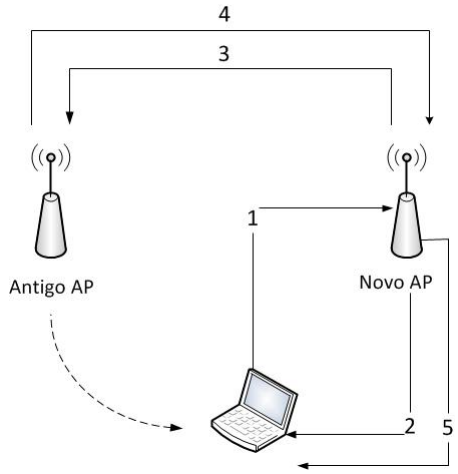

Figura 4: Processo de reassociação em redes IEEE 802.11

1. **Requisição de reassociação**: o cliente móvel envia um quadro para o novo AP contendo o pedido de reassociação e informações sobre a associação com o antigo AP.

2. **Resposta de reassociação**: o AP processa o pedido de reassociação e responde ao cliente móvel informando seu novo ID de associação.

3. **Contato com o antigo AP**: o novo AP faz contato com o antigo AP para finalizar a antiga associação e obter pacotes remanescentes do cliente móvel.

4. **Envio de pacotes remanescentes para o novo AP**: o antigo AP envia pacotes remanescentes do cliente móvel, caso exista.

5. **Envio de pacotes remanescentes para o cliente móvel**: o novo AP repassa os pacotes remanescentes que estavam no antigo AP para o cliente móvel.

2.1.2 Handoff da Camada de Rede

O processo de *handoff* da camada de enlace pode variar de algumas dezenas de milissegundos a centenas de milissegundos. Essa variação pode se dar pelos diversos fa-

tores citados na seção anterior, mas também devido as diferentes implementações entre os diversos fabricantes, visto que estes podem desenvolver mecanismos mais otimizados que acabam reduzindo esses atrasos, mas podem gerar também falta de interoperabilidade entre fabricantes diferentes. Pode-se notar através da Figura 1, como indicado nos resultado da pesquisa de Mishra [13], que o atraso dominante durante o *handoff* da camada de enlace é o atraso de *probe* na fase de *scan*, representando cerca de 90% de todo o processo.

Para que o cliente móvel possa estabelecer, manter ou reativar conexões com a rede, é necessário ainda que ele receba a configuração adequada para sua camada de rede, fase que caracteriza o *handoff* da camada de rede. Quando uma estação móvel se conecta a outra rede ou sub-rede, esta será auxiliada por um protocolo de configuração de rede que pode ser um protocolo de gerência de mobilidade, como o Mobile IP, por exemplo, ou em muitos casos o protocolo de configuração dinâmica de *host*, DHCP.

Durante o *handoff* da camada de rede podem ser executadas três funções básicas na ordem da sequência apresentada:

Configuração de rede: Fase em que a interface de rede do cliente móvel recebe a devida configuração dos parâmetros de rede através do processo de aquisição de IP.

Registro: Fase em que os clientes móveis são registrados pelo seu respectivo AP que informam a rede de origem sobre a nova associação.

Binding: Fase em que o antigo AP ou rede de origem localiza o cliente móvel dentro da nova rede ou novo AP e assim pode restabelecer as conexões do cliente móvel com seus nós correspondentes.

Estas funções fazem parte de uma heurística realizada normalmente por protocolos de gerência de mobilidade, como é o caso do protocolo Mobile IP. Entretanto, grande parte das WLANs (*Wireless Local Area Networks*) não utilizam protocolos de gerência de mobilidade. O protocolo comumente utilizado por estações clientes para configuração de rede é o DHCP. Neste caso, a única função executada por este protocolo é a configuração de rede através do processo de aquisição de IP.

De acordo com Hsieh e Kao [7], o procedimento de aquisição de IP realizado pelo DHCP é uma das fases que mais consome tempo durante todo o processo de *handoff*. O autor Hasan [16] conduziu um estudo acerca dos atrasos ocorridos durante as fases de *scan* e aquisição de IP em redes veiculares IEEE 802.11, onde foram realizados dois testes para verificar a latência despendida durante a fase de aquisição de IP. No primeiro teste, o atraso gerado pelo DHCP no processo de alocação de IP foi de 0.453 segundos, considerando que o teste foi realizado em rede *indoor* e o cliente móvel estava diretamente associado ao servidor DHCP sem a intervenção de múltiplos saltos. No segundo teste, que foi realizado em uma rede *outdoor*, o atraso gerado pelo DHCP foi de 2.870 segundos, considerando novamente que o cliente móvel estava interagindo diretamente com o servidor DHCP.

O *handoff* das camadas de enlace e de rede imprimem um atraso que pode variar conforme os fatores que já foram apontados. Porém o atraso de *handoff* da camada de

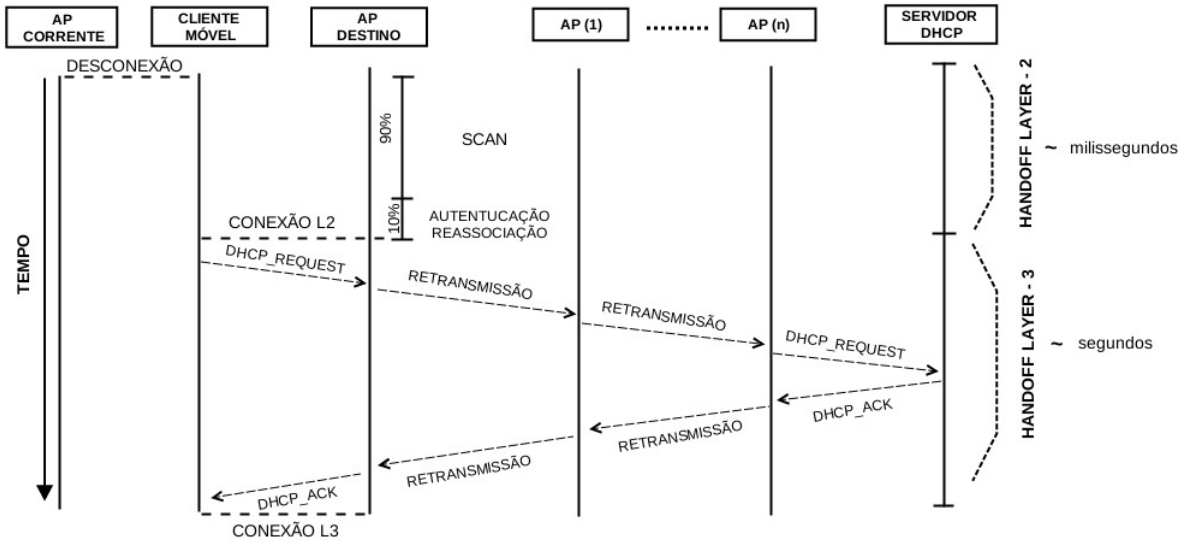

Figura 5: Handoff em redes sem fio de múltiplos saltos utilizando DHCP.

rede experimentado pelas redes sem fio de múltiplos saltos pode sofrer uma variação ainda maior. Xie e Wang [17] analisaram o processo de gerência de mobilidade em redes em malha sem fio e conduziram um experimento no simulador OPNET, onde empregaram o protocolo Mobile IP sobre uma rede em malha sem fio e descobriram que o atraso total de *handoff* aumenta significativamente conforme o número de saltos, sendo que o atraso de *handoff* da camada de enlace quase não sofre alteração, ao passo que o atraso de *handoff* da camada de rede aumenta substancialmente.

Esta observação se deve ao fato de que nas redes sem fio infraestruturadas a sobrecarga de sinalização gerada pelos protocolos de gerência de mobilidade recai sobre a rede cabeada, enquanto que nas redes em malha sem fio a comunicação ocorre através de múltiplos saltos pelo próprio enlace sem fio que possui maior taxa de erro e dispõe de menos recursos. Da mesma forma, o processo de aquisição de IP realizado pelo DHCP em redes sem fio de múltiplos saltos pode apresentar valores de atraso maiores se comparado com as redes sem fio infraestruturadas, já que o cliente pode estar a vários saltos distante do servidor DHCP como pode ser visto através da Figura 5.

2.2 DHCP e Agente DHCP Relay

DHCP [6] é um protocolo utilizado para prover configuração automática de parâmetros de rede a clientes que se conectem a uma rede TCP/IP. O DHCP é baseado no protocolo BOOTP [18] que foi concebido com a finalidade de configurar parâmetros de inicialização para estações clientes. Apesar de parecido e compatível com o BOOTP, o DCHP trouxe a capacidade de alocação dinâmica de endereçamento, o que permitiu o melhor uso dos endereços IPs. Outra diferença do DHCP em relação ao seu antecessor é que o DHCP provê mecanismo para que a estação cliente adquira todos os parâmetros de

configuração da camada IP necessários para operar na rede.

O DHCP manteve o formato das mensagens BOOTP para manter a compatibilidade já que o BOOTP era largamente utilizado. Entretanto o campo `BOOTP_VENDOR_EXTENSION` foi transformado no campo `DHCP_OPTIONS` para atender algumas necessidades específicas do DHCP. O campo `DHCP_OPTIONS` é variável e deve ter um tamanho de no mínimo 312 Bytes.

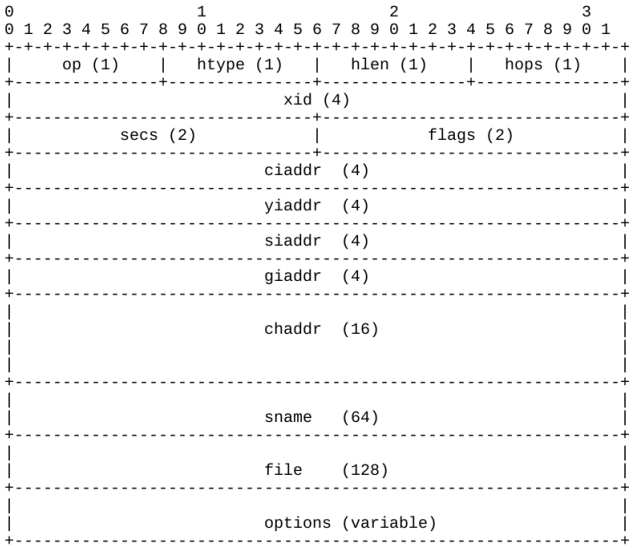

Figura 6: Formato da mensagem DHCP [6].

A Figura 6 ilustra o formato da mensagem DHCP e a Tabela 1 descreve cada um desses campos. Os números em parênteses indicam o tamanho, em Bytes, de cada campo. As mensagens DHCP podem ser de tamanhos variáveis, diferente das mensagens BOOTP, devido a mudança do campo `BOOTP_VENDOR_EXTENSION`, que possuía um tamanho fixo de 64 Bytes, pelo campo `DHCP_OPTIONS` que pode variar de tamanho. Essa característica evidencia que o protocolo DHCP tem um lista de opções mais rica do que o seu antecessor.

Tabela 1: Campos da mensagem DHCP.

CAMPO	TAMANHO	DESCRIÇÃO
op	1 Byte	Campo herdado do BOOTP que indica se a mensagem é do tipo *request* ou *replay*. O valor 1 indica que é uma mensagem do tipo `BOOTREQUEST` enquanto que o valor 2 indica uma mensagem do tipo `BOOTREPLAY`. Mensagens do tipo `BOOTREQUEST` são enviadas pelo cliente e mensagens do tipo `BOOTREPLAY` são enviadas pelo servidor DHCP. O tipo específico de mensagem é informado no subcampo `DHCP_MESSAGE_TYPE` no campo `DHCP_OPTIONS`.
htype	1 Byte	Este campo especifica o tipo de hardware utilizado pela rede local e tem a mesma semântica do campo HRD das mensagens ARP.

hlen	1 Byte	Este campo especifica o tamanho do endereço físico contido nas mensagens e tem a mesma semântica do campo HLN das mensagens ARP.
hops	1 Byte	Este campo é incrementado pelos agentes DHCP *relay* e serve para informar a quantidade destes ao longo do percurso entre cliente e servidor.
xid	4 Bytes	Este campo é sempre preenchido pelo cliente DHCP e serve como uma identificação única para cada transação entre cliente e servidor. Por exemplo, durante o processo de aquisição de IP são trocadas quatro mensagens, cada uma com o mesmo xid pois se referem a mesma transação.
secs	2 Bytes	Este campo indica o número de segundos transcorridos desde o início de uma requisição ou renovação de IP. Este campo pode ser utilizado por servidores DHCP para priorizar o atendimento quando houver solicitações de vários clientes.
flags	2 Bytes	Este campo é sempre preenchido pelo cliente DHCP nas mensagens *DHCPDISCOVER* ou *DHCPREQUEST* para informar sua capacidade de receber a resposta em *unicast* ou *broadcast* quando o cliente não possui endereço IP definido.
ciaddr	2 Bytes	Este campo representa o endereço IP do cliente requisitante e deve ser somente preenchido nos casos em que o cliente tem um endereço efetivamente válido, ou seja, nos casos em que o cliente estiver nos estados *BOUND*, *RENEW* OU *REBINDING*.
yaddr	4 Bytes	Este campo é preenchido pelo servidor para informar o endereço IP atribuído ao cliente requisitante.
siaddr	4 Bytes	Este campo é preenchido pelo servidor para informar seu próprio endereço IP.
giaddr	4 Bytes	Este campo indica o endereço IP dos agentes DHCP *relay*.
chaddr	16 Byets	Este campo indica o endereço de camada de enlace do cliente requisitante.
sname	64 Bytes	Este campo pode ser opcionalmente preenchido pelo servidor para informar seu próprio nome.
file	128 Bytes	Este campo indica o arquivo de *boot* que pode ser utilizado pelo cliente para configuração de seu sistema operacional.
option	Variável	Este campo pode conter uma coleção de parâmetros que são utilizados para o funcionamento adequado do protocolo. O campo `OPTIONS` possui o seguinte formato: `CODE`, `LEN` e `DATA`. Onde `CODE` representa o código da opção, `LEN` representa o tamanho dos dados da respectiva opção e `DATA` contem o valor da opção em hexadecimal.

Segundo a RFC 2131, o DHCP consiste em dois componentes: um mecanismo de alocação e gerência de endereços IP e um protocolo de comunicação cliente-servidor. O lado cliente executa as rotinas de requisição de informações. O protocolo implementado no lado servidor além de responder as requisições dos clientes também deve manter consistente a base de informações sobre os parâmetros da rede local e a faixa de IPs disponíveis.

O DHCP suporta três mecanismos de alocação de endereço: **dinâmico**, **manual** e **automático**. Dos três tipos, a alocação dinâmica é a que permite o reuso de IP, isto porque é estabelecido um período de tempo limite (*lease time*) em que o IP ficará alocado, podendo ser sempre renovado a pedido do cliente, mas que se tornará disponível na rede em caso contrário. Na alocação manual um administrador deve cadastrar no servidor DHCP os clientes que deverão receber endereços IP. Neste caso, cada cliente cadastrado tem seu endereço físico (MAC – *Media Access Control*) associado a um IP. Já na alocação automática o servidor DHCP realiza a atribuição de IP a um cliente por um período de tempo permanente.

A interação entre cliente e servidor DHCP ocorre através do protocolo de transporte UDP (*User Datagram Protocol*). O cliente DHCP utiliza a porta 68 para se comunicar com o servidor, este por sua vez utiliza a porta 67. O cliente deve usar o protocolo DHCP sempre que notar mudanças na configuração dos seus parâmetros de rede local, como por exemplo, quando o cliente inicializar ou reinicializar seu sistema ou quando houver desconexões com a rede local. Ao enviar uma mensagem para o servidor, o cliente deve informar o tamanho máximo da mensagem DHCP suportável e uma lista de parâmetros no campo `DHCP_OPTIONS`, contudo opções adicionais requeridas pelo cliente podem ser ignoradas pelo servidor.

Ao todo existem oito tipos de mensagens DHCP. Deste total apenas três são enviadas pelo servidor que são as mensagens `DHCPOFFER`, `DHCPACK` e `DHCPNACK`. A Tabela 2 informa o que cada uma dessas mensagens significa.

Tabela 2: Tipos de mensagem DHCP.

MENSAGEM	DESCRIÇÃO
DHCPDISCOVER	Mensagem enviada pelo cliente no processo inicial de alocação de endereço IP. É enviada em *broadcast*.
DHCPOFFER	Mensagem enviada pelo servidor em resposta a uma mensagem `DHCPDISCOVER`. Contém um endereço IP válido e uma lista de parâmetros de configuração, como máscara de rede, *gateway*, DNS, entre outros. Pode ser enviada em *unicast* ou *broadcast*, dependendo da condição contida na *flag broadcast* determinada pelo cliente.

DHCPREQUEST	É uma mensagem enviada pelo cliente e pode ser utilizada em três casos. Pode ser enviada para requisitar as informações oferecidas pelo servidor como reposta à mensagem `DHCPOFFER`. Pode ser enviada quando o cliente notar mudanças na configuração da rede local, por exemplo, após reinicialização do sistema ou desconexão, e desejar verificar a conformidade das informações previamente configuradas. Em terceira hipótese, esta mensagem pode ser enviada quando o cliente deseja renovar o período da *lease time* do endereço IP.
DHCPACK	Mensagem enviada pelo servidor para confirmar a requisição do cliente na mensagem `DHCPREQUEST` e finalizar o processo de configuração DHCP.
DHCPNACK	Mensagem enviada pelo servidor para negar a requisição do cliente.
DHCPINFORM	Mensagem enviada pelo cliente quando este já possui um endereço IP, mas deseja obter informação adicional sobre configuração de rede local.
DHCPRELEASE	Mensagem enviada pelo cliente para cancelar a *lease time* do seu endereço IP, permitindo que o servidor possa disponibilizar novamente tal endereço IP.
DHCPDECLINE	Mensagem enviada pelo cliente para negar um um endereço IP oferecido pelo servidor, indicando que o endereço IP já está em uso.

Como pode ser visto na Tabela 2 o cliente DHCP implementa a maioria das mensagens. A interação entre cliente e servidor pode ser observada através da máquina de estados implementada pelo cliente DHCP. Ao todo, o cliente DHCP pode assumir seis estados bem definidos que determinam o ciclo de vida do endereço IP. A Figura 7 ilustra a máquina de estados do cliente DHCP, onde os retângulos indicam os estados.

A máquina de estados apresentada na Figura 7 mostra, sumariamente, o comportamento do cliente DHCP interagindo com um único servidor DHCP. Assim que o cliente ingressa na rede, encontra-se no estado `INIT` e portanto envia uma mensagem `DHCPDISCOVER` em *broadcast* a fim de contatar com qualquer servidor disponível. O servidor tão logo receba a mensagem, responde com uma mensagem `DHCPOFFER`, contendo um endereço IP e uma lista de parâmetros de configuração. Ao receber a mensagem `DHCPOFFER` do servidor, o cliente passa para o estado `SELECTING` e envia uma mensagem `DHCPREQUEST` para requisitar o IP oferecido. Após receber a mensagem `DHCPREQUEST` do cliente, o servidor confirma o processo com uma mensagem `DHCPACK`. Quando o cliente recebe a mensagem `DHCPACK`, migrará para o estado `BOUND`, mas caso o cliente detecte que o IP esteja sendo usado, o cliente envia uma mensagem `DHCPDECLINE` e retorna para o estado `INIT`.

É no estado `BOUND` que o cliente pode permanecer a maior parte do tempo es-

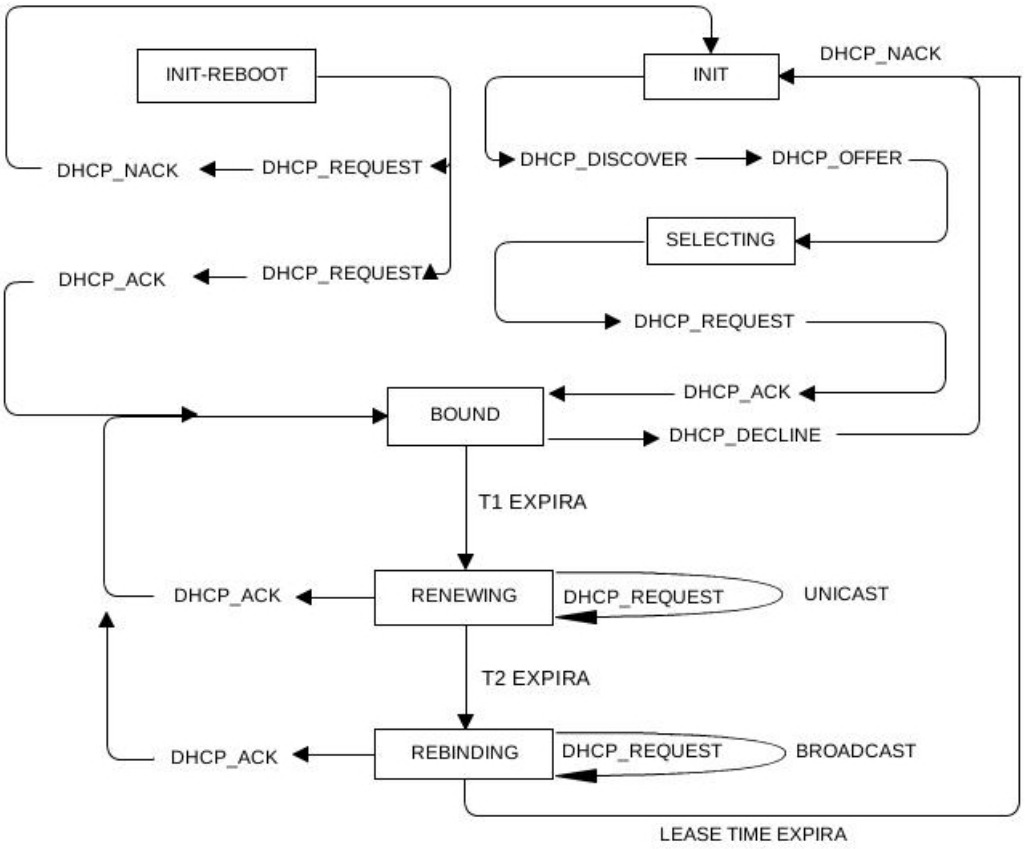

Figura 7: Máquina de estados do cliente DHCP [6].

tabelecido pela *lease time* do IP. A *lease time* é composta por dois períodos: T1 e T2. Esses dois contadores servem para indicar ao cliente a necessidade de renovar a *lease time*, isto é, o período de permanência com o IP. T1 e T2 representam, respectivamente, 50% e 87,5% da *lease time*. Assim que o cliente alcança T1, passará para o estado `RENEWING`, onde tentará contatar o servidor através de uma mensagem `DHCPREQUEST` enviada em *unicast*. Enquanto não receber reposta do servidor (`DHCPACK`), o cliente deverá permanecer neste estado até que ao final de T2, passará para o estado `REBINDING`, onde continuará tentando renovar a *lease time*, mas desta vez enviando mensagens em *broadcast*. Isso acontece porque se o cliente não conseguir renovar com o seu servidor de origem durante o estado `RENEWING`, então tentará com qualquer outro servidor DHCP que possa ouvi-lo.

Durante o período da *lease time*, porém, podem ocorrer outros eventos que induzem o cliente a mudar de estado. Um deles é, por exemplo, quando o cliente desliga ou reinicializa seu sistema. Após a inicialização do sistema, se o cliente possui uma *lease time* válida, ele recomeçará o processo de alocação de IP no estado `INIT-REBOOT`. Outra situação é se o cliente reconecta ou troca de rede, nesta caso ele recomeçará o processo a partir do estado `SELECTING`.

Um outro elemento importante dentro da arquitetura do protocolo é o agente DHCP *relay*. O funcionamento do DHCP tem escopo dentro de uma rede local (LAN ou

WLAN) por isso é necessário que o servidor DHCP esteja dentro do mesmo domínio de *broadcast* dos seus clientes, caso contrário, as mensagens `DHCPREQUEST` e `DHCPDISCOVER`, enviadas em *broadcast*, nunca atingiriam seu objetivo. Essa característica exigiria que cada sub-rede tivesse seu próprio servidor DHCP, o que eliminaria os benefícios de se ter um único servidor central para redes grandes.

Devido a essa questão, quando surgiu o protocolo BOOTP, foi pensado em uma entidade cuja principal finalidade seria o "roteamento" de mensagens DHCP entre cliente e servidor situados em redes locais distintas. Na especificação original do BOOTP essa entidade foi brevemente comentada, sendo intitulada de "BOOTP Forwarding Agent". Mais tarde, na RFC 1542 [19], a entidade foi melhor definida e passou a ser chamada "BOOTP Relay Agent". Mas somente na RFC 3046 [20] a entidade passou a ser chamada "DHCP Relay Agent" e foi encorporada ao conjunto de opções do DHCP.

A função do agente DHCP *relay* pode se confundir com a de um roteador IP, entretanto, o primeiro executa uma tarefa que o diferencia deste último. Enquanto um roteador realiza o repasse de datagramas IP entre redes diferentes, o agente DHCP *relay* não faz o roteamento propriamente dito. Ao invés disso, ele recebe a mensagem DHCP como se fosse um servidor e então gera uma nova mensagem DHCP com destino endereçado ao servidor DHCP. No sentido contrário o agente DHCP *relay* atua da mesma forma, recebendo a mensagem DHCP do servidor e gerando uma nova, endereçada ao cliente. Portanto, o agente DHCP *relay* atende somente as mensagens UDP nas portas 68 (cliente) e 67 (servidor). As demais mensagens que não se encaixam nesse padrão não serão tratadas pelo agente DHCP *relay*. Assim, com o uso dos agentes DHCP *relay*, as mensagens trocadas entre cliente e servidor podem ser endereçadas em *unicast*, evitando a replicação de mensagens.

CAPÍTULO 3

Trabalhos Relacionados

Muitos trabalhos têm sido realizados na tentativa de minimizar a latência gerada durante o processo de *handoff*. Um grande número destes se ocupa com a otimização do processo de *handoff* da camada de enlace em redes IEEE 802.11. Ou seja, tentam reduzir os atrasos das fases de descoberta e reautenticação. É o caso, por exemplo, dos trabalhos [21], [22] e [23] que utilizam abordagens diferentes para tratar o mecanismo de *scan*, buscando reduzir o período em que o cliente móvel realiza a busca por novos de pontos de acesso.

Existem também muitos trabalhos que abordam o processo de *handoff* da camada de rede denominado de *handoff layer* 3 ou *handoff* L3. Neste grupo estão trabalhos que tratam de questões como gerência de localização, roteamento e controle do fluxo de dados. Akyildiz [24] classificou as soluções de mobilidade da camada de rede em dois grupos: macro mobilidade e micro mobilidade. No primeiro grupo pode ser destacado o famoso Mobile IP [5], já no segundo grupo as principais soluções são HMIP [25], Cellular IP [26] e HAWAII [27].

Os trabalhos citados no parágrafo anterior são propostas que foram desenvolvidas voltadas para redes sem fio infraestruturadas. Segundo Xie e Wang [17] a gerência de mobilidade em redes sem fio de múltiplos saltos não é uma simples extensão das redes infraestruturadas, visto que neste último caso a gerência de mobilidade recai sobre rede cabeada enquanto nas redes *ad hoc* esse processo se dá por meio do enlace sem fio, cujos recursos são mais escassos e o meio é mais propenso a erros. Na pesquisa de Xie e Wang [17] são apresentados alguns trabalhos que tratam da gerência de mobilidade em redes em malha sem fio.

Embora muitos trabalhos tenham sido realizados a respeito das questões apresentadas nos parágrafos anteriores, um número menor têm tratado a questão da redução do tempo de alocação de IP durante o *handoff* da camada de rede. Levando em consi-

deração que o DHCP é um protocolo amplamente utilizado na configuração automática de clientes que utilizam o protocolo IP, e é frequentemente utilizado em redes sem fio para configuração dos clientes móveis, a pesquisa conduzida neste trabalho não encontrou propostas de otimização do DHCP aplicadas diretamente a redes sem fio de múltiplos saltos com o objetivo de reduzir a latência de *handoff*. Contudo, serão apresentados alguns trabalhos que envolvem o protocolo DHCP, mobilidade e redução do tempo de aquisição de IP.

3.1 Dynamic Registration and Configuration Protocol

A proposta entitulada DRCP (*Dynamic Registration and Configuration Protocol*) [28] é um *Internet-Draft* da IETF (*International Enginnering Task Force*). O trabalho propõe uma alternativa ao DHCP, cujo principal objetivo é acelerar o processo de aquisição de IP através da redução do número de mensagens trocadas entre cliente e servidor. A proposta é voltada para cenários de mobilidade dentro da mesma rede de acesso. A Figura 8 ilustra o cenário de aplicação do DRCP.

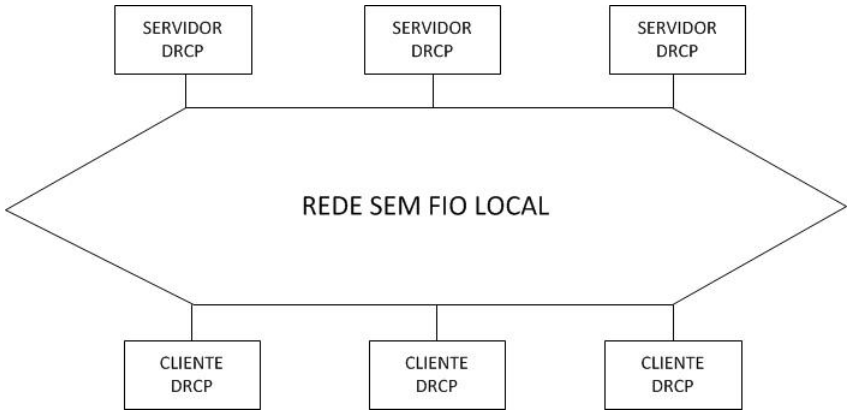

Figura 8: Arquitetura da proposta DRCP.

O modelo cliente servidor do DRCP é similar ao modelo adotado no DHCP, porém ambos, cliente e servidor, devem executar o mesmo programa com a diferença que o servidor deve possuir informações sobre os parâmetros de configuração. A semântica das mensagens do protocolo DRCP também é semelhante a das mensagens DHCP. A diferença é que no DRCP o cabeçalho das mensagens possui menos campos e existem duas mensagens a mais que são `ACCEPT` e `ADVERTISEMENT`. O servidor DRCP envia periodicamente a mensagem `ADVERTISEMENT` em *broadcast* contendo informações sobre o IP do servidor e o endereço da rede.

Como mostra a Figura 9, a principal diferença do DRCP em relação ao DHCP é que no processo de aquisição de IP realizado pelo DRCP, assim que o cliente recebe um `OFFER` ele passa a usar imediatamente o IP oferecido e envia uma mensagem `ACCEPT`

como resposta afirmativa à mensagem `OFFER`. Portanto, o servidor não precisa mandar uma mensagem `ACK` para confirmar todo o processo.

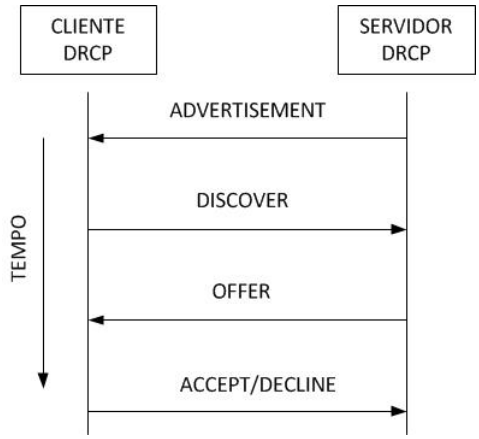

Figura 9: Funcionamento do DRCP.

Como se pode observar, este processo economiza uma mensagem em comparação com o DHCP. Apesar desse fato tornar a protocolo DRCP mais rápida que o DHCP no processo inicial de configuração de IP, a proposta não atenta para o problema das redes sem fio de múltiplos saltos, pois se o servidor estiver distante do cliente por vários saltos, as mensagens continuaram experimentando considerável atraso.

3.2 Rapid Commit Option

A RFC 4039 [29], diferente da proposta DRCP, não é uma alternativa ao DHCP é apenas uma extensão para este protocolo. A proposta foi criada para ambientes de alta mobilidade onde ocorrem mudanças frequente de ponto de acesso dos clientes móveis dentro da mesma rede de acesso. Por isso, o objetivo desta proposta, assim como o DRCP, é agilizar o processo inicial de configuração dos clientes realizado pelo DHCP. Ao invés de 3 mensagens trocadas como propõe o DRCP, a opção *Rapid Commit* permite que o processo de aquisição de IP seja efetuado com a troca de apenas duas mensagens.

Para isso é necessário que o uso da opção *Rapid Commit* seja suportada por ambas as entidades cliente e servidor DHCP. O cliente deve fazer uso da opção somente nas mensagens `DHCP_DISCOVER` e o servidor deve sinalizar a mesma opção apenas nas mensagens `DHCP_OFFER` ou `DHCP_ACK`. Como mostra a Figura 10, o servidor DHCP que suporta a opção *Rapid Commit*, ao receber uma mensagem `DHCP_DISCOVER` do cliente contendo também a mesma opção, enviará no lugar da mensagem `DHCP_OFFER` uma mensagem `DHCP_ACK` finalizando todo o processo. Com isso estima-se que o tempo do processo inicial de aquisição de IP seja reduzido pela metade.

O uso da opção *Rapid Commit* deve ser utilizada se obedecer um dos seguintes requisitos: possuir apenas um servidor DHCP na rede, que seria a opção mais adequada, ou quando possuir mais de um servidor, estes devem ter um número suficiente de endereços

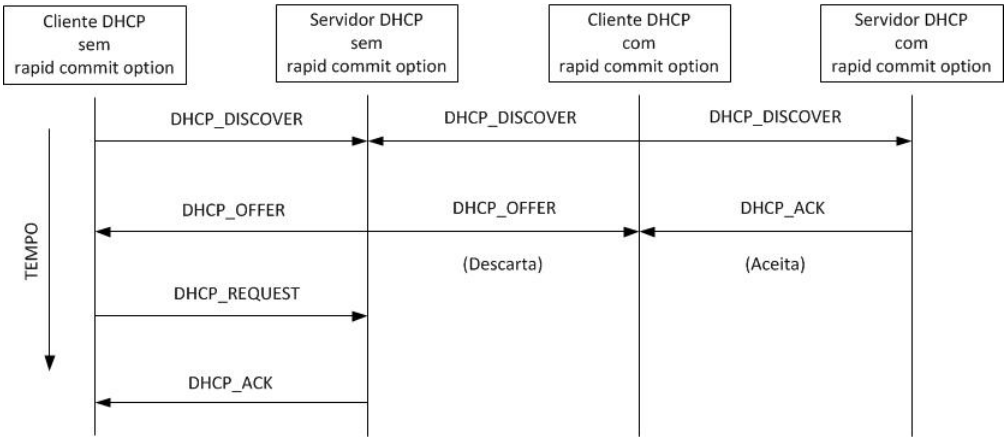

Figura 10: Funcionamento do DHCP com e sem Rapid Commit Option.

IPs para ser atribuído sempre que um cliente utilizar a opção *Rapid Commit*. Em outras palavras, quando um cliente DHCP envia uma mensagem `DHCP_DISCOVER` contendo a opção *Rapid Commit*, embora seja escolhido apenas um dos servidores, todos os outros servidores que enviaram IPs terão esses endereços indisponíveis durante o tempo que durar a *lease time* oferecida.

O servidor DHCP não tem o controle de saber se o cliente efetivamente está utilizando o IP oferecido pois não há qualquer tipo de confirmação do cliente. Além disso, assim como a proposta DRCP, a proposta *Rapid Commit Option* não endereça o problema da configuração do DHCP em redes sem fio de múltiplos saltos. Isto é, durante o processo de *handoff*, se o servidor DHCP estiver distante do cliente por múltiplos saltos, o processo de *handoff* experimentará atraso semelhante ao do processo do protocolo DHCP padrão.

3.3 Ad Hoc DHCP

A proposta AH-DHCP (*Ad Hoc* DHCP) [30] foi concebida com o objetivo de otimizar o processo de configuração do protocolo DHCP em redes sem fio de múltiplos saltos. A arquitetura de rede adotada para aplicação da proposta pode ser vista na Figura 11. Trata-se de um rede hibrida que possui nós IEEE 802.3 e nós IEEE 802.11. A rede sem fio é composta de APs que atuam como *gateways*. Os nós móveis formam uma rede *ad hoc* de múltiplos saltos orientada por um protocolo de roteamento *ad hoc*. A rede possui um servidor DHCP central servindo tanto à rede cabeada quanto à rede sem fio. Os clientes móveis, portanto, trocam mensagens com o servidor DHCP através de múltiplos saltos sobre o enlace sem fio.

A proposta AH-DHCP requer a modificação de duas entidades, o cliente móvel e os agentes DHCP *relay*. Os clientes móveis também podem atuar como agente DHCP *relay* e assim o fazem após a fase inicial de aquisição de IP. A ideia principal da proposta é reduzir a sobrecarga de mensagens e a taxa de perdas ocasionadas pelo DHCP neste tipo de cenário. Para isso, todo cliente móvel deve selecionar, de uma lista de vizinhos

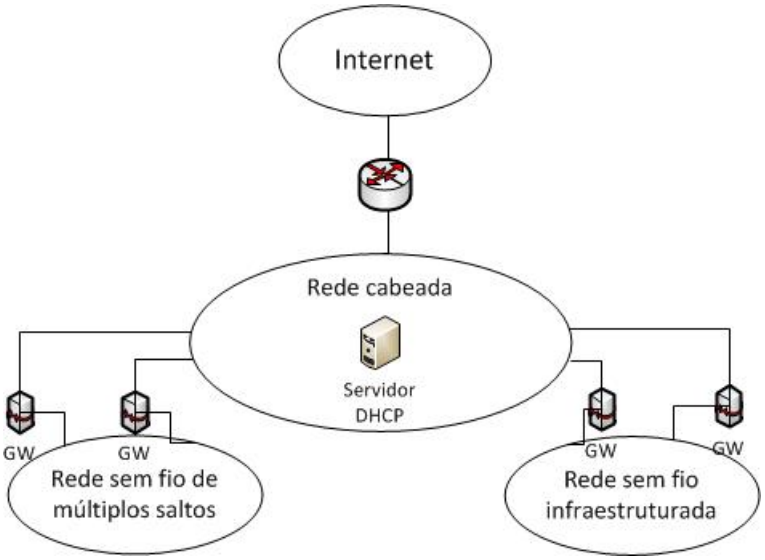

Figura 11: Arquitetura da proposta AH-DHCP.

de um salto, o melhor agente DHCP relay. O critério utilizado na proposta foi a menor distância entre o agente DHCP *relay* e o *gateway*.

Embora a proposta seja voltada para redes sem fio de múltiplos saltos, ela não endereça a problemática da configuração do protocolo DHCP durante o *handoff*. A principal contribuição do trabalho é a diminuição da sobrecarga de mensagens DHCP que pode ser gerada em redes sem fio de múltiplos. Além disso, a proposta exige modificação nos clientes móveis o que torna sua adoção mais difícil.

3.4 Fast Handoff Optimization

O trabalho intitulado *"Handoff optimization in 802.11 wireless networks"* [7] propõe o mecanismo FHO (*Fast Handoff Optimization*) para redes infraestruturadas IEEE 802.11. Os autores dividem o processo total de *handoff*, que inclui as camadas de enlace e de rede, em cinco fases: seleção de AP, troca de AP, controle de admissão de chamada, realocação de IP e configuração de rede.

O mecanismo propõe modificação nas fases de seleção de AP, realocação de IP e controle de admissão de chamada. No que concerne ao DHCP, o mecanismo reduz o número de mensagens trocadas durante o processo de aquisição de IP. Durante o *handoff* o cliente aceita incondicionalmente o endereço IP contido na mensagem `DHCPOFFER`, passando a usá-lo imediatamente. As mensagens posteriores, `DHCPREQUEST` e `DHCPACK`, seriam omitidas nesse processo. Com isso o número de mensagens seria reduzido pela metade, o que levaria a uma redução de tempo equivalente.

Assim como as demais, a proposta FHO não leva em consideração o problema dos múltiplos saltos em redes sem fio. Além disso, a proposta incorre em um problema para o protocolo DHCP: o cliente móvel ao receber a mensagem `DHCPOFFER` passa a

usar incondicionalmente o novo IP oferecido. Tal fato pode gerar inconsistência para o protocolo DHCP, uma vez que o servidor espera uma mensagem `DHCPREQUEST`. Caso isso não aconteça, então o IP que foi oferecido será mantido como disponível, mas no caso da proposta FHO, estará sendo utilizado, o que pode causar duplicidade de IPs na rede. Adicionalmente, a proposta FHO requer que as modificações sejam feitas no cliente DHCP. Este fato é indesejável por questões de escalabilidade, trazendo problemas para administração da rede.

CAPÍTULO 4

Proposta

O protocolo DHCP foi originalmente projetado para redes cabeadas onde os *hosts* estão fixos, em um cenário de mobilidade o desempenho do DHCP é afetado sobretudo pela alta taxa de erro. A própria rede sem fio pode ser afetada pelo protocolo, já que o seu funcionamento pode gerar tempestade de *broadcast* na camada de enlace. Os problemas citados se acentuam ainda mais em redes sem fio de múltiplos saltos.

Um outro ponto importante a se considerar também é o uso de aplicações de multimídia e de tempo real neste cenário. De todo o processo de *handoff*, o *handoff* da camada de rede é o que apresenta maior latência, sendo o DHCP apontado como o maior responsável, visto que o processo de configuração realizado pelo protocolo pode chegar a ordem de segundos. Este atraso pode inviabilizar o uso das aplicações que possuem restrição de tempo.

A proposta intitulada FHDRA (*Fast Hanfoff DHCP Relay Agent*) tem como objetivo a redução do atraso imposto pelo processo de *handoff* da camada de rede através de um esquema que reduz o tempo de aquisição de IP realizado pelo DHCP em redes sem fio de múltiplos saltos. A proposta FHDRA também reduz o número de mensagens DHCP durante o processo de *handoff* e mantém o funcionamento padrão tanto dos clientes quanto do servidor DHCP.

4.1 Arquitetura para Aplicação da Proposta

A proposta é voltada para redes sem fio de múltiplos saltos onde os roteadores estão fixos. Diferente das redes sem fio tradicionais como a rede de celulares e as redes sem fio infraestruturadas IEEE 802.11, nas quais a comunicação sem fio ocorre apenas a um salto da estação base, em redes sem fio de múltiplos saltos, a comunicação sem

fio pode ocorrer com a participação de vários nós intermediários formando um caminho de múltiplos saltos sobre o enlace sem fio. Devido a essa característica as soluções de mobilidade voltadas para redes sem fio tradicionais contam geralmente com infraestrutura da rede cabeada e por isso sofrem menos com atrasos, perdas e sobrecarga de pacotes. Portanto, algumas soluções e protocolos de mobilidade propostos para as redes sem fio infraestruturadas não são inteiramente adequadas às redes sem fio de múltiplos saltos.

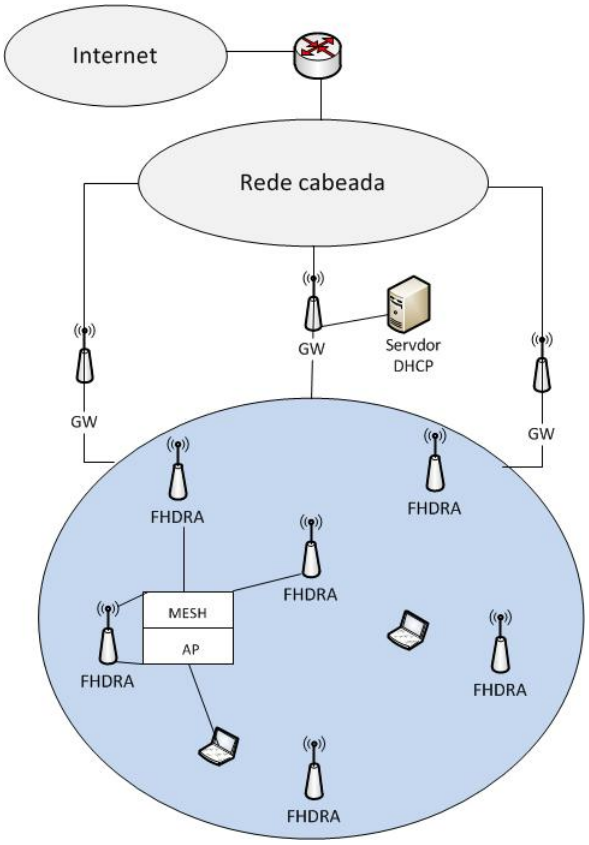

Figura 12: Arquitetura de rede para aplicação da proposta FHDRA.

De acordo com o modelo de arquitetura de rede idealizado, foi utilizada uma rede em malha sem fio para a aplicação da proposta FHDRA. Esta é um tipo de rede sem fio de múltiplos saltos onde os roteadores são fixos. Atualmente, o grupo que vem trabalhando no desenvolvimento de um padrão para as redes em malha sem fio é o IEEE 802.11s [31]. O padrão ainda não foi definitivamente homologado, mas os últimos *drafts* lançados já possibilitaram o desenvolvimento de algumas implementações por parte dos fabricantes e da comunidade *open source* [32].

Na arquitetura utilizada existe a presença de somente um servidor DHCP que pode ser qualquer um dos roteadores sem fio da rede ou pode estar situado na rede cabeada. A adoção de um único servidor DHCP centraliza a gestão de configuração dos clientes sendo importante também para manter a consistência dos IPs em uso na rede. Desse modo, todos os dispositivos desta rede sem fio estão no mesmo domínio e por isso a movimentação dos clientes não necessita a mudança de IP. Os roteadores sem fio atuarão como agentes DHCP *relay* executando o algoritmo FHDRA. A Figura 12 ilustra

a arquitetura de rede que foi utilizada para a implantação da proposta.

4.2 Definição da Proposta

Analisando o cenário da Figura 12, quando um cliente móvel ingressa nessa rede, será executado o procedimento padrão realizado pelo DHCP, que consiste na troca das quatro mensagens `DHCP_DISCOVER`, `DHCP_OFFER`, `DHCP_REQUEST`, `DHCP_ACK`, conforme exposto na Figura 13. Pode haver mudanças nesse procedimento padrão de acordo com as máquinas de estado cliente e servidor, como pode ser analisado na Figura 7.

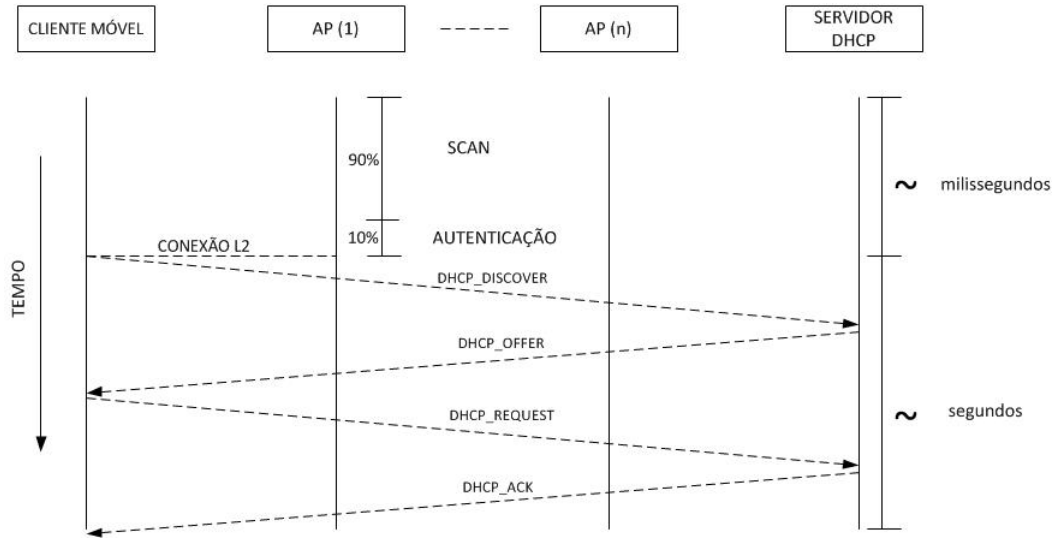

Figura 13: Procedimento padrão do DHCP em uma rede sem fio de múltiplos saltos.

Entretanto, no caso da rede da Figura 12, como se trata de uma rede sem fio de múltiplos saltos, entre cliente e servidor DHCP é possível existir vários nós intermediários disputando os recursos do escasso meio de comunicação. Isso significa que as quatro mensagens trocadas experimentarão um atraso superior àquele causado nas redes cabeadas ou redes sem fio infraestruturadas, onde os clientes móveis estão a um salto da estação base.

À medida que o cliente móvel se desloca dentro da rede sem fio, poderá sair do alcance do seu AP corrente até que efetivamente se desassocie, é quando então ele buscará se associar a outro AP da mesma rede e reconfigurar seus parâmetros de rede. O processo de *handoff* discutido passou pelas fases de *handoff* da camada de enlace e de rede. Durante o *handoff* da camada de rede, ainda que o cliente móvel permaneça na mesma sub-rede, ele executará o processo DHCP cliente. A diferença agora é que o cliente DHCP não executará o mesmo processo inicial em que eram trocadas quatro mensagens. Uma vez que o cliente DHCP ainda possui uma *lease time* válida para o endereço IP atual e permanece na mesma sub-rede, ele enviará uma mensagem `DHCP_REQUEST` requisitando o mesmo endereço IP utilizado. O servidor DHCP, por sua vez, após verificar a disponibilidade do IP, enviará uma mensagem `DHCP_ACK`, renovando a *lease time* do IP requisitado. A Figura

14 mostra o comportamento do DHCP durante o *handoff* em redes sem fio de múltiplos saltos.

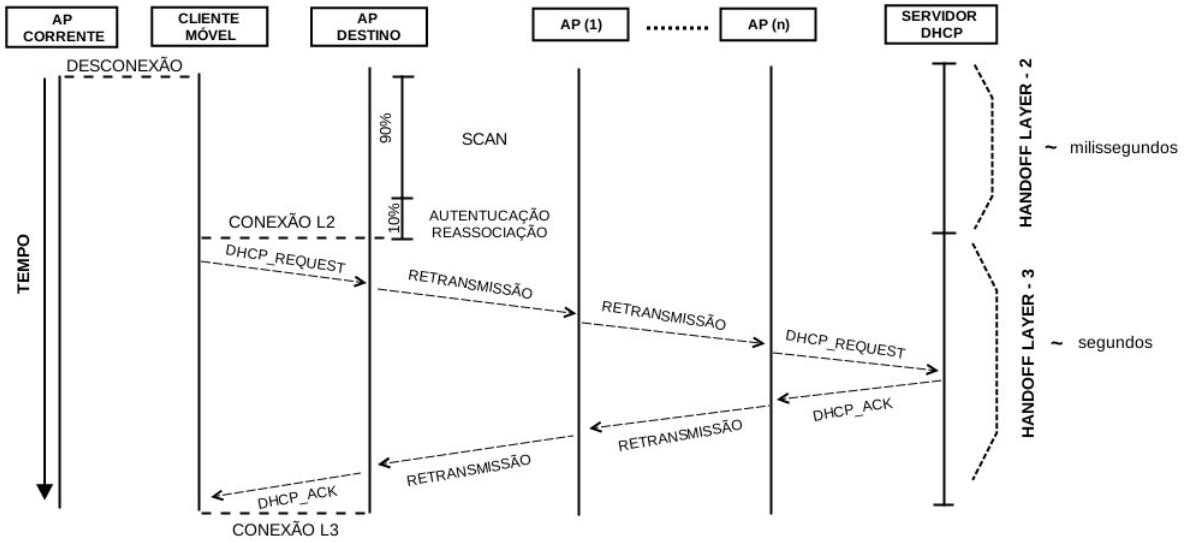

Figura 14: Handoff com DHCP em redes sem fio de múltiplos saltos.

Ao observar o processo de *handoff* nesse cenário, percebe-se que mesmo durante o processo de *handoff* realizado dentro da mesma sub-rede, quando são trocadas duas mensagens ao invés de quatro, o processo de aquisição de IP realizado pelo DHCP contribui para que o *handoff* da camada de rede apresente alta latência. Isso se deve a questão dos múltiplos saltos, ou seja, as mensagens podem ter que atravessar vários nós intermediários até chegar ao destino.

A solução pensada para minimizar a latência gerada durante o processo de aquisição de IP foi abstrair o número de saltos que separa cliente e servidor DHCP. Inicialmente, pensou-se em criar uma entidade que atuaria em cada AP da rede funcionando como um pseudo servidor DHCP. Mas logo se percebeu que esta solução pode prejudicar o funcionamento adequado do DHCP, gerando inconsistência de informações entre o pseudo servidor e servidor DHCP real. Essa estratégia também pode gerar maior sobrecarga na rede devido a troca de mensagens necessária para tentar manter as duas entidades sincronizadas. Adicionalmente, seria necessário modificar a máquina de estados padrão do servidor DHCP para reconhecer as mensagens adicionais que seriam trocadas com o pseudo servidor.

Para manter o funcionamento padrão das entidades cliente e servidor DHCP e evitar inconsistências para o protocolo, decidiu-se modificar o funcionamento do agente DHCP *relay*. Como já foi dito anteriormente, o agente DHCP *relay* atua como um retransmissor de mensagens DHCP. A proposta FHDRA agrega inteligência ao agente DHCP *relay*, tornando-o capaz de identificar o processo de *handoff* do cliente DHCP, e assim, atender de imediato a requisição de um cliente, ao invés de repassá-la ao servidor DHCP e ter que aguardar a resposta. A proposta é transparente tanto paro o cliente quanto para o servidor DHCP, ou seja, não necessita mudanças na máquina de estados

de ambos. A Figura 15 ilustra o comportamento do DHCP durante o processo de *handoff* com a proposta FHDRA.

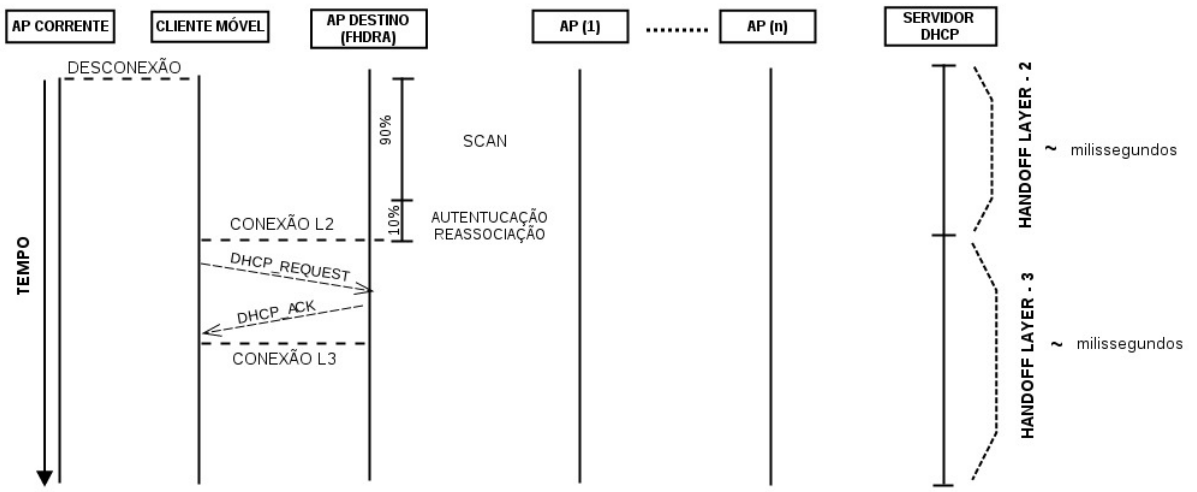

Figura 15: Handoff com a proposta FHDRA em redes sem fio de múltiplos saltos.

Para verificar a viabilidade de implementação da proposta no agente DHCP *relay*, foi necessário identificar o formato da mensagem DHCP enviada pelo cliente móvel durante o *handoff*. Em testes realizados com o apoio da ferramenta *sniffer Wireshark* [33] e *tcpdump* [34] foi constatado que no momento do *handoff* o cliente móvel envia uma mensagem `DHCP_REQUEST` no formato que corresponde ao estado `INIT-REBOOT`, conforme pode ser visto na Tabela 3. A partir dessa informação foi definido um algoritmo para o agente DHCP *relay*, tornando-o capaz de identificar um evento de *handoff*.

Tabela 3: Mensagem `DHCP_REQUEST` enviada em diferentes estados.

	INIT-REBOOT	**SELECTING**	**RENEWING**	**REBINDING**
broad/unicast	broadcast	broadcast	unicast	broadcast
ip_servidor	não	sim	não	não
ip_requisitado	sim	sim	não	não
ciaddr	não	não	sim	sim

A mensagem `DHCP_REQUEST` no estado `INIT-REBOOT` se distingue das demais mensagens. As únicas ocasiões em que o cliente envia a mensagem `DHCP_REQUEST` no estado `INIT-REBOOT` é quando ocorre um evento de *handoff* ou após a inicialização ou reinicialização do cliente quando este ainda possui uma lease time válida. O algoritmo mostrado na Figura 16 demostra o comportamento do agente DHCP *relay* com a proposta FHDRA.

Quando o agente DHCP *relay* recebe a mensagem DHCP é verificado, inicialmente, se a mensagem é do tipo `BOOTREPLAY` ou `BOOTREQUEST`, conforme explicado na Tabela 1. Caso seja uma mensagem do tipo `BOOTREPLAY`, significa que veio do servidor e deve ser repassada para o cliente. Caso seja uma mensagem do tipo `BOOTREQUEST`, deve ser analisada se não é uma mensagem que caracteriza o *handoff*. Como dito anteriormente, a mensagem que caracteriza um evento de *handoff* tem um formato que se enquadra no

```
1 switch (msg.header.op) {

2 case bootreplay:
3        envia_msg_para_cliente();

4 case bootrequest:
5      if { (verifica_ip(msg.header.opt(50)) = true)
6           else if {
7                    (msg.header.opt.code(53) = dhcp_request &&
                      msg.sent = broadcast &&
                      msg.header.siaddr = 0 &&
                      msg.header.ciaddr = 0 )

8                    envia_ack_para_cliente();
9                    }
10          else {envia_msg_para_servidor();}
11     }
12 }
```

Figura 16: Algoritmo FHDRA.

estado `INIT-REBOOT`, como mostra a Tabela 3. Dessa forma, é necessário verificar se a mensagem satisfaz os requisitos (linha 7 da Figura 16). Para evitar que seja enviado uma mensagem `DHCP_ACK` para um cliente que requisite um IP diferente do usado na rede, é realizada a verificação conforme linha 5 da Figura 16. Se o IP requisitado faz parte da rede, então foram satisfeitas as condições que caracterizam o evento de *handoff*. Nesse caso, ao invés da mensagem ser enviada para o servidor DHCP, será enviado uma mensagem `DHCP_ACK` diretamente para o cliente através da função **envia_ack_para_cliente()** (linha 8 da Figura 16).

Um ponto importante a se destacar é manter o servidor DHCP com sua base de informações consistente. O servidor DHCP possui um repositório que mantém atualizadas informações sobre tempo de uso e disponibilidade dos endereços IPs. O fato de delegar ao agente DHCP *relay* a responsabilidade enviar `DHCP_ACK` para o cliente móvel que efetua um *handoff*, requer que o agente DHCP *relay* não aumente o tempo de validade do IP na rede, evitando assim o uso de IPs duplicados na rede.

Para evitar esse problema a proposta FHDRA adotou a estratégia que consiste em reduzir a *lease time* do IP requisitado durante o *handoff*. Quando o servidor DHCP atua no modo dinâmico, cada IP atribuído possui uma *lease time* que representa seu período de validade. Como discutido na seção 2.2, a *lease time* tem dois contadores, **T1** e **T2**, que servem para orientar o cliente sobre o momento de renovar a *lease time* do seu IP. T1 e T2 equivalem, respectivamente, a 50% e 87,5% da *lease time* do IP. O que significa que na metade do tempo de validade do IP, o cliente deve realizar o processo de renovação do seu IP, caso não obtenha sucesso, quando atingir o tempo T2 deverá fazer novas tentativas. Caso, ainda assim, o cliente não consiga renovar a *lease time* do seu IP, ele voltará para o estado `INIT`, de onde recomeçará o processo de aquisição de IP,

enviando uma mensagem `DHCP_DISCOVER`.

Seja **La** o período da *lease time* original atribuída pelo servidor DHCP e que equivale, portanto, ao tempo de validade do IP na rede, sendo **Ta1** e **Ta2** os tempos que representam os contadores de **La**. Seja **Lb** o período da *lease time* atribuída pelo agente DHCP *relay* com a proposta FHDRA e que equivale a 12,5% da *lease time* original, sendo **Tb1** e **Tb2** os tempos que representam os contadores de **Lb**. Seja **Tt** um dado tempo dentro de **La** que significa tempo transcorrido desde o início de **La** até o momento do *handoff*. Seja **Tr** o tempo restante para o término de **La** a partir de **Tt**, portanto $\mathbf{La} = \mathbf{Tt} + \mathbf{Tr}$. Seja **C1** o caso em que o *handoff* ocorre quando $\mathbf{Tt} < \mathbf{Ta1}$, então $\mathbf{Lb} < \mathbf{Tr}$. Seja **C2** o caso em que o *handoff* ocorre quando $\mathbf{Ta1} < \mathbf{Tt} < \mathbf{Ta2}$, então $\mathbf{Lb} < \mathbf{Tr}$. Seja **C3** o caso em que o *handoff* ocorre quando $\mathbf{Tt} > \mathbf{Ta2}$, então $\mathbf{Lb} > \mathbf{Tr}$.

Ao analisar os casos **C1** e **C2**, quando o cliente móvel realizar o *handoff* significa que a nova *lease time* **Lb** terá validade durante o período de validade do IP na rede, pois **Lb** estará compreendida dentro de **La**. **C3** é o único caso em que pode gerar inconsistência para o servidor DHCP, já que $\mathbf{Lb} > \mathbf{Tr}$. Embora seja um caso a se considerar, **C3** é um caso que tem baixa probabilidade de ocorrer pois o mecanismo padrão do protocolo DHCP instrui o cliente a realizar a renovação de IP a partir da metade do tempo de sua *lease time*.

Em teste realizados neste trabalho em 100% dos casos o cliente móvel conseguiu renovar sua *lease time* antes do período **Ta2**. Para este teste foram utilizados os seguintes parâmetros: $\mathbf{La} = \mathbf{20\ min}$, portanto $\mathbf{Ta1} = \mathbf{10\ min}$, $\mathbf{Ta2} = \mathbf{17{,}5\ min}$, $\mathbf{Lb} = \mathbf{2{,}5\ min}$. O teste foi repetido dez vezes e ocorreu no mesmo *testbed* utilizado para validar a proposta, como pode ser visto na Figura 18 do capítulo 5. Considerando o caso **C3**, mesmo que $\mathbf{Lb} > \mathbf{Tr}$, a probabilidade de inconsistência com o servidor DHCP é pequena pois se ocorrer $\mathbf{Tb1} + \mathbf{Tb2} < \mathbf{Tr}$, ou seja, o cliente tentará a renovação do IP antes do término de **La**. A Figura 17 ilustra o esquema de funcionamento da *lease time* inserida na proposta FHDRA.

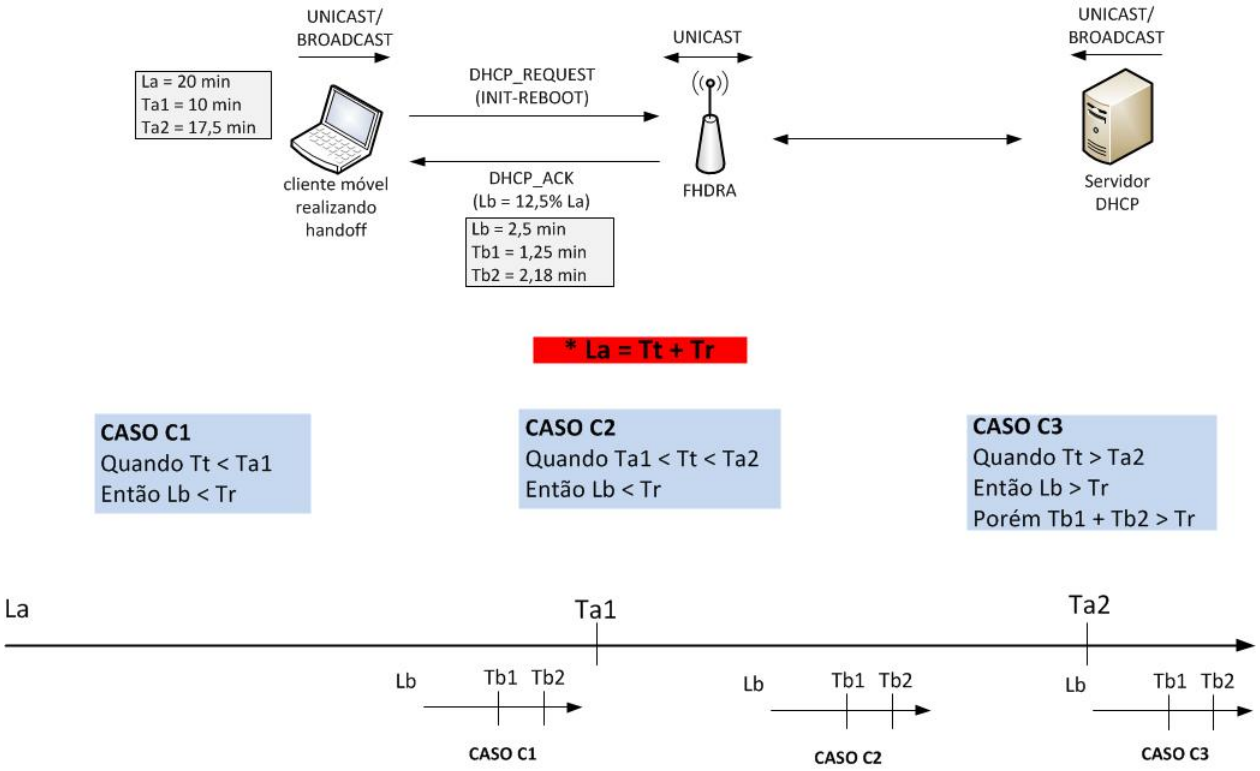

Figura 17: Esquema de funcionamento da *lease time*.

CAPÍTULO 5

Avaliação de Desempenho

5.1 Cenário

Para avaliação da proposta foi montado um *testbed outdoor* no campus da Universidade Federal do Pará, como ilustrado na Figura 18. Foram utilizados cinco roteadores da marca TP-LINK modelo TL-WR1043ND. Os roteadores vêm de fábrica com três antenas omini-direcionais destacáveis, cada uma com 3dBi de ganho, mas estas foram substituídas por apenas uma antena omini-direcional de 2dBi em cada um dos roteadores. A intenção desta mudança foi diminuir o poder de alcance dos roteadores de tal forma que cada um só pudesse ter alcance até seus vizinhos de um salto. Dessa forma a rede se comportaria efetivamente como uma rede de múltiplos saltos, onde a comunicação entre dois roteadores separados por `n` nós, passaria necessariamente pelo intermédio desses `n` nós. Portanto, de acordo com a Figura 18, só havia comunicação direta entre os roteadores adjacentes.

A distância entre os roteadores era de aproximadamente 20m com uma altura de 1m em relação ao solo, sendo que a distância entre os roteadores 1 e 2 era de aproximadamente 35m e não havia comunicação direta entre eles. Havia a presença de interferências ao redor do *testbed*, tais como prédios, árvores e o trânsito variável de pessoas entre os roteadores. O *firmware* original dos roteadores foi substituído pela distribuição Linux para dispositivos embarcadas OpenWRT [10]. Foi utilizada uma implementação *open source* do protocolo IEEE 802.11s [32].

Foram coletados alguns parâmetros da rede utilizada. Através do utilitário PING obteve-se o número de pacotes perdidos, o RTT (*Round Trip Time*) máximo, mínimo e médio do total de pacotes enviados. Foi utilizado um *notebook* com uma distância de 10m do `ROTEADOR 1`. A partir desse *notebook* foram executados PINGs de 50 pacotes com tamanho padrão de 64 Bytes para cada um dos cinco roteadores, consecutivamente. A Tabela 4 mostra os resultados. Durante a coleta não havia tráfego de *background* na rede.

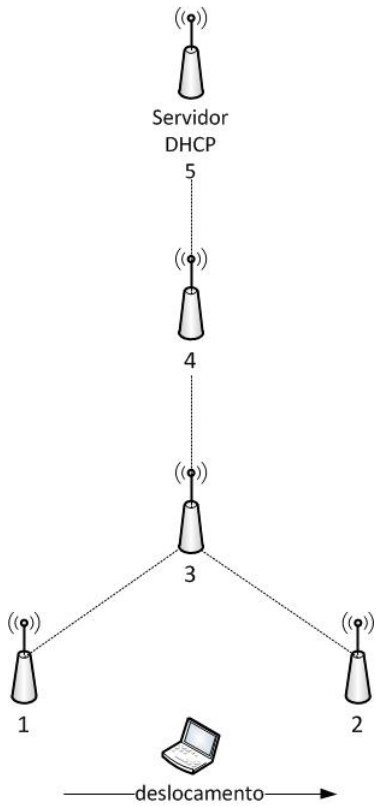

Figura 18: Testbed utilizado para a avaliação da proposta.

Tabela 4: Resultados obtidos com PING.

AP	RTT_MIN	RTT_MAX	RTT_MED	PERDAS
1	0.727	39.199	5.649	0
2	205.452	3128.122	428.078	2
3	1.610	109.346	13.368	1
4	197.374	3102.344	404.150	2
5	479.296	3270.469	634.294	8

5.2 Experimentos

O objetivo dos experimentos é avaliar a latência provocada pelo DHCP durante o processo de *handoff*, que em outras palavras é a diferença de tempo entre o momento em que o cliente móvel envia a primeira mensagem `DHCP_REQUEST` e o momento em que o mesmo recebe do servidor uma mensagem `DHCP_ACK`. A medição foi realizada com a intervenção da ferramenta *Wireshark*.

Foram realizados dois experimentos: no **experimento 1** não conteve tráfego de *background* na rede, já no **experimento 2** foi introduzido tráfego de *background* na rede com o objetivo de simular os efeitos de uma rede em produtividade. Em cada um dos dois experimentos foram executados três casos:

1. **DHCP**: este caso foi realizado somente com a presença do servidor DHCP.
2. **DHCP RELAY**: neste caso cada AP da rede estava configurado como agente DHCP *relay*.
3. **FHDRA**: neste caso cada AP da rede estava configurado com a proposta FHDRA.

O tráfego de *background* foi gerado com a ferramenta Iperf [34]. A partir dos dispositivos `ROTEADOR 1`, `ROTEADOR 2` e `ROTEADOR 3` foi transmitido um fluxo UDP com taxa de bits constante de 100 Kb/s com destino ao servidor DHCP. O fluxo foi transmitido dos três dispositivos, paralelamente. O tráfego de *background* gerado ocorreu durante todo o período de coleta das amostras do segundo experimento. Em cada um dos dois experimentos nos três casos, o número amostras coletas foi igual a dez com intervalo de confiança de 90%.

A coleta das amostras ocorreu em dias e horários distintos e portanto em condições de temperatura e umidade do ar variáveis. Embora os testes tenham sido realizados com o *testbed* montado sempre no mesmo local, o cenário para o *testbed* não era fixo e precisava ser sempre desmontado ao final do dia e montado novamente para novas coletas.

5.2.1 Análise do Experimento 1

No primeiro experimento, onde não há a presença de tráfego de *background*, os valores das amostras para os três casos estão abaixo de 1 segundo. O máximo valor obtido foi na quinta amostra, 987ms, com uso de DHCP, conforme mostra o gráfico da Figura 19. O mínimo valor obtido, 14ms, foi na sétima amostra com uso da proposta FHDRA, como mostra o gráfico da Figura 20.

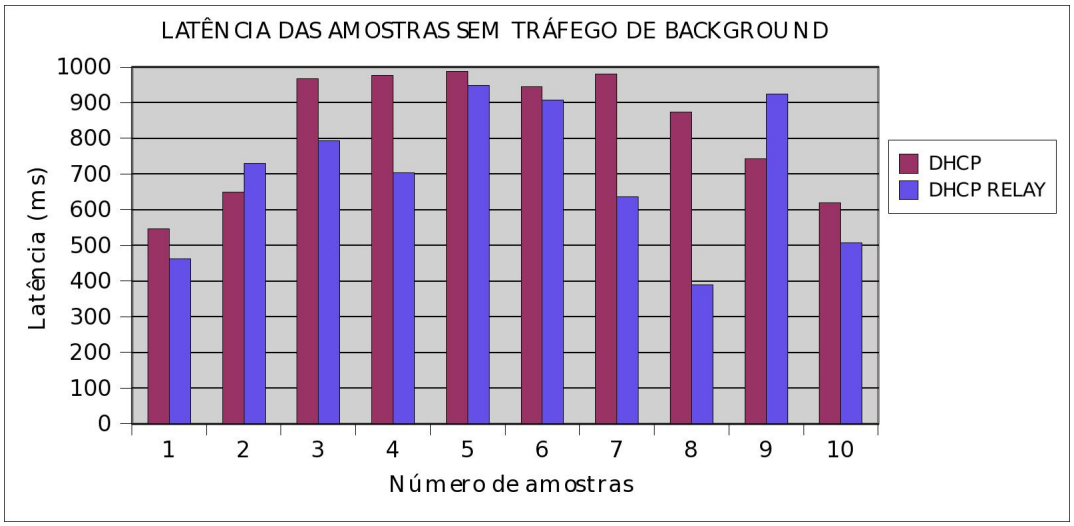

Figura 19: Resultado DHCP e DHCP RELAY sem tráfego de *background*.

Nota-se, comparando os gráficos das Figuras 19 e 20 que no primeiro experimento todas as amostras coletadas, utilizando a proposta FHDRA, estão com valores considera-

velmente abaixo dos valores obtidos nos outros dois casos. O máximo valor obtido com a proposta FHDRA no primeiro experimento foi de 30ms contra 987ms com DHCP e 948ms com DHCP RELAY.

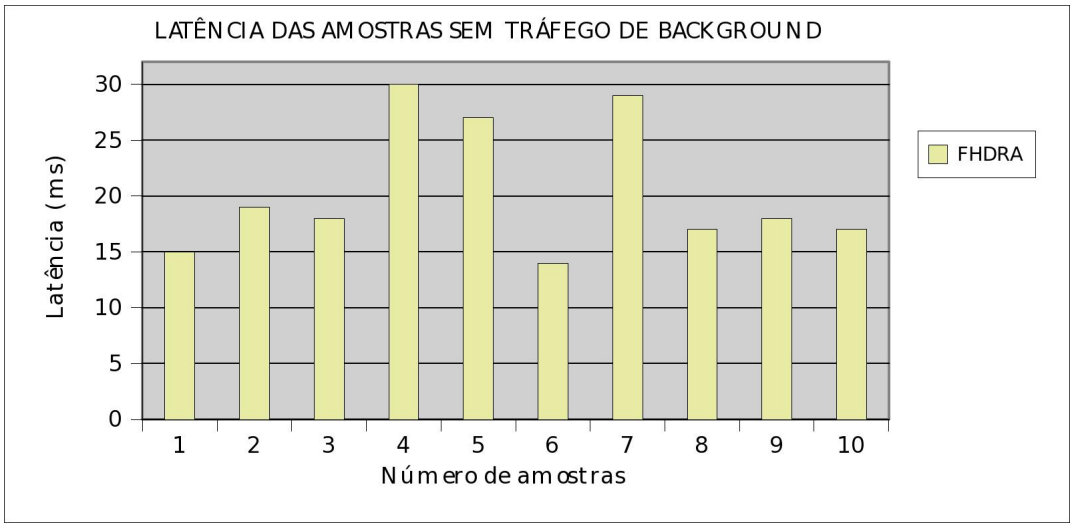

Figura 20: Resultado com a proposta FHDRA sem tráfego de *background*.

O gráfico da Figura 21 ilustra a média e o desvio padrão das amostras do primeiro experimento. A proposta FHDRA teve desempenho superior obtendo uma média de 20ms ao passo que nos casos com DHCP e DHCP RELAY a média foi 814ms e 700ms, respectivamente. Ao analisar o valor das médias no primeiro experimento, verifica-se que a proposta FHDRA teve um ganho de 3892% sobre o DHCP e 3333% comparado com o DHCP RELAY.

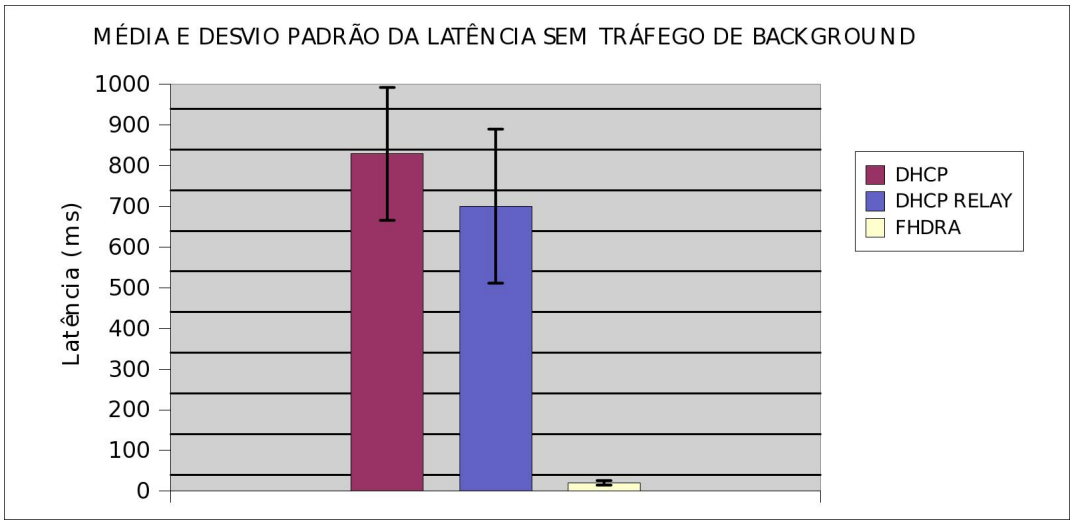

Figura 21: Resultado da média das amostras sem tráfego de *background*.

5.2.2 Análise do Experimento 2

Os gráficos das Figuras 22, 23 e 24 são referentes ao segundo experimento, no qual foi introduzido tráfego de *background* na rede. Com um tráfego de 300Kb/s fluindo na rede percebe-se através do gráfico da Figura 22 que com carga na rede os valores de latência ultrapassam os milissegundos chegando a ordem de segundos. Entretanto, com pode ser visto no gráfico da Figura 23, os valores de latência obtidos com uso da proposta FHDRA permanecem na ordem de milissegundos.

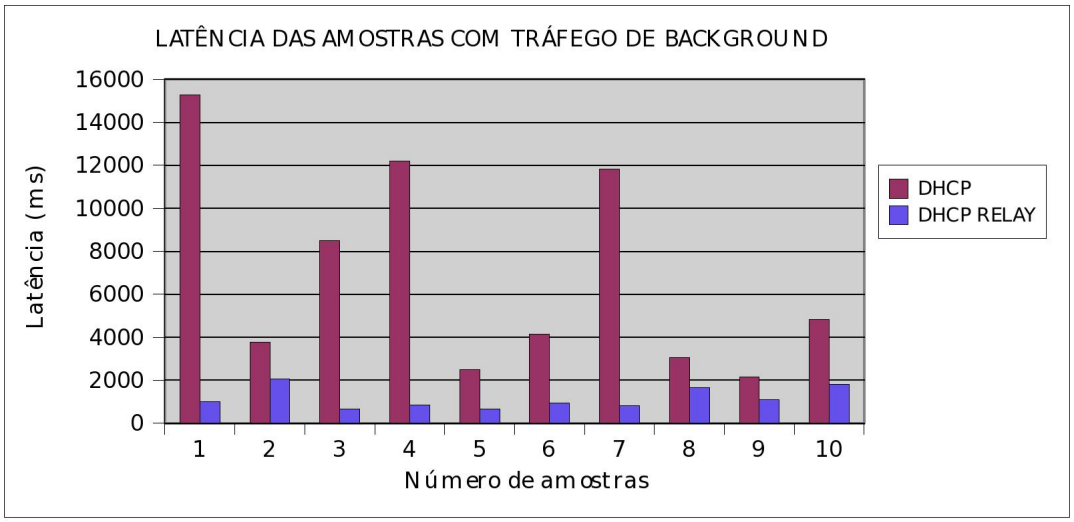

Figura 22: Resultado DHCP e DHCP RELAY com tráfego de *background*.

No segundo experimento o máximo valor de latência obtido foi com o DHCP, alcançando o tempo de 15s e 277ms. O maior valor obtido com o DHCP RELAY foi de 2s e 75ms. Novamente a proposta FHDRA atingiu o menor tempo que foi de 15ms e o máximo de 35ms. Isso demonstra que com uso da proposta FHDRA, mesmo com tráfego constante na rede, o atraso gerado durante o processo de *handoff* não sofreu efeito. Os valores das médias no segundo experimento foram de 6s e 824ms para o DHCP, 1s e 143ms para o DHCP RELAY e 22ms para a proposta FHDRA. Comparando as médias, a proposta FHDRA teve um desempenho de 30918% superior ao DHCP e 5140% superior ao DHCP RELAY.

A grande variação de atraso das amostras com DHCP, mostrada no gráfico da Figura 22, revela o comportamento típico do DHCP em redes com considerável nível de perdas, como foi o caso do segundo experimento. As mensagens DHCP são enviadas via protocolo de transporte UDP que não provê mecanismos de confirmação e retransmissão. Esse fato faz com que o próprio protocolo DHCP forneça os mecanismos necessários para manter confirmação e retransmissão através de seu grupo de mensagens. Ademais, o cliente DHCP é o único que efetua retransmissão: é quando o cliente envia as mensagens `DHCP_DISCOVER` e `DHCP_REQUEST` e não recebe resposta. Neste caso, o cliente DHCP obedece a um algoritmo de *backoff* exponencial, que determina o atraso entre as tentativas de retransmissão. Ou seja, o tempo de espera para que o cliente reenvie uma mensagem aumenta exponencialmente à medida que faz novas retransmissões.

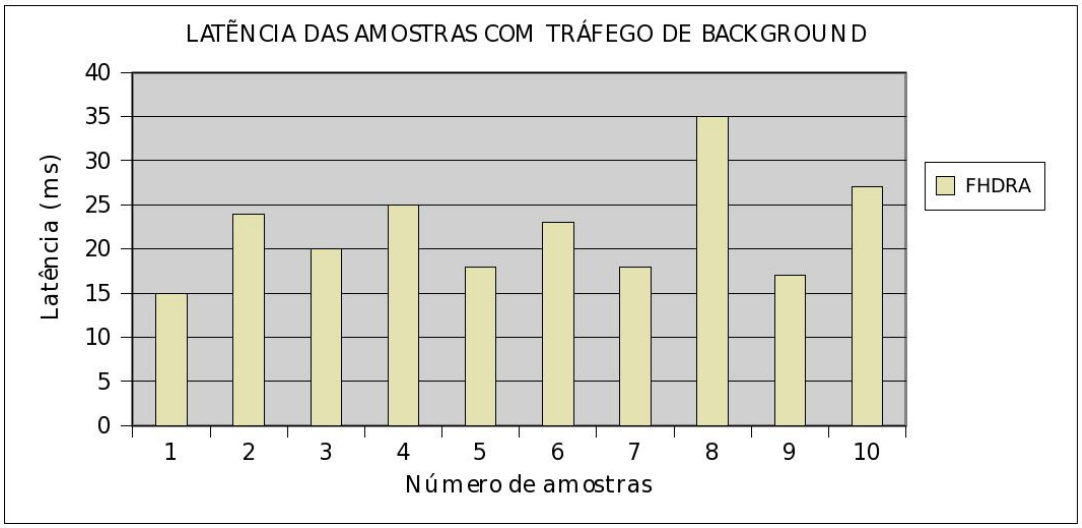

Figura 23: Resultado com a proposta FHDRA com tráfego de *background*.

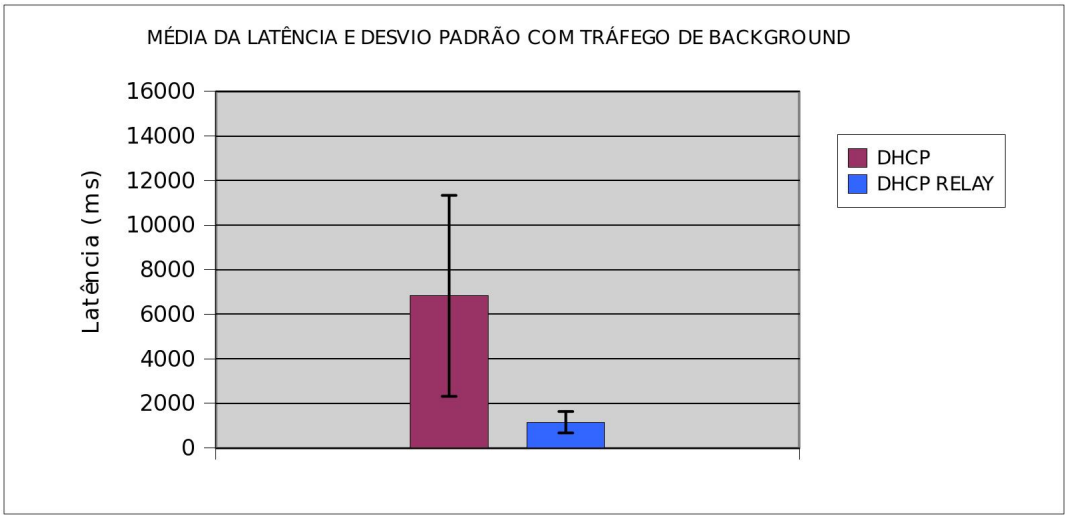

Figura 24: Resultado da média das amostras com tráfego de *background*.

Ao analisar os dois experimentos observa-se que a média das amostras com a proposta FHDRA permaneceu praticamente inalterada, demonstrado que a carga na rede não influenciou a latência durante o *handoff* dos clientes móveis pois com a proposta FHDRA não é necessário que as mensagens trocadas para efetuar a aquisição de IP viajem pela rede e sofram com os atrasos gerado pelo congestionamento de pacotes. O fato da proposta FHDRA manter o atraso médio abaixo de 23ms possibilita que sejam usadas aplicações com restrição de tempo sem que sofram com a latência tal como com o DHCP.

CAPÍTULO 6

Conclusão e Trabalhos Futuros

Foi visto que o tempo de aquisição de IP realizado pelo DHCP é uma das fases que mais consome tempo durante todo o processo de *handoff*, podendo chegar a marca dos segundos e que em redes sem fio de múltiplos saltos esse problema pode ser ainda mais acentuado. Visando como principal objetivo desse trabalho a redução do tempo de aquisição de IP durante o *handoff*, foi proposto o FHDRA voltado para redes sem fio de múltiplos saltos.

Embora existam muitos trabalhos explorando o *handoff* na camada de enlace e tantos outros na camada de rede, um número menor de trabalhos tem sido realizado para diminuir a latência gerada pelo processo de aquisição de IP realizado pelo DHCP e um número ainda menor tem tratado essa mesma abordagem em redes sem fio de múltiplos saltos. Nesse aspecto, a proposta FHDRA é um mecanismo que agrega inteligência ao agente DHCP *relay* tornando-o capaz de identificar um evento de *handoff* e rapidamente configurar o cliente móvel no cenário de mobilidade em redes sem fio de múltiplos saltos. A proposta FHDRA tem como principais contribuições:

- **Transparência de mobilidade:** o fato de ser utilizado um único servidor DHCP que centraliza o processo de endereçamento, permite que os clientes móveis mantenham seu endereço IP após o *handoff*. Com isso é possível manter as conexões dos clientes móveis ativas após a mudança de AP. E devido a considerável redução da latência na fase de aquisição de IP, a proposta FHDRA leva a uma redução no atraso total de *handoff*, influenciando de forma positiva a percepção de continuidade dos serviços para o usuário móvel.
- **Compatibilidade:** a proposta FHDRA não altera as máquinas de estado do cliente e servidor DHCP, sendo portanto, totalmente compatível com o protocolo DHCP vigente.

- **Fácil adoção e implantação:** a proposta FHDRA não requer mudanças nos dispositivos clientes, não requer modificação no protocolo de roteamento, é uma solução barata já que não requer o uso de protocolos ou equipamentos especializados, pode ser utilizada com *software* livre e rádios sem fio de baixo custo.

- **Escalabilidade:** como foi visto nos teste realizados neste trabalho, mesmo com tráfego constante na rede a proposta FHDRA manteve seu desempenho. E a medida que o número de saltos e a carga da rede aumenta, maior é o ganho da proposta em relação ao DHCP e DHCP RELAY. Independente do tamanho e do volume de tráfego na rede a proposta FHDRA mantém as taxas de latência na casa de poucas dezenas de milissegundos e sofrendo pouca variação.

Com os resultados obtidos nos experimentos, verificou-se que a proposta FHDRA reduz consideravelmente a latência durante a fase de aquisição de IP. Os resultados mostram que mesmo com tráfego constante na rede os valores de latência não ultrapassaram 35ms. Esse comportamento assinala que a proposta FHDRA é capaz de ser utilizada com aplicações que possuem restrições de tempo, tais como aplicações multimídia, cujo atraso deve ser mantido abaixo de 150 milissegundos.

Como trabalho futuro, pretende-se avaliar o uso da proposta FHDRA com aplicações que possuem restrição de tempo. Para isso é necessário a utilização de conteúdo multimídia e ferramentas de análise apropriadas como é o caso do evalvid.

Pretende-se investigar a adaptação da proposta FHDRA em redes sem fio de múltiplos saltos com mobilidade inter domínio. Nesse cenário surgem novos novos desafios, o principal deles é a mudança de endereço IP sempre que os clientes móveis transitarem entre redes distintas. Neste caso, deve-se integrar a proposta a um esquema de gerência de mobilidade.

Outro cenário que merece investigação é em MANETs que diferente do cenário onde a proposta FHDRA foi avaliada, além dos dispositivos cliente, há também mobilidade dos nós que compõem o *backbone* da rede.

Uma outra vertente da proposta FHDRA é sua adaptação para utilização em redes definidas por *software* (SDN – *Software Defined Network*). A ideia é utilzar o algortitmo FHDRA em controladores OpenFlow. Sabe-se que o princípio básico por trás de uma rede SDN é o uso de aplicações nos controladores que tornam a rede capaz de ser programada. Já vem sendo estudada a adoção do algortitmo FHDRA para ser implementado em uma aplicação SDN para garantir que os recursos de rede dos clientes móveis sejam preservados após o *handoff*, possibilitando assim a manutenção dos níveis de qualidade de serviço.

Referências

[1] I. Akyildiz and X. Wang, *Wireless Mesh Networks*. John Wiley & Sons Inc, 2009, vol. 1.

[2] ITU-T, "The world in 2013: ICT facts and figures," 2013. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

[3] Z. Zhu, R. Wakikawa, and L. Zhang, "A survey of mobility support in the internet," RFC 6301, July, Tech. Rep., 2011.

[4] "ITU-T Rec. G.114," *One-Way Transmission Time*, 2003.

[5] C. Perkins, *"RFC 5944 - IP Mobility Support for IPv4, revised"*, 2010.

[6] R. Droms, *"RFC 2131 - Dynamic Host Configuration Protocol (DHCP)"*, 1997.

[7] I. Hsieh and S. Kao, "Handoff optimization in 802.11 wireless networks," *EURASIP Journal on wireless communications and networking*, vol. 2011, no. 1, pp. 1–16, 2011.

[8] A. Forte, S. Shin, and H. Schulzrinne, "Improving layer 3 handoff delay in IEEE 802.11 wireless networks," in *Proceedings of the 2nd annual international workshop on Wireless internet*. ACM, 2006, p. 12.

[9] A. McAuley, S. Das, S. Baba, and Y. Shobatake, "Requirements for extending DHCP into new environments," *draft-ietf-dhc-enhance-requirements-00.txt*, 2000.

[10] OpenWrt, https://openwrt.org, accessado em Agosto de 2013.

[11] NS-3, http://www.nsnam.org, accessado em Agosto de 2013.

[12] OMNET++, http://www.omnetpp.org, accessado em Agosto de 2013.

[13] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the ieee 802.11 mac layer handoff process," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp. 93–102, 2003.

[14] "IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, 2012.

[15] "IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," *IEEE Std 802.11i-2004*, pp. 1–175, 2004.

[16] S. F. Hasan, N. H. Siddique, S. Chakraborty, X. Ding, and W. Gao, "Scanning and address allocation delays in vehicular communications," *Wireless Personal Communications*, vol. 68, no. 4, pp. 1415–1433, 2013.

[17] J. Xie and X. Wang, "A survey of mobility management in hybrid wireless mesh networks," *Network, IEEE*, vol. 22, no. 6, pp. 34–40, 2008.

[18] W. Croft and J. Gilmore, *"RFC 951 - Bootstrap Protocol"*, 1985.

[19] W. Wimer, *"RFC 1542 - Clarifications and Extensions for the Bootstrap Protocol"*, 1993.

[20] M. Patrick, *"RFC 3046 - DHCP Relay Agent Information Option"*, 2001.

[21] I. Ramani and S. Savage, "Syncscan: practical fast handoff for 802.11 infrastructure networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 1. IEEE, 2005, pp. 675–684.

[22] Y.-S. Chen, M.-C. Chuang, and C.-K. Chen, "Deucescan: deuce-based fast handoff scheme in ieee 802.11 wireless networks," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 2, pp. 1126–1141, 2008.

[23] H. Y. Lee, J. W. Park, T. M. Bae, S. U. Choi, and Y. H. Ha, "Adaptive scan rate up-conversion system based on human visual characteristics," *Consumer Electronics, IEEE Transactions on*, vol. 46, no. 4, pp. 999–1006, 2000.

[24] I. F. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-ip-based wireless systems," *Wireless Communications, IEEE*, vol. 11, no. 4, pp. 16–28, 2004.

[25] H. Soliman, L. Bellier, K. Elmalki, and C. Castelluccia, "Hierarchical mobile IPv6 (HMIPv6) mobility management," 2008.

[26] A. G. Valkó, "Cellular IP: a new approach to internet host mobility," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 1, pp. 50–65, 1999.

[27] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S.-Y. Wang, and T. La Porta, "Hawaii: a domain-based approach for supporting mobility in wide-area wireless networks," *Networking, IEEE/ACM Transactions on*, vol. 10, no. 3, pp. 396–410, 2002.

[28] A. McAuley, S. Das, S. Baba, and Y. Shobatake, "Dynamic Registration and Configuration Protocol (DRCP)," *draft-itsumo-drcp-01.txt*, 2001.

[29] S. Park, P. Kim, and B. Volz, *"RFC 4039 - Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)"*, 2005.

[30] E. Ancillotti, R. Bruno, M. Conti, and A. Pinizzotto, "Dynamic address autoconfiguration in hybrid ad hoc networks," *Pervasive and Mobile Computing*, vol. 5, no. 4, pp. 300–317, 2009.

[31] "IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 10: Mesh Networking," *"IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011)"*, pp. 1–372, 2011.

[32] "The open80211s Project," http://open80211s.org/open80211s, accessado em Agosto de 2013.

[33] A. Orebaugh, G. Ramirez, and J. Burke, *Wireshark & Ethereal network protocol analyzer toolkit*. Syngress Media Inc, 2007.

[34] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, and K. Gibbs, "Iperf: The TCP/UDP bandwidth measurement tool," 2005.