UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

HELGA DOLORICO BALBI

ESTUDO E IMPLEMENTAÇÃO DE CONTROLADOR CENTRAL PARA PONTOS DE ACESSO IEEE 802.11 DE BAIXO CUSTO

NITERÓI
2012

UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

HELGA DOLORICO BALBI

ESTUDO E IMPLEMENTAÇÃO DE CONTROLADOR CENTRAL PARA PONTOS DE ACESSO IEEE 802.11 DE BAIXO CUSTO

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Sistemas de Telecomunicações

Orientador:
Prof. Dr. Luiz Cláudio Schara Magalhães

NITERÓI
2012

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

B172 Balbi, Helga Dolorico

Estudo e implementação de controlador central para pontos de acesso IEEE 802.11 de baixo custo / Helga Dolorico Balbi. – Niterói, RJ : [s.n.], 2012.

157 f.

Dissertação (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense, 2012.

Orientador: Luiz Cláudio Schara Magalhães.

1. Sistema de telecomunicações. 2. Rede sem fio. 3. Tecnologia IEEE 802.11. 4. Sistema de Controle Inteligente para Redes sem Fio. I. Título.

CDD 621.382

ESTUDO E IMPLEMENTAÇÃO DE CONTROLADOR CENTRAL PARA PONTOS DE ACESSO IEEE 802.11 DE BAIXO CUSTO

HELGA DOLORICO BALBI

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Sistemas de Telecomunicações

Aprovada por:

_____

Prof. Dr. LUIZ CLAUDIO SCHARA MAGALHÃES - Orientador

Universidade Federal Fluminense

_____

Profª. Drª. NATALIA CASTRO FERNANDES

Universidade Federal Fluminense

_____

Prof. Dr. SIDNEY CUNHA DE LUCENA

Universidade Federal do Estado do Rio de Janeiro

Niterói, 18 de Dezembro de 2012

Dedico este trabalho a meus pais e professores.

AGRADECIMENTOS

Primeiramente, agradeço a minha família por me dar o apoio necessário em todas as minhas escolhas.

Aos meus colegas dos projetos RUCA e SCIFI, Arthur Guerrante e Felipe Rolim e Souza.

Aos companheiros do MídiaCom: Clayton, Edelberto e Diego, por perder seu precioso tempo inúmeras vezes para me ajudar nas mais diversas tarefas.

À Marister, por deixar o ambiente do MídiaCom sempre mais agradável.

Aos professores Débora Muchaluat, Célio Albuquerque, Ricardo Carrano, Natalia Castro Fernandes e Luiz Claudio Schara Magalhães pelo esforço constante em prol do crescimento e reconhecimento do nosso grupo de pesquisa.

E à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e Rede Nacional de Ensino e Pesquisa (RNP) por financiar o desenvolvimento da pesquisa descrita nesta dissertação.

RESUMO

Tendo em vista a escassez do espectro de frequências disponível, e a crescente demanda pela utilização da tecnologia IEEE 802.11, o compartilhamento do meio sem fio tem se tornado uma grande preocupação para administradores de redes. Buscando reduzir interferência entre os dispositivos sem fio, o administrador da rede pode escolher parâmetros de operação dos pontos de acesso. Atualmente, as soluções comerciais voltadas para este objetivo operam de forma centralizada e buscam automatizar a configuração dos pontos de acesso facilitando o processo de gerenciamento da rede. Entretanto, estas soluções são caras e trabalham com *hardwares* específicos. No caso da utilização de pontos de acesso baratos, que são destinados ao uso doméstico, existe a carência de um sistema que facilite o gerenciamento da rede, tratando o problema da interferência de forma automática e centralizada. Buscando suprir esta necessidade, o **S**istema de **C**ontrole **I**nteligente para redes sem **Fi**o (SCIFI) foi criado pela Universidade Federal Fluminense (UFF) com apoio da Rede Nacional de Ensino e Pesquisa (RNP). Os principais objetivos do SCIFI são reduzir as áreas de sobreposição de cobertura ocasionada entre pontos de acesso próximos através da escolha dinâmica de seus canais e potência de transmissão, e automatizar este processo, facilitando a gerência da rede. O sistema é capaz de operar com pontos de acesso de baixo custo desde que suportem a instalação de um *firmware* baseado em Linux. Ao contrário de outras propostas encontradas na literatura, o algoritmo de alocação de canais do SCIFI considera a interferência ocasionada por pontos de acesso que não pertencem ao mesmo domínio administrativo. Este trabalho mostra todo estudo realizado para a implementação do SCIFI, bem como os resultados dos testes que foram realizados em uma rede piloto instalada na UFF para a avaliação do sistema. Os resultados mostram que o sistema é capaz de beneficiar a rede como um todo, incluindo redes não administradas, através do aumento de suas vazões.

ABSTRACT

Given the scarcity of available frequency spectrum and increasing demand for the use of IEEE 802.11 technology, the sharing of the wireless medium has become a major concern for network administrators. Aiming to minimize the communication degradation caused by excessive interference between wireless devices, the network administrator can choose specific parameters of managed access points. Currently, commercial solutions that aim to reduce interference and automate the configuration of access points centrally, facilitating the management process, are expensive and work only with specific and expensive hardware. On the other hand, cheap access points are usually intended for domestic use and lack of a central system to facilitate the network management and to address the problem of interference automatically. Aiming to fill this need, the Intelligent Control System for Wireless Networks (SCIFI) was created by the Federal Fluminense University (UFF) with support from the National Education and Research Network (RNP). The main objectives of SCIFI are reduce overlapping areas of coverage caused among nearby access points through the dynamic choice of their operating channels and transmission power, and automate this process, facilitating network management. The system is capable of operating with low cost access points, since they can support the installation of a Linux-based firmware. Unlike other proposals found in literature, SCIFI´s channel allocation algorithm also considers the interference caused by unmanaged networks. This work shows the entire study for the implementation of SCIFI, and the results of tests that were performed on a pilot network installed in UFF for system evaluation. The results show that the network as a whole, including those belonging to other administrative domains, may benefit with the increase in its throughput when using the system.

PALAVRAS CHAVE

Redes sem fio, IEEE 802.11, OpenWRT, controle de potência, alocação de canais, sistema de controle, redes infraestruturadas.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE EQUAÇÕES

LISTA DE ACRÔNIMOS

ACK - Acknowledgment

ADSP - Motorola Air Defense Services Platform

AID - Association ID

AP – Access Point ou Ponto de Acesso

ARM - Adaptive Radio Management

ARQ - Automatic Repeat reQuest

AWMS - AirWave Wireless Management Suite

BSS - Basic Service Set

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CAPWAP - Control and Provisioning of Wireless Access Points protocol

CCA - Clear Channel Assessment

CMIP - Common Management Information Protocol

CSMA – Carrier Sense Multiple Access

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

CTS – Clear to Send

DCA - Dynamic Channel Assignment

DCF - Distributed Coordination Function

DHCP - Dynamic Host Configuration Protocol

DIFS - DCF Interframe Space

DS – Distribution System

DSSS - Direct-Sequence Spread-Spectrum

DTLS - Datagram Transport Layer Security

EAP - Extensible Authentication Protocol

EAPOL - EAP Over LANs

EIFS - Extended interframe space

ESS - Extended Service Set

ESSID - Extended Service Set ID

FHSS - Frequency-Hopping Spread-Spectrum

GPS - Global Positioning System

HCF - Hybrid Coordination Function

HTTP - Hypertext Transfer Protocol

HR/DSSS - High-Rate Direct-sequence Spread-spectrum

IBSS - Independent BSS

ICMP - Internet Control Message Protocol

IEEE – Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IP – Internet Protocol

LAN – Local Area Network

LAP - Lightweight Access Point

LCCS - Least Congested Channel Search

LWAPP - Lightweight AP Protocol

MAC - Medium Access Control

MIB - Management Information Base

NAT - Network Address Translation

NAV - Network Allocation Vector

NETCONF - Network Configuration protocol

OFDM - Orthogonal Frequency Division Multiplexing

OSI - Open Systems Interconnection

PAPI - Proprietary Access Protocol Interface

PC – Personal Computer

PCF - Point Coordination Function

PIFS - PCF Interframe Space

PHY - Physical layer

RAM - Random Access Memory

RF – Radio Frequency

RNP – Rede Nacional de Pesquisa

RSSI – Received Signal Strength Indication

RTS – Request To Send

RRM - Radio Resource Management

SCIFI - Sistema de Controle Inteligente para redes sem FIo

SCP - Secure Copy Protocol

SIFS - Short Interframe Space

SMI - Structure of Management Information

SNMP - Simple Network Management Protocol

SOHO – Small Office Home Office

SSH - Secure Shell

SSID – Service Set Identification

TCP – Transport Control Protocol

TPC - Transmit Power Control

UDP – User Datagram Protocol

UFF – Universidade Federal Fluminense

VLAN – Virtual LAN

Wi-Fi – Wireless Fidelity

WISP - Wireless Switch Protocol

WISPe - Wireless Switch Protocol enhanced

WLAN - Wireless LAN

WLC - Wireless LAN Controller

1. INTRODUÇÃO

A progressiva diminuição de custo aliada ao crescente uso de dispositivos móveis tem criado enorme demanda para a instalação de infraestrutura de redes sem fio baseadas no padrão IEEE 802.11 [1]. Com o aumento do número de usuários, é necessário também aumentar o número de pontos de acesso para atendê-los de forma a manter os requisitos tanto de cobertura como de banda disponível. Progressos como a adoção do novo padrão IEEE802.11n ajudam a aumentar a banda disponível, mas as redes com muitos pontos de acesso (APs - do inglês *Access Points*) possuem seus próprios desafios. Ao se aumentar a escala da rede sem fio de poucos *hotspots* para instalações onde se espera cobertura completa de todos os locais, a configuração e a administração da rede se tornam cada vez mais complexas.

A utilização de vários pontos de acesso pode ocasionar má utilização espectral caso seja realizada sem coordenação. Isto porque pontos de acesso com certa proximidade acabam por compartilhar o meio de radio frequência (RF), interferindo entre si, devido a dois motivos: apenas duas faixas de frequências estão disponíveis para o uso de redes 802.11 no Brasil (2,4 GHz e 5GHz), e o número de canais de operação dentro destas faixas é limitado, principalmente para o padrão 802.11g que é o mais utilizado atualmente. Além disso, como ambas as faixas não necessitam de licenciamento para operação, muitos outros dispositivos, como telefones sem fio, *Bluetooth* e fornos de micro-ondas, operam nestas faixas, representando fontes de interferência para os dispositivos 802.11. Neste cenário, a coordenação entre pontos de acesso se torna interessante por proporcionar redução da

interferência e consequente melhoria de desempenho da rede.

O emprego de vários pontos de acesso também é comum em ambientes com alta demanda por conexão, tendo em vista que o uso de vários canais (um canal por AP) aumenta a banda disponível e o número de associações que um AP pode suportar é limitado de acordo com sua capacidade de processamento. Entretanto, além da interferência, outro problema pode ocorrer neste caso. Tendo em vista que a associação ao ponto de acesso é comandada pelo dispositivo cliente e, atualmente, este processo não considera a carga na rede, não é garantido que, adicionando-se mais APs em uma mesma região, haverá distribuição homogênea de clientes entre eles. Desta forma, um AP pode se encontrar sobrecarregado, enquanto outro, que se encontra próximo deste, pode estar ocioso.

Pontos de acesso de baixo custo encontrados no mercado, em sua maioria, foram desenvolvidos para operar em ambientes domésticos com baixa demanda de usuários e cobertura. Geralmente, possibilitam configuração apenas através de interface *web* e não possuem mecanismos para coordenação automática entre APs, mesmo quando operam em uma mesma rede. Com isso, a gerência de redes compostas por muitos destes dispositivos se torna trabalhosa e, caso não seja realizado um estudo do ambiente (*site survey*), a configuração manual de cada AP pode ocasionar baixo desempenho, devido à má utilização espectral.

Atualmente, empresas do ramo de redes 802.11 disponibilizam dois tipos de soluções para instituições com alta demanda de usuários e cobertura, conhecidas como soluções *Enterprise*. O primeiro tipo fornece pontos de acesso de alto desempenho, que utilizam técnicas avançadas para aumentar o alcance e a quantidade de clientes suportada, podendo também incorporar mecanismos descentralizados para coordenação automática entre APs como, por exemplo, a seleção do canal de operação do AP. O segundo tipo de solução é a utilização do que se convencionou chamar “*thin APs*” ou "*fit APs*" [2] , que seriam pontos de acesso que transfeririam parte de suas funcionalidades para um controlador central.

Estas duas abordagens são significantemente mais onerosas do que a solução para ambientes domésticos, mesmo quando vários pontos de acesso são utilizados. Enquanto que, atualmente, cinco pontos de acesso domésticos podem ser adquiridos por cerca de mil reais, uma solução *Enterprise* que apresente capacidade ou cobertura equivalente facilmente chegará ao custo de mais de vinte mil reais (considerando dois pontos de acesso e um controlador de hardware). A grande desvantagem da solução de baixo custo, nesse caso, é a carência de coordenação entre pontos de acesso e dificuldade de configuração e

gerenciamento.

Tendo em vista esta dificuldade de gerenciamento de uma rede composta por muitos APs de baixo custo, e a interferência excessiva que pode ser ocasionada entre APs quando utilizados de forma descoordenada, o trabalho apresentado nesta tese busca a criação de um sistema de controle centralizado para redes 802.11 infraestruturadas capaz de tornar automática e dinâmica a configuração de pontos de acesso, de forma a facilitar a gerência da rede e reduzir a interferência excessiva nos pontos de acesso.

O controlador desenvolvido neste trabalho, intitulado **S**istema de **C**ontrole **I**nteligente para Redes Sem **FI**o (SCIFI), utiliza informações de interferência coletadas do ambiente e a informação do número de clientes associados aos pontos de acesso para executar três funções principais, que são:

1) Selecionar os canais de operação dos APs
2) Realizar a configuração da potência de transmissão dos APs.
3) Fornecer ao cliente informação de carga na rede, indicando quais são as melhores opções de associação.

As funções implementadas buscam a redução da interferência nos pontos de acesso e o balanceamento da carga na rede. Apesar de terem sido implementadas apenas três funcionalidades, a arquitetura modular do controlador permite que novas funcionalidades sejam adicionadas futuramente.

Os requisitos do sistema foram: a utilização do padrão 802.11, de forma a possibilitar a utilização do sistema em redes atuais; evitar modificações nos dispositivos clientes, buscando manter maior compatibilidade; utilizar *software* livre e ser compatível com *hardware* atual, de forma a reduzir custos de implantação da rede. O único requisito para os pontos de acesso deste sistema é que sejam compatíveis com uma versão de Unix (Linux) embarcada, como o OpenWRT [3]. Atualmente, já se pode encontrar no mercado brasileiro diversos modelos[1] de pontos de acesso de baixo custo compatíveis com este *firmware*, que se mostra interessante por ser livre, robusto, possibilitar instalação de novas ferramentas, suportar grande gama de dispositivos, e estar em constante desenvolvimento.

Esta dissertação, além de descrever o sistema de controle desenvolvido e seus algoritmos, mostra todo o estudo realizado como base para seu desenvolvimento. Além disso,

[1] Dentre os disponíveis, usamos os modelos Linksys WRT54G, DLink DIR320 e os modelos Bullet, NanoStation e PicoStation da Ubiquiti.

mostra o resultados dos testes de validação do sistema implementado, realizados em uma rede piloto instalada na Escola de Engenharia da Universidade Federal Fluminense (UFF).

O sistema está sendo utilizado como solução para instalação da rede sem fio institucional da UFF, devido ao seu baixo custo, facilidade de gerenciamento e instalação, e robustez. Outras universidades e centros de pesquisa, como a Universidade Federal de Ouro Preto, Universidade Federal do Paraná e Universidade Federal de Viçosa já estão usando ou começando a usar o SCIFI.

O trabalho está organizado da seguinte forma: o Capítulo 2 traz uma introdução ao padrão IEEE 802.11, suas arquiteturas de rede e seu mecanismo de acesso ao meio; o Capítulo 3 faz uma apresentação dos trabalhos relacionados ao sistema proposto e de alguns sistemas comerciais; o Capítulo 4 descreve o sistema de controle implementado; o Capítulo 5 mostra os testes realizados para validação do sistema; e por fim, conclusões sobre o trabalho são feitas no Capítulo 6.

2. O PADRÃO IEEE 802.11

2.1. ARQUITETURA

Segundo Gast [4] uma rede 802.11 é composta por quatro dispositivos principais, que são:

1) Estações (STA – *station*): são dispositivos que possuem interfaces sem fio 802.11 e trocam informações através da rede. Podem ser dispositivos móveis, como celulares, *laptops*, ou fixos, como Desktops;

2) Pontos de acesso (AP – *access point*): Pontos de acesso são um tipo especial de estação que podem exercer diversas funções. Entre elas, a função de *bridge*, na qual os dados da rede sem fio são convertidos para serem transmitidos em rede cabeada, é a mais importante. Basicamente, os pontos de acesso possibilitam a comunicação entre estações sem fio, e entre estações sem fio e cabeadas.

3) Meio sem fio: é o meio através do qual a informação irá trafegar. O mais comumente utilizado é o meio de rádio frequência.

4) Sistema de distribuição (DS – *Distribution System*): é o componente que interliga os pontos de acesso e possibilita a troca dados entre eles. O sistema de distribuição, ou *backbone*, é utilizado quando mais de um ponto de acesso é empregado na rede. O mais comum é a utilização de redes Ethernet como sistema de distribuição, entretanto, redes de outros padrões e até mesmo sem fio também podem ser utilizadas para exercer esta função.

Uma rede 802.11 é constituída por um conjunto de estações que podem se comunicar umas com as outras. Estas estações formam o BSS (*Basic Service Set*) e a área na qual a comunicação é possível é conhecida por *Basic Service Area*. Esta área é dada em função das características de propagação do meio, que podem variar dinamicamente e de forma imprevisível. Portanto, pequenas mudanças na posição ou direção dos dispositivos, bem como a movimentação de pessoas e objetos, podem resultar em grandes variações no nível de sinal recebido. Em uma mesma sala, por exemplo, a variação do nível de sinal em cada posição pode chegar a 50dB [1]. Desta forma, diagramas que por ventura forem encontrados nesta tese mostrando a área de cobertura de pontos de acesso como sendo circulares são apenas aproximações.

O BSS pode ser estruturado de forma independente (IBSS - *independent BSS*) ou de forma infraestruturada. Na forma independente, também conhecida como *ad hoc*, as estações se comunicam diretamente umas com as outras e, para tanto, ambas necessitam estar no alcance mútuo da transmissão/recepção de rádio. Na forma infraestruturada, um ponto de acesso é utilizado como origem ou destino de todas as transmissões, inclusive para intermediar a comunicação entre as estações sem fio. Desta forma, a *Basic Service Area* é definida como a área de alcance do ponto de acesso. Uma das vantagens desta arquitetura é que não há restrição de distância entre as estações, mas apenas entre a estação e o ponto de acesso. Além disso, a complexidade desta arquitetura é menor, dado que as estações não necessitam guardar informações sobre seus vizinhos, mas apenas sobre o ponto de acesso. Finalmente, acesso Internet só é comum em redes infraestruturadas, a não ser que as estações da rede ad hoc utilizem algum software de roteamento.

Em uma rede infraestruturada, as estações necessitam se associar e se autenticar a um ponto de acesso para que a comunicação entre eles possa ser realizada. Este processo é iniciado pela estação, também conhecida como cliente, e o ponto de acesso pode aceitar ou rejeitar uma associação. O padrão não restringe de forma prática o número de estações associadas a um ponto de acesso[2], entretanto, limitações podem ser ocasionadas pela

[2] Quando uma estação se associa a um AP, este designa à ela um valor conhecido por AID (*Association ID).* O valor máximo do AID é 2007 [4], o que limitaria o número de estações associadas a um único ponto de acesso em 2007, mas este valor é muito maior do que o aceitável atualmente para que se tenha um desempenho razoável da rede sem fio.

capacidade do hardware dos pontos de acesso em lidar com associações, e pela baixa vazão que pode ser disponibilizada para cada cliente da rede no caso em que muitos deles dividem o mesmo meio de transmissão.

Buscando a cobertura de grandes áreas, o padrão 802.11 possibilita que vários BSSs possam ser agrupados em um ESS (*Extended Service Set*). Para que isto seja possível, os BSSs devem ser interligados por uma infraestrutura de rede (*Distribution System* - DS) e devem possuir o mesmo SSID (*Service Set Identifier*), que é um parâmetro que representa o nome da rede para as estações clientes. Para que as estações do ESS possam se comunicar entre elas e trafegar entre diferentes BSSs, os pontos de acesso devem operar em camada 2 (enlace) como *bridges*, e o *backbone* também deve ser de camada 2, podendo englobar a utilização de *hubs*, *switches* ou de *VLANs*.

O sistema apresentado nesta dissertação foi desenvolvido para operar em redes 802.11 infraestruturadas e insere um novo dispositivo na arquitetura: o controlador central. Este controlador possui a função determinar os canais e potências de transmissão que serão utilizados pelos pontos de acesso da rede. Para tanto, ele se comunica com os pontos de acesso através de rede IP (camada 3) para ordenar que certas funções sejam executadas, dados sejam coletados e parâmetros de configuração sejam definidos. Mais detalhes sobre o sistema serão apresentados nas próximas seções.

2.2. MECANISMO DE ACESSO AO MEIO

O 802.11 é um membro da família IEEE 802, que engloba uma série de especificações tecnológicas para redes locais (LAN – *Local Area Network*). Especificações IEEE 802 abrangem as duas camadas mais baixas do modelo OSI (*Open Systems Interconnection*)[5], incorporando componentes das camadas física e de enlace. Todas as redes 802 possuem os componentes MAC (*Medium Access Control*) e PHY (*Physical Layer*), como mostra a Figura 1. O MAC engloba um conjunto de regras que determinam como se dá o acesso ao meio para o envio de dados, enquanto o PHY se encarrega dos detalhes da transmissão e recepção.

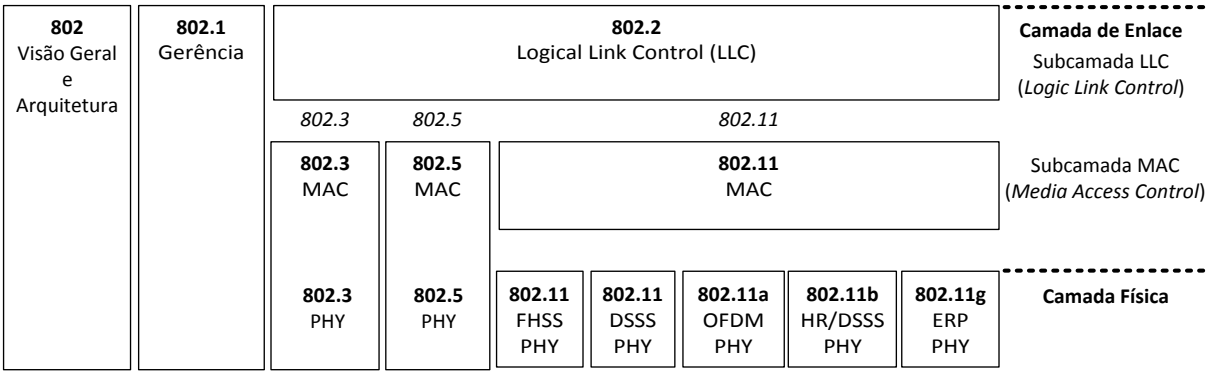


Figura 1. A família IEEE 802 e sua relação com o modelo OSI [4]

A especificação 802.11 original inclui o MAC do 802.11 e duas camadas físicas (PHY): FHSS (*frequency-hopping spread-spectrum*) e DSSS (*direct-sequence spread-spectrum*). Novas especificações de camadas físicas foram adicionadas em revisões posteriores do padrão. Dentre elas, o 802.11b especifica a camada HR/DSSS (*high-rate direct-sequence spread-spectrum layer*). Produtos baseados neste padrão chegaram ao mercado em 1999 e foram os primeiros consumidos em grande escala. Já o padrão 802.11a especifica a camada física baseada em OFDM (*orthogonal frequency division multiplexing*), enquanto o 802.11g, que é o mais utilizado atualmente, oferece altas taxas através do uso do OFDM sem perder compatibilidade com o padrão 802.11b. Entretanto, quando um ponto de acesso fornece compatibilidade e está atendendo a clientes de ambos os padrões (b e g), o desempenho da rede será deteriorado, tendo em vista que, mesmo ao se comunicar com clientes do padrão g, o cabeçalho dos quadros enviados pelo AP deverão sem compatíveis com o padrão b para que todos os clientes da rede, incluindo os que utilizam padrão b, possam recebê-lo.

Após o lançamento do 802.11, buscando promover a adoção da tecnologia, a aliança Wi-Fi (*Wireless Ethernet Compatibility Alliance*) [6] foi criada em 1999. A aliança, que é composta por empresas do ramo, certifica produtos que se enquadram em determinados padrões de interoperabilidade. Desta forma, o consumidor possui garantia de que seu dispositivo certificado pelo Wi-Fi será compatível com outros que também possuem o certificado. Entretanto, para que um dispositivo seja certificado, ele deve oferecer apenas determinados elementos críticos do padrão 802.11 e possuir características que são julgadas importantes pela aliança, como por exemplo, possuir determinada performance mínima em determinado quesito. Tendo em vista que este certificado não exige conformidade total com todos as elementos do 802.11 e é o mais respeitado atualmente, é esperado que algumas das

funcionalidades descritas no padrão não sejam encontradas comumente nos dispositivos comercializados. Um exemplo é a função *Point Coordination Function* (PCF), que será descrita a seguir. Esta função, apesar de estar descrita no padrão 802.11 não está inclusa na certificação Wi-Fi.

No 802.11, para que o meio rádio possa ser compartilhado por muitas estações, o acesso ao meio é controlado por uma das funções de coordenação. Existem três funções de coordenação, que são: DCF (*Distributed Coordination Function*); PCF (*Point Coordination Function*); e HCF (*Hybrid Coordination Function*). A função DCF, que é a função comumente utilizada[3] e é o foco deste trabalho, provê acesso ao meio com contenção através do mecanismo CSMA/CA (*Carrier Sense Multiple Access with Colision Avoidance*). A função PCF, que não é comumente empregada, foi criada para prover suporte a aplicações de tempo real e permite que uma rede 802.11 forneça acesso justo ao meio através de um mecanismo parecido com o de redes baseadas em *token*, no qual o ponto de acesso é encarregado das funções de controle do *token*. A terceira função, a HCF, foi criada para aplicações que necessitam de qualidade de serviço, mas não com o rigor oferecido pelo PCF. Esta função possibilita que as estações favoreçam o acesso ao meio para aplicações que requerem melhor qualidade de serviço.

O padrão 802.11 é um tipo de adaptação do padrão Ethernet (IEEE 802.3) para o funcionamento em enlaces rádio. Assim como o padrão Ethernet, o MAC do 802.11 possibilita, através da função DCF, a utilização do mecanismo CSMA (*Carrier Sense Multiple Access*) para controlar o acesso ao meio de transmissão de forma distribuída. Neste mecanismo, cada estação deve escutar o meio antes de realizar uma transmissão e só poderá transmitir caso este esteja ocioso. O padrão Ethernet também utiliza um mecanismo de detecção de colisão (CSMA/CD, do inglês, *Carrier Sense Multiple Access with Collision Detection*), que possibilita a verificação da ocorrência de transmissões simultâneas. Com este mecanismo, quando uma colisão é detectada, a transmissão pode ser interrompida evitando desperdício de utilização do meio. Já no 802.11, como um transmissor não consegue receber enquanto está transmitindo, ao invés de se utilizar o CSMA/CD, o mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), é utilizado. Uma colisão ocorre

[3] Porque é a única que está presente na especificação do Wi-Fi [6].

caso uma ou mais estações transmitam simultaneamente[4]. Após verificar uma colisão, para evitar que outras ocorram, cada estação deverá aguardar um período de tempo aleatório antes de realizar nova transmissão, conhecido como período de *backoff*. Os detalhes do funcionamento deste mecanismo serão apresentados adiante.

Com o objetivo de atenuar os problemas causados pela maior taxa de erros de bits do enlace rádio em relação ao enlace físico utilizado no Ethernet, o padrão 802.11 emprega um mecanismo de retransmissão conhecido por ARQ (*Automatic Repeat Request*). Neste mecanismo, quando uma estação recebe um quadro e este passa na verificação de erros, um quadro de reconhecimento conhecido por ACK (*Acknowledgment*) é enviado à estação transmissora. A sequencia Quadro–ACK, como mostra a Figura 2, é considerada uma operação atômica, ou seja, é considerada uma unidade de transação indivisível que só é realizada com sucesso caso todos os seus passos ocorram corretamente. Caso o ACK não seja recebido, seja pela ocorrência de erros no quadro ou pela perda do próprio ACK durante sua transmissão, a transação é perdida e o quadro deve ser retransmitido.

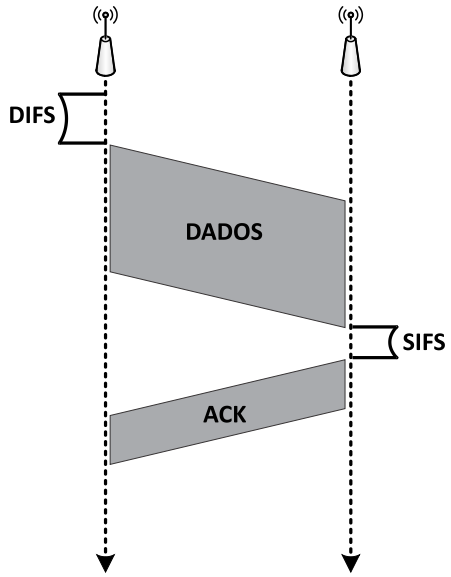


Figura 2. Operação Atômica Quadro-Ack do 802.11 no modo DCF [7]

Outro problema comum em enlaces sem fio é o problema do nó oculto, causado pelo fato de que um nó pode não receber o sinal proveniente de todos os nós da rede. Como mostra

[4] A janela de colisão é dada pela distância entre as estações e a velocidade de propagação do sinal.

a Figura 3, o nó B é capaz de receber o sinal proveniente da estação A, entretanto, a estação C não. Neste caso, se A está transmitindo para B, C não conseguirá perceber que o meio está ocupado, já que é incapaz de escutar o sinal de A. Portanto, C transmitirá para B, causando colisão em B. Neste primeiro exemplo, o sinal de A não alcança C devido à existência de uma montanha que o bloqueia, entretanto, problema semelhante pode ser notado no caso em que há desvanecimento do sinal na medida em que se propaga pelo meio. Por exemplo, como mostra a Figura 4, o nó B consegue receber o sinal dos nós A e C, já que se encontra entre eles. Entretanto, como A e C estão distantes, não recebem o sinal proveniente um do outro, ocasionando colisão em B como no exemplo anterior. Neste exemplo, C é um nó oculto para A e vice-versa.

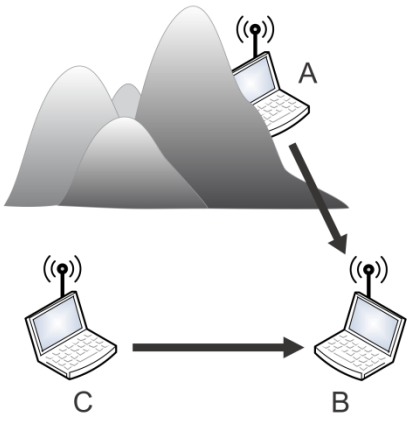


Figura 3. Problema do nó oculto [7]

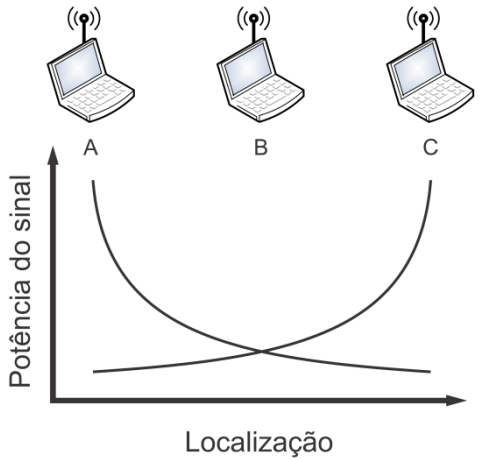


Figura 4. Problema do desvanecimento do sinal [7]

Buscando minimizar o problema de colisões causadas por nós ocultos e pelo desvanecimento do sinal, o 802.11 utiliza um mecanismo opcional para a alocação inteligente

do meio realizado através da troca de quadros curtos RTS (*request to send*) e CTS (*clear to send*). Nesta operação atômica, ou seja, funcionalmente indivisível, como mostra a Figura 5, quando a estação Fonte deseja transmitir, ela envia ao nó Destino um quadro RTS que expressa o seu desejo de transmitir. Ao receber este quadro, a estação Destino envia um quadro CTS destinado a todas as estações que seu sinal possa alcançar (*broadcast*). Este quadro, além de dar permissão de transmissão ao nó Fonte, também instrui os outros nós a não transmitir durante o tempo registrado no campo NAV (*Network Allocation Vector*) do quadro CTS, que informa o tempo que será utilizado para a transmissão atômica dados+ACK, como mostra a Figura 6. Como o CTS será capaz de alcançar estações ocultas ao nó Fonte, colisões provenientes destas estações poderão ser evitadas.

O mecanismo RTS/CTS pode ser de grande utilidade em ambientes densos, com muitas redes que possuem áreas de cobertura sobrepostas. Todas as estações que utilizam o mesmo canal físico e receberem o NAV irão considerá-lo, mesmo estando em redes diferentes. Entretanto, este mecanismo possui a desvantagem de consumir recursos e causar latência na transmissão. Por esta razão sua utilização é recomendada apenas para quadros grandes que seriam capazes de gerar maiores perdas no caso da ocorrência de uma colisão. Para estabelecer em que situações este mecanismo deve ser utilizado, um limiar (*threshold*) configurável é definido no ponto de acesso de forma que apenas quadros com comprimento maior do que este limiar sejam transmitidos com a utilização do RTS/CTS.

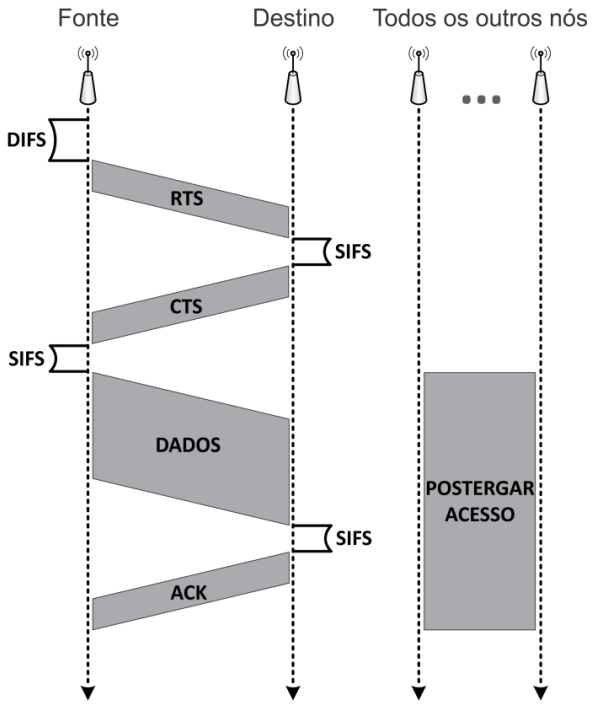


Figura 5. Utilização dos quadros RTS/CTS como prevenção de colisões [7]

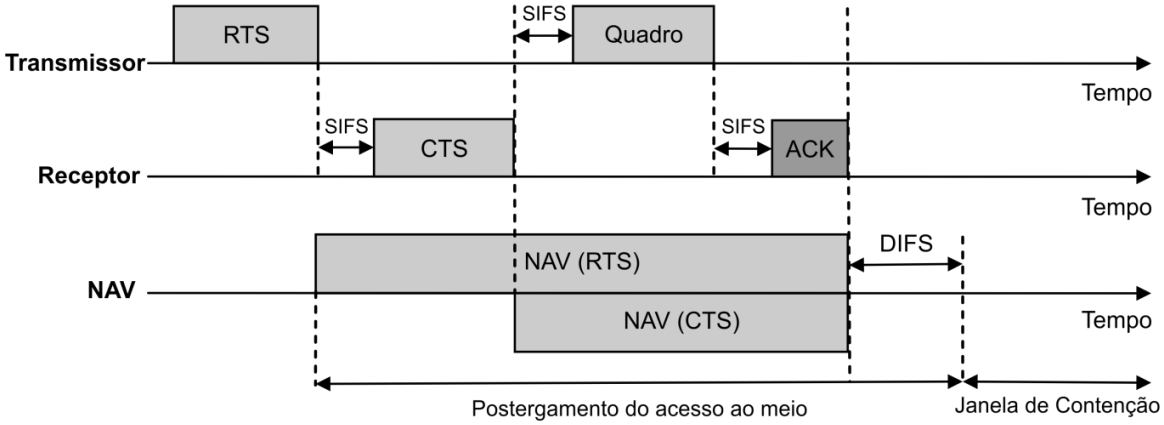


Figura 6. Utilização do campo NAV para reserva do meio na utilização do RTS/CTS [4]

Outra desvantagem do mecanismo RTS/CTS é que nem sempre ele é capaz de evitar o problema do nó escondido. A Figura 7 exemplifica o problema da "estação mascarada" (*masked-station problem* [8] *)*, que é uma situação em que isto ocorre. Nesta figura, suponha que D deseja transmitir para E e envia um quadro RTS. A estação E responde com um quadro CTS e a transmissão é iniciada. Neste momento, C está bloqueado devido ao RTS de D. Durante esta transmissão, A deseja transmitir para B e envia um quadro RTS. A estação B responde com um CTS, porém, C não é capaz de receber este quadro devido à transmissão de D para E, que já estava em andamento. Quando uma estação entra neste estado, ela é dada como "mascarada". Desta forma, assim que D completar sua transmissão, dois eventos podem

ocorrer: (a) a estação C inicia a transmissão para B ou D e o envio do RTS gera colisão em B, atrapalhando a transmissão que está em andamento de A para B; (b) a estação D envia um RTS para C, que responde com um CTS que irá interferir na transmissão de A para B. Neste caso, além dos dados serem perdidos, a estação B não receberá o CTS proveniente de C, se tornando "mascarada". Desta forma, as estações vizinhas mascaradas passam a ocasionar grandes sequencias de colisões.

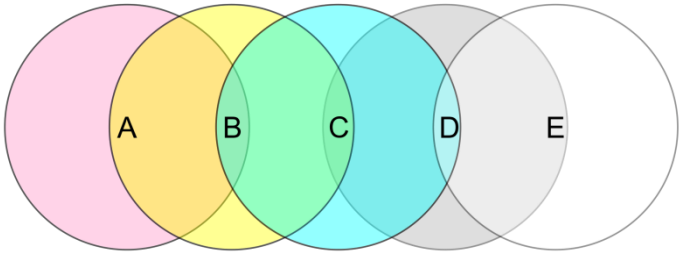


Figura 7. Exemplo em que o RTS/CTS não é capaz de solucionar o problema do nó oculto

Outra desvantagem conhecida é que o uso do RTS/CTS pode inibir transmissões de determinadas estações, mesmo quando teriam sucesso utilizando apenas o mecanismo CSMA/CA. A Figura 8 ilustra um exemplo deste problema. Nesta figura, os círculos indicam as áreas de cobertura de cada estação. Suponha que a estação A deseja transmitir para B. Para iniciar a transmissão, A envia o quadro RTS e B o recebe, respondendo com um quadro CTS, que é recebido por A e C. A seguir, a estação A inicia sua transmissão. No mesmo momento, D deseja transmitir para C e envia um quadro RTS. Neste caso, como C não está no alcance de A, poderia receber a transmissão de D com sucesso. Entretanto, como C recebeu o CTS de B, ele não pode responder ao CTS de D. Desta forma a transmissão não ocorre. Esta natureza inibidora do mecanismo RTS/CTS é conhecida como "*gagged-station problem"* [8].

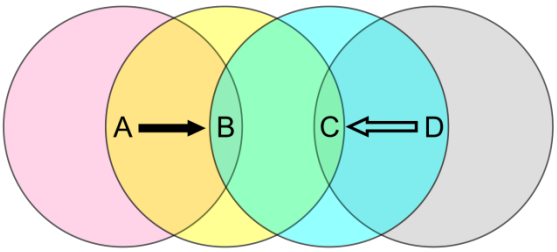


Figura 8. Exemplo em que o RTS/CTS inibe a comunicação de estações que não sofrem interferência.

Como foi dito anteriormente, no mecanismo CSMA/CA a estação verifica se o meio está livre antes de iniciar a transmissão. Existem dois mecanismos de detecção de portadora, o

físico e o virtual. Se um desses mecanismos indica que o meio está ocupado, o MAC reporta isso às camadas superiores. A detecção de portadora física é dada pela camada física e varia de acordo com a modulação utilizada. Já a detecção virtual é dada pelo NAV, que, como foi mostrado anteriormente, é um campo no cabeçalho que indica por quanto tempo (em *microssegundos*) o meio deve ser reservado para determinada transmissão. A estação que deseja enviar dados ajusta o NAV para a duração estimada do envio, incluindo todos os quadros envolvidos na transmissão. As outras estações decrementam o NAV e quando seu valor atinge o zero, o meio é considerado livre.

Para que uma transmissão possa ocorrer, o meio deve ter estado livre por mais do que um determinado tempo, conhecido por intervalo entre quadros (*interframe space*). O 802.11 utiliza três tipos de intervalo entre quadros para o acesso ao meio. Cada um deles possibilita diferente tipo de prioridade no envio de um quadro, já que possuem diferentes durações, como mostra a Figura 9. O SIFS (*Short interframe space*) é utilizado para transmissões de alta prioridade, como quadros ACK, CTS e sequência de quadros contendo fragmentos de um quadro maior, usado quando o tamanho do quadro excede o tamanho (configurável) máximo permitido no enlace. O PIFS (*PCF interframe space*) é utilizado na operação sem contenção provida pelo PCF. Já o DIFS (*DCF interframe space*) é utilizado no acesso com contenção provido pelo DCF. Além dos três *interframe spaces* mencionados, existe o EIFS (*Extended interframe space*), que é um intervalo com duração variável utilizado se houver erros durante a transmissão de quadros.

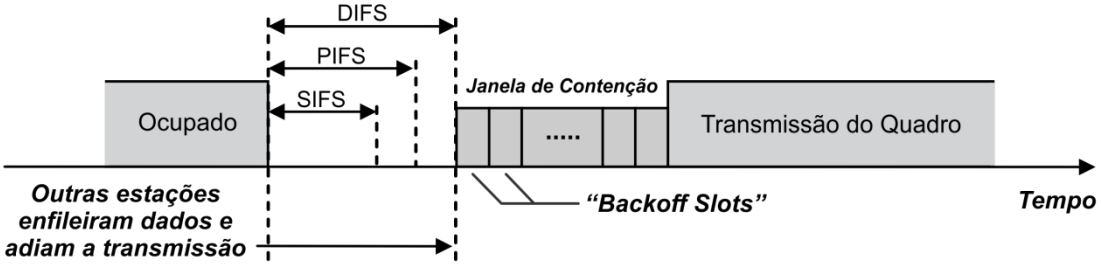


Figura 9. *Interframe spaces* e suas relações. Janela de contenção e seus *slots* [4]

Segundo Gast [4], ao analisar as regras de acesso ao meio do 802.11, existem duas regras básicas que se aplicam a todas as transmissões que utilizam o DCF:

1) Se o meio estiver desocupado por um período de tempo igual ou maior que o DIFS, a transmissão pode ser iniciada imediatamente. O meio deve ser escutado utilizando-se os mecanismos físico e virtual de detecção de portadora, já descritos

anteriormente.

a) Se o quadro anterior foi recebido sem erros, o meio deve permanecer ocioso por um intervalo de um DIFS para que a nova transmissão possa ser realizada.
b) Se houve erro na transmissão anterior, o meio deve permanecer ocioso por um intervalo de um EIFS para que a nova transmissão possa ser realizada.

2) Se o meio está ocupado, a estação deve esperar até que o meio fique ocioso. Esta espera é conhecida por Postergamento de Acesso (do inglês, *Access Deferral*). Neste postergamento, a estação deve aguardar até que o meio fique ocioso por um DIFS e a seguir deve realizar o procedimento conhecido por *Exponential Backoff* que evita que todas as estações tentem transmitir ao mesmo tempo. Após o período do DIFS, um período conhecido por janela de contenção (do inglês, *contention window* ou *backoff window*) é iniciado, como mostra a Figura 9. Esta janela é dividida em faixas (*slots*) cujo tamanho é dependente da taxa de transmissão utilizada. No procedimento do *Exponential Backoff*, as estações que encontram o meio ocupado devem sortear um *slot* no qual a transmissão será iniciada e, após aguardar o DIFS, devem realizar contagem regressiva até que este *slot* seja alcançado. Caso o meio se torne ocupado, o valor do contador permanece estacionário. O número de possíveis *slots* cresce exponencialmente a cada falha da transmissão. Por exemplo, na tentativa inicial, caso o meio esteja ocupado, uma estação 802.11b deverá escolher um dentre 31 *slots*. Caso a estação verifique uma nova falha, o número de *slots* cresce para 63. Caso ocorram duas falhas, o número aumenta para 127 e assim por diante. O número de *slots* é sempre uma potência de 2 reduzida de 1, isto é, 31,63,127,255, ... , e o tamanho máximo da janela depende da camada física. Quando seu tamanho máximo é alcançado, ela permanece neste valor até que possa voltar ao valor inicial. Isto ocorre quando a transmissão é realizada com sucesso ou quando o contador de retransmissões atinge seu valor máximo, ocasionando o descarte do quadro.

Regras adicionais devem ser aplicadas em determinadas circunstâncias:

1) Estações transmissoras são responsáveis pela retransmissão de quadros com erros. Portanto, devem esperar por ACKs e se responsabilizam por retransmitir quadros

até que sua transmissão ocorra com sucesso.

a) A recepção do ACK é o comprovante do sucesso da transmissão. Transações atômicas serão realizadas com sucesso somente se ocorrerem por completo. Se um ACK esperado não chegar, o transmissor deve considerar a transmissão perdida e retransmitir o quadro.
b) Todos os dados *unicast*, ou seja, destinados a um único destino, devem ser reconhecidos através de ACK. Dados *broadcast*, ou seja, destinado a todas as estações, não devem ser reconhecidos pó ACK.
c) A cada falha o contador de retransmissão deve ser incrementado e a retransmissão deve ser novamente realizada. Uma falha pode ser ocasionada quando uma estação não consegue o acesso ao meio ou quando um ACK esperado não é recebido.

2) O campo NAV deve ser atualizado a cada passo do processo de transmissão de sequencias de múltiplos quadros. Quando uma estação recebe uma reserva de meio que é maior do que o NAV corrente, ela deve atualizar o valor do NAV. O estabelecimento do valor do NAV é realizado em cada quadro.
3) Os seguintes tipos de quadros podem ser transmitidos a partir de um intervalo SIFS, recebendo maior prioridade: ACK, CTS e quadros de fragmentos em sequencia.
    a) Uma vez que uma estação transmitiu o primeiro quadro da sequencia de fragmentos, ele utilizará o SIFS como intervalo entre quadros, ganhando o meio para transmitir os próximos fragmentos.
4) Quadros adicionais na sequencia devem ter seu NAV atualizado para o tempo restante esperado de utilização do meio. No caso da fragmentação, cada fragmento configura o NAV para reservar o meio até o final do próximo fragmento a ser transmitido, caso este exista.
5) Pacotes maiores do que um determinado limiar (*threshold*) devem utilizar sequencia de quadros estendidas, ou seja:
    a) Pacotes maiores do que o limiar RTS devem ser precedidos por uma transação RTS/CTS;
    b) Pacotes maiores do que o limiar de fragmentação devem ser fragmentados. O limiar de fragmentação e de RTS/CTS geralmente é configurado com o mesmo valor.

O sistema de controle apresentado nesta dissertação busca ser compatível com dispositivos atuais e, portanto, trabalha com o padrão 802.11 sem a necessidade de alterações em seus mecanismos de acesso ao meio. O MAC do 802.11 provê um mecanismo distribuído para coordenar o acesso ao meio que possibilita que muitos dispositivos deste padrão possam operar corretamente em uma mesma banda de frequências. Entretanto, sua utilização degrada a vazão da rede ao gerar atraso no acesso ao meio devido ao processo de *backoff*. Além disso, a maior disputa pelo acesso pode ocasionar maior número de colisões e, consequentemente, retransmissões. Desta forma, o compartilhamento do meio também pode ser considerado como uma forma de degradação da vazão agregada da rede que deve ser levada em consideração pelo sistema como uma forma de "interferência".

3. TRABALHOS RELACIONADOS

3.1. SELEÇÃO DE CANAIS

Atualmente, duas bandas de espectro de frequência não licenciadas estão disponíveis para o padrão IEEE 802.11 no Brasil: 2,4 GHz e 5 GHz. O espectro de 2,4 GHz, que é utilizado pelos padrões mais comuns, o 802.11 b e g, e que são foco desta dissertação, possui até 14 canais disponíveis, de acordo com a região do mundo. Entretanto, com estes 14 canais, apenas três não se sobrepõem. No Brasil, os canais ortogonais são 1, 6 e 11, já que 12, 13 e 14 não estão disponíveis, como pode ser visto na Figura **10** [9].

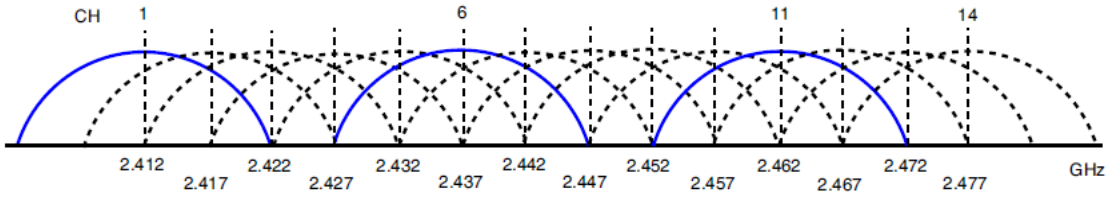


Figura 10. Os 14 canais disponíveis no padrão 802.11b e g. [9].

Ao se instalar uma rede sem fio, recomenda-se que pontos de acesso vizinhos sejam configurados para trabalhar em canais não sobrepostos de forma a não haver interferência entre eles. No entanto, muitas vezes o reuso de canais é necessário devido à escassez de canais não sobrepostos. Neste caso, técnicas de alocação de canais podem ser utilizadas para determinar uma configuração de canais que minimize a interferência entre dispositivos.

O reuso de canais em redes 802.11 é mais complexo do que o realizado em redes

celulares, dado que redes Wi-Fi são geralmente utilizadas em ambientes indoor, ocasionando irregularidade na área de cobertura. Além disso, em um mesmo ambiente muitas redes pertencentes a diferentes domínios administrativos podem coexistir, tornando mais difícil o planejamento. Tendo em vista estas diferenças e o fato de que geralmente, em uma rede celular, canais diferentes são utilizados para os tráfegos de dados e controle, o que não ocorre em um rede 802.11, técnicas criadas para o primeiro sistema não se aplicam diretamente ao segundo [9].

Ao escolher a alocação de canais em uma rede, duas formas de interferência podem ser consideradas. A primeira delas refere-se à interferência causada pelo mecanismo de contenção no acesso ao meio do 802.11, que é proporcional ao número de estações sem fio que transmitem em um mesmo canal e em uma mesma zona de alcance. A segunda delas é a interferência eletromagnética, que pode ser causada por dispositivos que operam em frequências vizinhas ou no mesmo canal de uma estação. A interferência causada entre dispositivos que operam em canais vizinhos é conhecida como interferência entre canais adjacentes. Já a ocasionada entre dispositivos que operam no mesmo canal é conhecida como interferência co-canal.

A interferência eletromagnética é prejudicial porque degrada a relação sinal ruído no canal, prejudicando a decodificação correta dos quadros, o que ocasiona perda de quadros e retransmissões. Este tipo de interferência pode ser causada por dispositivos que não são 802.11, mas que operam na mesma faixa de frequências do padrão, ou por uma estação 802.11 cujo sinal, ao atingir outras estações, se encontra abaixo do limiar de recepção e portanto não é interpretado como um quadro, mas sim, como ruído eletromagnético. Este tipo de interferência é conhecido como interferência de longo alcance.

Em redes domésticas, o canal de operação dos pontos de acesso é definido de acordo com técnicas dadas pelos fabricantes. A escolha do canal pode ser baseada em alguma métrica ou pode ser apenas aleatória. Um exemplo de técnica comumente utilizada é a LCCS (*Least Congested Channel Search*) [10]. Segundo [9], este mecanismo é empregado atualmente em muitos pontos de acesso da Cisco que funcionam sem um controlador central. Nesta técnica, cada AP coleta *beacons* provenientes de APs vizinhos em todos os canais, através dos quais informações sobre o número de clientes associados podem ser obtidas. Os campos extras criados para carregar as informações necessárias para o funcionamento do LCCS são proprietários da Cisco. O AP então escolhe o canal com menor número de clientes para operar, assumindo que cada cliente consome a mesma banda. Em uma segunda abordagem,

também descrita em [10], informações sobre o tráfego de cada cliente associado são enviadas através dos *beacons*, possibilitando que cada AP escolha o canal de menor tráfego para operação caso não exista um canal não sobreposto livre.

As propostas para alocação de canais encontradas na literatura, podem ser divididas em dois grupos principais: aquelas que consideram apenas a interferência observada pelos pontos de acesso, como as de [11], [12], [13], [14], [15], [16], e aquelas que também consideram a interferência observada pelos clientes da rede, como as de [17], [18] e [19]. Utilizar dados coletados pelos clientes possui a vantagem de revelar cenários de interferência que jamais poderiam ser revelados apenas por dados coletados em pontos de acesso. Um exemplo de cenário é o da Figura 11, abordado na proposta de [17] cujo objetivo da alocação de canais é fazer com que o maior número de clientes não sofra interferência de outros dispositivos (APs ou clientes) que estejam operando no mesmo canal.

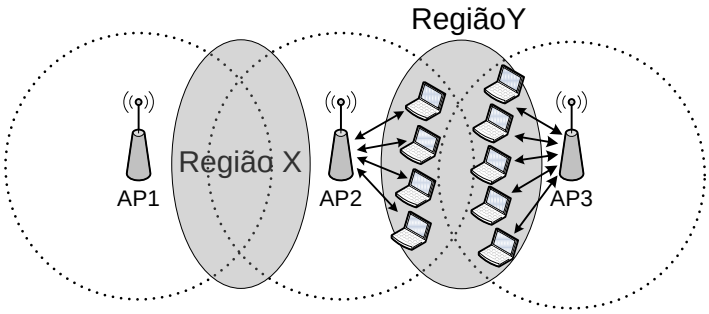


Figura 11. Cenário de interferência gerada entre clientes.

Nesta figura, os APs não interferem entre si, mas clientes associados a eles localizados na região X e Y podem causar interferência mútua. Para evitar esta situação, o ideal seria alocar canais diferentes para os APs 2 e 3. Como a região X não possui clientes, os APs 1 e 2 poderiam utilizar o mesmo canal. No entanto, para ser possível coletar esta informação é necessário que os dispositivos clientes realizem varredura espectral para verificar a existência de outros dispositivos que possam vir a interferir. Entretanto, a execução deste tipo de função não é comum em dispositivos clientes, tornando necessária a inclusão de alterações. Segundo [17], este problema poderá ser solucionado futuramente com a utilização do padrão 802.11K [20], que prevê a possibilidade de estações requererem a outras que realizem varredura espectral e reportem quais estações vizinhas foram encontradas. Tendo em vista que o controlador SCIFI possui requisito de trabalhar com toda a gama de dispositivos clientes atuais, ele busca não depender de características especificas nem introduzir alterações nestes dispositivos. Portanto, seu algoritmo de alocação de canais considera apenas a interferência

ocasionada entre APs.

Técnicas de alocação de canais voltadas para redes 802.11 infraestruturadas podem ser aplicadas de forma centralizada, como em [17], [21], [12], [19], ou descentralizada, como em [22], [11], [13], [15] e [18]. O gerenciamento centralizado é usualmente empregado em instituições como universidades, aeroportos, e empresas, nas quais um sistema de controle central se encarrega da configuração dos pontos de acesso pertencentes ao mesmo domínio administrativo. Já as técnicas descentralizadas não necessitam de um sistema de controle central e são mais aplicáveis em casos nos quais diversas redes de diferentes domínios administrativos coexistem, como, por exemplo, no caso de um prédio no qual cada morador possui um ponto de acesso. Para que a coordenação descentralizada seja possível, é necessário que os pontos de acesso sejam capazes de se comunicar entre si seguindo um determinado protocolo padrão, para que informações sejam trocadas e parâmetros sejam ajustados, o que aumenta a complexidade do algoritmo. Já a coordenação centralizada, além de possuir implementação mais simples, possibilita a visualização da rede como um todo no momento da definição dos parâmetros de controle. Buscando se valer destas vantagens, o sistema apresentado nesta dissertação e seus algoritmos foram desenvolvidos para operar de forma centralizada.

Dentre as propostas centralizadas, existem as que buscam maior redução da interferência através da agregação de técnicas de posicionamento prévio dos APs, como é o caso da proposta de [21]. O objetivo desta proposta é escolher canais não sobrepostos para APs de forma a minimizar áreas sobrepostas de cobertura cocanal entre células adjacentes. O maior desafio das propostas que usam tais técnicas é superar a irregularidade de cobertura ocasionada pelas características de propagação em ambiente interno (*indoor*), e a variação da demanda de tráfego em cada área [9]. Técnicas que consideram o planejamento prévio do posicionamento dos APs possuem a desvantagem de apenas poderem ser realizadas em cenários nos quais o administrador da rede possui total controle sobre a localização de cada ponto de acesso, o que nem sempre é possível. Portanto o algoritmo de alocação de canais do SCIFI não inclui tais técnicas.

Outra técnica que também pode ser agregada à alocação de canais é a de balanceamento de carga. Tal técnica busca reduzir a interferência excessiva causada pela associação descoordenada de clientes aos APs, que se traduz em redução da vazão da rede. De forma a melhorar determinada métrica da rede, clientes são desassociados/associados a determinados APs e novas associações são controladas [9]. Um exemplo de trabalho que

utiliza esta técnica é o de [17], que realiza o balanceamento no momento da definição dos canais de forma que cada cliente seja associado ao AP que minimize a sua interferência. O balanceamento de carga é interessante, porém de difícil implementação, já que a decisão de associação parte do cliente e não do ponto de acesso e sua implementação necessita de alterações mais profundas no padrão de funcionamento dos dispositivos da rede. O novo padrão 802.11k [1] traz meios para que a associação ocorra de forma consciente e poderá contribuir para a solução deste problema futuramente.

Um fator importante que deve ser considerado no desenvolvimento de um algoritmo para alocação de canais é o uso ou não de canais sobrepostos. Em algumas propostas, o mecanismo de alocação de canais possibilita que pontos de acesso próximos utilizem canais sobrepostos, ou seja, canais cujo espectro se sobrepõe, como é o caso de [11], [12], [18], [13], [17], [14] e [19]. O trabalho de [23], que se diz ser o primeiro que explora esta área, aponta que é mais interessante que dois pontos de acesso operem em canais sobrepostos do que no mesmo canal, já que, tendo em vista que no primeiro caso o raio de interferência entre pontos de acesso é reduzido em relação ao segundo, o reuso espacial em uma WLAN, ou seja, a frequência com que um mesmo canal poderá ser utilizado por outros pontos de acesso, poderá ser aumentado. Entretanto, o trabalho de [14] mostra através de resultados experimentais que, quando o intervalo de canais entre pontos de acesso próximos é menor do que 4, é mais interessante que eles operem no mesmo canal. De fato, o protocolo MAC do 802.11 funciona melhor para pontos de acesso operando no mesmo canal do que em canais sobrepostos próximos, tendo em vista que o sinal de um ponto de acesso que opera em um canal parcialmente sobreposto é detectado como interferência pelo AP vizinho. Esta interferência degrada a relação sinal ruído e ocasiona a perda de quadros e retransmissão, degradando a vazão da rede. Caso os APs operassem no mesmo canal, o sinal não seria detectado como interferência, mas sim, como o envio de um quadro, o que acionaria o mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) utilizado pela camada MAC (*Media Access Control*) do 802.11 para prevenir colisões, evitando perda de quadros e retransmissões.

Tendo em vista que a utilização de canais parcialmente sobrepostos pode causar redução significativa da vazão da rede, o sistema SCIFI, assim como as propostas de [15] e [16], não utiliza canais sobrepostos, embora seu algoritmo possa ser estendido para considerar a utilização de tais canais ao incluir um fator de ponderação apropriado, como ocorre em [18]. Neste trabalho, os autores consideram que a escolha de canais parcialmente sobrepostos para pontos de acesso vizinhos gera maior interferência entre eles do que a escolha de canais não

sobrepostos. Entretanto, esta interferência é menor do que se fossem utilizados canais iguais. A quantificação desta interferência é dada pela relação sinal ruído normalizada verificada em todos os canais por um ponto de acesso que recebe o sinal proveniente de um vizinho transmitindo em um determinado canal, e é considerada como um fator multiplicativo de ponderação do peso da aresta. Desta forma, para casos em que se deseja apenas utilizar canais não sobrepostos do 802.11 b e g (1,6 e 11), o fator multiplicativo é considerado 1 para canais iguais e 0 para canais diferentes. No caso em que se deseje utilizar todos os canais (1 ao 11), o fator multiplicativo é o mesmo do caso anterior para canais não sobrepostos. Já para os canais sobrepostos, o fator possui um valor entre 0 e 1.

Outra questão que pode ser abordada no momento da alocação de canais em uma WLAN é a consideração da interferência causada por APs que não estão sob o mesmo domínio de gerencia e, portanto, não podem ter seus canais alterados. Esta interferência é considerada importante porque, diferentemente da maioria das propostas encontradas na literatura, o SCIFI possui a finalidade de operar em uma rede controlada que compartilhará o meio com APs que não estão sob o gerenciamento do controlador. Portanto, assim como a proposta de [12], a interferência causada pela operação próxima de APs pertencentes a diferentes domínios de gerência é considerada.

As propostas encontradas na literatura também se diferenciam na forma como a computação da alocação de canais é realizada, podendo utilizar programação linear ou uma heurística. Propostas baseadas em programação linear, como é o caso de [19], possuem a desvantagem de requerer grande processamento computacional devido a sua grande complexidade. Como exigem maior intervalo de tempo para processamento, estas propostas são mais aplicáveis a casos estáticos, ou seja, casos em que a alocação de canais é realizada apenas uma vez ou em grandes intervalos de tempo. Tornar o processo de alocação de canais estático não é desejável, já que a interferência na rede pode se alterar no decorrer do tempo. Desta forma, o ideal é que o processo da alocação de canais seja dinâmico, como ocorre nas propostas baseadas em heurísticas de [17], [11], [18], [13], [14], [15] e [16]. Soluções baseadas em heurísticas são interessantes por possuir complexidade computacional reduzida. Nestes casos, uma solução sub ótima é aceitável e, por serem executadas em menor tempo, possibilitam a realização da alocação de canais em intervalos mais curtos, de forma mais dinâmica e adaptativa às alterações do meio. O algoritmo implementado no sistema SCIFI busca ser adaptativo e, portanto, realiza a computação da alocação de canais através de uma heurística.

Dentre os mecanismos para adaptação da alocação de canais às condições do ambiente, existem os baseados em intervalo de tempo e os baseados em comparações das métricas de interferência. Como exemplo, na proposta descentralizada de [16], os autores sugerem que o algoritmo seja executado periodicamente ou quando informações sobre a topologia da rede sejam recebidas. Já na proposta de [22] a alteração do canal de um AP só deve ocorrer se a utilização do canal atual ultrapassar um determinado nível. Caso isso ocorra, são listados N canais com menor utilização, e o que possuir o menor nível de ruído dentre eles é escolhido. No SCIFI, para prover a adaptação, o algoritmo de alocação de canais é executado de tempos em tempos, de acordo com a preferência do administrador da rede.

Dentre as propostas baseadas em heurísticas, as de [11] e [15] utilizam modelos de propagação para o cálculo da atenuação do sinal entre APs interferentes. A utilização de tais modelos não é desejável no SCIFI, já que não caracterizam com exatidão determinados ambientes, como os ambientes *indoor*, nos quais o sistema pretende ser utilizado.

As propostas que mais se mostraram interessantes diante dos requisitos de nosso sistema foram as de [16], [14] e [13]. As três propostas estão relacionadas entre si, e mostram o progresso do desenvolvimento de um algoritmo para alocação de canais. Em [16] os autores mostram que técnicas de coloração de grafo podem ser utilizadas como base teórica para protocolos de alocação de canais em redes 802.11. Com esta técnica, uma WLAN e a interferência entre seus "N" APs são modelados através da utilização de um "grafo de interferência". Neste grafo, os nós (vértices) representam os pontos de acesso e, caso haja interferência entre os nós, estes devem ser conectados por arestas unidirecionais. A seguir, o problema da alocação de canais se torna o clássico problema da coloração de vértices aplicado ao grafo de interferências, no qual as cores representam os possíveis canais que podem ser utilizados pelos APs. O objetivo da coloração é utilizar o mínimo número de cores de forma que cores diferentes sejam atribuídas a nós que possam se interferir. Após verificar que a coloração é um problema NP difícil, os autores propõe a utilização da heurística DSATUR [24] para sua solução. O algoritmo calcula o "grau de saturação" dos vértices, ou seja, o número de cores diferentes ocupadas por vértices vizinhos. Se existe apenas um vértice, este é escolhido para ser colorido. Se mais de um vértice existe, estes são ordenados decrescentemente de acordo com seu grau de saturação. Dessa forma, o vértice com maior "grau de saturação" é colorido primeiro. Caso mais de um vértice possua o mesmo grau de saturação, o que possuir maior número de vértices vizinhos descoloridos deverá ser colorido primeiro. Caso o desempate não ocorra, é proposto que uma função determinística baseada em

alguma característica dos nós, como o endereço MAC, seja utilizada para a decisão.

Em [13] os autores apresentam outros algoritmos que utilizam canais parcialmente sobrepostos e que realizam a coloração de forma adaptativa. A seguir, realizam simulações utilizando o DSATUR para verificar sua performance em relação à alocação de canais realizada de forma randômica. Em [14] os autores complementam a heurística inserindo um novo mecanismo para utilização de canais parcialmente sobrepostos e definem a arquitetura de implementação do algoritmo, que inclui um servidor central no qual o algoritmo DSATUR é executado e um protocolo para troca de mensagens entre o servidor e os APs e entre os APs. Após implementar o algoritmo, testes de performance são foram realizados em uma rede real.

A técnica de coloração de grafos e sua realização através da heurística DSATUR [24] se mostra interessante por ser de fácil implementação, possuir execução rápida, e produzir bons resultados. Devido a suas qualidades, esta técnica, conforme é descrita em [16], foi escolhida para ser a base do mecanismo de seleção de canais implementado no controlador SCIFI. A proposta de [13], apesar de ser mais recente e completa não foi escolhida porque o SCIFI não possuía objetivo de utilizar canais parcialmente sobrepostos.

Para suprir todos os requisitos do sistema, modificações no algoritmo original [16] foram inseridas, incluindo uma nova métrica de interferência e a consideração da interferência causada por APs que não estão sob o mesmo domínio de gerência e, portanto, não podem ter seus canais alterados. O objetivo foi a criação de um algoritmo centralizado, de fácil implementação e rápida execução, que fosse capaz de reduzir a interferência ocasionada entre pontos de acesso que compartilham o mesmo meio de transmissão, incluindo os que não pertencem ao mesmo domínio de gerência, sem a necessidade de profundas alterações no padrão 802.11 ou nos dispositivos clientes utilizados atualmente, de forma a prover maior compatibilidade com dispositivos atuais.

3.2. CONTROLE DE POTÊNCIA

A seleção de canal e o controle de potência estão diretamente relacionados, já que a área de interferência depende da potência de cada AP. Caso fosse possível trabalhar com todos os pontos de acesso em canais diferentes, não existiria interferência cocanal. Como isto não é possível, eventualmente pontos de acessos vizinhos terão de operar no mesmo canal. Quando isto ocorrer, mecanismos de controle de potência podem ser utilizados em busca da redução

da interferência entre pontos de acesso.

Atualmente, até mesmo pontos de acesso 802.11 de baixo custo permitem a configuração manual da potência de transmissão. Entretanto, uma vez definida a potência de operação ela é utilizada para comunicação com todos seus clientes. Comumente, ao ligar-se o dispositivo, a potência máxima de transmissão é utilizada por padrão, sem considerar a ocupação da célula ou distância até o cliente.

Em redes 802.11a, a emenda 802.11h define o serviço de TPC (*Transmit Power Control*), que possibilita o ajuste dinâmico da potência de transmissão dos dispositivos da rede. Esta emenda foi criada para suprir a necessidade de padrões europeus, que requerem que as estações que operam na banda de 5 GHz controlem suas potências para não interferirem em outros sistemas que utilizam a mesma banda, como sistemas de satélites . Pontos de acesso compatíveis com este padrão são capazes de anunciar a potência máxima permitida e rejeitar associações de clientes que não seguirem a regulamentação, e clientes se tornam capazes de ajustar sua potência para a mínima necessária, gerando economia de energia e redução da interferência. Entretanto, os dispositivos clientes no Brasil, em sua maioria, não utilizam este padrão. Sistemas celulares possuem mecanismos semelhantes desenvolvidos para aumentar a duração da bateria dos aparelhos e diminuir a interferência [4].

Dentre as técnicas encontradas na literatura para controle de potência em redes 802.11, muitas delas são voltadas para redes ad hoc e propõem a modificação do protocolo MAC de forma a adaptá-lo para funcionar com variadas potências de transmissão. Estas propostas, além de gerar redução do consumo de energia nos dispositivos móveis, são capazes de reduzir a interferência cocanal. Dentre elas, [25] e [26] propõem um novo protocolo MAC que leva em consideração os problemas de nós escondidos e compartilhamento injusto do canal, gerados pela utilização de diferentes potências de transmissão. O trabalho de [27], propõe um algoritmo de controle de potência descentralizado, que busca utilizar a potência mínima necessária para comunicação com um determinado destino. Estas soluções, por serem voltadas para redes ad hoc, não são aplicáveis ao SCIFI devido a características intrínsecas desta arquitetura que não são comuns à arquitetura infraestruturada que é utilizada no sistema, como a mobilidade dos nós, necessidade de cooperação entre eles e limitação de energia. Além disso, como o SCIFI pretende operar com dispositivos atuais, seu sistema não engloba alterações no padrão 802.11, incluindo seu mecanismo MAC.

Dentre as propostas para redes infraestruturadas, existem as que se focam na economia

de energia, como é o caso de [28]. Esta proposta, voltada para redes 802.11a, seleciona a combinação de taxa e potência de transmissão de forma que os dados sejam transmitidos com o menor gasto de energia possível, levando em consideração informações de atenuação do sinal no canal entre os dois nós comunicantes e a perda de quadros. Outro trabalho voltado para redes infraestruturadas é o de [29], que propõe um algoritmo de controle de potência para redes que operam em um mesmo ambiente e que são implementadas de maneira espontânea sem administração centralizada (redes caóticas). O algoritmo busca reduzir a potência de transmissão do AP até o mínimo valor de forma que o maior valor da taxa de transmissão entre o AP e um cliente seja mantida. O objetivo do algoritmo escolhido para ser implementado no SCIFI é primordialmente a redução da interferência, portanto, as propostas [28] e [29] fogem às necessidades do sistema.

Um dos principais problemas ocasionados pela utilização de diferentes potências de transmissão entre dispositivos de uma rede é a divisão injusta de recursos gerada pela existência de enlaces assimétricos [30]. A Figura 12 exemplifica um cenário no qual este problema ocorre. Nesta figura, os nós B e C pretendem se comunicar com A e D, respectivamente. Como os nós A e B estão próximos, B pode utilizar uma potência de transmissão mais baixa do que a utilizada por C, que está distante de D. Neste caso, o sinal de B não interferirá em C, enquanto o sinal transmitido por C irá interferir em B. Como resultado, apesar de B estar transmitindo, C irá encontrar o meio disponível para realizar sua transmissão, interferindo na comunicação de B. Caso C transmita continuamente, B nunca encontrará o meio livre e será impossibilitado de se comunicar.

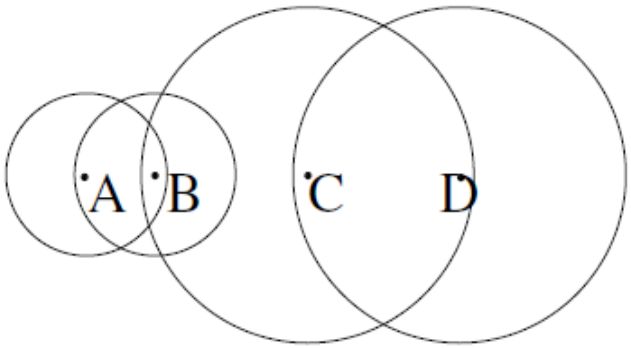


Figura 12. Enlaces assimétricos [30]. Círculos representam a potência de transmissão.

O trabalho de [30], que propõe um mecanismo de controle de potência para reduzir a interferência em redes 802.11 densas, busca evitar este problema através da utilização do

ajuste conjunto da potência de transmissão e da sensibilidade de portadora em um nó, parâmetro utilizado pelo MAC do 802.11 para detectar se o meio está livre para transmissão. Após o ajuste, nós que transmitam com maior potência devem diminuir seu limiar de verificação de canal livre (*Clear Channel Assessment* - CCA), ou seja, aumentar sua capacidade de "escutar" nós vizinhos. Já os nós que trabalhem com menores potências devem utilizar limiares mais altos, de forma que o produto entre o limiar e a potência utilizada pelos nós seja constante. A desvantagem desta proposta é a consideração de que os clientes devem utilizar a mesma potência de transmissão e o mesmo limiar CCA dos pontos de acesso ao qual estão associados e, dada a grande variedade de dispositivos clientes e o padrão tecnológico atual, não é garantido que todos sejam capazes de realizar tal ajuste sem a realização de alterações em seu *software* ou *hardware*.

Por fim, o controle de potência em ambientes *indoor* pode ser prejudicado por fenômenos que interferem na propagação do sinal eletromagnético, como reflexões e multipercurso, que podem vir a tornar as mudanças na potência de transmissão imperceptíveis para o receptor. Para solucionar esta questão, o trabalho de [31] propõe um algoritmo que determina a distribuição de probabilidade da potência de recepção, dada uma determinada potência de transmissão e realiza comparação entre diferentes potências de transmissão para verificar quais podem ser consideradas diferentes do ponto de vista do receptor. Posteriormente, estas potências podem ser utilizadas pelo mecanismo de controle de potência.

Tendo em vista a dificuldade de implementação de algoritmos de controle de potência que envolvem alteração da potência dos dispositivos clientes, no SCIFI, o controle de potência foi implementado de forma a restringir apenas as potências dos pontos de acesso da rede. Um mecanismo simples foi desenvolvido buscando complementar o algoritmo de alocação desenvolvido, objetivando reduzir a sobreposição de áreas de cobertura entre pontos de acesso vizinhos que operam no mesmo canal, como mostrará a seção 4.

3.3. BALANCEAMENTO DE CARGA

Em uma rede 802.11 infraestruturada com alta demanda por conexão, a adição de novos pontos de acesso é uma possível solução para o aumento de sua capacidade e consequente melhora da qualidade de conexão aos clientes. Entretanto, o efeito desejado pode

não ser alcançado, já que o cliente é que decide a que ponto de acesso irá se associar, e, tendo em vista que esta escolha geralmente não leva em consideração informação sobre a carga na rede, um ponto de acesso sobrecarregado pode ser escolhido.

O processo de descoberta de redes 802.11 realizado por um dispositivo cliente que deseja se associar a um AP pode ser realizado de forma ativa ou passiva. Na forma ativa, o cliente envia quadros de *Probe Request*, que especifica um SSID e suas taxas de transmissão suportadas. Os APs que recebem o *Probe Request* utilizam estas informações para determinar se o cliente pode se associar a ele. Para que a união seja possível, o cliente deve suportar todas as taxas de dados exigidas pelo AP, e deve aceitar se associar ao AP que contém o SSID determinado. O cliente também pode ser configurado para se associar a qualquer rede compatível, independentemente de seu SSID. Neste caso, o cliente deve utilizar o SSID de *broadcast* nos quadros de *Probe Request*. Caso um AP que receba um *Probe Request* possua parâmetros compatíveis com o cliente que o enviou, irá responder ao cliente com quadro *Probe Response*, tornando-o ciente de sua presença. No método passivo, o cliente escuta quadros de *beacons*, que são enviados frequentemente pelos APs.

Baseando-se nas informações contidas nos quadros de *probe response* ou *beacons*, o cliente decide a qual AP irá se associar. Atualmente, a maioria dos dispositivos 802.11 encontrados no mercado opta por se associar ao AP com o maior nível de sinal (maior RSSI - *Received signal strength indication*) [32], [33] e [34].

A Figura 13 exemplifica um cenário em que a utilização da qualidade de sinal para decisão de associação, provavelmente, será prejudicial ao cliente. Nesta figura, um ponto de acesso sobrecarregado, porém com nível de sinal maior, será escolhido para associação, em detrimento de um ponto de acesso com nível de sinal um pouco menor, que, entretanto, não possui nenhum cliente associado. O balanceamento de carga objetiva resolver este problema.

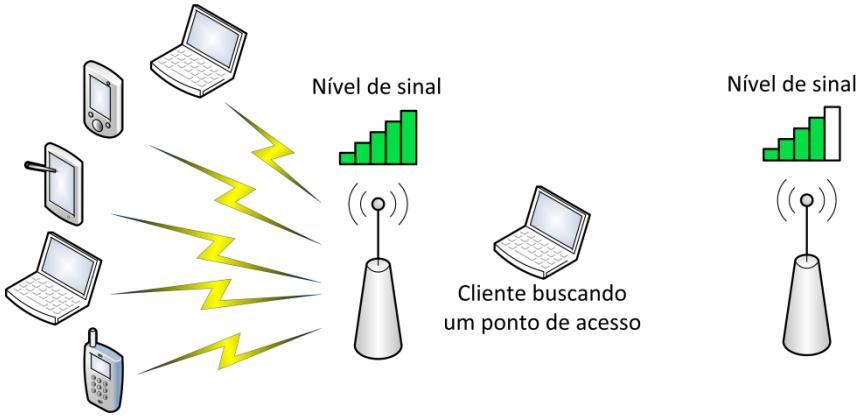


Figura 13. Exemplo de associação de uma estação a um ponto de acesso.

Independentemente de como o balanceamento de carga será realizado, o primeiro passo para sua realização é a escolha de métricas para definir o nível de carga na rede. Após escolhida a métrica, é necessário definir como utilizá-la para determinar se o ponto de acesso está sobrecarregado ou não.

O trabalho de [33] apresenta um estudo sobre as soluções encontradas na literatura para o problema do balanceamento de carga. Segundo os autores, dependendo de qual parte da rede realizará o processo de balanceamento, as técnicas podem ser classificadas em duas categorias principais:

- Baseada no cliente: o cliente, obtendo informações de carga dos pontos de acesso, decide qual deles é a melhor opção de associação;

- Baseada na rede: uma entidade da rede, como, por exemplo, um controlador central, administra a distribuição da carga na rede, sem a participação do cliente.

As soluções baseadas no cliente, geralmente, não são dirigidas para o balanceamento da rede como um todo, entretanto possuem a vantagem de não necessitarem de alterações profundas nos pontos de acesso para seu funcionamento. Por outro lado, soluções baseadas na rede não necessitam de modificações nos clientes e, por poder utilizar uma entidade de controle central, possibilitam o balanceamento de carga em toda a rede. O sistema apresentado nesta dissertação foi desenvolvido de forma a ser o mais abrangente possível e funcionar com dispositivos clientes atuais, portanto, não contou com a realização de modificações nestes dispositivos.

Dentre as métricas encontradas na literatura, a mais simples é a que se baseia no

número de clientes associados aos pontos de acesso. Um exemplo de trabalho que utiliza esta métrica é o de [35], que busca distribuir o número de clientes associados aos APs mantendo o sinal entre o AP e o cliente em nível aceitável. Outro exemplo é o trabalho de [32], que, após distribuir os APs nos diversos canais, busca distribuir os clientes entre os APs levando em consideração o número de clientes já associados e a qualidade do enlace entre AP e cliente. Ambos os trabalhos possuem a desvantagem de necessitarem de alterações nos clientes da rede.

É interessante considerar a relação sinal ruído no processo de escolha do ponto de acesso ao qual o cliente se associará [34], tendo em vista que um ponto de acesso, apesar de estar menos sobrecarregado, pode oferecer uma experiência de acesso frustrante devido ao baixo sinal e/ou alta interferência existente no meio, que sofre variações no decorrer do tempo. Esta baixa relação sinal ruído se traduz em perdas de pacotes e retransmissões.

A métrica baseada no número de clientes associados foi criada a partir do pensamento intuitivo de que mais clientes são capazes de gerar mais tráfego e também mais contenção, dada a grande competição para o acesso ao meio, indicando maior carga na rede. Este pensamento intuitivo pode ser confirmado caso seja considerado o caso específico no qual todos os clientes geram tráfego máximo em todo o tempo. Entretanto, em outros casos ela pode não ser uma boa estimativa de carga, tendo em vista que a banda utilizada pelas estações clientes nem sempre são as mesmas e o tráfego gerado por um mesmo cliente pode variar com o tempo [36], [33] e [37].

A Figura 14 exemplifica um cenário em que a utilização do número de estações associadas ao ponto de acesso como métrica de carga pode não ser eficaz. Nesta figura, existem dois pontos de acesso A e B operando em canais ortogonais. Os clientes C1, C2, C3, C4 e C5 estão associados ao ponto de acesso A. Dentre estes clientes, C1 utiliza a rede com pouca frequência, gerando baixo tráfego, enquanto C2, C3, C4 e C5 estão inativos, ou seja, não estão gerando tráfego. Já o ponto de acesso B possui duas estações associadas, C6, C7 e C8, que estão ativas, gerando alto tráfego e disputando pelo acesso ao meio. De acordo com esta definição de carga, novas associações seriam dirigidas ao ponto de acesso B, pois este possui menor número de clientes em relação a A. Entretanto esta escolha não é a melhor para o cliente e para a rede neste momento, já que a nova estação iria disputar o uso do meio RF com os clientes C6, C7 e C8, que estão plenamente ativos. Em outro momento, dada a grande variabilidade da demanda de tráfego, poderia ocorrer o contrário, por exemplo, os clientes C6,

C7 e C8 poderiam ficar inativos, enquanto C1, C2, C3, C4 e C5 poderiam entrar em atividade. Neste caso, esta métrica ocasionaria a melhor escolha. É importante notar que o tráfego gerado por um cliente pode variar de forma imprevisível.

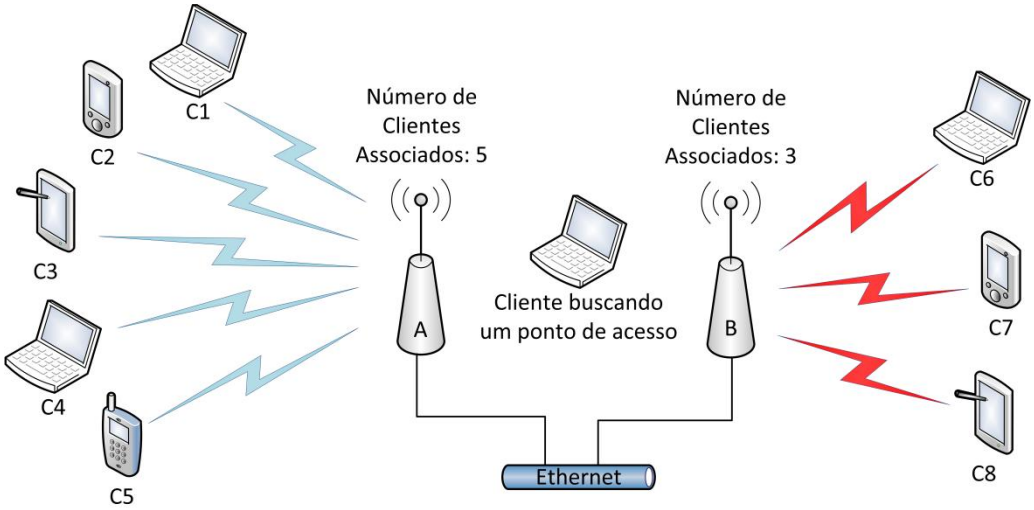


Figura 14. Desvantagens da métrica baseada no número de clientes

Outra métrica de carga que pode ser utilizada é vazão da rede. Trabalhos como o de [36] e [38], se baseiam nesta métrica. O primeiro deles define o nível de carga de cada AP com base em sua vazão, enquanto o segundo busca minimizar a soma do atraso potencial dos clientes associados a um AP através da minimização da soma do inverso da vazão para cada cliente. A vazão, por ser uma taxa dada em *bits* por segundos, ao ser invertida, resulta no tempo necessário para a transmissão de um *bit (*segundos por *bits).* Portanto, ao minimizar o inverso da vazão, estaremos minimizando o atraso para a transmissão de um *bit.* O primeiro trabalho, ao contrário do segundo, é interessante por não necessitar de alterações nos dispositivos clientes e será abordado novamente mais adiante.

Segundo alguns autores, a métrica baseada na vazão é insuficiente por não ser capaz de estimar o nível de congestionamento no canal de operação do ponto de acesso. Por exemplo, considerando a Figura 15, suponha uma rede com dois APs A e B operando em canais ortogonais. O ponto de acesso A possui vários clientes associados, todos eles disputando o meio para realizar transmissões. Consequentemente, colisões ocorrem em A, acarretando redução da vazão. Já o ponto de acesso B possui um único cliente associado que transmite seus quadros sem disputar o meio com outras estações e, portanto, consegue enviar um maior número de quadros por unidade de tempo. De acordo com esta métrica, o ponto de

acesso A, por operar com menor vazão, seria considerado menos carregado em relação ao ponto de acesso B, e novos clientes seriam forçados a se associar a A, o que pioraria a condição da rede [37].

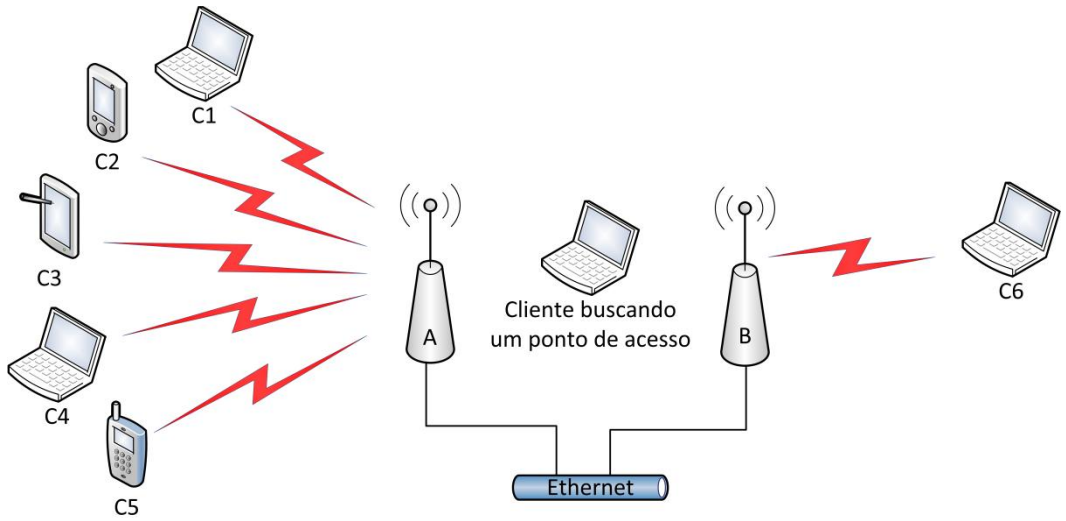


Figura 15. Desvantagens da métrica baseada na vazão do ponto de acesso.

Outra desvantagem da utilização da vazão como métrica em uma rede 802.11 é causada pela possibilidade de utilização de diferentes taxas para transmissão. Tendo em vista que diferentes clientes podem se comunicar com o AP com diferentes taxas de transmissão, o tempo decorrido para o envio de um quadro irá variar para determinado cliente. Por exemplo, um cliente transmitindo a 1Mbps irá gerar baixa vazão, porém ocupará o meio impedindo que clientes a taxas maiores realizem suas transmissões. Consequentemente, uma determinada vazão pode indicar congestionamento para uma determinada taxa, e baixa carga para taxas maiores.

Outra definição de métrica que pode ser encontrada na literatura é a baseada na porcentagem de tempo em que o canal permanece ocupado pelo AP para a realização de transmissões e recepções. Esta métrica pode indicar a carga de forma incorreta caso não considere os intervalos de tempo que não são utilizados para transmissão mas que fazem parte do processo de acesso ao meio, como os tempos de *backoff*, DIFS e SIFS. Por exemplo, na Figura 15, o tempo de ocupação do canal para o AP B, considerando-se apenas transmissões e recepções, é maior em relação ao do AP A, tendo em vista que os clientes de A disputam o acesso ao meio, gerando colisões, maiores janelas de contenção, e, consequentemente, maiores tempos de *backoff*. Portanto, um novo cliente seria indicado a se associar ao AP A, o

que pioraria a condição da rede [37].

Outra desvantagem desta métrica é sua incapacidade de considerar diferentes taxas de transmissão. Por exemplo, um AP trabalhando no padrão 802.11g com ocupação do canal de 80%, é capaz de proporcionar maior vazão para um novo cliente em relação a outro AP de padrão 802.11b com ocupação do canal de 40%, apesar de este último possuir menor ocupação do canal, ou seja, menor carga [33].

Um exemplo de trabalho que utiliza esta métrica é o de [39], no qual a associação do cliente ao AP é determinada pela porcentagem do tempo em que o AP transmite ou recebe e pelo nível do sinal recebido. Outras propostas que utilizam esta métrica, levando em consideração o espaçamento entre quadros (*interframe spacing)* e o tempo de *backoff* decorrido antes das transmissões são os de [40] e [41]. O primeiro utiliza APs específicos para captura de quadros através dos quais o tempo de ocupação do canal é calculado considerando uma estimativa para determinar qual parte do tempo ocioso corresponde a períodos de *backoff*. O segundo trabalho citado busca garantir determinada qualidade de serviço aos clientes através da utilização do balanceamento de carga, beneficiando aplicações de tempo real e com taxa constante. Os três trabalhos citados neste parágrafo fogem ao foco do sistema proposto nesta tese, o primeiro e o terceiro por necessitarem de alterações nos dispositivos clientes, e o segundo por utilizar APs específicos para captura de quadros.

Tendo em vista todas as desvantagens das métricas de carga anteriores, o trabalho de [37] propõe uma nova métrica baseada no tamanho da janela de contenção utilizada para transmissões recentes. Para que o valor da janela seja obtido, o cliente deve enviar ao AP o tamanho da janela utilizada em cada quadro, o que não será possível no trabalho desenvolvido nesta tese. Segundo os autores, o tamanho da janela indica o nível de contenção que ocorre em um BSS e, quanto maior o tamanho da janela, maior será a dificuldade de transmissão do cliente associado. Desta forma, quanto menor a dificuldade de transmissão proporcionada aos clientes associados, menos carregado é considerado o AP.

Após definir qual ou quais métricas serão utilizadas para a realização do balanceamento de carga, é necessário estipular como será inferido o estado da sobrecarga de um ponto de acesso. Segundo [33], este estado pode ser relativo ou absoluto, ou seja, pode depender ou não das informações dos outros pontos de acesso da rede.

Por exemplo, a proposta apresentada em [36] utiliza a informação de vazão de todos

os pontos de acesso para determinar se a rede está balanceada. Caso não esteja, o estado de cada ponto de acesso é estipulado através da comparação de sua vazão com a média da vazão dos vizinhos. O ponto de acesso pode assumir um dentre três estados possíveis: se sua vazão estiver abaixo da média, ele é considerado descarregado; se sua vazão estiver entre a média e uma constante δ, ele é considerado balanceado; caso a vazão esteja acima da média somada a constante δ, ele está sobrecarregado.

Semelhante à proposta apresentada anteriormente, em [42], trabalho baseado na técnica de *Cell Breathing,* que utiliza a potência de transmissão do AP para determinar sua área de cobertura e controlar o número de clientes associados, três estados são definidos. No primeiro deles, o estado *Fair*, a carga de um ponto de acesso é semelhante à média dos seus vizinhos, levando-o a manter suas configurações atuais. No estado *Gull*, a carga do ponto de acesso é maior que a dos seus vizinhos, o que o leva a tentar reduzir sua área de cobertura em busca da redução do número de clientes associados. No último estado, definido como *Willing*, o ponto de acesso possui poucos clientes e deseja aumentar sua área de cobertura para atrair uma quantidade maior. A técnica de *Cell Breathing* será abordada novamente adiante.

Um exemplo de proposta que define o estado de carga do ponto de acesso de forma absoluta é a de [39], no qual o ponto de acesso calcula localmente seu nível de carga com base no tempo em que passa transmitindo ou recebendo dados, e repassa esta informação aos clientes através de quadros de *beacon* ou *Probe Responses*. O cliente então compara este valor com um limiar fixo para determinar qual o melhor AP para associação, levando também em consideração o nível de sinal recebido. Portanto, esta proposta necessita de alterações nos dispositivos clientes para sua aplicação.

Após determinado o nível de carga de um ponto de acesso, torna-se necessário definir como este nível deve ser controlado, ou seja, como deve ocorrer a associação ou desassociação de clientes. De acordo com [33] , para soluções de balanceamento de carga baseadas na rede, que são o foco deste trabalho, existem três formas de realizar este processo:

- Ajuste da cobertura: Pontos de acesso aumentam ou diminuem sua área de cobertura de acordo com sua carga, através do uso de diferentes potências de transmissão. Os trabalhos baseados na técnica conhecida por *Cell Breathing* [42] utilizam esta técnica.

- Controle de admissão: O ponto de acesso rejeita a associação de novos clientes caso esteja sobrecarregado. Pontos de acesso não sobrecarregados aceitam novas associações

somente se seu nível de carga não for ultrapassado.

- Administração de associações: O ponto de acesso pode reduzir sua carga transferindo clientes para pontos de acessos vizinhos menos sobrecarregados. É nesta categoria que o trabalho de [36] se encaixa. Um desafio desta técnica é como realizar a desassociação de um cliente e associá-lo a outro ponto de acesso. Além disso, é necessário definir qual cliente será desassociado e em qual ponto de acesso ele deverá se associar de forma a melhorar o balanceamento da rede. Esta técnica pode ser utilizada em conjunto com o controle de admissão.

No método baseado na administração de associações, apresentado anteriormente, é necessária a realização da desassociação do cliente e sua consequente associação em um novo ponto de acesso para que haja o controle do nível de carga. Existem diferentes possibilidades para determinar quem será desassociado e qual ponto de acesso receberá o cliente.

A possibilidade de desassociação mais simples é a randômica. Porém esta abordagem pode não descongestionar o ponto de acesso. Em [36], o cliente a ser desassociado é aquele cuja vazão é a mais próxima da diferença entre a carga média e a carga do ponto de acesso. O processo de desassociação é realizado através do envio de uma mensagem de sinalização padronizada do 802.11 conhecida por “notificação de desassociação” ao cliente escolhido, que a seguir, só poderá se associar a pontos de acesso que estejam com a carga abaixo da média. Esta proposta é interessante porque não necessita de alteração no dispositivo cliente, entretanto, não garante que o cliente irá se associar ao novo ponto de acesso, já que a decisão de associação depende do cliente. Como os pontos de acesso sobrecarregados não aceitarão associações, este cliente poderá se deparar com grande demora no processo da nova associação, podendo até mesmo não conseguir realizá-la.

Outro exemplo de trabalho que utiliza controle de admissão em conjunto com a administração de associações é o de [41]. Nesta proposta, cuja métrica de carga se baseia no tempo de ocupação do canal, o controle de admissão se baseia no tempo esperado de ocupação do meio que será gerado pelo novo cliente que se associará ao AP. A carga gerada não deve ultrapassar determinado limite de forma que determinada qualidade de serviço possa ser garantida. A estimativa do tempo é calculada levando em consideração a perda de quadros, retransmissões, erros de bit e tráfego no AP. Para a realização da distribuição de carga, os APs monitoram suas cargas e fazem *broadcast* desta informação. Quando um AP se encontra sobrecarregado, uma mensagem MOVETO é enviada ao novo AP que deverá receber

o cliente, e uma mensagem HANDOFF é enviada para o cliente, forçando-o a se associar ao novo AP. Além de possuir carga menor em relação ao AP de origem, o novo AP deve propiciar nível de sinal suficiente para comunicação com o novo cliente. A desvantagem desta proposta é que ambas as informações de carga do AP e as mensagens utilizadas não fazem parte do padrão 802.11. Entretanto, os autores ressaltam que o padrão 802.11k possibilitará futuramente que mensagens semelhantes sejam trocadas entre APs e clientes, facilitando a implementação da proposta. Atualmente este padrão, por ser ainda emergente, não é suportado pela maioria dos dispositivos clientes.

Como, no padrão atual, a decisão de associação é restrita aos dispositivos clientes, existe uma grande dificuldade de implementação de um mecanismo de balanceamento de carga automático sem a inserção de alterações nestes dispositivos. Em uma hipótese, o ponto de acesso poderia ser indicado a "expulsar" um cliente associado e não aceitar mais sua associação, entretanto esta decisão não garantiria que este cliente encontrasse um novo ponto de acesso para realizar nova associação. Neste caso, o ponto de acesso teria que aceitar novamente a associação deste cliente, gerando desconexões momentâneas.

Tendo em vista estas dificuldades, no SCIFI o mecanismo de balanceamento de carga implementado buscou apenas possuir caráter informativo, de forma a possibilitar que o usuário da rede possa se locomover para áreas de menor carga caso considere ruim a experiência de acesso no local atual.

Tendo em vista que a métrica de vazão possui muitas desvantagens e as demais métricas encontradas na literatura necessitam de alteração nos dispositivos clientes ou de outras alterações que fogem ao escopo desta tese, no SCIFI, optamos por utilizar a métrica mais simples, que é o número de clientes associados ao pontos de acesso. Para a definição do *status* de carga dos pontos de acesso, limiares de carga baixa e carga alta são utilizados. Uma descrição completa do mecanismo será apresentada adiante na seção 4.

3.4. SOLUÇÕES PROPRIETÁRIAS DISPONÍVEIS NO MERCADO

Muitas empresas do ramo de redes disponibilizam sistemas baseados na utilização de controladores centrais capazes de realizar a alocação de canais, controle de potência e balanceamento de carga dos pontos de acesso de uma rede de forma automática e dinâmica.

Estas soluções geralmente possuem alto custo e trabalham com dispositivos específicos e sofisticados, como APs com diversos rádios, maior capacidade de processamento e memória, e software/hardware controladores capazes de administrá-los.

O sistema implementado neste trabalho se diferencia destas soluções por possuir foco na utilização de pontos de acesso de baixo custo, que, geralmente, carecem destas características e de uma plataforma de controle centralizada. Tendo isto em vista, este trabalho busca a criação de um sistema de controle centralizado, o SCIFI, que é capaz de operar em *hardware* de baixo custo, como um microcomputador padrão, utilizando sistema operacional e *softwares* livres. Além disso, o sistema busca suportar equipamentos de diversos fabricantes, compondo uma estrutura de rede não homogênea, o que não ocorre em soluções proprietárias.

O SCIFI busca operar com padrões e dispositivos atuais e, portanto, o conhecimento das soluções proprietárias é interessante por revelar técnicas que são utilizadas na prática atual. Entretanto, o acesso a detalhes mais profundos sobre estas soluções é difícil. Tendo isto em vista, a seguir serão apresentadas algumas soluções proprietárias para controle e gerência de redes sem fio existentes atualmente no mercado, obtidas através de manuais de operação e informações disponibilizadas em *web sites* dos fabricantes.

3.4.1. Motorola

De acordo com o site da empresa [43], a Motorola possui um conjunto de soluções específicas para redes sem fio, dentre as quais se encontram *hardwares* controladores, pontos de acesso e *softwares* administrativos. A empresa almeja alcançar várias vertentes do mercado e, para isso, oferece diversas tecnologias voltadas para criação e manutenção de redes empresariais, redes externas, enlaces ponto a ponto e ponto multiponto.

Dentre as soluções oferecidas, se destaca o *One Point Wireless Suite*, que é um conjunto de ferramentas voltadas para projeto, implantação, gestão e segurança de redes sem fio internas ou externas.

Os principais *softwares* presentes nesta suíte são:

- *Air Defense Security & Compliance*: provê ferramentas para identificação de vulnerabilidades da rede, e intervenção de ataques mal intencionados. Possibilita o controle

através de uma plataforma central, o *Motorola Air Defense Services Platform* (ADSP), compatível com infraestrutura de redes sem fio da Cisco e Motorola.

- *PTP LINK Planner*: ferramenta para planejamento e configuração de enlaces ponto a ponto, com base na geografia local, distância, tipo de antena, potência de transmissão e outros fatores, de forma que o sistema possa ser avaliado antes de sua implementação e equipamentos adequados possam ser escolhidos.

- *Broadband Planner*: ferramenta voltada para o projeto de médias e grandes redes externas, que obtém informações de distâncias e relevo através do *Google Earth*, para que o comportamento das ondas de rádio frequência possa ser previsto. A ferramenta prevê quais equipamentos devem ser utilizados e qual a melhor localização para eles, mostrando a variação da potência de transmissão através de mapas de calor.

- *Wireless Manager*: ferramenta para monitoramento da rede, que permite a visualização da rede externa em mapas do *Google Maps* e permite a configuração de parâmetros da rede, provisionamento, emissão de alertas e visualização de relatórios. Esta ferramenta funciona com equipamentos da Motorola, mas pode se integrar a equipamentos que possuam suporte a SNMP (*Simple Network Management Protocol*).

- *LAN Planner Software*: indica o melhor posicionamento e número de equipamentos de forma a otimizar o desempenho da rede local, levando em consideração o número de usuários, o ambiente, a tecnologia e as aplicações a serem utilizadas. Além disso, uma ferramenta de *site survey* é disponibilizada para a validação da rede e resolução de possíveis problemas.

- *Broadband Scanner*: ferramenta de medição de sinal de rádio frequência que permite visualização dos dados coletados e localização através de GPS (*Global Positioning System*).

Dentre as soluções oferecidas, a que mais se assemelha ao trabalho proposto nesta tese é a *Air Defense*, por utilizar controladores centrais através dos quais se torna possível, segundo a empresa, atualizar o *firmware* e configurações dos pontos de acesso, monitorar seus estados, capturar falhas, solucionar problemas de configuração e recolher estatísticas de rede.

Dentre os controladores oferecidos pela Motorola, pode-se citar como exemplo o RFS7000. Em seu manual [44] pode-se verificar que este controlador possui um sistema, conhecido por *Smart RF* (*Self-Monitoring At Run Time*), que utiliza informações sobre a interferência de outros dispositivos para determinar qual o melhor canal e potência de trabalho

para um determinado ponto de acesso, de forma que a interferência seja a menor possível. O gerenciamento realizado pelo *Smart RF* se divide em duas fases, a fase de calibração e a fase de monitoramento.

A fase de calibração é iniciada pelo administrador e pode ser realizada em intervalos de tempo específicos. Nesta fase, as seguintes atividades são conduzidas:

- Os rádios são calibrados, de forma automática, para a maior potência possível;

- Alguns rádios são escolhidos como "detectores". Rádios detectores são aqueles que trabalham na identificação de pontos de acesso intrusos na rede.

- Os melhores canais são escolhidos para a operação dos rádios, buscando a redução da interferência externa e que rádios com intercessão de áreas de cobertura não operem no mesmo canal;

- A potência de transmissão de operação dos rádios é calculada;

-Parâmetros de "autocura" são configurados automaticamente. Com isso, certos rádios recebem a denominação de *Caretaker* e outros de *Caregiver*. Um rádio que perde sua comunicação pode ser chamado de *Caretakers*. Quando este fato ocorre, vizinhos escolhidos pelo controlador, os chamados *Caregivers*, automaticamente aumentam suas potências de transmissão de forma que a cobertura no local da falha possa ser restabelecida.

A fase de monitoramento ocorre continuamente e as seguintes atividades são realizadas:

- O funcionamento dos rádios é monitorado, de forma que o mecanismo de "autocura" possa ser ativado no caso da verificação de uma falha.

- A interferência é monitorada;

- Falhas na cobertura são monitoradas e novas taxas e potência de transmissão são determinadas, caso necessário. A potência é aumentada quando uma falha na cobertura é encontrada;

- As interferências são monitoradas e classificadas de acordo com sua proveniência e estas informações são guardadas para futuras reconfigurações "inteligentes".

Os valores de potência e canal de determinados rádios podem ser fixados pelo administrador, evitando que o mecanismo de controle do *Smart RF* possa modificá-los.

O RFS7000 também apresenta mecanismo de balanceamento de carga. De acordo com seu manual, existem duas formas de balanceamento, o balanceamento de associados entre diversos pontos de acesso (*MU Load balancing*) e o balanceamento de pontos de acesso entre diversos *switches* controladores (*AP Load balancing*). O primeiro tipo de balanceamento é o que se pretende utilizar no sistema apresentado nesta tese, portanto será melhor detalhado a seguir.

Segundo o manual do RFS7000, para que o balanceamento de carga seja realizado, pontos de acesso próximos e com características parecidas devem ser agrupados pelo administrador. Sem essa configuração, o balanceamento de carga não é aplicado automaticamente a nenhum ponto de acesso. Uma dentre duas métricas de balanceamento pode ser escolhida: o número de clientes associados a um ponto de acesso ou a vazão total dos associados. O número mínimo de associados pode ser determinado, de forma que, abaixo deste valor, a realização do balanceamento é cancelada.

Para implementar o balanceamento de carga, o controlador da Motorola utiliza o *QBSS Load Element* enviado nos *beacons* (especificado no padrão IEEE 802.11e [45]), e um elemento proprietário criado pela Motorola, o *MU count*, que também é transmitido através de *beacons*. A utilização do campo *QBSS Load Element* é interessante, porém, como o padrão 802.11e é relativamente novo, atualmente, nem todos dispositivos clientes possuem suporte a ele, o que não garante que o balanceamento de carga baseado nesta informação funcione plenamente de acordo com o desejado.

Apesar de os *softwares* e *hardwares* oferecidos pela Motorola se apresentarem muito úteis para o projeto e implantação de grandes redes, possuem a desvantagem do elevado custo (por exemplo, apenas o RFS700 possui custo superior a US$5000 – nos EUA) e trabalham com hardwares específicos, cujos custos são superiores aos dos equipamentos populares (o custo dos pontos de acesso compatíveis gira em torno de US$300- nos EUA). Há também o problema de compatibilidade com dispositivos de outras empresas.

3.4.2. Cisco

A Cisco, assim como a Motorola, também fornece diversos produtos para gerência de redes sem fio [46]. Seus controladores, conhecidos por WLC (*Wireless LAN Controller*),

realizam funções que, comumente, seriam realizadas pelos APs, como a autenticação e associação dos clientes. Aos APs, conhecidos por LAP (*Lightweight Access Points),* são designadas apenas funções de tempo real, como a criptografia de camada 2, possibilitando o suporte da rede a aplicações de tempo real, como as de telefonia e *streaming* de vídeo. Esta arquitetura, na qual o AP exerce apenas funções de tempo real e o controlador exerce funções da camada MAC que não são de tempo real, é conhecida como *Split MAC* [2].

Os LAPs funcionam somente em conjunto com os WLCs, que são responsáveis por realizar todas as configurações e atualização de *firmware*. Dentre as configurações realizadas pelo controlador, pode-se citar o controle da potência e escolha dos canais utilizados pelos pontos de acesso. Para isso, o controlador possui um conjunto de algoritmos, conhecido por RRM (*Radio Resource Management*), que opera de forma a otimizar os parâmetros de operação do AP. Por padrão, os RRM é habilitado automaticamente e é possível que seu intervalo de execução seja escolhido. Caso seja desejado, o administrador da rede também pode escolher os parâmetros de configuração dos APs manualmente [47].

Segundo o documento disponibilizado pela Cisco que descreve o RRM [48], a princípio, mensagens são trocadas entre os pontos de acessos e os controladores da rede para que estes conheçam quais são os APs vizinhos de cada ponto de acesso. Com esta informação, os pontos de acesso e seus respectivos controladores são divididos em grupos e, para cada um deles, é eleito um controlador líder de grupo, responsável pela execução dos algoritmos de seleção de canal (DCA - *Dynamic Channel Assignment*), e controle de potência (TPC - *Transmit Power Control*).

O algoritmo de seleção de canal se aplica a pontos de acesso vizinhos, ou seja, pontos de acesso que são capazes de receber sinal uns dos outros. Para determinar em qual canal o rádio irá operar e quando é necessária a mudança de canal, o controlador utiliza diversas informações coletadas dos pontos de acesso, que são:

- Medição de Carga: porcentagem do tempo em que o ponto de acesso passa transmitindo ou recebendo quadros 802.11.

- Ruído: cada ponto de acesso calcula o nível de ruído em cada canal disponível.

- Interferência: cada ponto de acesso calcula a porcentagem de tempo que o meio é ocupado por outros pontos de acesso.

- Força do Sinal: cada ponto de acesso registra a potência recebida dos pontos de

acesso vizinhos, em todos os canais. Esta é a informação mais importante para as decisões do algoritmo DCA.

Esses valores são recebidos pelo controlador, que os analisa e determina se existe alguma configuração de canais que possa melhorar em, no mínimo, 5dB a relação sinal ruído do ponto de acesso mais desprivilegiado. Se uma opção melhor existir, ela é aplicada. Preferências são dadas a pontos de acesso de acordo com sua carga, de forma que o ponto de acesso mais operante tenha menor possibilidade de ter seu canal alterado, evitando que a comunicação com seus clientes seja interrompida. A preferência de manutenção de canal também é dada a pontos de acesso que possam desencadear uma modificação geral dos canais na rede.

O algoritmo de controle de potência (TPC), que roda a cada 10 minutos por padrão, calcula a proximidade RF (rádio frequência) entre os pontos de acesso e limita a potência deles de forma que a interferência cocanal e a sobreposição excessiva de células de cobertura não ocorra. Seu funcionamento ocorre da seguinte forma:

- Cada ponto de acesso faz uma lista com seus vizinhos e a potência recebida de cada um deles;

- Caso um AP possua 3 ou mais vizinhos, e o terceiro possua valor acima de um determinado limite, o TPC é acionado de forma que o sinal recebido do terceiro vizinho alcance a potência de -70dBm (ou menor). Este valor limite pode ser configurado pelo administrador da rede. Além disso, uma determinada condição de histerese deve ser satisfeita, de forma que variações bruscas de potências sejam evitadas.

O TPC é responsável apenas por diminuir as potências de transmissão dos APs. No caso da necessidade do aumento das potências para cobrir falhas na cobertura, existe o algoritmo de controle e correção de falhas na cobertura (*Coverage Hole Detection and Correction*).

O *Coverage Hole Detection and Correction* busca corrigir falhas de cobertura causadas por falhas de pontos de acesso ou a má qualidade de sinal entregue aos clientes associados. Por utilizar estatísticas de clientes, este algoritmo é executado de forma independente em cada controlador e não apenas no controlador líder de grupo, funcionando da seguinte forma:

- A falha na cobertura é identificada quando a relação sinal ruído de um cliente está

abaixo de um determinado limite. Este limite é independente para cada ponto de acesso e está relacionado a sua potência de transmissão, de forma que pontos de acesso com maiores potências de transmissão toleram menores valores de relação sinal ruído. O administrador pode interferir neste limite através de uma variável, o *Coverage Profile Value*.

A equação que determina o limite de relação sinal ruído aceita no cliente é dada por:

Client SNR Cutoff Value (|dB|) = [*AP Transmit Power* (dBm) – *Constant* (17 dBm) – *Coverage Profile* (dB)]

- dado que a média das relações sinal ruído dos clientes tenham ficado abaixo do limite por 60 segundos ou mais, a potência do ponto de acesso ao qual estão associados é aumentada.

Este algoritmo é executado a cada 180 segundos por padrão.

O algoritmo apresentado executa de forma concorrente com o TPC, ou seja, os valores de potência já definidos pelo primeiro podem ser alterados pela execução do segundo.

Os controladores da Cisco provêm o balanceamento de clientes associados a um ponto de acesso através da técnica conhecida como *Aggressive load balancing*. A função de balanceamento de carga é executada por cada controlador caso o administrador da rede a habilite [48].

O balanceamento ocorre na fase de associação do cliente e nunca desconecta um cliente já associado. Quando este tenta se associar a um ponto de acesso que já atingiu o seu limite de ocupação, quadros de resposta (*association response frames*) são enviados com o código 17, indicando que o ponto de acesso está muito ocupado para aceitar novas associações. Segundo determina o padrão 802.11, o cliente, ao receber esta mensagem, deve procurar outro ponto de acesso para se associar. Entretanto existem clientes que não respeitam o padrão, portanto, a associação é permitida após duas tentativas de associação consecutivas, de forma que o cliente não permaneça sem acesso à rede.

A métrica de carga usada pela Cisco é o número de clientes associados ao ponto de acesso. O limite máximo de clientes pode ser definido pelo administrador. Por padrão, o mecanismo de balanceamento, após ser ativado, possui limite de 5 clientes. Caso um cliente tente se reassociar a um ponto de acesso ao qual estava associado previamente, ele não sofrerá ação do balanceamento de carga.

Assim como as soluções da Motorola, as da Cisco se mostram interessantes, porém possuem a desvantagem do alto custo e a necessidade da utilização de pontos de acesso específicos que também possuem alto custo.

3.4.3. Aruba Networks

Assim como a Motorola e a Cisco, a Aruba Networks também oferece diversos softwares e hardwares voltados para o planejamento, implantação e administração de redes sem fio.

Seu conjunto de softwares, o *Mobility Management System* [49], fornece capacidade de planejamento, monitoramento, gerenciamento de falhas, relatórios, cobertura de RF e visualização local dos pontos de acesso da rede.

A solução de mobilidade empresarial da Aruba oferece o gerenciamento centralizado da rede através da utilização de controladores, que trabalham em conjunto com os *Thin Access Points* da Aruba, e operam com o sistema operacional *ArubaOS* [50], que suporta diversas funcionalidades. Uma delas é o *Adaptive Radio Management* (ARM) [51], sistema capaz de realizar a alocação de canais e controle de potência de forma a reduzir a interferência entre os pontos de acesso, e, ao mesmo tempo, maximizar a cobertura.

A Aruba também oferece um módulo de captura de informações sobre interferências, o *RFProtect* [52]. Este módulo, que utiliza os próprios pontos de acesso para a realização da varredura espectral, pode trabalhar em conjunto com o ARM, embasando suas decisões, além de fornecer uma interface gráfica para a visualização das informações coletadas. O ARM também realiza o balanceamento de carga, possibilitando que os clientes sejam divididos de forma justa entre os pontos de acesso e canais de frequência.

O algoritmo de seleção de canal da Aruba [53] é executado em cada ponto de acesso, sem coordenação central. Para isso, cada ponto de acesso realiza uma varredura espectral para verificação da existência de interferências, pontos de acesso vizinhos e ruído de fundo. No decorrer desta varredura, os clientes ficam sem comunicação e, tendo este fato em vista, esta ação pode ser suspensa no caso da detecção de atividades específicas, como chamadas de voz.

Após a varredura, são determinados dois índices: o índice de cobertura (*coverage*

index) e o de interferência (*interference index*), utilizados para o cálculo do melhor canal e potência de transmissão do ponto de acesso. O índice de interferência representa tanto sinais provenientes de redes Wi-Fi, quanto a interferência proveniente de outros dispositivos que operam na mesma faixa de frequências. Quando o índice de interferência no canal corrente for alto, comparado com os outros canais, o AP irá procurar operar em um canal com menor índice de interferência. Desta forma, o algoritmo é capaz de reduzir a interferência cocanal causada por outros APs e também a causada por outros dispositivos que estejam irradiando na mesma faixa de frequências.

O índice de cobertura engloba o número de pontos de acesso transmitindo no mesmo canal, ponderados pela potência dos sinais recebidos em um ponto de acesso. O algoritmo do ARM busca maximizar e equalizar esse índice em todos os pontos de acesso. O índice de cobertura é o principal parâmetro determinante para a definição da potência de transmissão de um ponto de acesso.

Os algoritmos do ARM possibilitam que limiares sejam determinados, como potência máxima e mínima, intervalo de canais, taxa de erro necessária para a realização da mudança de canal, mesmo que interferências não sejam detectadas. Além disso, a frequência de operação dos algoritmos também pode ser controlada.

É permitido que pontos de acesso sejam designados apenas para a monitoração do espectro, de forma que os responsáveis pela comunicação com clientes nunca sejam interrompidos para a realização da varredura. Esta varredura também pode ser suspensa quando um determinado limite de tráfego no ponto de acesso é ultrapassado, já que, neste caso, uma pausa na comunicação poderia ocasionar grandes perdas de dados. Além disso, quando um ponto de acesso, ao executar o algoritmo, encontra um índice de cobertura suficiente para todos os canais, pode ser configurado para entrar no modo *Mode Aware* ARM, no qual passa a operar apenas para monitoração do espectro.

Para a realização do balanceamento de carga, o ARM possui o mecanismo *Band Steering*. Como a maioria dos dispositivos utilizam a banda de 2,4GHz, este mecanismo tenta impedir que dispositivos capazes de utilizar a banda de 5Ghz, utilizem a de 2,4GHz. Desta forma, a banda de 2,4GHz se torna menos carregada e clientes com restrição de frequência passam a ter melhor acesso à rede. A verificação de capacidade dos clientes é feita através da verificação dos quadros de *probe request* enviados pelos clientes na banda de 5GHz. Os pedidos de conexão em 2.4GHz são recusados para clientes que também tentem se conectar

em 5GHz. O algoritmo também permite que clientes, ao se recusarem a realizar a troca de banda, sejam conectados em 2.4GHz.

Além desse mecanismo, o ARM realiza o balanceamento de clientes por canal, e não por ponto de acesso. Este balanceamento é realizado através do envio de *response frames* que tentam forçar o cliente a se associar utilizando o canal menos sobrecarregado.

Outro mecanismo, que busca e redução da interferência cocanal utilizado pelo ARM, é a redução da sensibilidade de recepção dos pontos de acesso, que é feita de forma que quadros com potência abaixo de um certo limite de sensibilidade não sejam vistos como quadros 802.11, evitando que o ponto de acesso não consiga realizar transmissões devido ao controle de acesso ao meio. Quanto mais sensível o ponto de acesso, maior o seu domínio de colisão. Diminuindo sua sensibilidade, os clientes que possuem localização mais próxima do que pontos de acesso vizinhos poderão ser atendidos com maior vazão. O nível de ruído permanecerá menor do que o nível de potência recebido dos clientes, e, consequentemente, mudanças perceptíveis na taxa de erro não ocorrerão.

Para executar este mecanismo, o algoritmo ARM mede a potência dos sinais recebidos dos clientes e aplica uma média móvel para alterar a sensibilidade de recepção do ponto de acesso, baseando-se no cliente que possui menor sinal. Este ajuste é dinâmico, e ocorre de forma que, se os clientes possuírem bom sinal, a sensibilidade é consideravelmente reduzida. A redução é menor no caso de existirem clientes distantes, com má qualidade de sinal.

A modificação, da sensibilidade, além de reduzir a interferência cocanal, também é utilizada pelo ARM com o intuito de reduzir a interferência em canais adjacentes. Dado que a máscara espectral que delimita os canais do 802.11 se sobrepõem nas bordas, como mostra a Figura 16, a alteração da sensibilidade, além de reduzir a interferência entre canais adjacentes, também torna mais viável, caso seja desejado, a utilização de quatro canais do espectro (1, 4, 8 e 11), ao invés de apenas três canais ortogonais (1, 6 e 11).

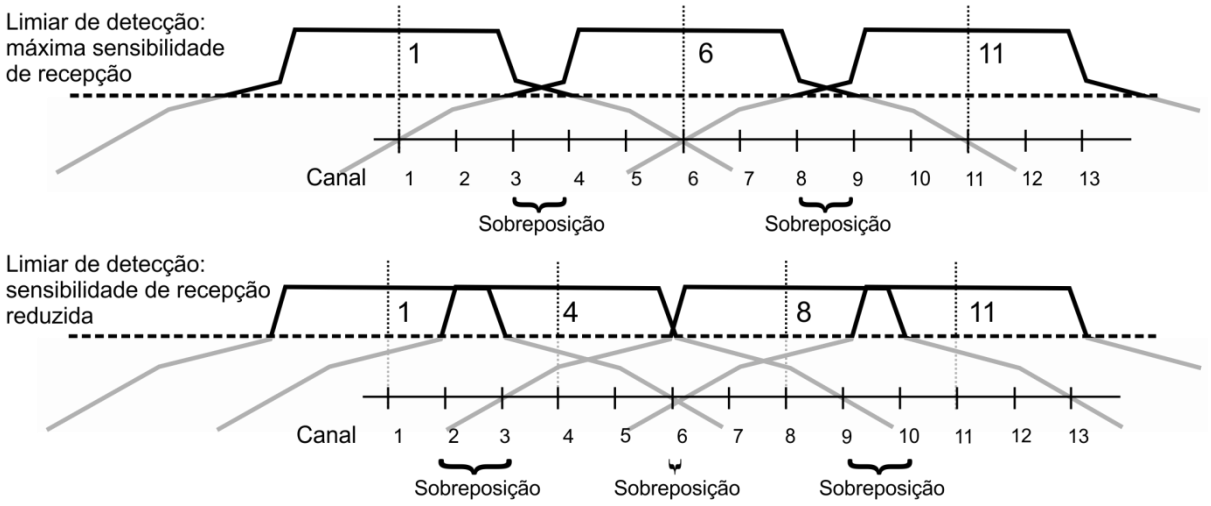


Figura 16. Reduzir a sensibilidade de recepção do AP ajuda a reduzir a interferência entre canais adjacentes. [53]

3.5. PROTOCOLOS DE COMUNICAÇÃO ENTRE CONTROLADOR E PONTOS DE ACESSO

Atualmente, os principais mecanismos utilizados para configuração de pontos de acesso 802.11 são: configuração estática manual via HTTP (*Hypertext Transfer Protocol*); configuração de múltiplos pontos de acesso através de uma plataforma central utilizando o protocolo de gerência padronizado; configuração automática através da utilização de um controlador central que se comunica com os pontos de acesso via protocolos proprietários ou padronizados; ou a utilização de pontos de acesso auto configurantes.

A configuração manual através da interface Web do ponto de acesso, quando realizada por usuários sem experiência em redes 802.11, pode ocasionar má utilização do espectro de frequências caso uma análise espectral não seja realizada previamente. Além disso, esta configuração é estática e incapaz de se adaptar a mudanças do ambiente, por exemplo, ao surgimento de interferência no canal de operação do ponto de acesso. Outra desvantagem deste método é o fato de que a configuração deve ser realizada individualmente para cada ponto de acesso, tornando trabalhoso o processo de configuração de grandes redes.

A gerência e configuração de múltiplos pontos de acesso pode ser facilitada através da utilização de soluções centralizadas, que geralmente utilizam protocolos padronizados para a

comunicação entre uma entidade de gerência e dispositivos gerenciados. Um exemplo de solução é o *Wireless Access Point Utilities for UNIX* [54], que possibilita a gerência e configuração de diversos pontos de acesso a partir de um microcomputador através da utilização do protocolo SNMP (*Simple Network Management Protocol*). Esta solução é compatível com a maioria dos pontos de acesso que possuem *chipset* Atmel e suportem SNMP. Outras soluções com esta mesma finalidade também são disponibilizadas por fabricantes como Cisco, Aruba e Meru.

Segundo [7], os padrões de gerenciamento de rede começaram a amadurecer no final da década de 80, sendo que o CMIP (*Common Management Information Protocol*), protocolo da família OSI (*Open Systems Interconnection*) definido na recomendação ITU-T X.711 [55] e ISO 9596, e o SNMP, protocolo padronizado pelo IETF (*Internet Engineering Task Force*) [56], emergiram como os dois padrões mais importantes. Como este último foi projetado e oferecido rapidamente em uma época em que as redes necessitavam de gerência, este foi amplamente aceito e atualmente é o protocolo de gerência mais utilizado.

O SNMP é um protocolo de aplicação padronizado que possibilita não só o controle e gerência de pontos de acesso, mas também de uma gama de dispositivos de rede, como *gateways*, servidores e roteadores. Os dispositivos gerenciáveis contém dois elementos principais:

1) o Agente de Gerenciamento, que é um processo executado no Dispositivo Gerenciável. Este processo se comunica com a Entidade Gerenciadora e executa ações locais sob o controle desta entidade;

2) a Base de Informações de Gerenciamento (MIB, do inglês *Management Information Base*), que armazena informações relativas ao conjunto de Objetos Gerenciáveis (conhecidos por Objetos MIB [7]) contidos no dispositivo, como por exemplo, informações sobre o tráfego e parâmetros de funcionamento. Objetos MIB relacionados são agrupados em Módulos MIB.

As regras de construção das estruturas da MIB e a identificação dos objetos gerenciais são definidos no padrão chamado SMI (*Structure of Management Information*) [57]. O SMI define com exatidão como os objetos gerenciados são nomeados e especifica os respectivos tipos de dados associados.

Toda a comunicação para a troca de informações e comandos de gerência entre o

Agente de Gerenciamento e as Entidades Gerenciadoras é realizada através do protocolo SNMP. As mensagens possibilitam que as informações contidas na MIB sejam consultadas pela Entidade Gerenciadora, ou alteradas em certos casos. O SNMP também possibilita que eventos excepcionais ocorridos nos Dispositivos Gerenciados sejam informados à Entidade de Gerência.

Ao longo dos anos, o protocolo foi aprimorado e atualmente se encontra em sua terceira versão. As principais melhorias ocorreram no campo administrativo e nas capacidades de segurança, através da inserção de novas formas de requisições de informações e utilização de mecanismos de criptografia, autenticação e verificação de integridade das mensagens.

O SNMP foi uma das alternativas de protocolo estudadas neste trabalho para a realização de configurações e coleta de informações dos pontos de acesso. Entretanto, esta opção não foi escolhida devido a restrição de informações disponíveis em MIBs convencionais, tornando-se necessária a criação de um novo módulo MIB. Além disso, diferentes *drivers* de variados pontos de acesso respondiam ou não às requisições SNMP e de forma diferenciada. Outro problema encontrado foi o alto gasto de recursos como memória e processamento dos pontos de acesso utilizados no projeto, que por requisito deveriam ser de baixo custo, apresentando, na maioria das vezes, escassez desses recursos.

Outro protocolo de gerência de dispositivos de rede que também foi proposto pelo IETF é o NETCONF (*Network Configuration Protocol*) [58]. Entretanto, por ser mais atual (proposto em 2006), não é tão amplamente utilizado e suportado como o SNMP, se mostrando uma alternativa menos interessante para utilização no trabalho aqui proposto.

É importante notar que o SNMP não toma decisões, mas sim, fornece mecanismos de gerência e controle aos administradores de rede. Para que a configuração automática de pontos de acesso seja realizada, é necessário que algoritmos de controle sejam executados para definir os valores dos parâmetros a serem utilizados pelos pontos de acesso. Estes algoritmos podem ser executados localmente em cada ponto de acesso, com ou sem a troca de informações entre pontos de acesso da rede, ou podem ser executados em um controlador central, que toma as decisões e depois as repassa aos pontos de acesso.

A utilização de um controlador central, solução adotada neste trabalho, é interessante porque possibilita que parâmetros sejam configurados levando em consideração a rede como um todo sem a necessidade de inserção de complexidade no pontos de acesso, mantendo seu

baixo custo.

Controladores centrais, além de realizar configuração dos pontos de acesso, também podem incorporar outras funções que outrora eram realizadas pelos pontos de acesso, como a associação e autenticação de clientes. Trabalhando desta forma, os pontos de acesso, conhecidos por *Lightweight Access Points* , *Thin APs* ou *Fit APs* [2], passam a realizar menos funções e podem ser fabricados com menor custo.

Como foi descrito na seção 3.4, diversas soluções que integram um controlador central são encontradas no mercado. Na maioria delas, a comunicação entre pontos de acesso e controlador central é realizada através de um protocolo proprietário, entretanto, já existem esforços no sentido de se criar um protocolo padronizado para tal finalidade.

Um exemplo de protocolo de comunicação entre pontos de acesso e controlador utilizado em alguns produtos Cisco é o LWAPP (*Lightweight AP Protocol*), que é um rascunho (*draft*) da IETF (*Internet Engineering Task Force*), cujos detalhes encontram-se descritos na RFC 5412 [59]. Este protocolo não é especifico para redes 802.11 e define como deve ser realizada a troca de mensagens de controle e dados entre um controlador e terminais de acesso sem fio genéricos. A comunicação entre os dispositivos pode ser realizada sobre protocolos de camada de enlace ou através de uma rede IP roteada.

O LWAPP é iniciado com uma fase de descobertas, na qual os terminais sem fio enviam aos controladores quadros de Pedido de Descoberta (*Discovery Request frame*). Os controladores, por sua vez, ao receberem estes pedidos, devem responder com um quadro de Resposta de Descoberta (*Discovery Response*). A partir das respostas, cada terminal sem fio deve escolher a qual controlador irá se associar. A associação é realizada através da troca de quadros *Join Request* e *Join Response*. Estes quadros também carregam informações sobre o tamanho máximo do quadro que pode ser trocado entre controlador e terminal sem fio, para que o LWAPP realize fragmentação quando necessário.

Após a associação entre terminal sem fio e controlador, uma troca de configurações é realizada para que os dois dispositivos operem em versões compatíveis. No caso de redes 802.11, durante o período de configuração o terminal sem fio pode realizar *download* de *software* caso o atual seja incompatível, e também pode receber configurações de SSID, parâmetros de segurança, taxa de transmissão, canal de operação, entre outras. A seguir o terminal sem fio é habilitado para operação e o LWAPP se encarrega de encapsular todo o

tráfego trocado entre terminal sem fio e controlador, incluindo dados de usuários sem fio e de controle. O protocolo também possibilita o envio de comandos a serem executados nos terminais sem fio com a finalidade de armazenamento e coleta de dados estatísticos. Outra funcionalidade é a preservação do canal de comunicação entre controlador e terminal sem fio, de forma que, caso a comunicação seja perdida, o terminal possa se associar a outro controlador.

Em versões mais recentes dos controladores Cisco, o protocolo utilizado é o CAPWAP (*Control and Provisioning of Wireless Access Points protocol*). Este protocolo é um padrão proposto pelo IETF [60], que busca a interoperabilidade entre dispositivos de diversos fabricantes. Seu desenvolvimento foi baseado no protocolo LWAPP, com a diferença de adotar o DTLS (*Datagram Transport Layer Security)* [61] como solução de segurança para a troca de mensagens entre controlador e terminais sem fio.

Assim como o LWAPP, o CAPWAP é um protocolo genérico que possibilita que um Controlador de Acesso gerencie um conjunto de Terminais sem Fio, independentemente da tecnologia utilizada nas camadas física e de enlace. Para acomodar as necessidades específicas de cada tecnologia sem fio de forma padronizada, "especificações de ligação" (*Binding Specifications*) são criadas para o uso de determinada tecnologia em conjunto com o CAPWAP. Por exemplo, no caso do 802.11, estes requerimentos são especificados pela RFC5416, "*Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11*" [62].

O CAPWAP mantém funcionalidades do LWAPP explicadas anteriormente, como o encapsulamento do tráfego, fragmentação, mecanismo de descobertas e associação de terminais sem fio, envio de comandos a serem executados nos terminais e preservação do canal de comunicação entre controlador e terminal sem fio. Uma das diferenças entre os protocolos é o estabelecimento de uma sessão DTLS segura é entre o terminal e o controlador durante a fase de associação.

Em virtude de sua padronização, que possibilita a interoperabilidade entre dispositivos de diversos fabricantes, o CAPWAP pode vir a ser adotado futuramente pelas diversas empresas que comercializam sistemas 802.11 controlados além da Cisco, como Motorola, Aruba, Meru e Juniper. Seria interessante a utilização deste protocolo no trabalho aqui apresentado, entretanto, ainda não existe uma implementação do CAPWAP disponível para utilização em conjunto com *firmware* OpenWRT, tornando necessária sua implementação, o

que foge ao escopo deste projeto. Outro problema é a existência de algumas desavenças em relação ao uso do protocolo. A primeira delas é em relação a direitos de propriedade intelectual. Segundo uma declaração da Aruba [63], qualquer fabricante que implementar o CAPWAP pode estar sujeito a cobranças de *royalties*, tendo em vista que a Cisco não revelou exatamente quais partes do protocolo são de sua propriedade intelectual.

Outro problema relatado pela Aruba é a escassez de funcionalidades e suporte às diferentes arquiteturas existentes nos protocolos proprietários. A empresa afirma que, dado o estado atual do mercado Wi-Fi, um sistema proprietário é requerido para suportar o ritmo de desenvolvimento tecnológico. Como exemplo, o CAPWAP atual não leva em consideração os novos padrões 802.11 n, k, r e y desenvolvidos pelo IETF, e dada sua velocidade de desenvolvimento, o CAPWAP levaria anos para acompanhar essas novas tecnologias. Tendo em vista estas desavenças, a Aruba não planeja substituir seu protocolo proprietário atual, o PAPI (*Proprietary Access Protocol Interface*), e oferece como solução de interoperabilidade, o software *AirWave Wireless Management Suite* (AWMS), que é capaz de gerenciar equipamentos de múltiplos fabricantes, como Cisco e Meru, através do uso de protocolos padronizados como SNMP e SSH [64].

Outro exemplo de protocolo de controle proprietário utilizado em controladores antigos da Motorola é o WISP (*Wireless Switch Protocol*). Equipamentos mais modernos desta empresa utilizam o protocolo WISPe (*Wireless Switch Protocol Enhanced*), que foi criado com base no CAPWAP, e integra as etapas de descoberta, associação e troca de configurações entre pontos de acesso e controlador [65].

Como o foco deste trabalho não é o desenvolvimento de protocolo de comunicação entre dispositivos de rede, e protocolos padronizados como o SNMP e CAPWAP não se adéquam aos requisitos do projeto, para a implementação do SCIFI foi escolhida a utilização do protocolo SSH (*Secure Shell*) [66] para a troca de informações e comandos entre APs e controlador. Este protocolo é padronizado pelo IETF e é amplamente utilizado para conexão entre dispositivos da rede e execução remota de comandos. Através dele, o controlador se conecta de forma segura ao ponto de acesso e executa programas locais para a configuração de parâmetros e coleta dos dados necessários para a execução dos algoritmos de controle, que ocorre no controlador central. Esta solução se mostra interessante por ser segura e ser amplamente suportada pelos pontos de acesso, além de consumir poucos recursos de processamento e memória RAM (*Random Access Memory*).

4. SISTEMA DE CONTROLE SCIFI

Para que uma rede sem fio tenha um bom desempenho é necessário que a interferência excessiva seja evitada. Ao se fazer uma instalação, pode-se escolher, por exemplo, qual canal será utilizado por cada AP de forma a minimizar a interferência. No entanto, uma configuração estática ficará rapidamente obsoleta em um ambiente mutável, onde novas redes podem ser instaladas, e outras, existentes, desligadas. Outra questão que deve ser considerada é a dificuldade de gerenciamento de uma rede que contenha muitos pontos de acesso de baixo custo. Como este tipo de equipamento carece de um sistema de controle, a instalação, configuração e manutenção de cada ponto de acesso devem ser realizadas individualmente, o que se torna cada vez mais difícil conforme o número de pontos de acesso aumenta. Buscando resolver estes problemas, o SCIFI (Sistema de Controle Inteligente para redes sem FIo) [67] foi criado. O sistema engloba um controlador central que se encarrega da coordenação dos pontos de acesso, tornando a configuração da rede automática e dinâmica. Com isto, a instalação e gerência da rede é facilitada e a interferência observada por cada AP se torna reduzida, já que o controlador se encarrega por pesquisar interferências no ambiente e escolher os canais e potências de transmissão com os quais cada AP devem operar.

O SCIFI é um sistema voltado para redes de comunicação sem fio 802.11 infraestruturadas compostas por dispositivos de diversas marcas e de baixo custo, e se mostra como uma alternativa aos sistemas proprietários de alto custo fechados, ou seja, sistemas que não suportam a interoperação entre dispositivos de diferentes fabricantes. Suas principais funções são minimizar a interferência entre pontos de acesso vizinhos e ajudar no equilíbrio

do número de estações clientes associadas entre os pontos de acesso, bem como facilitar a instalação e gerência de grandes redes. Para realizar essas tarefas, o controlador utiliza três técnicas, que são: (1) seleção de canais de operação dos APs pertencentes à rede; (2) controle de potência de transmissão dos APs; (3) indicação da carga em cada AP da rede.

A Figura 17 mostra a arquitetura de rede utilizada pelo sistema SCIFI, que se assemelha a uma rede infraestruturada com a adição de um controlador central. Os quatro dispositivos básicos que compõe esta rede são:

(1) pontos de acesso de baixo custo, com o requisito de operar com o sistema operacional embarcado de código aberto OpenWRT [3] ou outro sistema Linux embarcado;

(2) um controlador central, que possuirá a visão da rede como um todo e definirá quais os melhores canais e potências de transmissão a serem utilizados pelos pontos de acesso de acordo com os algoritmos do sistema;

(3) um *switch* (ou uma rede de camada 2) que interliga os pontos de acesso e o controlador central através da rede cabeada, possibilitando a comunicação entre eles;

(4) clientes sem fio que acessam a rede através dos pontos de acesso;

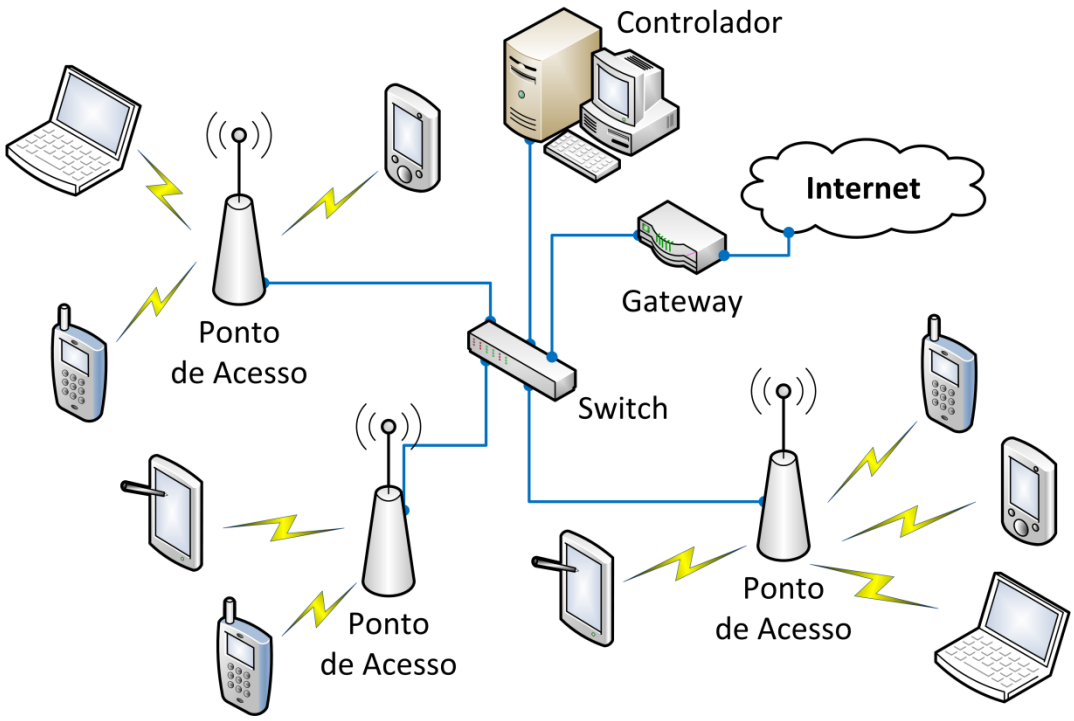


Figura 17. Arquitetura de rede utilizada pelo SCIFI.

Nesta arquitetura, se for desejado, o serviço de DHCP (*Dynamic Host Configuration Protocol*) e NAT (*Network Address Translation*) pode ser implementado de forma centralizada e não individualmente em cada ponto de acesso. Esta configuração não é necessária para o funcionamento do sistema SCIFI, porém, possibilita que o cliente sem fio mantenha seu IP no momento em que realizar *roaming* entre os APs da rede. Para que o *roaming* ocorra, também é necessário que os APs possuam o mesmo SSID, como foi descrito na seção 2.1.

A próxima seção (4.1) apresenta mais detalhes sobre o funcionamento do controlador SCIFI.

4.1. VISÃO GERAL DO SISTEMA SCIFI

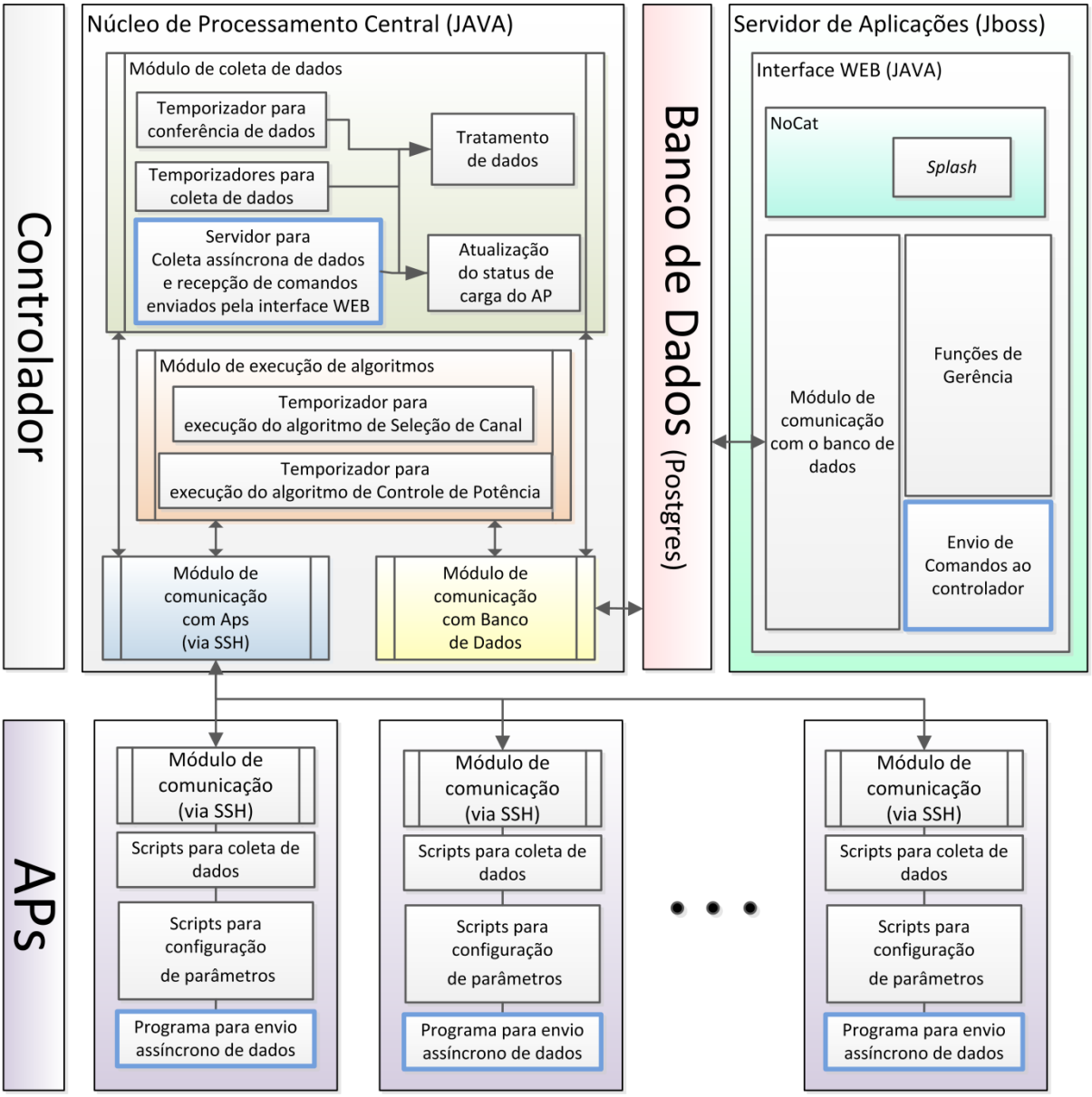


Figura 18. Arquitetura do sistema SCIFI

A arquitetura de *software* do sistema SCIFI, é apresentada na Figura 18. Nesta figura, pode-se observar que parte do sistema opera no controlador central (parte superior da figura), e outra parte opera nos pontos de acesso (parte inferior da figura).

O subsistema que opera no Controlador Central se subdivide em três partes principais: Núcleo de Processamento Central, Banco de Dados e Interface Web.

O Núcleo de Processamento Central é responsável pela definição dos parâmetros de canal e potência utilizados pelos pontos de acesso e se subdivide em quatro módulos básicos: Módulo de Coleta de Dados, Módulo de Execução de Algoritmos, Módulo de Comunicação

com o Banco de Dados e Módulo de Comunicação com APs.

O Módulo de Coleta de Dados contém os Temporizadores para Coleta de Dados, que agendam a execução da coleta de dados em cada ponto de acesso controlado. Os intervalos de tempo entre execuções das coletas podem ser definidos pelo administrador da rede através da interface web de administração do controlador. Basicamente, três tipos de dados são coletados: informações de *scan*, informações de *station dump*, e informações sobre as configurações de canal e potência dos pontos de acesso.

O processo de *scan* é a execução da varredura espectral no ponto de acesso. Através desta varredura, quadros de *beacon*, contendo informações relativas ao sinal proveniente de pontos de acessos vizinhos, são capturados. Estas informações são utilizadas pelos algoritmos de seleção de canal e controle de potência para a realização do cálculo da interferência entre os pontos de acesso. O processo de varredura espectral é realizado de forma sequencial em cada ponto de acesso, permitindo que, enquanto um ponto de acesso execute o *scan*, os outros operem normalmente e enviem quadros de *beacon* em seu canal de operação. Após a realização da coleta, os dados são tratados pelo controlador e inseridos no banco de dados.

Tendo em vista que os dados reportados pelo *scan* podem sofrer alterações abruptas devido a certas alterações no ambiente, como a movimentação de pessoas ou de objetos, para amenizar a influência de tais alterações o controlador realiza a ponderação dos valores de potência e qualidade de sinal antes de armazená-los no banco de dados. O valor armazenado é resultado de uma média móvel exponencial, de forma que os valores mais antigos de potência de sinal e qualidade possuem um peso na definição do novo valor. Este peso pode ser definido pelo administrador da rede através da Interface Web de gerência do controlador. A equação que determina o valor ponderado é:

$$Valor\_Ponderado = (Valor\_Antigo * Alfa) + Valor\_Atual*(1-Alfa)$$

Equação 1. Média móvel exponencial utilizada para cálculo dos valores de sinal e qualidade a serem armazenados no banco de dados.

, onde Valor_Ponderado é o valor de qualidade ou sinal que será inserido no banco de dados; Valor_Antigo é o valor de qualidade ou sinal que estava previamente no banco de dados; Valor_Atual é o valor de qualidade ou sinal que acabou de ser obtido através da execução da

tarefa de *scan* no ponto de acesso; e Alfa é o fator multiplicativo que determina qual a porcentagem do valor antigo que irá compor o novo valor ponderado.

Outro tipo de informação coletada pelo controlador central é a obtida através do processo conhecido por *station dump*. Esta informação revela o número de usuários associados a cada ponto de acesso controlado e é utilizada pelos algoritmos de balanceamento de carga e seleção de canal. Sua coleta é realizada paralelamente em cada ponto de acesso e, após sua realização, os dados são tratados pelo controlador e as informações sobre o *status* de carga do AP e clientes associados são inseridas no banco de dados.

Tendo em vista que a associação de novos clientes pode ocorrer no intervalo entre coletas, foi criado o submódulo de Coleta Assíncrona de Dados. Este submódulo é dividido em duas aplicações, uma que opera no controlador (servidor), e outra que opera no ponto de acesso (cliente). O *software* cliente, ao perceber que uma nova estação se associou ou desassociou do ponto de acesso, envia as informações sobre a estação ao servidor, que faz o tratamento dos dados e atualiza as informações no banco de dados em tempo real. Isso garante o melhor funcionamento dos algoritmos de balanceamento de carga e seleção de canal. Este mesmo servidor também é responsável por receber e agendar a execução de comandos enviados através da interface Web de administração ao controlador.

Para conferir se as informações contidas no banco de dados sobre canal de operação e potência de transmissão dos pontos de acesso estão corretas, o controlador realiza um processo denominado "*check* de sanidade". Neste processo, informações sobre o canal de operação e potência de transmissão de cada AP são coletadas e comparadas com as guardadas no banco de dados. Caso alguma delas esteja incorreta, o controlador ordena reconfiguração do ponto de acesso com a informação contida no banco de dados. A conferência de dados é executada paralelamente nos pontos de acesso com intervalo de tempo definido através da interface web de administração do controlador.

O segundo módulo do Núcleo de Processamento Central é o Módulo de Execução de Algoritmos. Este módulo contém os Temporizadores para Execução de Algoritmos, que agendam a execução dos algoritmos de seleção de canal e controle de potência em cada ponto de acesso controlado. Os intervalos de tempo entre execuções desses algoritmos podem ser definidos pelo administrador da rede através da interface web de administração do controlador.

As informações necessárias para a execução dos algoritmos, como a lista de APs controlados, dados de varredura espectral e número de clientes associados, são buscadas no

banco de dados através do Módulo de Comunicação com o Banco de Dados. Após a configuração dos canais de operação e potência dos pontos de acesso, o banco de dados é atualizado com as novas informações.

A comunicação entre o controlador e os pontos de acesso é realizada através do Módulo de Comunicação, que utiliza o protocolo SSH (*Secure Shell*) [66] para a criação de um canal seguro para troca de dados entre os dispositivos. Para estabelecer o canal seguro, o controlador deve se conectar ao ponto de acesso e, a seguir, poderá copiar arquivos de dados dos pontos de acesso ou ordenar que executem scripts de coleta de dados ou configuração de parâmetros.

Para prover maior escalabilidade do sistema, os pontos de acesso controlados podem ser divididos em regiões de controle. Para cada região, o controlador irá iniciar uma instância de controle que executará os temporizadores de coleta de dados e execução dos algoritmos de forma independente. Os pontos de acesso devem ser distribuídos entre as regiões de acordo com suas posições geográficas de forma que, aqueles que tenham proximidade física e que possam vir a se interferir, devem ser cadastrados na mesma região de controle.

Na implementação atual do controlador, os pontos de acesso devem ser cadastrados manualmente para controle através da interface web de administração do controlador. Futuramente, uma forma de cadastro automático dos pontos de acesso será pesquisada e implementada.

O banco de dados utilizado pelo SCIFI, cuja estrutura é apresentada na Figura 19, armazena informações sobre os pontos de acesso controlados, regiões de controle, dados coletados dos APs, e parâmetros de execução do controlador. Nesta figura, cada bloco representa uma tabela que armazena determinado tipo de informação. O banco de dados contém sete tabelas ao total, que são:

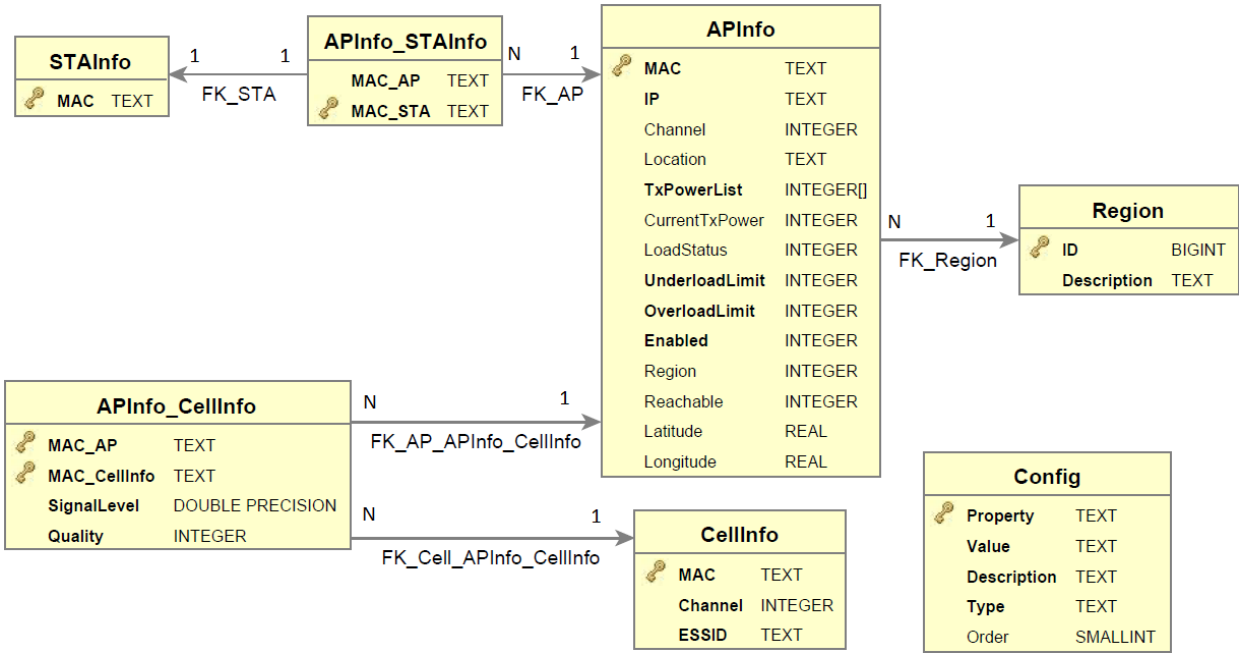


Figura 19. Estrutura do banco de dados do sistema SCIFI.

1) APInfo – Tabela que armazena informações dos pontos de acesso controlados. Cada linha desta tabela representa um AP e suas colunas armazenam, respectivamente, endereço MAC do AP, endereço IP, canal (*Channel*), localização (*Location*), lista de possíveis potências de transmissão (*TxPowerList*), potência de transmissão atual (*CurrentTxPower*), status de carga (*LoadStatus*), limiar de carga baixa (*UnderloadLimit*), limiar de sobrecarga (*OverloadLimit*), indicador de habilitação do AP para controle (*Enabled*), identificação da região de controle do AP (*Region*), indicador de conectividade via cabo entre AP e controlador (*Reachable*). Os limiares citados são utilizados na determinação do status de carga do ponto de acesso.

2) CellInfo – Tabela que armazena, em cada linha, informações sobre os pontos de acesso vizinhos aos APs da rede controlada, ou seja, pontos de acesso que possam vir a causar interferência, incluindo APs controlados ou não controlados. Suas colunas armazenam, respectivamente, endereço MAC, Canal (*Channel*) e ESSID de um AP vizinho. Estas informações são obtidas através da execução da varredura espectral nos APs controlados.

3) APInfo_CellInfo – Tabela que armazena a relação entre um ponto de acesso controlado e outro ponto de acesso, controlado ou não, que esteja armazenado na tabela CellInfo. Cada linha desta tabela indica qual AP (inserido na tabela APInfo) é capaz de

receber sinal de outro AP (inserido na tabela CellInfo). Suas colunas armazenam, respectivamente, o endereço MAC do AP controlado (MAC_AP), o endereço MAC do AP interferente (MAC_CellInfo), o nível de sinal recebido (*SignalLevel*) e sua qualidade (*Quality*).

4) STAInfo – Tabela que armazena informações sobre os clientes associados aos pontos de acesso controlados. Cada linha desta tabela contém um endereço MAC de uma estação associada.

5) APInfo_STAInfo - Tabela que armazena a relação entre um ponto de acesso controlado e um cliente associado. Cada linha desta tabela indica qual estação (STAInfo) está associada a qual AP (APInfo). Suas colunas armazenam, respectivamente, o endereço MAC do AP (MAC_AP) e da estação (MAC_STA).

6) Config – Tabela que armazena parâmetros de execução do controlador. Cada linha desta tabela representa um parâmetro. Suas colunas armazenam, respectivamente, o nome do parâmetro (*Property*), seu valor (*Value*) e sua descrição (*Description*) e a unidade de seu valor (*Type*).

7) Region – Tabela que armazena informações sobre as regiões de controle. Cada linha desta tabela representa uma região. Suas colunas armazenam, respectivamente, o número de identificação da região (ID) e o nome da região (*Description*).

A interface web de administração do controlador, cuja estrutura básica é apresentada na Figura 20, permite que o administrador da rede obtenha e modifique informações relacionadas ao controlador. Como apresentado na figura, a página inicial da interface Web dá acesso à área de administração do controlador, que requer o fornecimento de *login* e senha. Quando devidamente autenticado, o administrador ganha acesso às páginas de visualização e edição de APs, páginas de edição das regiões de controle, página de configuração dos parâmetros de execução do controlador e página de execução de comandos do controlador. Estes comandos permitem que o administrador execute, no momento em que o botão do comando for clicado, uma das tarefas do controlador, como por exemplo, a coleta de dados de *scan*. A Figura 21 mostra os demais comandos que podem ser executados.

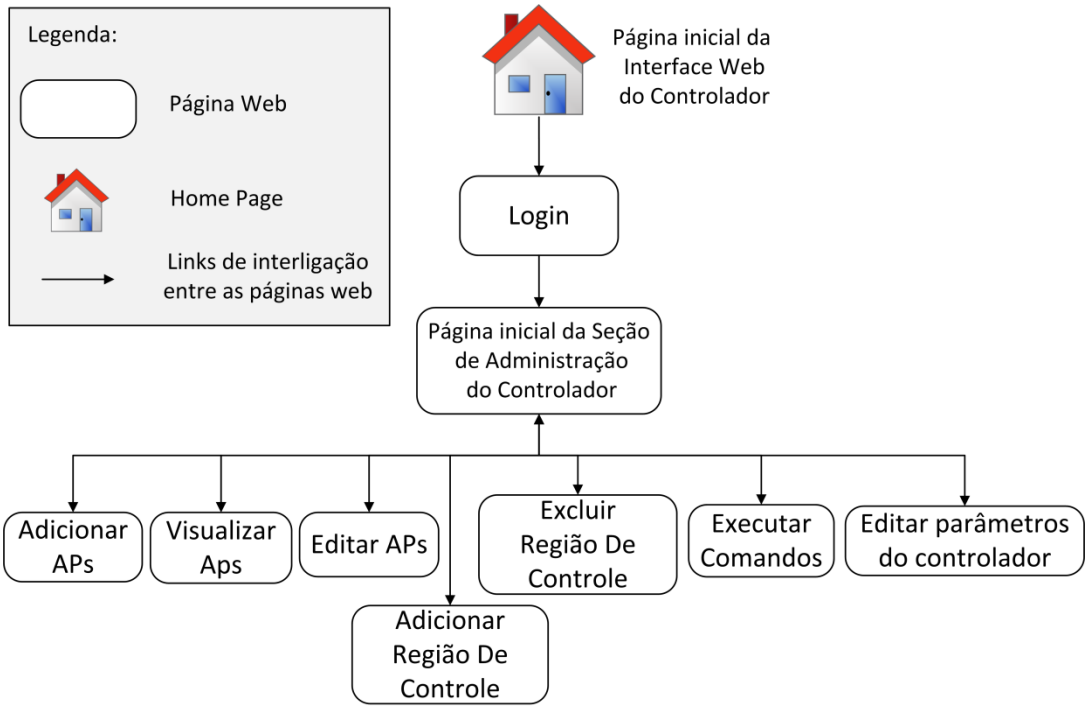


Figura 20. Estrutura da interface web de administração do controlador.

Figura 21. Execução de comandos do controlador via interface Web

No momento em que um usuário se associa à rede e tenta acessar uma página da

internet (HTTP), a página de *Splash* (Figura 22) é exibida. Para obter acesso à rede, o usuário deve clicar no botão “Entrar”. Esta funcionalidade, conhecida por *captive portal*, é fornecida pelo programa NoCatAuth [68], que foi alterado e agregado ao controlador. Modificações em seu código foram realizadas para que, no momento do acesso à página *Splash*, o MAC do cliente seja repassado controlador. Com esta informação, o controlador se torna capaz de indicar, na mesma página *Splash*, a qual ponto de acesso o cliente está associado.

A página de *Splash* é responsável por informar ao usuário o status de carga dos pontos de acesso da rede. Através desta página, o usuário é capaz de verificar a qual ponto de acesso está associado e, caso deseje uma melhor experiência de uso, poderá se dirigir à localização de um ponto de acesso com menor carga.

O Servidor de Aplicações possibilita o funcionamento da interface web do controlador. Este servidor suporta a tecnologia *JavaServer Faces* [69], com a qual a interface foi desenvolvida. Na implementação atual, o controlador SCIFI utiliza o JBoss [70] como seu Servidor de Aplicações.

Figura 22. Página de Splash

A parte do sistema SCIFI que opera nos pontos de acesso é composta pelo Módulo de

Comunicação, Scripts de Coleta de Dados, Scripts de Configuração de Parâmetros, e programa para envio assíncrono de dados, como mostra a Figura 18.

Os *scripts* de coleta de dados possibilitam a obtenção de informações sobre clientes associados ao AP (informações de *station dump*), obtenção da potência e qualidade do sinal recebido dos pontos de acesso vizinhos (informações de *scan*), e obtenção dos parâmetros de funcionamento do AP, como canal e potência de transmissão.

Já os scripts para configuração de parâmetros, possibilitam definir o canal e a potência de transmissão utilizada pelo AP. Esses scripts são acionados pelo Núcleo de Processamento Central do Controlador e os dados obtidos são armazenados no AP para posteriormente serem copiados pelo controlador. A recepção de comandos e a cópia de dados são realizadas através do módulo de comunicação, que utiliza SSH (*Secure Shell*) [66] para estabelecer uma conexão segura entre o controlador e o AP, como foi dito anteriormente. A utilização de *scripts* possui a vantagem de permitir que o controlador trabalhe com vários modelos de ponto de acesso, necessitando apenas de que cada um deles possua os *scripts* compatíveis.

Como foi dito anteriormente, o ponto de acesso também possui uma aplicação (cliente) para envio assíncrono de dados, que é capaz de informar ao controlador a ocorrência de eventos assíncronos. Na versão atual do SCIFI, o evento informado é a associação ou desassociação de uma nova estação ao ponto de acesso.

4.2. ALGORITMO DE ALOCAÇÃO DE CANAIS

O algoritmo de alocação de canais do sistema SCIFI [71] [72] modela a rede em um "grafo de interferências" no qual os nós (vértices) representam os pontos de acesso e, caso exista interferência entre eles, estes devem ser conectados por arestas ponderadas unidirecionais. Desta forma, o problema da alocação de canais se torna o clássico problema da coloração de grafos, no qual as cores representam os possíveis canais que podem ser utilizados pelos pontos de acesso. O objetivo da coloração de grafos é colorir os vértices de um grafo de forma que vértices adjacentes não possuam a mesma cor. Como este problema é classificado como NP Difícil, uma heurística é necessária para que seja resolvido em tempo viável. No SCIFI, a heurística utilizada se baseia na heurística do Grau de Saturação ou DSATUR [24], conforme foi dito no final da seção 3.1. A ideia básica desta heurística consiste em utilizar a informação de quantas cores adjacentes um determinado vértice possui (grau de saturação) para selecionar a ordem em que os vértices serão coloridos. Caso exista apenas um

vértice, este é escolhido para ser colorido. Caso existam mais de um vértice, o que possuir maior grau de saturação deve ser colorido primeiro, com a primeira cor disponível. Em [16], os autores propõe a utilização desta heurística em redes IEEE 802.11 e sugerem uma implementação descentralizada. Em [13] são apresentados resultados de simulações mostrando que o algoritmo é capaz de trazer benefícios em relação à escolha de canais descoordenada.

No SCIFI, a proposta de [16] foi aperfeiçoada de acordo com os requisitos definidos para o sistema. Primeiramente, para reduzir sua complexidade de implementação e se valer da vantagem de utilizar a informação global da rede, o algoritmo foi implementado de forma centralizada. Isso possibilita que um controlador central possa coletar informações de todos os pontos de acesso da rede e as utilizar como base para a execução do algoritmo. Além disso, a consideração da interferência ocasionada por pontos de acesso que não pertencem ao mesmo domínio administrativo no processo de escolha dos canais dos pontos de acesso controlados foi inserida no algoritmo. No algoritmo do SCIFI, a escolha das cores foi alterada para ser realizada com base na qualidade do sinal interferente recebido de outros APs e não escolher a primeira cor livre, como foi indicado na proposta original de [16]. Caso mais de um AP possua o mesmo grau de saturação, o que obtiver o maior número de clientes terá prioridade na escolha do canal. Caso novo empate ocorra, o número IP do ponto de acesso deve ser utilizado, de forma que o que possuir o menor IP deve ganhar prioridade. No algoritmo original, se mais de um vértice possui o mesmo grau de saturação, o autor sugere a utilização do "grau de vértices", ou seja, número de vértices vizinhos descoloridos, para o desempate e, caso o desempate não ocorra, é proposto que uma função determinística baseada em alguma característica dos nós, como o endereço MAC, seja utilizada para a decisão.

O objetivo do algoritmo de seleção de canais do SCIFI é definir um conjunto de canais para os APs controlados que se aproxime do ideal em termos de minimização da interferência gerada por APs vizinhos, levando em consideração a interferência de redes não controladas. Na implementação centralizada realizada, a escolha dos canais se restringiu a um dos três canais não sobrepostos do espectro do 802.11g, ou seja, os canais 1, 6 e 11, porém o algoritmo pode facilmente ser adaptado para redes 802.11a que opera com 12 canais, sendo todos não sobrepostos.

A Figura 23 apresenta o pseudocódigo da operação básica do algoritmo de seleção de canais. Em sua execução, são utilizadas informações de varredura espectral e número de clientes associados coletadas previamente de cada AP através do Módulo de Coleta de Dados.

Estas informações são representadas pela variável "ListaDeDadosDosAps[]" e, através delas, é possível determinar, para cada AP controlado, quais são seus vizinhos interferentes, incluindo APs não gerenciados. Nesta etapa, os pontos de acesso controlados trabalham em um canal que será alterado ao final do algoritmo. A seguir o controlador constrói o grafo de interferências, que é representado pela variável "Grafo" (linha 1). Este grafo é formado por vértices que representam os APs e arestas ponderadas, que representam a interferência entre eles. Esta ponderação é dada pela qualidade do sinal interferente recebido. Pontos de acesso não gerenciados são representados por vértices já coloridos. Posteriormente, o controlador cria uma lista com os vértices que não estão coloridos, representada por "ListaDeVérticesDescoloridos[]"(linha 2). A princípio, os vértices descoloridos são aqueles que correspondem aos APs gerenciados.

```
SelecionarCanais(ListaDeDadosDosAps[],ListaDePossiveisCanais[])
   // O grafo de interferência é criado com base nas informações de varredura espectral dos APs,
   //contendo todos os vértices e as arestas ponderadas que os interligam.
   //APs de redes vizinhas não gerenciadas entram no grafo como vértices já coloridos.
1: Grafo ← CriarGrafoDeInterferências(ListaDeDadosDosAps[]);
   //Uma lista de vértices descoloridos é criada. No caso, essa lista contém os APs da rede gerenciada.
2: ListaDeVérticesDescoloridos[] ←  ListarVerticesDescoloridos(Grafo);
   // Este bloco define a prioridade de coloração dos vértices descoloridos e os colore um a um.
3: enquanto tamanho da ListaDeVérticesDescoloridos[] > 0, faça
        //A lista de vértices descoloridos é ordenada por prioridade de escolha de canal.
        //O  vértice com maior grau de saturação será colorido primeiro. Caso mais de um vértice possua
        //o maior grau, o que possuir maior número de clientes dentre eles ganha prioridade.
4:      ListaDeVérticesOrdenada[] ← OrdenarVérticesPorPrioridade (ListaDeVérticesDescoloridos[]);
5:      VérticeSelecionado ← ListaDeVérticesOrdenada [0];
        //O canal do vértice é escolhido pela função ColorirVértice.
6:      ColorirVértice(VérticeSelecionado, ListaDePossiveisCanais[]);
        // O vértice que acabou de ser colorido é retirado da lista de vértices descoloridos e o processo é
        // repetido para os restantes. Agora este vértice irá influenciar no grau de saturação dos outros.
7:    ListaDeVérticesDescoloridos[]←RemoverVértice(VérticeSelecionado,ListaDeVérticesDescoloridos[]);
8: fim enquanto
   //Os canais dos APs são atualizados após todos os vértices serem coloridos.
9: AtualizarCanalDosAPs();
```

Figura 23. Pseudocódigo básico do algoritmo de alocação de canais do SCIFI

Cada um dos vértices descoloridos será colorido no bloco "enquanto" que se inicia na linha 3 . Inicialmente, os vértices são ordenados pela prioridade de escolha de canal (linha 4). A prioridade é dada ao vértice que possui o maior grau de saturação. Este grau indica o número de cores diferentes utilizadas por vértices vizinhos e não considera vértices que não

foram coloridos. Seu cálculo é realizado com base nas informações de varredura espectral coletadas nos pontos de acesso controlados, que detectam redes vizinhas através da recepção de quadros de *beacon* emitidos por elas. Caso mais de um vértice possua o mesmo grau de saturação, dentre eles, aquele que possuir maior número de clientes associados terá preferência na escolha de canal. Caso ocorra novo empate, a escolha da prioridade deve ser feita com base no endereçamento IP do ponto de acesso, de forma que um IP menor possui prioridade.

No algoritmo implementado, a interferência gerada por vizinhos em canais diferentes de 1, 6 ou 11 é considerada como se atuasse em um desses canais (o mais próximo), já que os espectros desses canais acabam, em parte, por se sobrepor, como mostra a Figura 10. Por exemplo, um vizinho não controlado operando no canal 2 ou 3 é considerado como se estivesse no canal 1; já um vizinho no canal 4 ou 5 é considerado como se estivesse no 6. Tendo em vista que isto pode inserir um pequeno erro, futuramente pretende-se implementar um mecanismo mais aprimorado de utilização de canais sobrepostos. A princípio, os pontos de acesso controlados não são considerados no cálculo do grau de saturação, já que seu novo canal será ainda determinado. Mas, a partir do momento em que um AP da rede ganha um novo canal, ele passa a influenciar no cálculo do grau de saturação de seus vizinhos.

```
//Esta função determina o melhor canal de operação, dentre os possíveis, para um vértice
ColorirVértice(VérticeSelecionado, ListaDePossiveisCanais[])
    //Uma lista contendo todas as arestas ponderadas do vértice é criada
 1: ListaDeArestas[] ← ListarArestasDoVértice(VérticeSelecionado);
    //A lista de arestas é varrida e os canais que estão ocupados por APs vizinhos
    // interferentes  são retirados da lista, restando os canais desocupados.
 2: ListaDeCanaisDesocupados[] ← RemoverCanaisOcupados(ListaDeArestas[],ListaDePossiveisCanais[])
    // Se existe algum canal desocupado, o primeiro da lista é escolhido.
 3: se tamanho da ListaDeCanaisDesocupados[] > 0
 4:     CorEscolhida ← ListaDeCanaisDesocupados[0];
        // O vértice é marcado como colorido, seu canal é configurado. No  final do algoritmo, APs
        //representados por seus respectivos vértices serão configurados fisicamente.
 5:     DefinirCorDoVértice(VérticeSelecionado, CorEscolhida);
 6:     retornar
 7: fim se
    //Caso contrário, o canal com menor soma de qualidades das arestas é escolhido.
 8: senão
 9:     CorEscolhida ←
        EcolherCanalComMenorSomaDeQualidades(ListaDeArestas[],ListaDePossiveisCanais[])
        // O vértice é marcado como colorido, seu canal é configurado. No  final do algoritmo, APs
        //representados por seus respectivos vértices serão configurados fisicamente.
10:     DefinirCorDoVértice(VérticeSelecionado, CorEscolhida);
11:     retornar
12: fim senão
```

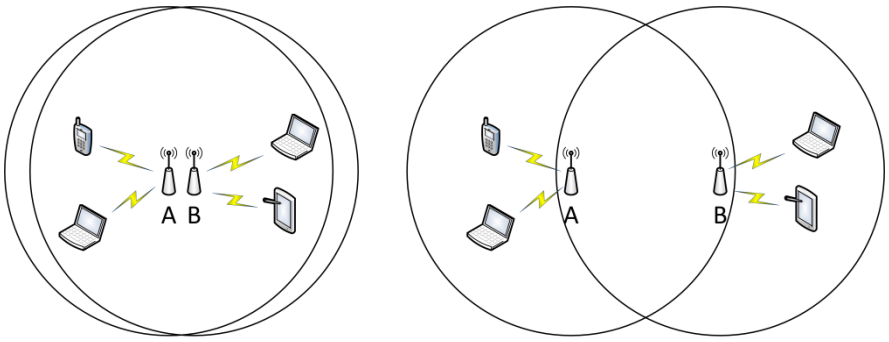
Figura 24. Pseudocódigo da função que escolhe a cor que será atribuída a um vértice.

Após determinado o vértice que será colorido, sua cor deve ser definida. Esta tarefa é realizada pela função "ColorirVértice" (Figura 23 - linha 6), cujo pseudocódigo simplificado pode ser visto na Figura 24. Inicialmente, uma lista com todas as arestas de interferência do vértice é criada (Figura 24- linha1). A seguir, o controlador varre esta lista para verificar quais dos possíveis canais estão ocupados, ou seja, quais deles possuem algum AP em operação. Os canais ocupados são retirados da lista, restando apenas os canais desocupados (Figura 24 - linha 2). Caso existam canais desocupados o primeiro canal da lista será escolhido (Figura 24 - linha 4). Caso não existam canais desocupados, o controlador buscará o canal com menor interferência. Para isso, ele varre novamente a lista de arestas e realiza, para cada canal, a soma das qualidades das arestas. O canal que apresentar menor soma de qualidades será escolhido.

A escolha do canal é feita desta forma porque, como foi dito anteriormente, a métrica de interferência utilizada pelo algoritmo é a qualidade do sinal interferente recebido. Neste algoritmo, consideramos que, quanto menor a qualidade, menor é a área de interferência daquele ponto de acesso, pois a relação sinal ruído do canal é pior, indicando maior distância

entre os APs. Sendo assim, o controlador deve escolher o canal com menor qualidade do sinal recebido para reduzir a área de interferência e, no caso de existir mais de um ponto de acesso vizinho em um mesmo canal, a soma das qualidades dos sinais recebidos no canal deve ser considerada.

A Figura 25 demonstra como a qualidade do sinal recebido influencia na área de interferência entre dois APs. No cenário à esquerda, o AP A recebe sinal com qualidade alta proveniente do AP B. A alta qualidade indica a grande proximidade rádio entre os dois pontos de acesso. Consequentemente, haverá grande sobreposição das áreas de cobertura dos dois APs, gerando uma grande área de interferência. Já no cenário da direita, o AP A recebe sinal com baixa qualidade proveniente do AP B, indicando maior distância rádio entre os dois APs. Neste caso, a área de cobertura em comum é menor, ocasionando menor área de interferência entre os APs.



AP A recebe sinal com qualidade alta proveniente do AP B, e vice-versa

AP A recebe sinal com qualidade baixa proveniente do AP B, e vice-versa.

Figura 25. A qualidade do sinal recebido indica a área de interferência entre os APs

Voltando à Figura 24, após o vértice ser colorido (linha 6), ele é retirado da lista de vértices descoloridos e é marcado como colorido para que os próximos vértices considerem sua interferência no processo de escolha do canal. O processo é repetido para os vértices até que todos sejam coloridos. Ao final, os canais dos APs são configurados fisicamente de acordo com os canais escolhidos para seus respectivos vértices (linha 9).

Para se adequar às modificações do ambiente, como o surgimento ou desligamento de APs interferentes, o algoritmo é executado com intervalo de tempo definido pelo administrador da rede através da interface web de administração do controlador.

4.3. ALGORITMO DE CONTROLE DE POTÊNCIA

Após executado o algoritmo de seleção de canal, caso haja pontos de acesso operando no mesmo canal, há a chance de que haja interferência entre eles. Para que esta interferência seja reduzida, o controlador central configura as potências de transmissão dos pontos de acesso da rede.

O mecanismo de controle de potência implementado no SCIFI dispensa alterações nos dispositivos clientes e busca complementar o algoritmo de alocação de canais de forma a reduzir ainda mais a área de interferência entre pontos de acesso vizinhos. O algoritmo se divide em duas etapas principais, uma que realiza a redução da potência, buscando a redução da interferência, e outra que realiza o aumento da potência, buscando a ampliação da cobertura.

Na primeira etapa, o controlador ordena que cada ponto de acesso interferente reduza sua potência de transmissão até que seu sinal deixe de alcançar outros APs controlados, ou até que uma determinada potência mínima de transmissão seja alcançada. Um ponto de acesso interferente é aquele cujo sinal pode ser recebido por um dos outros APs da rede controlada. A redução da potência é realizada de foram gradual a cada execução do algoritmo, e as potências utilizadas em cada passo são determinadas pelo administrador da rede.

Por exemplo, se forem escolhidas as potências {6,8,12,14,20} para um determinado AP, na primeira execução do algoritmo, caso este AP esteja interferindo outros APs da rede, sua potência será reduzida de 20 dBm para 14 dBm. Na próxima execução, caso a interferência permaneça, sua potência será reduzida de 14 dBm para 12 dBm, e assim por diante, até que o AP deixe de interferir ou até que a potência de 6 dBm (potência mínima determinada) seja alcançada. O conjunto de possíveis potências pode possuir o número de níveis desejado pelo administrador da rede.

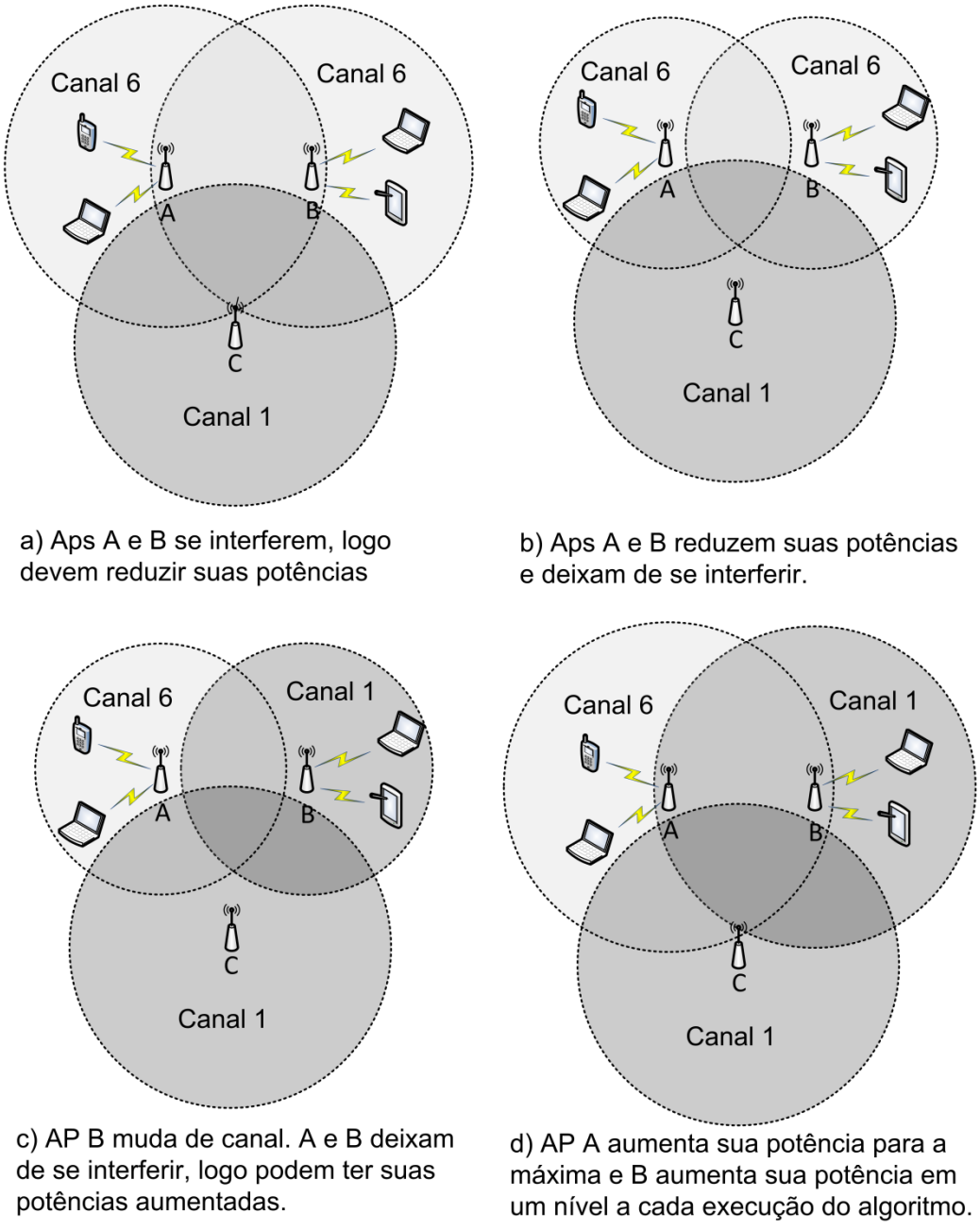


Figura 26. Exemplo de utilização do mecanismo de aumento de potência.

Na segunda etapa, como o fato de um ponto de acesso deixar de interferir a outros pode representar a diminuição excessiva de sua potência, mal funcionamento ou a mudança de canal de algum dos APs da rede, o controlador determina que os APs que não são interferentes aumentem sua potência gradativamente até que seu sinal volte a alcançar algum outro AP. No caso em que um AP seja o único operando em um determinado canal, sua potência deve ser aumentada ao máximo.

Por exemplo, a Figura 26 mostra uma situação na qual um AP deve ter sua potência aumentada. No cenário (a), os APs A e B operam no mesmo canal e causam interferência mútua, enquanto o AP C opera em um canal diferente. Portanto, as potências de A e B devem ser reduzidas passo a passo até que os APs deixem de se interferir, o que ocorre no cenário (b). No cenário (c) AP B tem o seu canal alterado e, com isso, A e B deixam de se interferir. Neste momento, não faz sentido manter a configuração de potência atual destes APs. Como o AP A agora é o único em seu canal, sua potência deve ser aumentada ao máximo e, como o AP B agora compartilha canal com o AP C e não está causando interferência a este AP, sua potência deve ser aumentada gradativamente em níveis, como mostra o cenário (d).

```
//Esta função define se o ponto de acesso deve aumentar ou reduzir sua potência
RealizarControleDePotência(ListaDeAPsControlados[], ListaDeDadosDeInterferência[])
 1: enquanto tamanho da ListaDeAPsControlados[]> 0, faça
        //A lista de APs controlados é varrida e os APs que estiverem no mesmo canal do
        // AP atual e estiverem interferindo serão separados nesta lista
 2:     ListaDeAPsInterferentes[] ←
        RetornaAPsInterferentes(APAtual,ListaDeAPsControlados[],ListaDeDadosDeInterferência []);
 3: fim enquanto
 4: enquanto tamanho da ListaDeAPsInterferentes[] > 0, faça
        // A lista de APs interferentes é varrida e cada um deles terá sua potência reduzida em um
        //nível
 5:     ReduzirPotênciaEmUmNível(APAtual);
 6: fim enquanto
 7: enquanto tamanho da ListaDeAPsControlados[]> 0, faça
        //A lista de APs controlados é varrida. Caso o AP atual não esteja na lista de APs interferentes e
        //seja o único no canal, sua potência será aumentada ao máximo. Caso ele não esteja na lista e
        //não seja o único no canal, sua potência será elevada em apenas em um nível.
 8:     se o AP atual não está na lista de APs interferentes
 9:         se o AP atual está sozinho no canal
10:             ConfigurarPotênciaMáxima(APAtual);
11:         fim se
12:         senão
13:             AumentarPotênciaEmUmNível(APAtual);
14:         fim senão
15:     fim se
16: fim enquanto
```

Figura 27. Pseudocódigo simplificado do algoritmo de controle de potência do SCIFI

A Figura 27 mostra o pseudocódigo da operação básica do algoritmo de controle de potência implementado no SCIFI, com maiores detalhes sobre a operação deste algoritmo. Durante a execução do algoritmo, são utilizadas informações de varredura espectral coletadas previamente de cada AP através do Módulo de Coleta de Dados. Como o algoritmo é

dependente destas informações, é importante que o intervalo entre coletas seja menor do que o intervalo entre execuções do algoritmo.

Utilizando as informações de varredura espectral, que são representadas pela variável "ListaDeDadosDeInterferência[]" na Figura 27, o controlador varre a lista de APs controlados e verifica quais APs são capazes de causar interferência a outros APs da rede (linhas 1,2 e 3). Estes APs são separados em uma lista de APs interferentes, representada pela variável "ListaDeAPsInterferentes[]" (linha 2). A seguir, o controlador ordena que cada AP interferente reduza sua potência em um nível dentre os possíveis determinados pelo administrador da rede através da interface web de administração do controlador (linhas 4,5 e 6).

Posteriormente o controlador varre a lista de APs controlados novamente (bloco que se inicia na linha 7) e verifica se o AP atual está na lista de APs interferentes (linha 8). Caso ele não esteja, é verificado se ele é o único AP em seu canal dentre os APs controlados (linha 9). Caso seja, o controlador ordena que sua potencia seja aumentada para a máxima dentre as possíveis potências (linha 10). Caso não seja, o controlador ordena que a potência do AP seja aumentada em um nível (linha 13). Ao final, as novas potências são configuradas nos pontos de acesso e o algoritmo é agendado para ser executado novamente com intervalo de tempo definido pelo administrador da rede através da interface web de administração do controlador.

4.4. BALANCEAMENTO DE CARGA

O balanceamento de carga tem por objetivo a distribuição de estações clientes entre os pontos de acesso da rede, de forma que um ponto de acesso não fique sobrecarregado em relação aos outros, e a rede como um todo possa atender com qualidade equilibrada todas as estações associadas.

Como foi dito na Seção 3.3, no padrão 802.11 atual é o cliente que escolhe a qual ponto de acesso irá se associar baseando-se em informações contidas em quadros de *probe response* ou *beacons*. O método de escolha pode variar de acordo com o dispositivo, porém a maioria deles opta por se associar ao AP com maior nível de sinal.

Um dos requisitos de desenvolvimento do SCIFI é que o sistema funcione sem a necessidade de alterações nos dispositivos clientes, de forma que seja compatível com dispositivos atuais. Devido à dificuldade de forçar um dispositivo cliente a trocar de ponto de acesso ou escolher a qual ponto de acesso ele deve se associar, sem realizar alterações nos dispositivos clientes, o balanceamento de carga do SCIFI busca prover informações ao

usuário para que ele decida a qual ponto de acesso deve se associar. As informações são mostradas na página de Splash (Figura 22), que é exibida no primeiro acesso web do usuário, após sua conexão com algum ponto de acesso da rede. Esta página contém dados sobre a localização do usuário e dos pontos de acesso da rede, além do status de carga dos APs. Com estas informações, o usuário se torna capaz de avaliar a carga dos pontos de acesso e, caso deseje uma melhor experiência de acesso, pode se dirigir à localização do AP menos carregado.

A métrica utilizada para a determinação do status de carga dos pontos de acesso é o número de clientes associados. Se este número estiver abaixo de um determinado limiar de carga baixa (UnderloadLimit), o AP é considerado com “Carga Baixa”. Caso esteja acima do limiar de carga alta (OverloadLimit), o AP é considerado “Sobrecarregado”. Caso esteja entre os dois limiares, o AP é considerado com “Carga Média”. Os valores limiares são determinados pelo administrador da rede, através da interface web, e podem variar de um ponto de acesso para outro. A atualização do status de carga do ponto de acesso é realizada após a execução da coleta de dados (*station dump*) do AP ou após a recepção de dados assíncronos pelo controlador informando a associação de uma nova estação.

5. TESTES PARA AVALIAÇÃO DO SISTEMA

A avaliação do SCIFI foi realizada através de diversos testes com variados objetivos. Um primeiro conjunto de testes objetivou a avaliação dos algoritmos de alocação de canais e controle de potência, que se deu através de testes de vazão executados em uma rede montada para tal finalidade. Um segundo conjunto de testes objetivou a avaliação da escalabilidade do sistema, bem como a avaliação dos potenciais prejuízos que a execução das tarefas necessárias ao controle podem causar aos clientes da rede. A descrição dos testes realizados e os resultados obtidos podem ser vistos nas próximas seções.

5.1. AVALIAÇÃO DOS ALGORITMOS DE ALOCAÇÃO DE CANAL E CONTROLE DE POTÊNCIA

5.1.1. Introdução

A avaliação dos algoritmos de alocação de canal e controle de potência implementados no SCIFI foi realizada através montagem de uma rede infraestruturada 802.11 g composta por um microcomputador, encarregado de exercer a função do controlador SCIFI, sete pontos de acesso de baixo custo operando com sistema operacional embarcado OpenWRT, e um *switch*, através do qual a comunicação entre controlador e os APs foi realizada. Além desta estrutura,

sete *laptops* foram utilizados como clientes da rede, cada um deles associado a um respectivo ponto de acesso.

A ideia básica da avaliação foi mostrar um exemplo de cenário de rede simples dentre os vários que podem ser beneficiados com a utilização do controlador SCIFI e seus mecanismos de redução de interferência. Os benefícios foram demonstrados através da comparação da vazão agregada obtida na rede operando com e sem o controlador SCIFI.

Os testes foram divididos em duas etapas. A primeira etapa buscou avaliar os benefícios do algoritmo de alocação de canais, e não tratou o problema do controle de potência. Na segunda etapa, o controle de potência do SCIFI foi ativado e os resultados obtidos com a utilização deste mecanismo foram comparados com os resultados obtidos sem sua utilização. Os resultados mostram que o algoritmo de alocação de canais implementado é capaz de propiciar boa distribuição de canais entre APs que interagem em um ambiente, mesmo com alguns deles não sendo controlados, e a utilização do algoritmo de controle de potência favorece ainda mais a redução da interferência. Como consequência, a rede como um todo é beneficiada com o aumento de sua vazão.

A Figura 28 mostra a parte da planta do 4° andar do bloco E da Universidade Federal Fluminense, no qual a rede para testes foi montada. Nesta planta, os APs controlados são representados por um círculo cinza escuro e os não controlados são representados por um círculo contendo um “x”. Cada *laptop* cliente foi posicionado em um raio de distância não maior do que 2 metros do ponto de acesso ao qual foi associado. O modelo do laptop utilizado foi o OLPC XO-1[73] com interface de rede Marvell Libertas e driver versão 2.6.25-20080925. Dois modelos de pontos de acesso da Ubiquiti foram utilizados na rede. Um deles foi o NanoStation Loco M2 [74] com *firmware* OpenWRT [3] versão Backfire 10.03 r20728, que pode ser distinguido na figura pela presença de setas que representam a direção de sua antena setorial de 60° e 8 dBi. O outro modelo foi o PicoStation 2 [75] com *firmware* OpenWRT versão Backfire 10.03.1 r29592, que possui antena omnidirecional de 6 dBi.

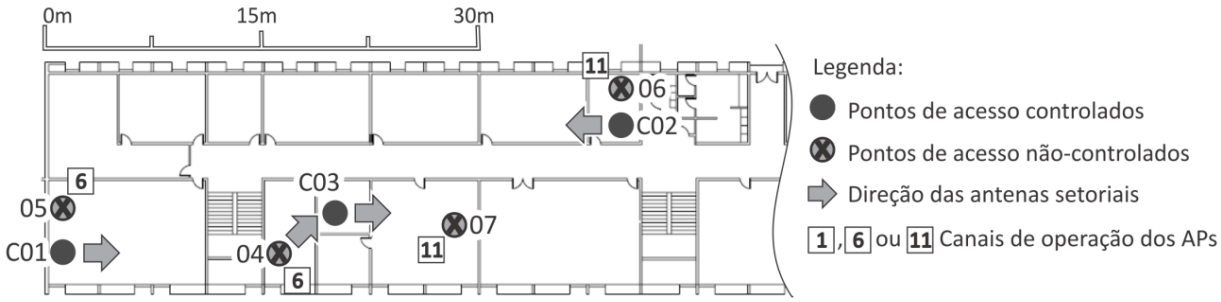


Figura 28. Posicionamento dos pontos de acesso da rede de testes

Utilizando a estrutura de rede descrita, testes de vazão foram realizados para a validação dos algoritmos propostos. Em todos os testes, os canais dos pontos de acesso não controlados, 04, 05, 06 e 07, foram mantidos em 6, 6, 11 e 11, respectivamente, como mostra a Figura 28, e suas potências de transmissão foram mantidas no padrão, ou seja, potência máxima de acordo com o modelo do ponto de acesso utilizado, conforme mostra a tabela .

Tabela 1. Potência de transmissão padrão dos pontos de acesso não controlados

Ponto de Acesso:	**04**	**05**	**06**	**07**
Potência (dBm):	27	20	20	20

As próximas seções descreverão os resultados obtidos nos testes de avaliação do algoritmo de alocação de canais e controle de potência realizados.

5.1.2. Primeira Etapa: Avaliação do algoritmo de alocação de canais

No teste realizado sem o controlador SCIFI, os canais dos APs controlados (C01, C02 e C03) foram determinados sem considerar a presença de APs não gerenciáveis, alocando os canais 6, 11 e 1, respectivamente (Figura 29). Pode-se notar que a configuração evita interferência entre APs da rede controlada, já que aloca um canal não sobreposto para cada ponto de acesso. Entretanto, como mostrarão os testes de vazão, estes canais não estão bem distribuídos quando consideramos a operação de APs vizinhos não controlados.

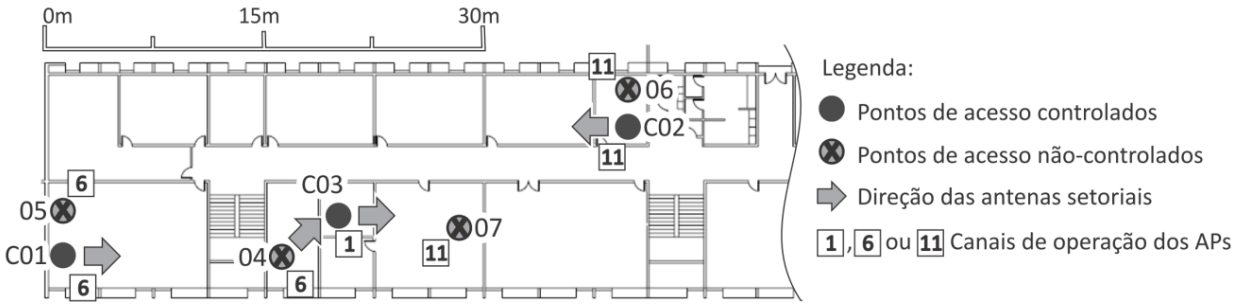


Figura 29. Configuração de canais do teste realizado sem o controlador SCIFI

No teste realizado com a utilização do controlador SCIFI, o algoritmo de alocação de canais foi executado tendo como base as informações de interferência contidas na Tabela 2. Esta tabela mostra quais pontos de acesso foram encontrados por cada AP controlado após realização de varredura espectral, e a qualidade com que o sinal de cada AP encontrado foi recebido. Por exemplo, analisando-se o cruzamento entre a coluna C01 com a linha 05, podemos concluir que o AP C01 recebe sinal proveniente do AP 05 com qualidade máxima (70/70). Já as células com um "-" representam casos em que não há comunicação entre os pontos de acesso, como ocorre entre C01 e C02. A escala de qualidades, que neste caso abrange valores de 0 até 70, é determinada pelo *driver* da interface sem fio. Os pontos de acesso utilizados nos testes trabalham com *drivers* Madwifi ou Ath9k [76] e o valor da qualidade reportada por esses *drivers* representa a Relação Sinal Ruído média calculada para os últimos quadros recebidos [77].

Com as informações da Tabela 2 o controlador monta o grafo de interferências apresentado pela Figura 30, que é a base para a execução do algoritmo. O próximo passo é a definição do Grau de Saturação dos pontos de acesso, ou seja, o número de canais ocupados por APs vizinhos. Observando-se a Figura 30, pode-se verificar que o grau de saturação de C01 é 2, já que ele encontrou APs nos canais 6 e 11 (APs 04, 05 e 07) ao realizar sua varredura espectral. Da mesma forma, pode-se verificar que C02 e C03 também possuem grau de saturação igual a 2.

Tendo em vista que o grau de saturação é igual para todos os APs, o algoritmo determina que, dentre os APs com maior grau de saturação, a prioridade na escolha do canal seja dada ao AP com maior número de clientes associados. Entretanto, como a rede está em testes, apenas 1 cliente está associado a cada ponto de acesso. Neste caso, como um novo empate foi verificado, o algoritmo determina que o AP com menor número IP (considerando o

byte mais a direita), tenha prioridade. Neste caso o AP C01, que possuía o menor IP, foi ser selecionado para realizar a escolha do canal primeiro.

Tabela 2. Qualidade do sinal recebido

Canal	APs encontrados: / AP que realiza varredura:	C01	C02	C03
-	C01	x	-	38/70
-	C02	-	x	50/70
-	C03	35/70	46/70	x
6	04	39/70	34/70	70/70
6	05	70/70	-	29/70
11	06	-	70/70	49/70
11	07	31/70	49/70	70/70

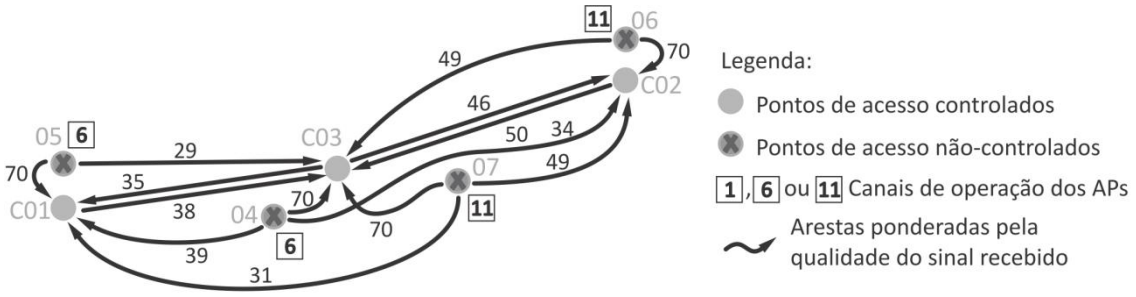


Figura 30. Grafo de interferência criado pelo controlador SCIFI.

Após definir a prioridade de C01 para a escolha de canal, este deve verificar se existem canais livres para utilização e selecionar o menor deles, dentre 1, 6 e 11. Como apenas os canais 6 e 11 estão ocupados, o canal 1 é escolhido e o processo é repetido para C02 e C03, considerando que agora C01 possui canal 1, como mostra o grafo da Figura 31.

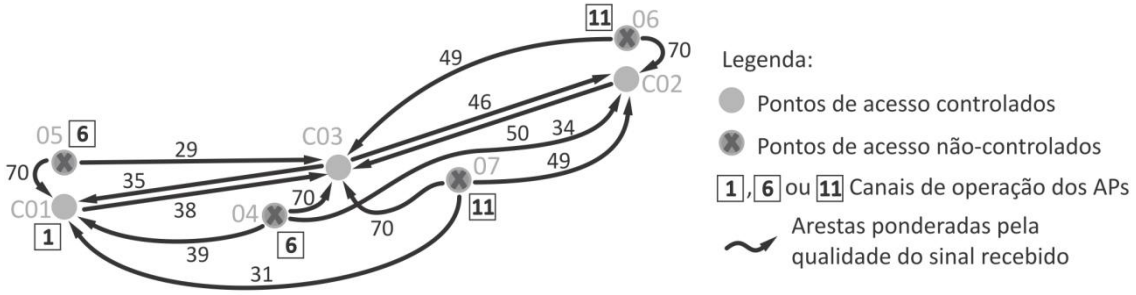


Figura 31. Grafo utilizado na segunda etapa do algoritmo de seleção de canais

Calculando-se novamente o Grau de Saturação, percebemos que C02 mantém seu grau 2, enquanto C03 passa a possuir grau 3, já que agora encontra pontos de acesso nos canais 1 (C01), 6 (04 e 05) e 11 (06 e 07). Com isto, C03 ganha prioridade na escolha de canal. Como não existem canais livres, a soma das qualidades em cada canal deve ser calculada, para que o canal com menor soma seja escolhido. Analisando-se o canal 1, verifica-se que a soma de qualidades observadas por C03 é 38 (referente a C01). Analisando-se o canal 6, verifica-se que a soma é 70+29=99 (APs 04 e 05). Analisando-se o canal 11, verifica-se que a soma é 49+70=119 (APs 06 e 07). Sendo assim, C03 escolhe o canal 1 para operação, já que este possui a menor soma das qualidades. O novo grafo, considerando esta nova alocação de canal é apresentado na Figura 32.

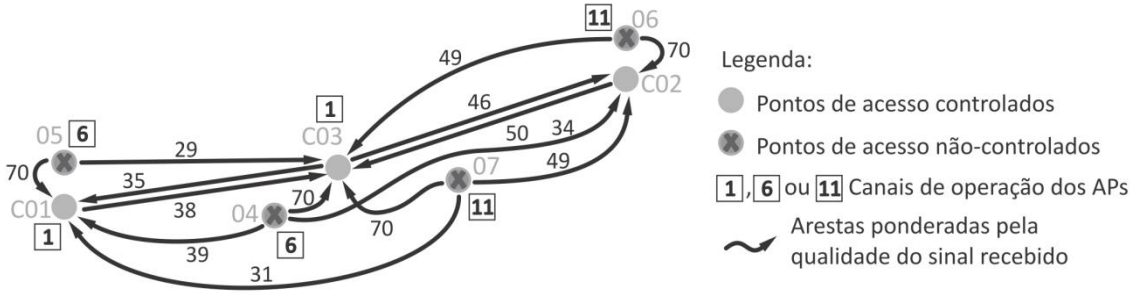


Figura 32. Grafo utilizado na terceira etapa do algoritmo de seleção de canais

Por fim, o último AP controlado, C02, deve escolher seu canal de operação. A princípio verifica-se que não existem canais livres, já que C02 encontra APs vizinhos nos três canais disponíveis. Somando-se as qualidades coletadas por C02 em cada canal, verifica-se que o canal 1 possui soma de qualidades de 46 (AP C03), o canal 6 possui soma de 34 (AP 04) e o canal 11 possui soma de 70+49 = 119 (APs 06 e 07). Sendo assim, C02 escolhe o canal 6 para operação, já que sua soma de qualidades é menor. Após a execução do algoritmo,

os canais escolhidos são configurados nos pontos de acesso pelo controlador. A Figura 33 mostra a configuração de canais que foi obtida através do algoritmo.

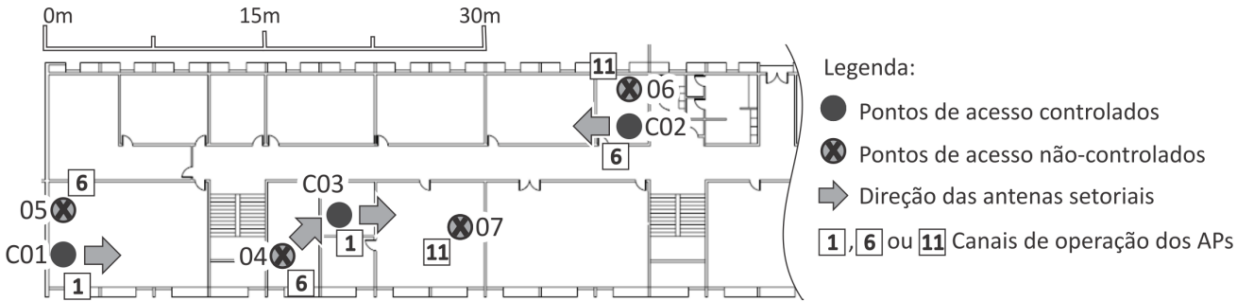


Figura 33. Configuração de canais do teste realizado com o controlador SCIFI

Para a realização dos testes de vazão, o programa Iperf [78] foi utilizado para gerar tráfego UDP partindo de cada ponto de acesso para seu cliente associado, utilizando datagramas de 1470 bytes. Para cada etapa de testes, o tráfego UDP foi gerado simultaneamente a partir dos sete pontos de acesso da rede e amostras de vazão foram coletadas a cada 5 segundos. As primeiras e últimas amostras coletadas foram desprezadas, considerando o pequeno erro que poderia ser causado pela não simultaneidade da ativação do Iperf em todos os APs. Cada amostra reportada pelo Iperf representa a vazão média no intervalo. O tráfego partindo do ponto de acesso com datagramas de 1470 bytes foi escolhido por ser considerado o mais utilizado do ponto de vista da estação cliente. A vazão obtida representaria a taxa disponível para *download* por parte do cliente. A utilização do UDP foi escolhida em detrimento do TCP porque o TCP possui mecanismo de controle de congestionamento que pode causar alterações nos resultados de vazão obtidos de acordo com a ocorrência de perdas de segmentos. Como no meio sem fio a perda de quadros pode ocorrer devido à fatores externos que não são controláveis, por exemplo, a locomoção de pessoas no local dos testes, estes fatores externos poderiam impactar os resultados, o que não era desejado.

Nos testes realizados sem a utilização do controlador SCIFI, foram coletadas 3626 amostras de vazão. Já nos testes que utilizaram o controlador SCIFI, foram coletadas 3430 amostras. Os testes foram realizados, cada um deles, em dois dias diferentes. Os valores médios das amostras obtidas por cada ponto de acesso estão apresentados na Figura 34, com margens de erro dadas pelo Intervalo de Confiança de 95%. As barras de erros se mostram pequenas devido ao grande número de amostras.

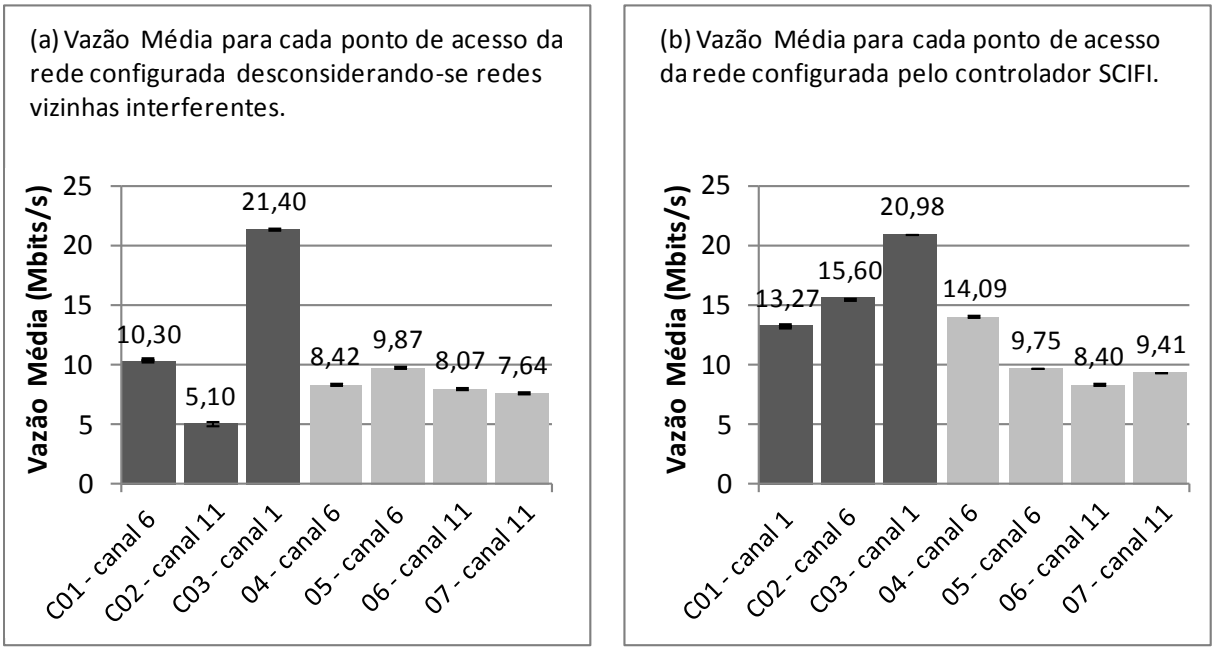


Figura 34. Teste de Alocação de canais - Gráficos da Vazão Média por Ponto de Acesso

Comparando-se os resultados mostrados na Figura 34 a e b, nota-se que, a utilização do controlador SCIFI (Figura 34 - b), no geral, ocasionou melhoria da vazão dos pontos de acesso da rede controlada e também das redes não gerenciadas. Isso mostra que o algoritmo implementado e sua métrica de interferência são eficazes para a definição de uma configuração de canais melhor, em termos de vazão, quando comparada com uma configuração que não considera APs não gerenciáveis. Apesar de parecer bom utilizar os três pontos de acesso gerenciados nos canais 6, 11 e 1 (Figura 34 - a), os resultados de vazão foram melhores quando dois deles operaram dividindo o canal 1 (Figura 34 - b), já que nesta configuração, sofreram menos interferência ocasionada por APs não controlados.

Para ajudar a visualização da melhoria da vazão global na rede ocasionada pela utilização do algoritmo, são apresentados na Figura 35 os gráficos de vazão agregada média, com margens de erro dadas pelo Intervalo de Confiança de 95%. A Figura 35 (a) mostra a vazão agregada da rede, incluindo os sete pontos de acesso. Neste gráfico, pode-se notar o aumento expressivo da vazão da rede (mais de 29% neste cenário de testes) quando o controlador SCIFI foi utilizado. Parte deste aumento foi ocasionado pela melhora da vazão dos APs gerenciados, como mostra a Figura 35 (b). Outra parte foi ocasionada pela melhora da vazão dos APs não gerenciados, como mostra a Figura 35 (c). Esses resultados mostram

que a rede como um todo, incluindo redes vizinhas não gerenciadas, pode ser beneficiada com a utilização do algoritmo descrito neste trabalho.

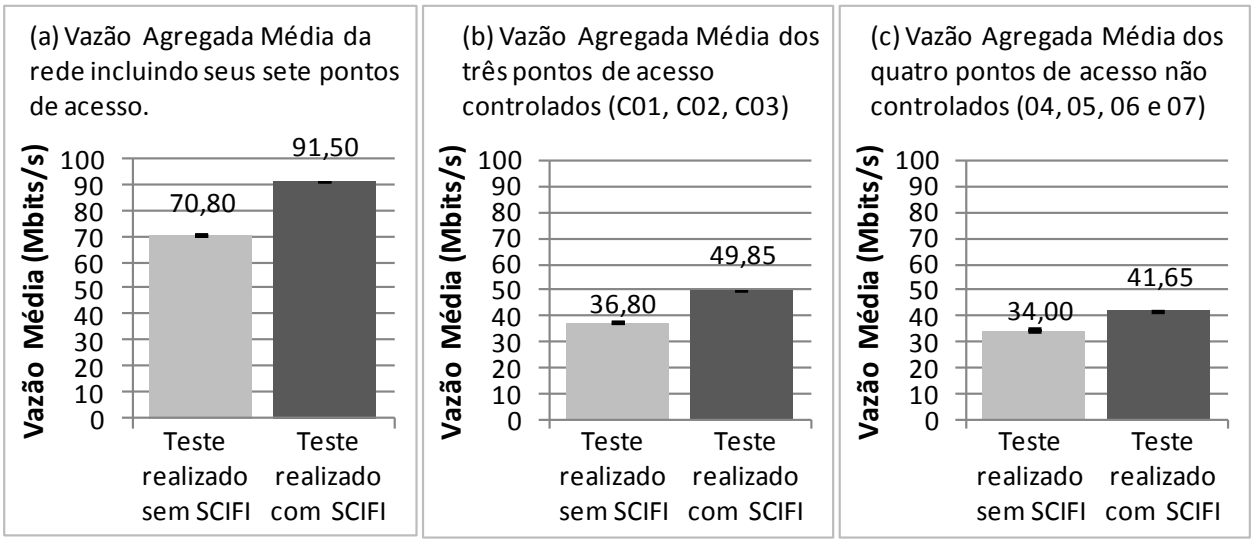


Figura 35. Teste de Alocação de canais - Gráficos da vazão agregada média

5.1.3. Segunda Etapa: Avaliação do algoritmo de controle de potência

Na etapa de avaliação do algoritmo de controle de potência, a configuração de canais utilizada nos testes de avaliação do algoritmo de alocação de canais (seção 5.1.2) foi mantida e o algoritmo de controle de potência foi executado em busca da redução da interferência causada entre os pontos de acesso controlados que operam no mesmo canal. Através da Figura 33, verifica-se que, dentre os pontos de acesso controlados, C01 e C03 operam no mesmo canal, e, através da informação de varredura espectral contida na Tabela 2, pode-se verificar que ambos se interferem.

Segundo determina o algoritmo, se um ponto de acesso causa interferência em algum de seus vizinhos controlados, este deve diminuir sua potência até que os vizinhos interferidos deixem de receber seu sinal ou um nível de potência mínimo seja alcançado. Desta forma, ambos C01 e C03 devem reduzir suas potências até que deixem de interferir um ao outro. Neste teste, o nível de potência de transmissão mínimo estabelecido foi de 6 dBm e as potências foram diminuídas gradativamente na sequência {27, 24, 22, 20, 18, 16, 14, 12, 10, 8, 6}, sendo que, a cada passo, uma nova varredura espectral foi realizada para verificar o

novo cenário de interferências. Após a diminuição gradativa das potências de C01 e C03 como descrito, foi verificado que C01 deixa de receber sinal de C03 quando este opera em 10 dBm e vice versa.

A seguir, o algoritmo determina que, caso um AP deixe de interferir seus vizinhos, ele deve ter sua potência aumentada novamente, o que causaria uma oscilação da potência de C01 e C03 entre 10 e 12 dBm. Tendo em vista que a execução do algoritmo de controle de potência ocorre em intervalos definidos pelo administrador da rede, nos testes, buscando evitar esta oscilação, um intervalo longo foi utilizado, de forma que ambos os pontos de acesso permanecessem com potência de 10dBm. A Tabela 3 mostra as configurações de canal e potência utilizadas nesta etapa de testes para pontos de acesso controlados (C01, C02 e C03) e não controlados (04, 05, 06 e 07). Nesta tabela, pode-se notar que os pontos de acesso mantiveram suas potências de transmissão padrão (máxima), exceto os pontos de acesso controlados interferentes (C01 e C03), que tiveram suas potências ajustadas pelo algoritmo.

Tabela 3. Configurações utilizadas no teste do algoritmo de controle de potência

Ponto de Acesso:	**C01**	**C02**	**C03**	**04**	**05**	**06**	**07**
Canal:	1	6	1	6	6	11	11
Potência (dBm):	10	27	10	27	20	20	20

Após definidas as potências, assim como nos testes da seção 5.1.2, o programa Iperf [78] foi utilizado para gerar tráfego UDP partindo, simultaneamente, de cada ponto de acesso para seu cliente associado, utilizando datagramas de 1470 bytes. Neste teste, 1765 amostras de vazão foram coletadas a cada 5 segundos e as primeiras e últimas amostras foram desprezadas considerando-se o pequeno erro que poderia ser introduzido pela não simultaneidade da ativação do Iperf em todos os pontos de acesso. Os valores médios das amostras obtidas por cada ponto de acesso podem ser vistos na Figura 36 (a), com margens de erro dadas pelo Intervalo de Confiança de 95%. Para melhor comparação entre os resultados obtidos nos testes sem e com o controle de potência ativado, o item (b) desta figura mostra os resultados obtidos no teste anterior, que utilizou apenas o algoritmo de seleção de canais do SCIFI (seção 5.1.2).

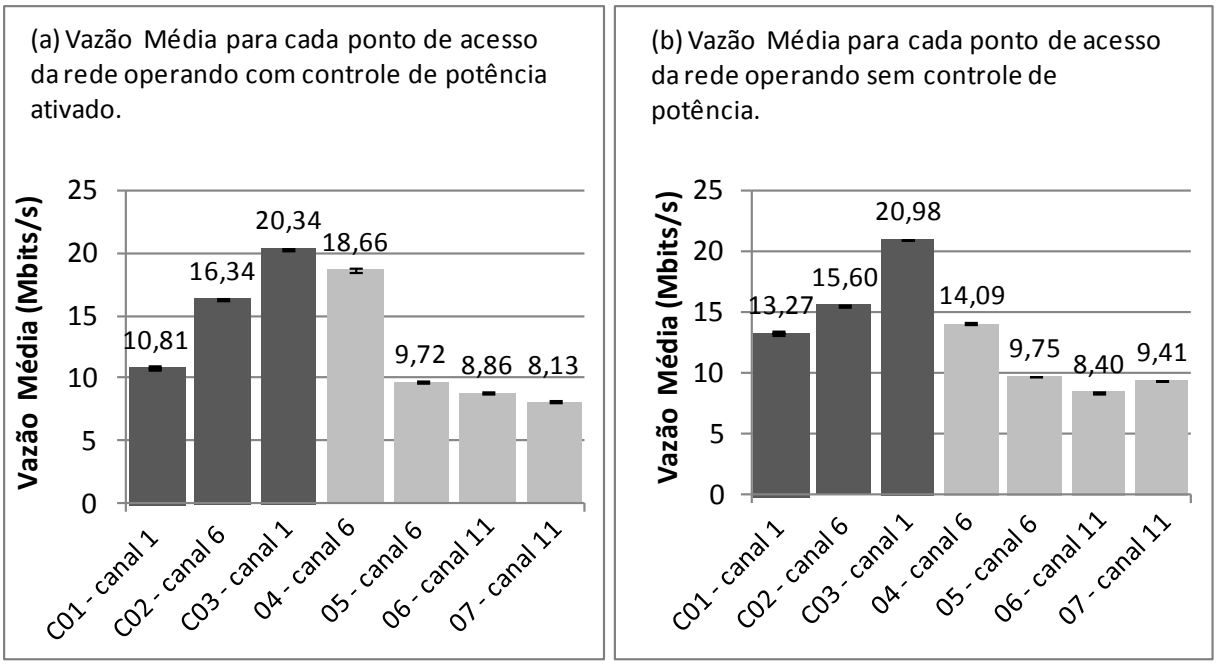


Figura 36. Teste do Controle de potência - Gráficos da Vazão Média por Ponto de Acesso

Comparando-se os resultados obtidos com e sem a ativação do algoritmo de controle de potência apresentados em Figura 36 (a) e (b), respectivamente, pode ser verificado que os valores de vazão média obtidos para os pontos de acesso C03, 05, 06 e 07 foram parecidos em ambos os testes. Dentre os pontos de acesso restantes, C02 e 04 apresentaram melhoras relativamente significantes em sua vazão, enquanto C01 obteve uma vazão reduzida.

Analisando-se a vazão agregada da rede, apresentada na Figura 37 (a), nota-se que a rede com um todo obteve pequena melhora em sua vazão (1,48%). Analisando-se os itens (b) e (c) desta mesma figura, nota-se que esta melhora foi proveniente dos pontos de acesso não controlados.

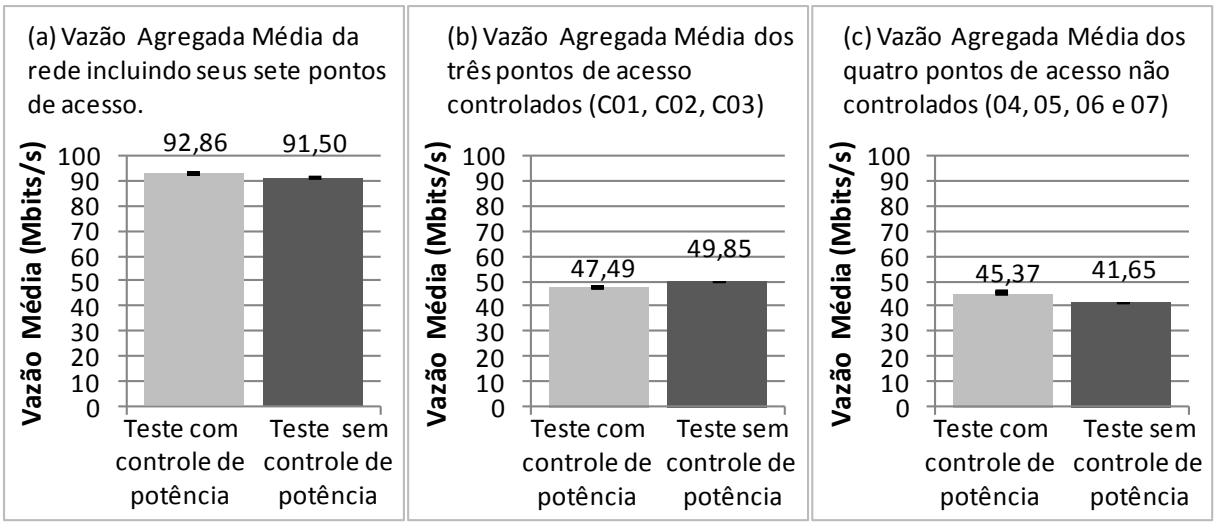


Figura 37. Teste do Controle de potência - Gráficos da vazão agregada média

5.1.4. Conclusão

Os testes de avaliação do algoritmo de alocação de canais do SCIFI mostraram que o algoritmo é capaz de propiciar boa distribuição de canais entre os APs que interagem em um ambiente, mesmo no caso em que alguns deles não pertencem ao mesmo domínio administrativo. Os testes foram realizados em uma rede composta por sete pontos de acesso, dos quais, três deles eram controlados e os quatro restantes não. A vazão na rede foi comparada com e sem a utilização do algoritmo, sendo que os canais dos pontos de acesso não controlados foram mantidos fixos e, no cenário sem a utilização do algoritmo, os canais dos pontos de acesso controlados foram determinados de forma a minimizar a interferência entre eles, porém sem considerar os vizinhos não gerenciados. Os resultados obtidos mostram que a utilização do algoritmo foi capaz de propiciar um aumento 29,4% da vazão agregada na rede como um todo, sendo que 63,04% deste aumento se deu na vazão agregada da rede gerenciada, enquanto 36,96% se deu na vazão agregada da rede não gerenciada.

Os testes de avaliação do algoritmo de controle de potência mostraram ligeira melhora na vazão agregada da rede, porém não são conclusivos. Como a diminuição da potência tende a piorar a relação sinal ruído, e esta está ligada a taxa de codificação do IEEE802.11, é possível que ao usarmos potência menor para diminuir a interferência causemos um impacto negativo na vazão da rede que está operando com potência reduzida. Assim veríamos uma diminuição na vazão local mas possivelmente um incremento da vazão agregada, dada a menor interferência. Os testes mostram isto, mas o efeito é muito sutil.

5.2. TESTES DE AVALIAÇÃO GERAL DO SISTEMA

5.2.1. Teste 1: Execução do Scan

5.2.1.1. Objetivo

Como é necessário encontrar de tempos em tempos quais são os vizinhos, todos pontos de acesso realizam a função de *scan* de tempos em tempos. O objetivo deste teste é avaliar o quanto o *scan* (varredura espectral) é prejudicial ao cliente da rede sem fio. Através dos testes serão verificados o tempo em que o cliente permanece sem comunicação com o ponto de acesso e o tempo de duração do *scan.* Os resultados obtidos poderão embasar a escolha da frequência com que o *scan* deve ser executado pelo controlador.

5.2.1.2. Introdução

O processo de *scan* é realizado nos pontos de acesso e revela informações sobre a interferência de redes vizinhas que são essenciais para o funcionamento dos algoritmos de seleção de canal e controle de potência executados pelo controlador SCIFI.

Durante a execução do *scan*, o ponto de acesso interrompe suas atividades de transmissão e recepção de dados e apenas recebe quadros de *beacon* provenientes de outros pontos de acesso ao seu redor, o que pode ser prejudicial aos clientes da rede associados a este ponto de acesso. Para que a pesquisa por pontos de acesso vizinhos ocorra em todos os canais, o AP alterna seu canal de operação durante o processo, o que leva tempo. Neste método de varredura, que é conhecido como método passivo, o AP não envia quadros para pesquisa de redes vizinhas, mas apenas recebe quadros de *beacon*.

Este teste buscará revelar a duração do processo de *scan* e o comportamento dos dispositivos cliente diante de sua execução.

5.2.1.3. Procedimento

O dispositivo cliente deve ser conectado ao ponto de acesso e mensagens ICMP *echo request* [79] devem ser enviadas com intervalo de 10 ms através da ferramenta *ping* [80] com destino ao PC servidor conectado à rede cabeada (Figura 38). Este valor foi escolhido porque é pequeno o suficiente para realizar as medições e pode ser cumprido pela interface sem fio do dispositivo sem causar estouro no *buffer* de saída. O AP deverá encaminhar o tráfego entre

cliente e servidor e, no mesmo momento, a captura do tráfego entre cliente e o AP (tráfego sem fio) e entre o AP e o servidor (tráfego na rede cabeada) deve ser realizada. A seguir, o processo de *scan* deve ser executado pelo AP. A Figura 38 mostra a rede de testes montada para a realização do teste de *scan*. Apesar de serem mostrados dois dispositivos clientes, o teste foi realizado com um dispositivo cliente por vez.

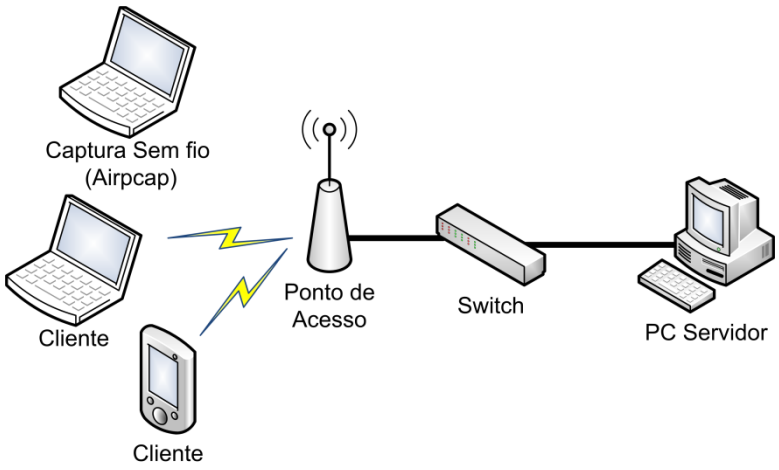


Figura 38 - Teste 1: execução do *scan*

5.2.1.4. Equipamentos Utilizados

O ponto de acesso utilizado nos testes foi o Ubiquiti Nanostation Loco M2 [74], com *firmware* OpenWRT [3], versão Backfire 10.03 r20728 e configurações padrão com segurança desabilitada. Esta última opção não foi escolhida por motivos específicos. Apenas é importante lembrar que, já que a rede de testes estava aberta, os intervalos de tempo registrados nos testes não incluem o processo de autenticação do cliente, que ocorreria após a associação caso a rede estivesse com segurança habilitada. O *laptop* cliente utilizado foi o IBM ThinkPad com interface de rede sem fio Intel PRO/Wireless 2200BG e *driver* ipw2200. Os testes também foram realizados com um segundo dispositivo cliente para comparação do comportamento de diferentes interfaces sem fio, que foi o celular Samsung Galaxy 5 GT-I5500 [81] com interface sem fio baseada no *chipset* Atheros AR6003 e *driver* AR6k . A captura de quadros sem fio foi realizada através da interface Airpcap Nx [82], que é uma interface própria para realizações de capturas sem fio e, portanto, é capaz de capturar mais quadros em relação a uma interface comum. Além disso, interfaces comuns podem não suportar o modo monitor, que é o modo que permite a captura de todos os quadros que alcançam a interface sem fio sem a necessidade de ela estar associada a um ponto de acesso.

5.2.1.5. Resultados

Ao realizar o teste com o *laptop* IBM ThinkPad, pode-se verificar que, no momento em que o AP inicia o processo de *scan*, o *laptop* envia o ICMP *echo request* e recebe alguns *ACKs* do AP, porém estas mensagens não chegam ao servidor. No *log* da ferramenta *ping*, verifica-se uma primeira rajada de perdas referentes a estas mensagens. O atraso dos *ACKs* relativos a estas mensagens é maior do que o comum e continua aumentando até que o AP para de responder. A seguir o cliente continua tentando enviar as mensagens *echo request* e, como não há resposta do AP (*ACK*), o cliente faz retransmissão.

Depois de certo intervalo de tempo tentando fazer retransmissões sem sucesso, o cliente manda quadros de desassociação (*Disassociate*) para o AP. Neste momento, as mensagens *echo request* não são mais enviadas e começam a ser armazenadas na fila de saída da interface do *laptop* cliente. A fila enche e algumas mensagens *echo request* são perdidas. No *log* da ferramenta *ping* verifica-se uma segunda rajada de perdas devido a estas mensagens.

A seguir, o cliente manda quadros de *probe request* procurando por APs para que possa se associar novamente. Após o *scan*, o AP volta a responder e envia algumas mensagens ICMP *echo reply*, porém o cliente está desassociado e não as recebe. O AP tenta então retransmitir estas mensagens e, como não consegue, envia quadros *Request to Send* (*RTS*), provavelmente, buscando evitar colisões e novas perdas.

Algum tempo depois, o cliente se autentica e se associa novamente ao AP. A seguir, ele começa a enviar as mensagens de *echo request* que estavam na fila de sua interface. O AP responde a estas mensagens (*ACK*) e as repassa ao servidor. No *log* da ferramenta *ping*, verifica-se uma rajada de *pings* com grande atraso, devido ao enfileiramento na saída da interface do *laptop* cliente.

Por fim, após enviar todas as mensagens de *echo request* da fila, o tempo de resposta verificado no *log* do *ping* volta a ser baixo.

Ao realizar o teste com o celular Galaxy 5, foi verificado um comportamento diferenciado de sua interface de rede sem fio. Ao contrário do *laptop* IBM ThinkPad, este dispositivo não se desconectou do ponto de acesso no momento do *scan*, e por isso seu tempo sem comunicação com o AP foi menor. No arquivo de *log* da ferramenta *ping*, verifica-se uma pequena rajada de perdas no inicio do *scan*, referente às mensagens ICMP *echo request* que

receberam *ACK* do AP porém não foram repassadas ao servidor e mensagens que sofreram retransmissão porém não foram recebidas pelo AP. Em certos casos, verifica-se um ou dois *pings* com grandes atrasos, referentes àqueles que foram repassados ao servidor antes do início do *scan*, porém suas respostas (ICMP *echo reply*) foram entregues apenas ao final do processo de *scan.*

A partir dos testes realizados, dois resultados principais foram obtidos. O primeiro, que buscou verificar o tempo em que o cliente permanece sem comunicação com o AP durante o processo de *scan*, revelou que, por sofrer processo de desconexão, o *laptop* IBM ThinkPad obteve, em média, quase o dobro do tempo em relação ao celular Galaxy 5. É importante lembrar que, como a rede estava com segurança desabilitada, as amostras de tempo coletadas não incluíram o tempo necessário para autenticação do cliente, que ocorre após a nova associação. Caso a segurança estivesse habilitada, os valores obtidos seriam ainda maiores. Também foi verificada uma maior variância no resultado do IBM ThinkPad, que obteve amostras de tempo com valores entre 1,070654 e 1,849925 ± 0,005 s.

A Figura 39 mostra os gráficos das médias dos intervalos de tempo em que o cliente permanece sem comunicação com o AP para o laptop IBM ThinkPad (coluna da esquerda) e para o celular Galaxy 5 (coluna da direita). No primeiro caso foram coletadas 28 amostras de intervalo de tempo e no segundo, 32. Em ambos os gráficos o erro é dado pelo intervalo de confiança de 95% somado ao erro de 5 ms ocasionado pela utilização do tempo registrado em *pings* enviados com intervalo de 10 ms para a determinação do valor de tempo do início do processo de *scan*. A partir dos resultados, verificamos que o *scan* não é tão prejudicial ao cliente Galaxy 5 quanto ao IBM ThinkPad. No caso do cliente Galaxy 5, dado o pequeno valor obtido, apenas aplicações de tempo real poderiam ser momentaneamente prejudicadas. Já os clientes IBM ThinkPad, dada a maior variância das amostras obtidas, poderiam ser mais prejudicados caso obtivessem valores mais altos de tempo em que permanecem desconectados. Em redes com segurança habilitada, este intervalo seria ainda maior. Os testes apresentados mais adiante na seção 5.2.5 mostram resultados de medições do intervalo de tempo necessário para a realização da autenticação, que é realizado após a associação do cliente em redes com segurança habilitada.

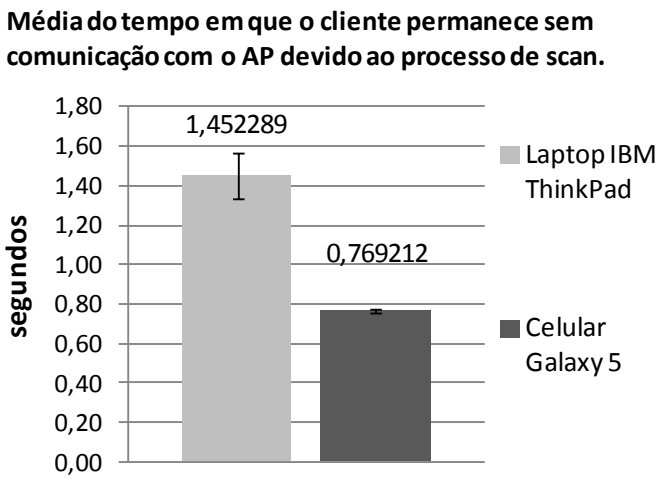


Figura 39. Média do tempo em que o cliente permanece sem comunicação com o AP devido ao processo de *scan*.

Os tempos que determinaram o início e o fim dos intervalos medidos nos testes foram obtidos através dos arquivos de captura sem fio. O início do período em que o cliente permaneceu sem conexão foi determinado pelo tempo registrado para a primeira mensagem ICMP *echo request* (da rajada de perdas ocasionadas pelo *scan*) que não foi repassada para o servidor. Este valor de tempo representa o início do processo de *scan.* O término do período, no caso do *laptop* IBM ThinkPad, foi determinado pelo quadro de *Reassociation Response* enviado do AP ao cliente. Como este cliente sofre desconexão com o AP durante o *scan*, este quadro foi escolhido por representar o momento a partir do qual o cliente se torna apto a trocar informações com o AP novamente, já que é o último quadro enviado do AP ao cliente no período de associação. Já no caso do celular Galaxy 5, como não houve desconexão, o término do período foi delimitado pelo fim do processo de *scan*, a partir do qual o cliente se torna apto a trocar informações com o AP novamente. O fim do *scan* foi determinado pelo primeiro quadro enviado ou recebido pelo AP após o início do *scan*. Em grande parte das vezes este quadro foi um *echo request* enviado pelo cliente e repassado pelo AP ao servidor, ou um *echo response*, que provavelmente estava armazenado na fila de saída do AP para ser enviado ao cliente após o término do *scan*.

O segundo resultado obtido através dos testes foi o tempo de duração do *scan*. A duração do *scan* foi dada pelo intervalo de tempo entre a primeira mensagem ICMP *echo request* que não foi repassada para o servidor, como no cálculo anterior, e o primeiro quadro enviado ou recebido pelo AP após o início do *scan.* No caso do teste realizado com o cliente

Galaxy 5, o valor do intervalo do *scan* é o mesmo valor do intervalo em que o cliente fica sem comunicação com o AP. Já no caso do cliente IBM ThinkPad, o intervalo de *scan* se diferencia do intervalo sem comunicação devido a desconexão do cliente com o AP. Os resultados obtidos para ambos os clientes foram semelhantes, mostrando que o *scan* possui duração aproximada de 770 ms, como mostra a Figura 40. Nos testes com o *laptop* IBM (coluna esquerda) foram coletadas 31 amostras de intervalo de tempo e no teste com o Galaxy 5, foram coletadas 32. O erro é dado pelo intervalo de confiança de 95% somado ao erro de 5 ms ocasionado pela utilização do tempo registrado em *pings* enviados com intervalo de 10 ms para a determinação do valor de tempo do início do processo de *scan*.

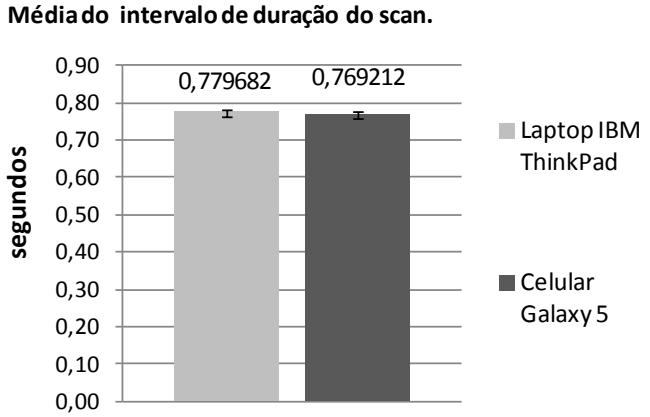


Figura 40. Gráficos do valor médio do intervalo de *scan*.

Após realizar testes quantitativos, foram realizados testes qualitativos, nos quais dois clientes foram conectados ao ponto de acesso e o aplicativo *Skype* [83] foi utilizado para realizar uma chamada de voz em tempo real entre os dois clientes. A seguir o *scan* foi executado no ponto de acesso algumas vezes. Os testes revelaram que, para ambos os clientes, houve um período de silêncio durante o *scan*, porém, ao final do processo, a comunicação voltou ao normal sem a necessidade de realização de nova chamada de voz.

Após a verificação de que diferentes clientes possuem diferentes comportamentos durante o processo de *scan*, e que determinados clientes podem sofrer desconexão, tornando o tempo de interrupção da comunicação maior, métodos para evitar a desconexão foram pesquisados.

Um método que se mostrou eficaz foi o aumento do intervalo de envio entre *beacons* pelo AP. Através de análise do tráfego sem fio capturado, foi observado que, durante o processo de *scan*, o AP, além de não transmitir dados, não envia quadros de gerência,

incluindo quadros de *beacon*, que são transmitidos com determinada frequência (geralmente com intervalo de 100 ms) para anunciar a existência da rede. A partir dai, foi formulada a hipótese de que o cliente realizava a desconexão do AP porque estava deixando de receber um determinado número de *beacons* e, se o intervalo entre *beacons* fosse aumentado, o cliente não se desconectaria porque não deixaria de receber o número de *beacons* suficiente para tomar a decisão de desassociação.

Tendo isto em vista, foi feita uma análise das capturas de tráfego sem fio para determinar o tempo em que o AP permanecia sem enviar *beacons* antes de o cliente realizar a desconexão. Este intervalo foi calculado considerando o último *beacon* enviado antes do início do *scan* e o quadro de desassociação enviado pelo cliente IBM ThinkPad durante a realização do *scan.* A Figura 41 mostra o gráfico da média dos intervalos de tempo em que o cliente permanece sem receber *beacons* do AP (coluna esquerda) antes de realizar desconexão e, para comparação, mostra o tempo médio de duração do *scan* calculado na etapa anterior (coluna da direita). Através dos gráficos, nota-se que os dois intervalos são próximos.

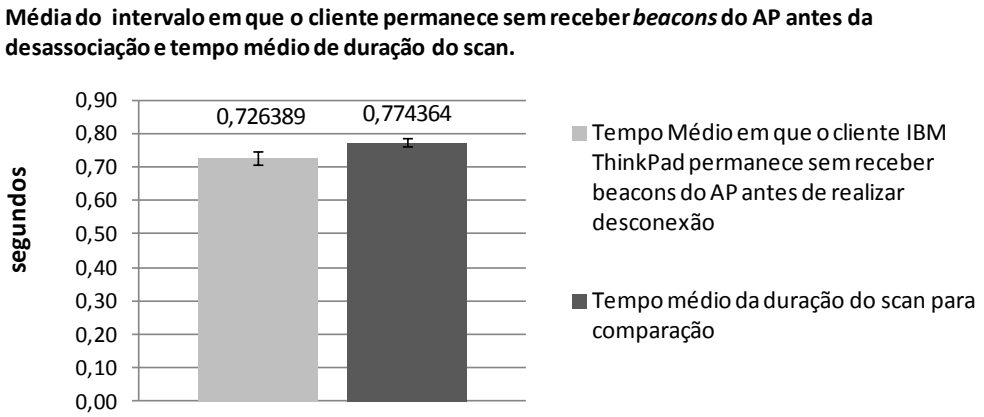


Figura 41. Gráfico do tempo médio em que o cliente permanece sem receber *beacons* do AP antes da desassociação e tempo médio da duração do *scan* para comparação.

Sabendo-se que o intervalo de envio entre *beacons* do AP era de 100 ms, na média, o cliente deixou de receber 7 *beacons* antes de se desconectar. Para que apenas 6 *beacons* fossem perdidos durante o *scan*, e considerando que o intervalo máximo de *scan* encontrado foi de 0,84, o intervalo de *beacon* do AP deveria ser reajustado para, no mínimo, 140 ms. A seguir, os testes foram repetidos com valores de intervalos de *beacons* de 150 ms e, dentre o total de 15 testes, o cliente IBM ThinkPad sofreu desconexão em apenas 3 deles. Utilizando intervalo entre *beacons* de 160 ms, do total de 20 testes, o cliente sofreu desconexão em apenas 1 deles. Por fim, utilizando intervalo entre *beacons* de 170 ms, do total de 30 testes, o

cliente não sofreu desconexão em nenhum deles, portanto, a princípio, este seria o intervalo entre envio de *beacons* indicado para utilização.

5.2.1.6. Conclusões

Através do teste de execução do *scan* pode-se perceber que diferentes dispositivos clientes possuem diferentes comportamentos diante da realização do *scan* (varredura espectral) no ponto de acesso, de forma que alguns perdem a conexão com o AP, enquanto outros não. Dispositivos que perdem conexão com o AP necessitam realizar nova fase de *probe*, ou seja, procurar por APs e escolher um novo AP ao qual irá se associar, além de realizar o processo de associação novamente. Com isso, o tempo em que este cliente permanece sem comunicação se torna maior, durando em média 1,45 segundos em uma rede aberta (com autenticação desabilitada). Já clientes que não sofrem desconexão não são tão prejudicados pelo processo de *scan*. Para estes clientes, o tempo em que ficam sem comunicação é semelhante ao tempo de duração do *scan*, que leva em média 0,77 s para o modelo de ponto de acesso testado.

Testes qualitativos, que envolveram a realização de chamada de voz através do aplicativo *Skype*, mostraram que, apesar da haver desconexão para certos clientes, para nenhum deles a chamada foi finalizada durante a realização do *scan*, e apenas um momento de silêncio foi obervado.

Como solução às desconexões, foi proposta a redução da frequência de emissão de *beacons* pelos pontos de acesso, com base na suposição de que o cliente se desconecta após deixar de receber um determinado número destes quadros. Verificamos que, em média, durante o *scan*¸ com o AP operando com o intervalo entre *beacons* padrão de 100 ms, sete *beacons* eram perdidos. A seguir, reajustamos o intervalo de *beacon* (*beacon interval*) para que um número menor de perdas ocorresse. Após realizar testes com diversos intervalos de *beacons*, verificamos que com o valor de 170 ms o cliente deixou de se desconectar.

5.2.2. Teste 2: Troca de Canal

5.2.2.1. Objetivo

O objetivo deste teste é verificar o quanto o processo de troca de canal do ponto de acesso é prejudicial aos clientes da rede sem fio. Através dos testes podem ser verificados o

tempo em que o cliente permanece sem comunicação com o AP e o tempo necessário para que o AP troque de canal. Os dados obtidos podem ser utilizados para embasar a escolha da frequência com que o algoritmo de seleção de canal deve ser executado pelo controlador.

5.2.2.2. Introdução

O controlador SCIFI é responsável por realizar a alocação automática de canais dos pontos de acesso da rede e, para escolher o melhor conjunto de canais que deve ser utilizado pelos APs, executa o algoritmo de alocação de canais. Após a execução deste algoritmo, a troca de canal dos APs pode ocorrer caso o novo canal escolhido para o AP seja diferente do utilizado anteriormente.

A frequência com que o algoritmo é executado pode ser escolhida pelo administrador da rede através da interface Web de administração do SCIFI. Entretanto, como o processo de troca de canal acarreta a interrupção da transmissão e recepção de dados pelo AP até que sua operação seja reestabelecida em um novo canal, o administrador deve ser cauteloso ao escolher esta frequência, para que os clientes da rede não sejam prejudicados. Com objetivo de embasar esta escolha, este teste de troca de canal foi realizado.

5.2.2.3. Procedimento

O dispositivo cliente deve ser conectado ao ponto de acesso e mensagens ICMP *echo request* devem ser enviadas com intervalo de 10 ms através da ferramenta *ping* [80] com destino ao PC servidor conectado à rede cabeada (Figura 38). Este valor foi escolhido porque é pequeno o suficiente para realizar as medições e pode ser cumprido pela interface sem fio do dispositivo sem causar estouro no *buffer* de saída. O AP deverá encaminhar o tráfego entre cliente e servidor e, no mesmo momento, a captura do tráfego entre cliente e o AP (tráfego sem fio) e entre o AP e o servidor (tráfego na rede cabeada) deve ser realizada. A seguir, o processo de troca de canal do AP deve ser realizado. A Figura 42 mostra a rede de testes montada para a realização do teste 2. Apesar de serem mostrados dois dispositivos clientes, o teste foi realizado com um dispositivo cliente por vez. Opcionalmente, os canais escolhidos para os testes foram 1 e 11.

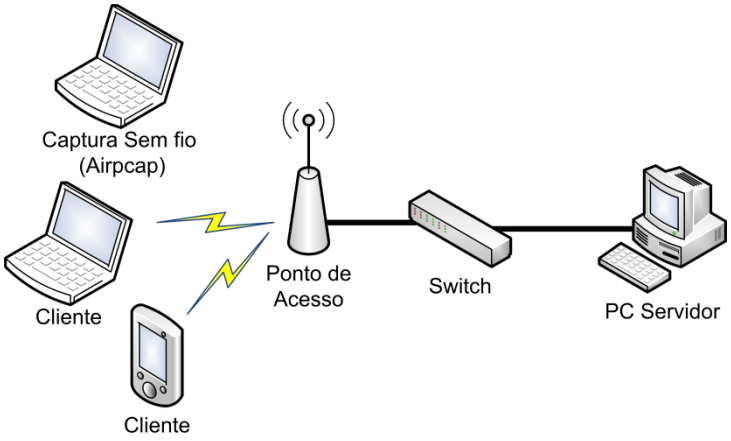


Figura 42 - Teste 2: troca de canal

5.2.2.4. Equipamentos Utilizados

O ponto de acesso utilizado nos testes foi o Ubiquiti Nanostation Loco M [74] com *firmware* OpenWRT [3], versão Backfire 10.03 r20728 e segurança desabilitada. Esta última opção não foi escolhida por motivos específicos. Apenas é importante lembrar que, já que a rede de testes estava aberta, os intervalos de tempo registrados nos testes não incluem o processo de autenticação do cliente, que ocorreria após a associação caso a rede estivesse com segurança habilitada. O *laptop* cliente utilizado foi o IBM ThinkPad com interface de rede sem fio Intel PRO/Wireless 2200BG e *driver* ipw2200. Os testes também foram realizados com um segundo dispositivo cliente para comparação do comportamento de diferentes interfaces sem fio, que foi o celular Samsung Galaxy 5 GT-I5500 [81] com interface sem fio baseada no *chipset* Atheros AR6003 e *driver* AR6k. A captura de quadros sem fio foi realizada através da interface Airpcap Nx [82], que é uma interface própria para realizações de capturas sem fio e, portanto, é capaz de capturar mais quadros em relação a uma interface comum.

5.2.2.5. Resultados

Os testes realizados com os clientes Samsung Galaxy 5 e IBM ThinkPad mostraram comportamentos diferentes para cada interface sem fio. Em ambos os casos, o AP, ao iniciar o processo de troca de canal, envia um quadro de desautenticação (*deauthentication*) para todos os seus clientes (*broadcast*) e, após realizar a troca de canal, envia, em seu novo canal de operação, outro quadro de desautenticação (*deauthentication*) em *broadcast.* Este quadro

possui funcionalidade de desautenticar o cliente e, como a autenticação é necessária para que haja a comunicação entre o cliente e o AP, o efeito destes quadros é a finalização da associação entre o cliente que o recebe e o AP.

No caso do cliente Galaxy 5, quando o primeiro quadro de desautenticação é recebido, sua interface sem fio para de enviar mensagens ICMP *echo request* e envia quadros de *probe request* para o AP em teste. O AP envia *ACKs* para estes quadros, entretanto, não envia *probe response*, provavelmente porque o processo de troca de canal já se iniciou. A seguir, o cliente tenta se autenticar novamente ao AP, enviando um quadro de autenticação (*authentication*), entretanto, da mesma forma como ocorreu com os *probe requests*, o AP envia *ACK* para este quadro, porém não envia a resposta da autenticação (*authentication response*). Após o processo de troca de canal do AP, o cliente procura um novo AP para se associar enviando quadros de *probe request* em *broadcast* e, após receber *probe responses* de alguns APs, escolhe se associar ao AP em teste novamente. No processo de associação, quadros de autenticação e associação são trocados entre o cliente e o AP e, a seguir, o cliente volta a enviar e receber tráfego ICMP normalmente.

Já no caso do cliente IBM ThinkPad, quando o primeiro quadro de desautenticação é recebido, sua interface continua enviando mensagens ICMP *echo request.* O AP envia *ACKs* para algumas dessas mensagens, porém elas não são repassadas ao servidor, já que o processo de troca de canal já se iniciou. A seguir, o AP para de enviar *ACKs* e o cliente realiza retransmissão destas mensagens. Após algum tempo, o cliente se desassocia do AP enviando quadros de desassociação (*disassociate*) e, a partir de então, procura por pontos de acesso para associação enviando quadros *probe request* em *broadcast*. Durante esta etapa em que o cliente procura por novos APs, o AP em teste termina seu processo de troca de canal e envia o quadro de desautenticação (*deauthentication*) em seu novo canal de operação. A seguir, ele responde ao cliente enviando quadros de *probe response*. Por fim, o cliente se associa novamente ao AP trocando quadros de autenticação e associação e, a seguir, volta a enviar e receber tráfego ICMP normalmente.

A partir dos testes realizados, foram obtidos dois resultados principais. O primeiro deles buscou avaliar o tempo em que o cliente permanece sem comunicação com o ponto de acesso devido ao processo de troca de canal realizado pelo AP e o segundo avaliou o intervalo de tempo necessário para que o AP troque de canal.

Como foi descrito anteriormente, nos testes realizados tanto com o cliente IBM ThinkPad quanto com o celular Galaxy 5, houve desconexão entre o cliente e o AP durante a

troca de canal. Por este motivo, os resultados mostraram que o período em que o cliente permanece sem comunicação com o AP é por volta de duas vezes mais extenso do que o intervalo de tempo que o AP leva para realizar a troca de canal. Isto ocorre porque, antes de realizar a nova associação, o cliente realiza um processo de busca por novos APs (fase de *probe*) e, além disso, em certos casos o AP pode não responder de imediato às requisições de associação do cliente, tornando o processo de associação ainda mais lento.

Os tempos que determinaram o início e o fim dos intervalos medidos nos teses foram obtidos através dos arquivos de captura sem fio. Para ambos os clientes, o início do período em que o cliente permaneceu sem conexão foi determinado pelo tempo registrado no primeiro quadro de desautenticação (*deauthentication*) enviado pelo AP, representando o início do processo de troca de canal. O término do período foi determinado pelo quadro de confirmação de associação (A*ssociation Response)* enviado do AP ao cliente. Como os clientes sofrem desconexão do AP durante a troca de canal, este quadro foi escolhido por representar o momento a partir do qual o cliente se torna apto a trocar informações com o AP novamente, já que é o último quadro enviado do AP ao cliente no período de associação.

A Figura 43 mostra os gráficos das médias do tempo em que os clientes permaneceram sem comunicação com o AP. A coluna da esquerda representa a média das 30 amostras coletadas nos testes com o cliente IBM ThinkPad, e a coluna da direita representa a média das 33 amostras coletadas para o cliente Galaxy 5. O erro é dado pelo intervalo de confiança de 95%. Ambos os testes apresentaram grandes variações das amostras coletadas, o que se pode perceber pelo grande intervalo de erro obtido. Analisando-se os dados da captura sem fio, pode-se verificar que este fato se deve à variação no tempo de resposta do AP às requisições de autenticação do cliente. Nos casos em que os intervalos foram maiores, o AP não respondeu de imediato a estas requisições, tornando necessário que o cliente realizasse novas tentativas. Em um caso extremo, o intervalo obtido para o *laptop* IBM ThinkPad foi de 10,02 segundos.

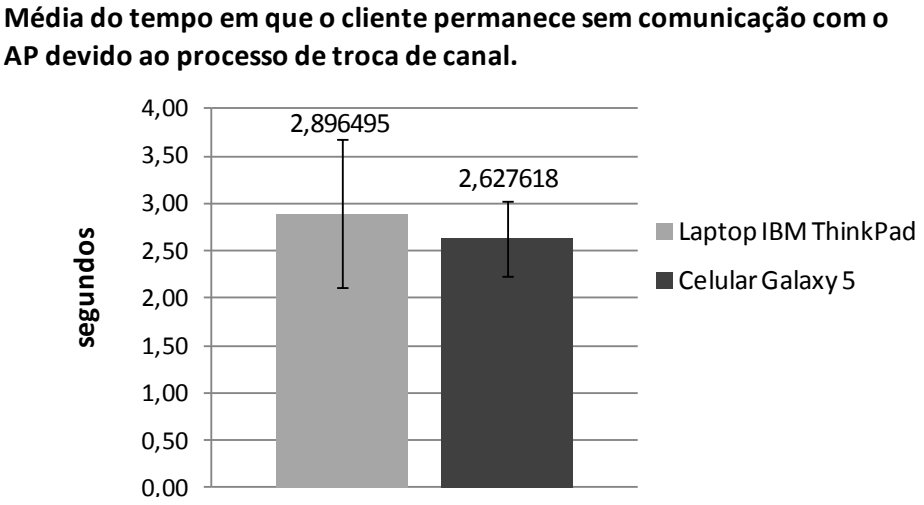
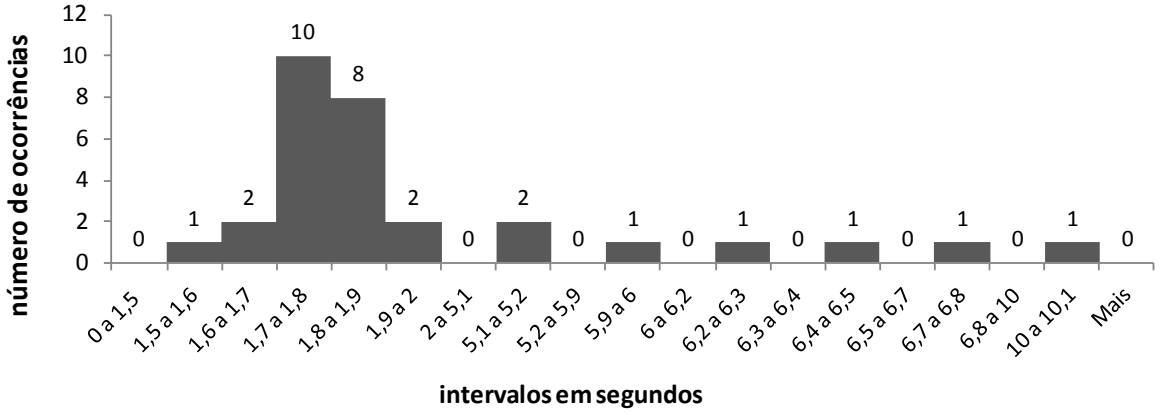
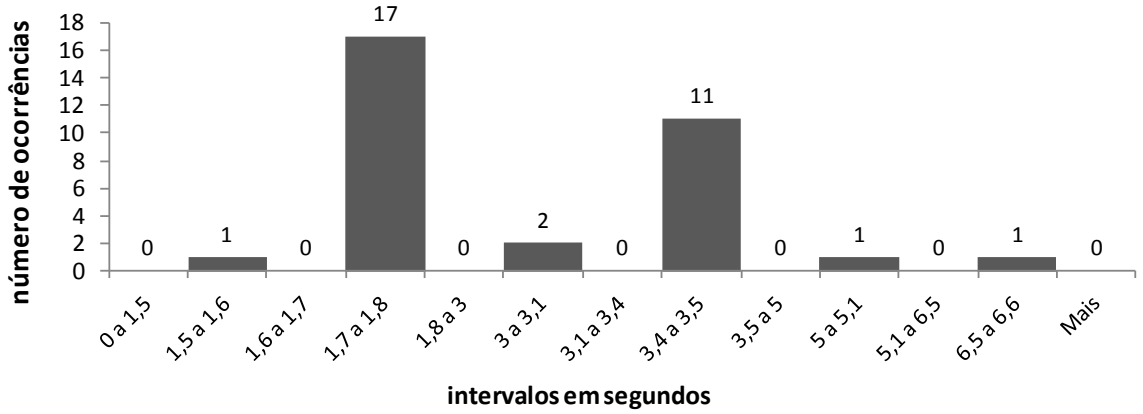


Figura 43. Média do tempo em que o cliente permanece sem comunicação com o AP devido ao processo de troca de canal.

Analisando-se os resultados mais profundamente, podemos verificar que grande concentração das amostras obtidas possuem intervalo entre 1,5 a 2 segundos, o que pode ser visto na Figura 44. Esta figura mostra os histogramas dos intervalos de tempo obtidos no teste para o *laptop* IBM ThinkPad (gráfico superior) e para o celular Galaxy 5 (gráfico inferior). No caso do *laptop* IBM, das 30 amostras, 23 estão localizadas neste intervalo, o que representa 76,6 % das amostras. Já no caso do celular Galaxy 5, das 33 amostras, 18 estão localizadas neste intervalo, representando 54,54% do total de amostras. Para este cliente também percebe-se uma grande concentração de amostras com intervalos entre 3,4 a 3,5 segundos, representando 33,33% do total de amostras.



a) Histograma dos intervalos de tempo em que o cliente IBM Thinkpad permanece sem comunicação com o AP devido a troca de canal.



b) Histograma dos intervalos de tempo em que o cliente Galaxy 5 permanece sem comunicação com o AP devido a troca de canal.

Figura 44. Histograma dos intervalos de tempo em que os clientes IBM ThinkPad (a) e Galaxy 5 (b) permanecem sem comunicação como AP devido a troca de canal.

O segundo resultado obtido através destes testes foi o intervalo de tempo necessário para que o AP troque de canal. O início do processo de troca de canal foi determinado pelo tempo registrado no primeiro quadro de desautenticação enviado pelo AP, e o término do período foi determinado pelo segundo quadro de desautenticação enviado pelo AP em seu novo canal de operação.

A Figura 45 mostra os gráficos das médias dos intervalos para troca de canal obtidos através dos testes realizados com os clientes IBM ThinkPad (coluna da esquerda) e Galaxy 5 (coluna da direita). No primeiro caso foram coletadas 30 amostras de intervalo de tempo e no segundo, 40 amostras. Em todos os casos o erro é dado pelo intervalo de confiança de 95%. Os resultados obtidos com ambos os clientes foram semelhantes, mostrando que o processo de

troca de canal possui duração aproximada de 940 ms.

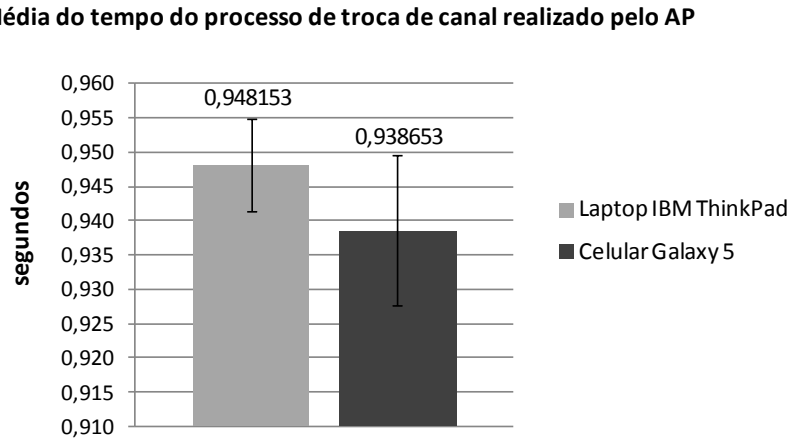


Figura 45. Média do processo de troca de canal obtido nos testes realizados com clientes IBM ThinkPad e Galaxy 5.

Após realizar testes quantitativos, foram realizados testes qualitativos, nos quais os clientes foram conectados ao ponto de acesso e o aplicativo *Skype* [83] foi utilizado para realizar uma chamada de voz em tempo real entre cada cliente e um dispositivo localizado em outra rede. A seguir, o processo de troca de canal foi executado no ponto de acesso algumas vezes. Os testes revelaram que, para ambos os clientes, houve um período de silêncio durante a troca de canal do AP, porém, ao final do processo, a comunicação voltou ao normal sem a necessidade de realização de nova chamada de voz.

Durante a realização dos testes, também foi observado que é muito comum a ocorrência da reinicialização do ponto de acesso durante a troca de canal, após a realização deste processo muitas vezes consecutivas. O problema não foi pesquisado mais a fundo para que o motivo fosse encontrado.

5.2.2.6. Conclusões

Através do teste de troca de canal, percebemos que os dispositivos clientes sofrem desconexão e necessitam realizar nova conexão após o processo. Apesar de a troca de canal do AP durar em média 0,94 segundos, devido à desconexão e a necessidade de realização de nova fase de *probe*, ou seja, pesquisa por novos APs, os clientes permaneceram em média 2,7 segundos sem conexão, em uma rede aberta (com autenticação desativada).

Após realizar testes com dois tipos de dispositivos, verificamos diferentes comportamentos de suas interfaces sem fio, como foi o caso da interpretação do quadro de desautenticação que é enviado pelo AP no início do processo de troca de canal. Os testes

mostram que o cliente IBM ThinkPad ignora estes quadros, enquanto o Galaxy 5 não. Apesar das diferenças, os intervalos em que o cliente permanece sem comunicação com o AP não variaram muito de um cliente para o outro, durando na média, 2,89 segundos para o cliente IBM ThinkPad e 2,62 segundos para o Galaxy 5.

Os testes qualitativos, que envolveram a realização de chamada de voz através do aplicativo *Skype*, mostraram que, apesar da haver desconexão dos clientes, para nenhum deles a chamada foi finalizada durante a realização da troca de canal, e apenas um momento de silêncio foi obervado.

5.2.3. Teste 3: Duração da execução das tarefas de controle

5.2.3.1. Objetivo

O objetivo deste teste é verificar a relação do tempo de execução da coleta de dados e dos algoritmos de seleção de canal e controle de potência com o número de APs controlados. Estes resultados poderão embasar a escolha do número (ou intervalo de números) ideal de pontos de acesso por região de controle do SCIFI.

5.2.3.2. Introdução

As principais funções do controlador SCIFI são determinar, através da utilização de seus algoritmos de seleção de canal e controle de potência, os canais e potências que serão utilizados pelos pontos de acesso da uma rede controlada. Antes da execução dos algoritmos, é necessário que informações de varredura espectral (*scan*) e número de clientes associados aos pontos de acesso (*station dump*) sejam coletadas diretamente de cada um deles para que o controlador central possa definir os canais e potências a serem utilizados. Após executados os algoritmos, o controlador necessita se conectar novamente aos pontos de acesso para configurar fisicamente estes parâmetros. Na versão atual do sistema, a comunicação entre controlador e pontos de acesso é realizada através de SSH (*Secure Shell*) [66] e dados são coletados via SCP (*Secure Copy Protocol*). Conforme o número de APs controlados aumenta, o intervalo de tempo necessário para a execução das tarefas de *scan*, *station dump* e execução dos algoritmos também aumentam.

Buscando a escalabilidade do SCIFI, o sistema de regiões de controle foi criado, no qual pontos de acesso capazes de se interferir são agrupados em uma mesma região e, para cada região, os algoritmos são executados de forma independente, sem considerar os pontos

de acesso pertencentes a outras regiões. Desta forma, as coletas de dados e os algoritmos podem ser executados paralelamente em cada região, tornando o sistema escalável. Entretanto, uma região pode se tornar extensa e, buscando avaliar quantos pontos de acesso são indicados para operar em uma mesma região sem causar atrasos excessivos na execução das funções do controlador, os testes aqui apresentados foram executados. Os resultados esperados são o intervalo necessário para a execução das tarefas de *scan*, *station dump* e algoritmos em função do número de pontos de acesso da rede, e uma estimativa do número máximo de pontos de acesso que deve ser utilizado por região de controle.

5.2.3.3. Procedimento

Através da interface de controle Web do SCIFI comandos devem ser enviados ao controlador ordenando a coleta de dados de *scan*, *station dump*, e execução dos algoritmos de seleção de canais e controle de potência. Através do arquivo de *log* do controlador, os tempos inicial e final de cada uma destas etapas devem ser verificados. O processo deve ser repetido para diferentes números de pontos de acesso operando em uma mesma região.

5.2.3.4. Equipamentos Utilizados

Os testes foram realizados na rede piloto do SCIFI montada na UFF, composta por 22 pontos de acesso da marca Ubiquiti [84], distribuídos pela UFF e interligados por diversos *switches*. Três modelos distintos de pontos de acesso operando com o *firmware* OpenWRT [3] compõe esta rede, que são:

- Nanostation Loco M2 [74], com OpenWRT versão Backfire 10.03, r20728;
- Picostation M2 [74], com OpenWRT versão ATTITUDE ADJUSTMENT (bleeding edge, r28314);
- Bullet M2 [74], com OpenWRT versão Backfire 10.03, r20728;

Os comandos de execução das funções do SCIFI foram enviados através da interface de controle Web mostrada na Figura 46.

Figura 46. Execução de comandos do SCIFI via interface Web

Os resultados foram coletados a partir dos arquivos de *log* do controlador, que registram o momento em que cada função se inicia e termina, como mostra a Figura 47.

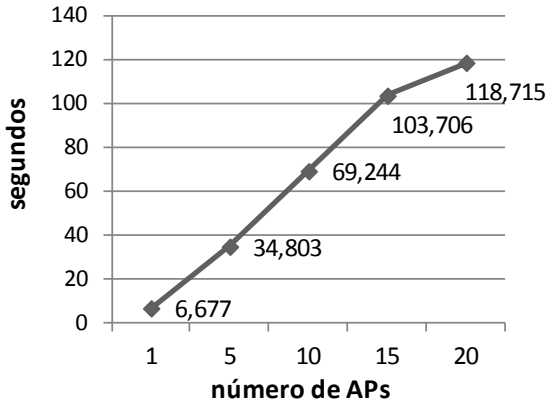
```
controlador@controlador-SciFi:/etc/Controlador$ tail -f Java_Engenharia_2012-08-23.log
INFO - Station Dump started at: 11:08:50.578
INFO - Station Dump ended at: 11:08:58.467
INFO - Scan started at: 11:08:58.467
INFO - Scan ended at: 11:10:46.833 for 16 APs
INFO - Station Dump started at: 11:10:46.833
INFO - Station Dump ended at: 11:11:02.568
INFO - Station Dump started at: 11:11:32.567
INFO - Station Dump ended at: 11:11:47.453
INFO - Station Dump started at: 11:12:17.453
INFO - Station Dump ended at: 11:12:25.259
```

Figura 47. Log do controlador que informa o início e término das funções executadas.

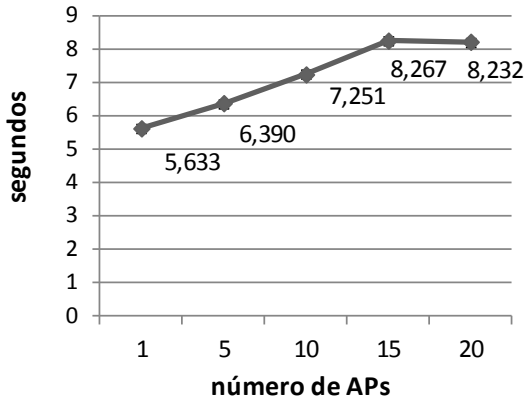
5.2.3.5. Resultados

Após a realização dos testes, os intervalos para execução dos algoritmos e coleta de dados de *scan* e *station dump* foram obtidos para a rede operando com 1, 5, 10, 15 e 20 pontos de acesso, respectivamente, todos sob uma mesma região de controle. Cada função foi executada 10 vezes para cada conjunto de APs, gerando 10 amostras de intervalo tempo. A

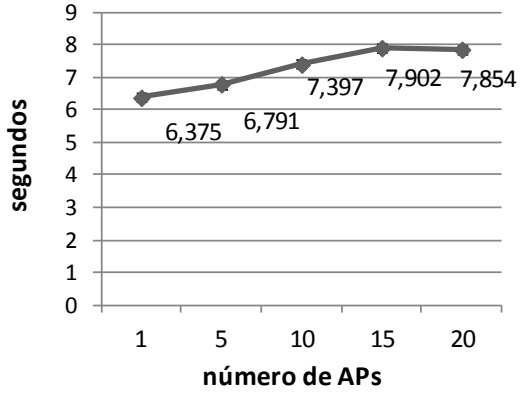
Figura 48 mostra os gráficos das médias dos intervalos obtidos em função do número de APs para a coleta de dados de *scan* (a), coleta de dados de *station dump* (b), execução do algoritmo de seleção de canal (c) e execução do algoritmo de controle de potência (d). Nestes gráficos, o erro foi dado pelo intervalo de confiança de 95%, entretanto, como em todos os casos o erro foi muito pequeno (inferior a 10^{-5}), a barra não pode ser visualizada.



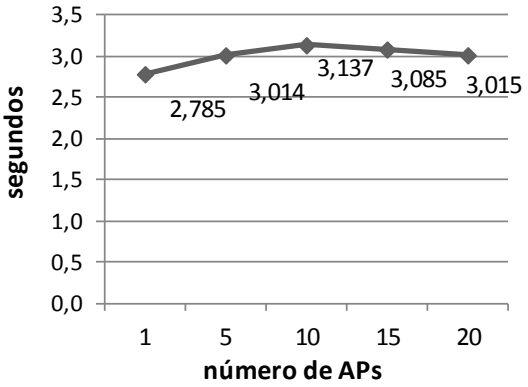
a) Tempo necessário para executar a coleta de dados de *scan* em função do número de pontos de acesso da rede.



b) Tempo necessário para executar a coleta de dados de *station dump* em função do número de pontos de acesso da rede.



c) Tempo necessário para executar o algoritmo de seleção de canais e reconfigurar os APs em função do número de pontos de acesso da rede.



d) Tempo necessário para executar o algoritmo de controle de potência e reconfigurar os APs em função do número de pontos de acesso da rede.

Figura 48. Duração das tarefas de controle do SCIFI em função do número de APs

Na Figura 48, podemos observar uma certa linearidade na relação entre o intervalo de tempo necessário para execução das funções e o número de pontos de acesso para os itens a,b e c. Dentre eles, observamos que o que possui maior crescimento é o referente ao processo de *scan* (a), que alcançou duração de 118,7 segundos para a rede operando com 20 APs. Isso pode ser explicado pelo fato de esta coleta ser realizada de forma sequencial em todos os APs. A coleta sequencial possibilita que, enquanto um AP realiza a varredura, os outros

permaneçam em operação para que possam ser detectados através de seus *beacons* enviados. Já as outras funções de coleta e configuração de parâmetros, executadas pelo *station dump* (b) e algoritmos (c e d), respectivamente, ocorrem de forma paralela em todos os pontos de acesso, ocasionando menores intervalos de tempo. Por exemplo, o *station dump* obteve duração de 8,2 segundos para 20 APs.

O intervalo obtido para a execução dos algoritmos (itens c e d da Figura 48) inclui o tempo necessário para a configuração física dos parâmetros nos pontos de acesso, que, como foi dito, é realizada de forma paralela. A partir dos gráficos, notamos maiores intervalos para o algoritmo de seleção de canal, o que pode ser explicado pela maior necessidade de computação. Entretanto, por este algoritmo ser uma heurística que busca encontrar um conjunto de canais próximo do ótimo em tempo viável, o intervalo obtido ainda se manteve pequeno, atingindo o valor de 7,8 segundos para 20 APs. Já o algoritmo de controle de potência não foi tão influenciado pelo número de APs, e obteve intervalos entre 2,7 e 3,0 segundos para 1 e 20 APs respectivamente.

A partir dos resultados, podemos verificar que o intervalo para coleta de dados de *scan* é o que mais cresce com o aumento do número de pontos de acesso, portanto, esta operação é a que traz maior preocupação em termos de escalabilidade do sistema. Como deve ser executada anteriormente aos algoritmos, estes devem definir sua frequência de execução.

Observando o gráfico da Figura 48 (a), podemos fazer uma estimativa da duração do *scan* para "N" pontos de acesso. Como os intervalos aumentam com certa linearidade em relação ao número de APs, uma linha de tendências linear foi traçada utilizando-se o método dos mínimos quadrados como mostra a Figura 49. Podemos observar que o valor de R-quadrado é 0,9828, que é um bom ajuste de linha para os dados. A equação obtida foi:

$$y = 6{,}0873x + 4{,}5388$$

Equação 2. Duração da coleta de dados de *scan* em relação ao número de APs

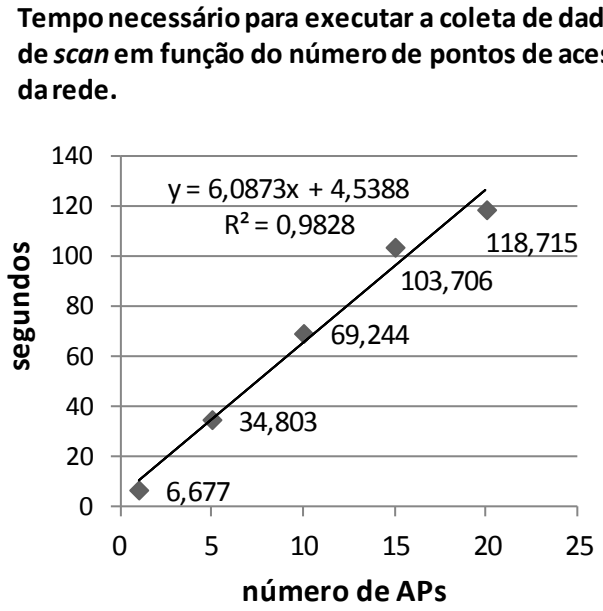


Figura 49. Gráfico do intervalo necessário para execução da coleta de dados de *scan* em função do número de APs controlados com linha de tendência.

O algoritmo de seleção de canal, atualmente, por padrão da rede piloto, é executado 4 vezes ao dia. Esta baixa frequência foi escolhida porque a alteração de canais causa desconexão dos clientes podendo prejudicá-los, o que não é desejado. Além disso, acreditamos que em um ambiente, a inserção/desligamento de novos pontos de acesso não ocorre com grande frequência. Portanto, a realização da escolha do canal 4 vezes ao dia parece suficiente.

Já o algoritmo de controle de potência é realizado por etapas, ou seja, a cada vez que é executado, define se o AP deve aumentar ou reduzir sua potência em um degrau dentre as potências definidas pelo administrador. Desta forma, sua convergência é mais lenta em relação ao algoritmo de seleção de canais, que define de uma só vez os canais a serem utilizados pelos APs. Tendo isto em vista, o algoritmo de controle de potência necessita ser executado com maior frequência para que tenha convergência mais rápida e, portanto, ele irá definir a frequência da coleta de dados de *scan.* Além disso, o fato de o *scan* também causar períodos de desconectividade aos clientes da rede também deve ser levado em conta no momento da definição de sua frequência de execução.

Por padrão na rede piloto, a execução do controle de potência ocorre a cada 600 segundos e o *scan*, a cada 500 segundos em duas regiões operando com 16 e 6 APs respectivamente. É importante notar que duas tarefas de controle não podem ser executadas

simultaneamente e caso estejam agendadas, devem aguardar a liberação dos pontos de acesso para que sejam executadas.

Através da Equação 2, podemos estimar que, para 16 APs, a coleta de dados de *scan* dura em torno de 101,93 segundos. Este valor de atraso não atrapalha o funcionamento da rede piloto, dado que o intervalo entre execuções do *scan* é bem maior do que este valor (500 s). Para uma boa operação do sistema, o número máximo de APs operando em uma região não deve ocasionar períodos de *scan* que se aproximem do intervalo agendado. Por exemplo, para que a coleta de *scan* causasse atraso em torno de 250 segundos, que é um intervalo máximo aceitável considerando-se as frequências de execução padrão e as eventuais execuções de outras funções entre as de coleta de *scan*, o valor estimado de APs por região seria 40, com base na equação da Figura 49. Desta forma, este é o valor máximo de pontos de acesso indicado por região de controle, dados os intervalos padrão especificados.

5.2.3.6. Conclusões

Os testes mostraram que no geral, as funções executadas pelo controlador SCIFI possuem intervalo de duração diretamente proporcional ao número de APs que operam em uma determinada região de controle. Dentre os intervalos obtidos, verificamos que o relativo à coleta de dados de *scan* é o que mais cresce com o aumento do número de APs e, portanto, esta operação é a que traz mais preocupações em termos de escalabilidade do sistema. Os intervalos obtidos para as demais operações crescem com taxas muito menores.

Analisando-se as amostras obtidas para 1, 5, 10 , 15 e 20 APs, e traçando a linha de tendência utilizando o método dos mínimos quadrados, obtemos a Equação 2, que estima o intervalo de tempo (y) dado o número de APs (x) para execução da coleta de dados de *scan*. Verificamos que a frequência desta operação deve ser escolhida com base na frequência de execução do algoritmo de controle de potência, tendo em vista que este algoritmo é mais executado do que o de seleção de canais.

Dado que, por padrão, o algoritmo de controle de potência é executado com intervalo de 600 segundos e o *scan* é executado com intervalo de 500 segundos, o número máximo de APs estimado, de acordo com a equação, para operar em uma região de controle é 40. Este valor é referente a um intervalo máximo de 250 segundos para execução da operação, que foi estimado considerando-se eventuais execuções de outras funções do controlador entre realizações de *scan* e eventuais atrasos durante o *scan.*

No caso da utilização de outras frequências de execução do algoritmo de controle de potência e *scan*, um novo número de APs deve ser estimado. Porém, o fato de a realização do *scan* causar momentos de falta de conectividade aos clientes da rede deve ser considerado, de forma que intervalos demasiadamente curtos não sejam escolhidos. A Figura 50 mostra um gráfico do número máximo de APs estimado por região de controle para diversos intervalos de execução da tarefa de scan. O número máximo de APs foi estimado de forma que o intervalo de duração do *scan* para este número não ultrapassasse 50% do valor do intervalo entre *scans*.

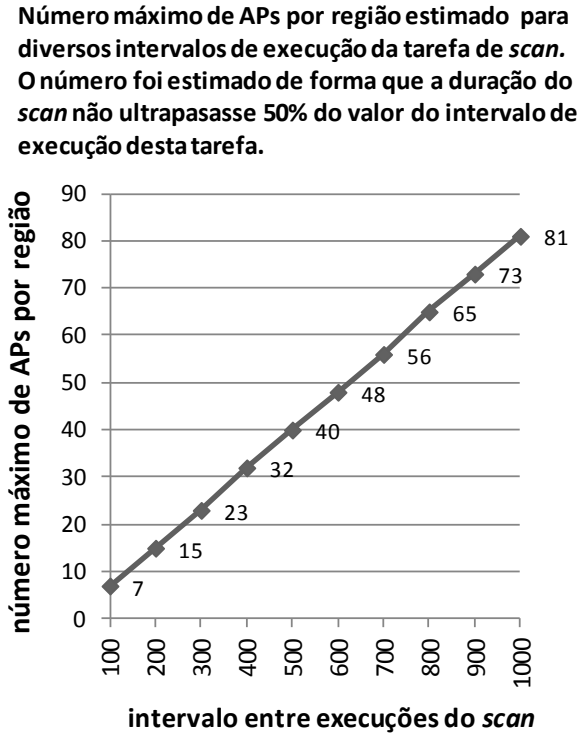


Figura 50. Gráfico do número máximo de APs por região estimado para diversos intervalos de execução da tarefa de *scan*.

5.2.4. Teste 4: Overhead do controlador na rede cabeada

5.2.4.1. Objetivo

O objetivo deste teste é verificar qual o *overhead* inserido pelos pacotes de gerência do controlador na rede cabeada que interliga o controlador aos pontos de acesso da rede. O resultado esperado é a taxa, em bytes por segundos, de tráfego de gerência trocado entre um AP e controlador e a realização de estimativa da taxa total em função do número de APs e frequência de execução das tarefas de controle.

5.2.4.2. Introdução

O controlador SCIFI tem como principais funções determinar, através da utilização de seus algoritmos de seleção de canal e controle de potência, os canais e potências que serão utilizados pelos pontos de acesso da rede controlada. Para tanto, antes da execução dos algoritmos, é necessário que informações de varredura espectral (*scan*) e número de clientes associados aos APs (*station dump*) sejam coletadas diretamente de cada AP, para que o controlador central possa escolher os canais e potências a serem utilizados. Após executados os algoritmos, o controlador necessita se conectar novamente aos APs para configurar fisicamente estes parâmetros. Além de configurar os APs, o controlador também realiza o *check de sanidade*, funcionalidade através da qual ele verifica se as configurações dos pontos de acesso estão de acordo com as últimas definidas por seus algoritmos.

Toda a comunicação entre controlador e pontos de acesso é realizada através de SSH (*Secure Shell*) [66] e dados são coletados via SCP (*Secure Copy Protocol*) . Através do SSH o controlador acessa remotamente os APs e executa *scripts* de coleta de dados ou configuração de parâmetros. No caso da coleta de dados, os *scripts* geram arquivos que são armazenados no ponto de acesso e posteriormente transferidos para o controlador por SCP. As informações trafegadas pela rede cabeada que são apenas destinadas ao controle do sistema são chamadas de tráfego de *Overhead* .

Os testes aqui apresentados buscam estimar a taxa do tráfego de Overhead (bytes/segundos) enviado pelo controlador em função do número dos pontos de acesso na rede e em função da frequência de execução das atividades de controle.

5.2.4.3. Procedimento

Através da interface de controle web do SCIFI, comandos devem ser enviados ao controlador ordenando a execução das tarefas de controle de forma consecutiva. Estas tarefas são:

- coleta de dados de varredura espectral nos pontos de acesso (*scan);*
- coleta de dados sobre clientes associados (*station dump);*
- execução do algoritmo de seleção de canais;
- execução do algoritmo de controle de potência;
- execução da análise de configuração dos APs (*check de sanidade*);

No mesmo instante, a captura do tráfego deve ser realizada na interface cabeada que interliga o controlador aos pontos de acesso. A seguir, os arquivos de captura devem ser filtrados para que se possa verificar quais quadros relativos às operações de SSH e SCP foram trocados entre o controlador e cada ponto de acesso. Desta forma, será possível obter o número total de bytes trafegados entre o controlador e cada AP para a realização de cada tarefa de controle.

Após obtidos os valores médios de bytes necessários para a execução de cada tarefa de controle para um AP, uma estimativa da taxa total do *Overhead* (bytes/segundos) deve ser realizada em função do número de execuções de cada tarefa no intervalo de um dia e do número de APs que operam na rede.

5.2.4.4. Equipamentos Utilizados

Os testes foram realizados na rede piloto do SCIFI montada na UFF, composta por 22 pontos de acesso da marca Ubiquiti [84], distribuídos pela UFF e interligados por diversos *switches*. Três modelos distintos de pontos de acesso operando com o *firmware* OpenWRT [3] compõe esta rede, que são:

- Nanostation Loco M2 [74], com OpenWRT versão Backfire (10.03, r20728)
- Picostation M2 [74], com OpenWRT versão ATTITUDE ADJUSTMENT (bleeding edge, r28314)
- Bullet M2 [74], com OpenWRT versão Backfire (10.03, r20728)

Os comandos de execução das funções do SCIFI foram enviados através da interface de controle Web mostrada na Figura 46. A interface cabeada utilizada para a comunicação do controlador com os pontos de acesso da rede possui capacidade nominal de transmissão de 1 Gbit por segundo.

5.2.4.5. Resultados

Após a realização dos testes, obtemos a média do número total de bytes necessários para a realização de cada tarefa de controle para um AP, como mostra a Figura 51. Para cada tarefa executada foram coletadas 16 amostras de total de bytes, exceto no caso do Algoritmo de Controle de Potência, no qual 12 amostras foram coletadas. Nesta figura, as barras de erros são dadas pelo intervalo de confiança de 95%.

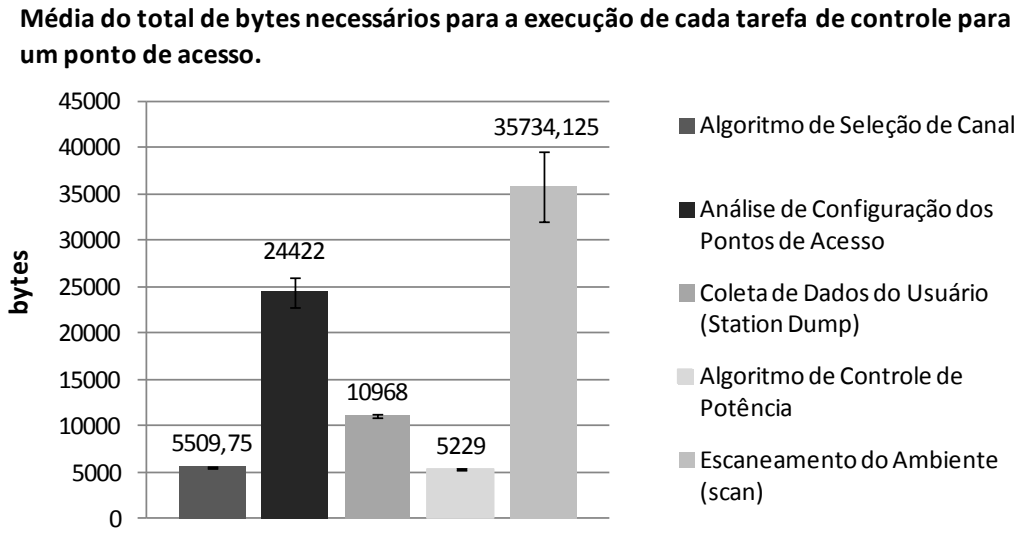


Figura 51. Média do total de bytes necessários para a execução das tarefas de controle na rede operando com 1 ponto de acesso.

Analisando-se os resultados apresentados na Figura 51, nota-se que a varredura do ambiente (*scan)* é a tarefa de controle que necessita de maior número de bytes para ser realizada. Isto pode ser explicado pelo fato de esta tarefa necessitar da transferência de um arquivo contendo todas as informações de *scan* do AP para o controlador. Além disso, conforme a quantidade de APs vizinhos aumenta, este arquivo se torna maior. Portanto é esperado que a barra de erros desta tarefa também seja maior.

Cada tarefa é executada pelo controlador em intervalos de tempo definidos pelo administrador do sistema. Por padrão, a rede piloto do SCIFI opera com os seguintes intervalos de tempo para cada tarefa:

- Intervalo entre a execução de *scans*: 500 segundos;
- Intervalo entre a obtenção de dados sobre os usuários de cada AP (*Station dump*): 30 s;
- Intervalo entre as análises de configurações (*check de sanidade*): 600 Segundos;
- Intervalo entre as execuções do algoritmo de seleção de canal: 21600 Segundos;
- Intervalo entre as execuções do algoritmo de controle de potência: 600 Segundos;

Com base nestes intervalos, sabemos que as tarefas são executadas um determinado número de vezes por dia, que são:

- Execução do *scan*: 172 vezes ao dia;
- Obtenção de dados sobre os usuários de cada AP (*Station dump*): 2880 vezes ao dia;

- Análise de configurações (*check de sanidade*): 144 vezes ao dia;
- Algoritmo de seleção de canal: 4 vezes ao dia;
- Algoritmo de controle de potência: 144 vezes ao dia;

Após verificar o total de bytes necessários para a realização de cada tarefa, e sabendo qual a frequência de execução de cada uma delas por dia, podemos estimar a média do total de bytes necessários para a execução de cada tarefa em um dia para a rede operando com um ponto de acesso:

- Execução do *scan*: 172 x 35734,125 = 6146269.5 Bytes;
- Obtenção de dados sobre os usuários de cada AP (*Station dump*): 2880 x 10968 = 31587840 Bytes;
- Análise de configurações (*check de sanidade*): 144 x 24422 = 3516768 Bytes;
- Algoritmo de seleção de canal: 4 x 5509,75 = 22039 Bytes;
- Algoritmo de controle de potência: 144 x 5229 = 752976 Bytes;

A seguir, dividindo estes resultados pelo número total de segundos em um dia (24x60x60 = 86400 segundos), podemos estimar a taxa média de *overhead* em bytes por segundo necessária para a execução de cada tarefa na rede operando com um AP, como mostra a Figura 52.

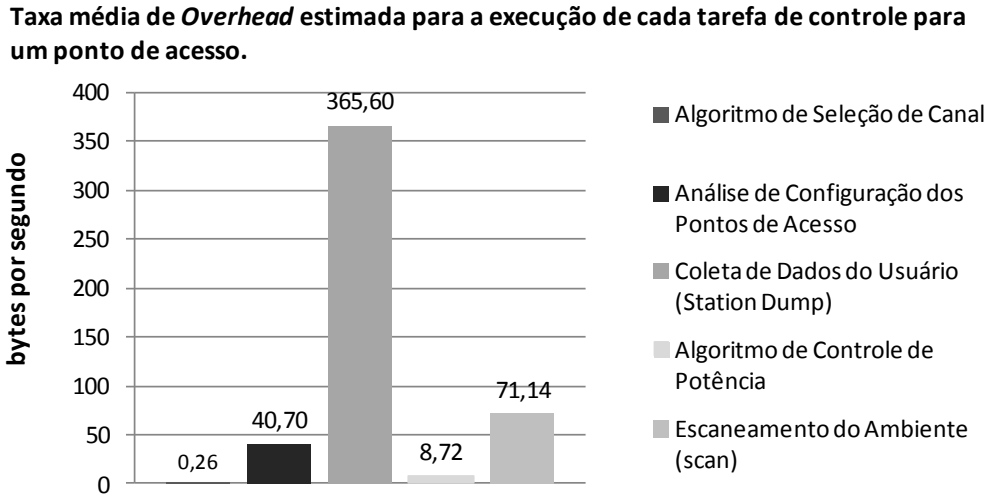


Figura 52. Taxa média de *overhead* estimada para a execução de cada tarefa de controle em uma rede operando com 1 ponto de acesso.

Analisando-se a Figura 52, notamos que a tarefa com maior taxa de *overhead* é a

coleta de dados de usuário (*station dump*). Isto pode ser explicado por sua maior frequência de execução durante o decorrer do dia em relação às outras tarefas.

Por fim, somando-se a taxa obtida para cada tarefa podemos estimar a taxa total de *overhead* do controlador para uma rede operando com um AP:

Taxa total de *overhead* para a rede operando com um AP: **486,4108 bytes/ segundo** ou **3,8 kbps**.

Esta taxa, que é parte trafegada no sentido *download* e parte tarfegada no sentido *upload*, é baixa comparada com a capacidade total do enlace cabeado que interliga o controlador aos pontos de acesso, que possui valor de 1Gbps, ou 134.217.728 bytes/segundo.

Tendo em vista que, conforme adicionamos pontos de acesso à rede, cada tarefa de controle deve ser executada para cada AP, para estimar a taxa total de *overhead* do controlador em função do número de pontos de acesso basta realizar o seguinte cálculo:

Taxa total de *overhead* para a rede operando com "N" APs: = **N x 486,4108 (bytes/ segundo)** , onde N é o número total de APs.

Equação 3. Taxa total de *overhead* do controlador em relação ao número de APs

Com base nesta fórmula a taxa de overhead da rede piloto do SCIFI, que possui 22 pontos de acesso seria: 10.701,04 bytes /segundo ou 10,45 kilobytes / segundo, ou ainda 83,60Kbps.

5.2.4.6. Conclusões

Os testes mostraram que as diferentes tarefas de controle necessitam de variados valores totais de bytes para sua execução. Dentre elas, a que necessita de maior número de bytes é a de *scan*, alcançando valor médio de 35.734 bytes. Entretanto, ao avaliar a frequência com que cada tarefa é executada no decorrer do dia, verificamos que a execução da coleta de dados de usuários (*station dump*), dada sua alta frequência, é responsável por gerar a maior parte da taxa de *overhead* inserida na rede cabeada pelo controlador, atingindo o valor de 365,60 bytes por segundo para cada ponto de acesso.

Analisando-se a taxa de *overhead* total obtida para um AP (486,4108 bytes/ segundo),

incluindo todas as tarefas de controle, verificamos que esta taxa é baixa em relação a capacidade do enlace cabeado que realiza a comunicação entre o controlador e os APs que possui valor nominal de 134.217.728 bytes/segundo (1Gbps).

A partir da taxa total de *overhead*, e tendo em vista que cada tarefa de controle deve ser executada para cada AP da rede conforme sejam adicionados, a Equação 3 foi formulada para estimar a taxa média de *overhead* do controlador em função do número de APs da rede.

5.2.5. Teste 5: Handoff

5.2.5.1. Objetivo

O objetivo deste teste é verificar se é possível a realização do processo de *handoff* na rede piloto do controlador SCIFI instalada na UFF e, caso seja possível, verificar qual é a duração deste processo.

5.2.5.2. Introdução

A Figura 53 mostra a arquitetura da rede piloto montada para os testes do controlador SCIFI, semelhante a de uma rede infraestruturada. Nesta rede os pontos de acesso operam em modo *bridge*, ou seja, atuam na camada de enlace realizando a transmissão do tráfego entre as interfaces sem fio e cabeada de forma que a rede sem fio se pareça com uma extensão da rede cabeada.

Na Figura 53, cada conjunto formado por um ponto de acesso e seus clientes é conhecido por *Basic Service Set (BSS)*. Quando um BSS não é capaz de fornecer a cobertura desejada, vários pontos de acesso podem ser utilizados buscando extensão da cobertura. A coleção de vários pontos de acesso conectados através de um sistema de distribuição, que no caso é representado pela infraestrutura cabeada, forma um *Extended Service Set (ESS).* Para que o *handoff* na rede fosse possibilitado, algumas configurações foram realizadas no controlador e nos APs:

- O controlador foi configurado para fornecer o serviço de DHCP (*Dynamic Host Configuration Protocol*), possibilitando que, o cliente, ao se reassociar a um novo ponto de acesso, fosse capaz de manter seu endereço de IP;
- Todos os pontos de acesso da rede foram configurados com o mesmo ESSID (*Extended Service Set ID*);
- Todos os pontos de acesso da rede foram configurados com o mesmo método de

segurança. No caso, o método utilizado foi o WPA2 Enterprise, que é baseado no padrão IEEE802.11i [85] e provê autenticação utilizando o padrão IEEE802.1X [86] e o protocolo EAP (*Extensible Authentication Protocol*) [87];

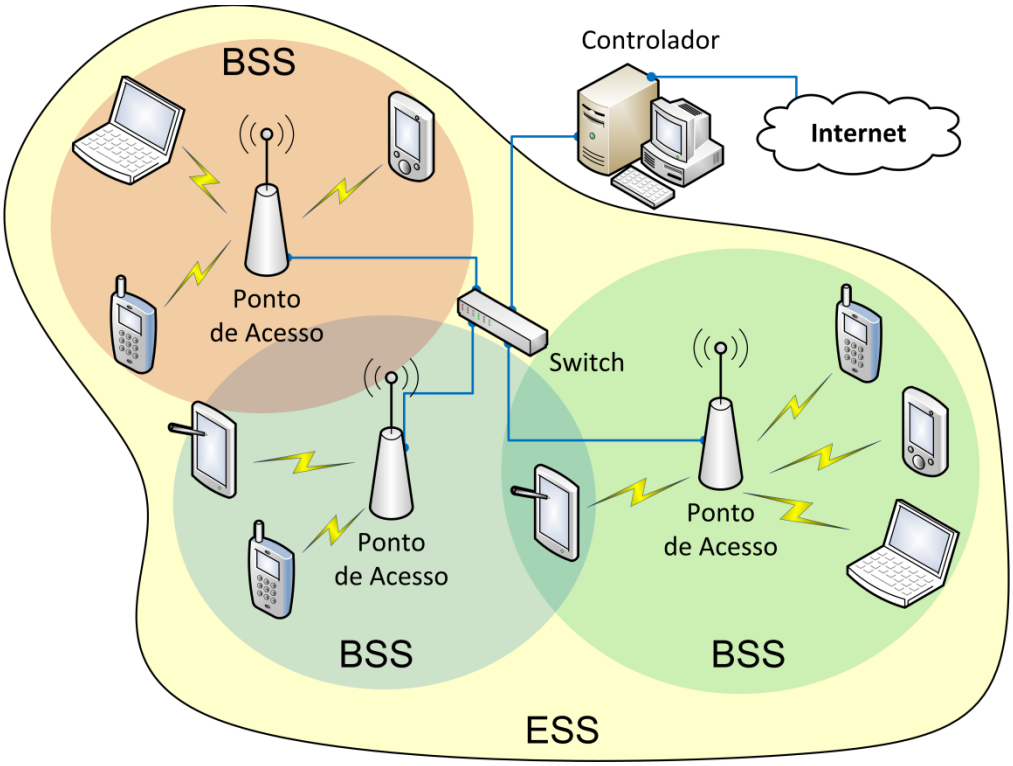


Figura 53. Arquitetura da rede de testes do SCIFI

O processo de *handoff* ocorre quando um cliente percebe que sua comunicação com o AP ao qual está associado está com baixa qualidade. A perda da qualidade pode ser causada, por exemplo, pelo distanciamento do cliente em relação ao ponto de acesso ou pela redução da potência de transmissão do AP. A partir desta constatação, o cliente busca por novos APs ao seu redor que possam fornecer melhor qualidade de comunicação e pertençam ao mesmo ESS (*Extended Service Set*). Este processo não é comandado pelo ponto de acesso, mas sim pelo cliente, e a forma como deve ser realizado não é padronizada, dependendo da interface de rede sem fio. O esperado é que, ao verificar um determinado nível de qualidade baixa de sinal, o cliente procure por outros pontos de acesso e realize o processo de reassociação a um AP que propicie melhor qualidade de sinal. No processo de reassociação, mensagens podem ou não ser trocadas entre os pontos de acesso pertencentes a ESS, entretanto esta questão não será analisada com mais profundidade nos testes aqui apresentados.

5.2.5.3. Procedimento

O dispositivo cliente deve ser conectado a um dos pontos de acesso pertencentes à rede (Figura 54 – AP 1) e mensagens ICMP *echo request* [79] devem ser enviadas com intervalo de 10 ms através da ferramenta *ping* [80] com destino ao PC servidor conectado à rede cabeada. O AP deverá encaminhar o tráfego entre cliente e servidor e, no mesmo momento, a captura do tráfego entre cliente e o AP (tráfego sem fio) deve ser realizada. A seguir, o cliente deve ser locomovido para as proximidades de outro ponto de acesso da rede (Figura 54 - AP 2), de forma que o nível de sinal do primeiro AP se torne baixo e o do segundo se torne alto, forçando o processo de *handoff* da estação. Nos testes, os APs estavam operando no mesmo canal para que o processo de captura de tráfego sem fio fosse facilitado.

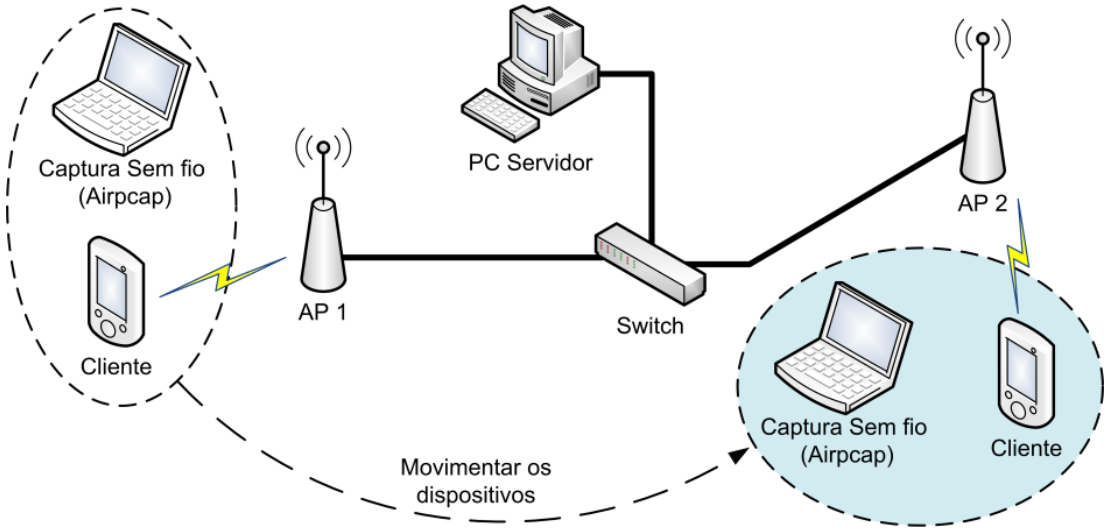


Figura 54. Teste 5: *Handoff*

5.2.5.4. Equipamentos Utilizados

Os testes foram realizados em duas redes distintas. Uma operando com dois pontos de acesso Ubiquiti Nanostation Loco M2 [74] com *firmware* OpenWRT [3] versão Backfire 10.03 r20728 e segurança desabilitada, e outra operando com cinco pontos de acesso Ubiquiti Picostation M2 [74], *firmware* versão Bleeding Edge r28314 e segurança WPA2 Enterprise. Na primeira rede testada, dois dispositivos clientes foram utilizados, o *laptop* IBM ThinkPad com interface de rede sem fio Intel PRO/Wireless 2200BG e *driver* ipw2200 e o celular Samsung Galaxy 5 GT-I5500 com interface sem fio baseada no *chipset* Atheros AR6003 e *driver* AR6k. Na segunda rede, apenas o celular Galaxy foi utilizado para comodidade de deslocamento do cliente, já que o celular é menor e mais leve em relação ao laptop. A captura de quadros sem fio foi realizada através da interface Airpcap Nx [82].

5.2.5.5. Resultados

Ao realizar o teste de *handoff* na rede com segurança desabilitada, foram verificados comportamentos distintos dos clientes (*laptop* IBM e celular Galaxy 5). Após a movimentação do dispositivo para as proximidades de um novo AP, no momento em que o *laptop* IBM verifica que a comunicação com o AP ao qual está associado está com nível de qualidade abaixo do desejado, ele envia quadros *probe request* em *broadcast* procurando por novos APs, com o valor do campo SSID (*service set ID*) igual ao ESSID da rede atual ou igual a "*broadcast"*. Durante o envio desses quadros, a transmissão de dados não é interrompida.

A baixa qualidade na comunicação ocasiona perdas e retransmissões das mensagens ICMP *echo request* que são enviadas pelo cliente. O mesmo ocorre para as mensagens ICMP *echo response* que são enviadas pelo AP. Antes de realizar novas retransmissões, o AP envia quadros *Request to Send* (RTS) para reservar o meio, provavelmente buscando evitar colisões e novas perdas. No *log* da ferramenta *ping,* verificam-se perdas e aumento no atraso de alguns dos *pings*.

Após enviar *probe requests* e receber *probe responses* provenientes dos APs ao seu redor, o cliente se desassocia do ponto de acesso enviando o quadro *Disassociate*. Neste momento, o tráfego de dados é interrompido e, a seguir, o cliente envia novos quadros de *probe request* como anteriormente. Após receber alguns *probe responses*, o cliente escolhe o novo AP ao qual irá se associar e realiza a autenticação trocando quadros *Authentication* com o AP, e, a seguir, finaliza a associação enviando o quadro *Association Request* ao AP, que responde com o quadro *Association Response*. Após concretizada a associação, o cliente volta a trocar tráfego de dados novamente com o AP.

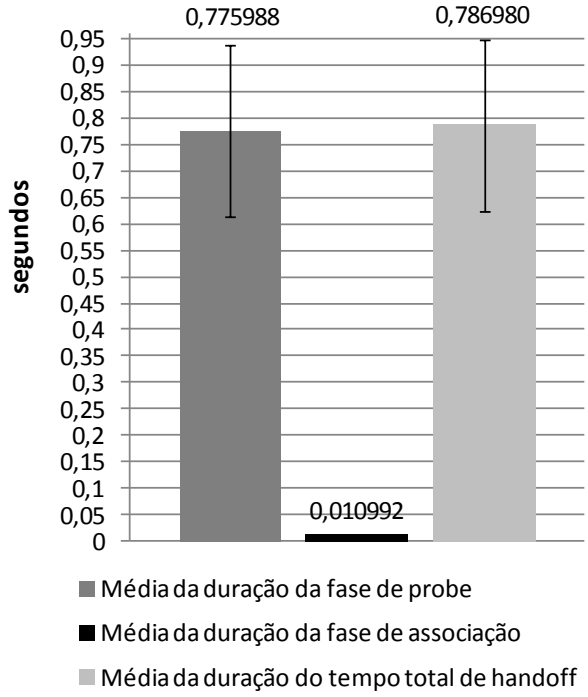
Ao realizar os testes com o cliente Galaxy 5, resultados diferentes foram encontrados. A interface deste dispositivo, ao verificar a redução da qualidade de comunicação com o ponto de acesso ao qual está associada, envia quadros de *probe request* buscando novos APs. Entretanto, estes quadros, na maioria das vezes, não são enviados em *broadcast* como ocorre com o cliente *laptop* IBM, mas apenas enviados para os APs conhecidos pertencentes à ESS. Nestes quadros, o campo SSID é preenchido com o ESSID da rede atual ao qual o cliente está associado. A comunicação de dados não é interrompida nesta etapa.

Após receber *probe responses*, o cliente se desassocia do ponto de acesso enviando quadros de *Disassociate* e *Deauthentication* ao AP. Neste momento, o tráfego de dados é

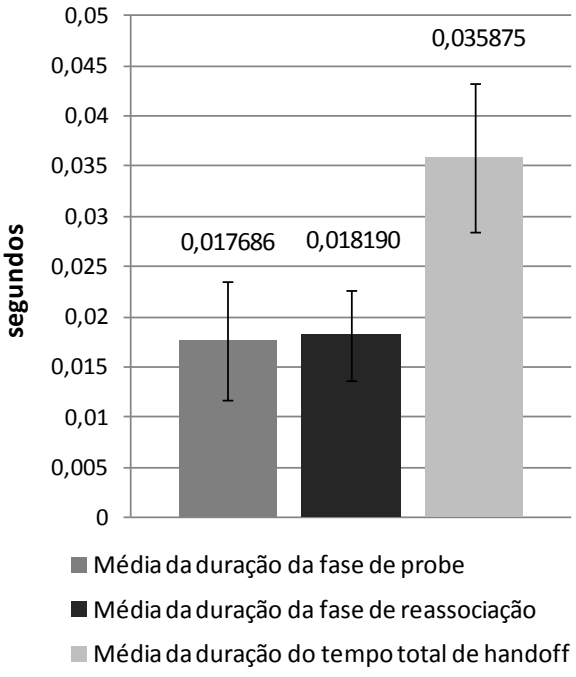
interrompido. A seguir, o cliente envia um quadro de *probe request* apenas para o novo AP escolhido e, caso receba um *ACK*, realiza a autenticação trocando quadros *Authentication* com este AP, e a seguir finaliza a associação enviando o quadro *Reassociation Request* ao AP, que responde com o quadro *Reassociation Response*. Após concretizada a associação, o cliente volta a trocar tráfego de dados novamente com o AP.

Analisando-se o comportamento das duas interfaces, duas diferenças principais podem ser percebidas. A primeira delas revela que o cliente Galaxy 5 realiza reassociação, enquanto o *laptop* IBM realiza uma nova associação. A segunda diferença é relativa à forma como a pesquisa por novos APs (fase de *probe)* é realizada. O cliente Galaxy 5, ao enviar menos quadros de *probe* durante o período em que está desassociado, é capaz de realizar o *handoff* em um intervalo de tempo menor, como mostram os resultados apresentados na Figura 55. Nesta figura, ao lado esquerdo, são apresentadas as médias para os intervalos da fase de *probe*, fase de associação e tempo total do *handoff* obtidos para o cliente *laptop* IBM ThinkPad, e, à direita, são apresentados os resultados para o cliente Celular Galaxy 5. No caso do *laptop* IBM, foram coletadas 29 amostras de intervalos de tempo, enquanto que para o Galaxy 5 foram coletadas 32.

A duração da fase de *probe* foi definida como o intervalo de tempo entre os quadros de desassociação (*Disassociate*) e de autenticação (*Authenticate*), ambos enviados pelo cliente. Já a fase de associação (*laptop* IBM) ou reassociação (Galaxy 5) foi definida pelo intervalo entre os quadros de autenticação (*Authenticate*), enviado pelo cliente, e de resposta de associação (*Association Response*) ou reassociação (*Reassociation Response*), enviada pelo novo AP ao qual o cliente se associou. Em ambos os gráficos, a barra de erros é dada pelo intervalo de confiança de 95%.



a) Média da duração das fases de probe, associação e tempo total de handoff para o cliente Laptop IBM em rede com autenticação desabilitada



b) Média da duração das fases de probe, reassociação e tempo total de handoff para o cliente Galaxy 5 em rede com autenticação desabilitada

Figura 55. Média da duração do processo de handoff e suas etapas para os clientes IBM (a) e Galaxy 5(b) em rede com segurança desabilitada.

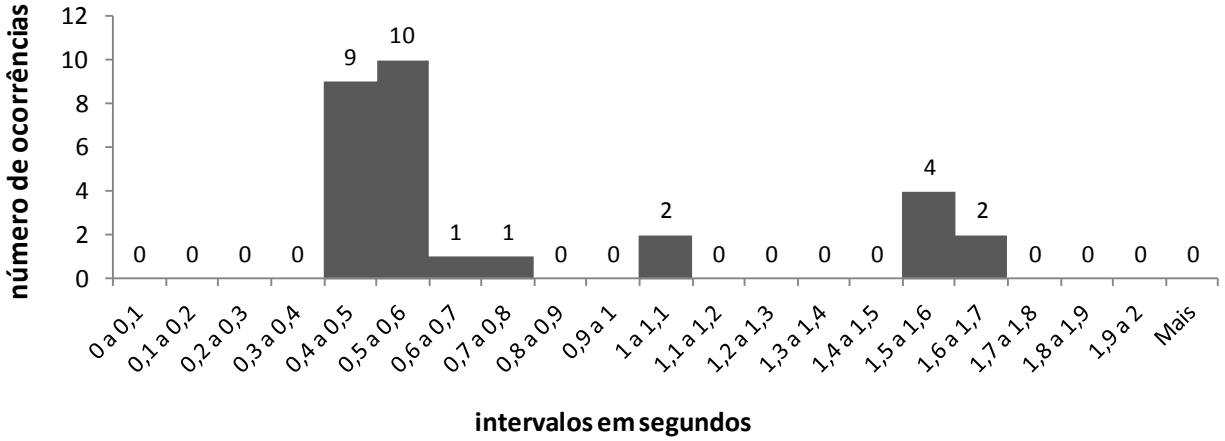
Para ambos os clientes, dentre os intervalos obtidos, alguns se destacaram pela maior amplitude. Ao analisar os arquivos de captura sem fio, verifica-se que, no geral, os maiores tempos de *handoff* são ocasionados em situações de baixa qualidade de comunicação entre o novo AP e o cliente, caracterizadas pela existência de muitos quadros de retransmissão ou pela existência de muitos quadros gerados por outras redes, ocasionando congestionamento no canal. No caso do Galaxy 5, esta baixa qualidade pode ocasionar falha na primeira tentativa de *handoff*, obrigando o cliente a realizar nova fase de *probe* em busca por um novo AP para se associar.

A Figura 56 mostra os histogramas das amostras de tempo total de *handoff* obtidas para os clientes *laptop* IBM (a) e Galaxy 5 (b). Analisando-se os resultados para o *laptop* IBM (a), verifica-se maior número de intervalos de *handoff* com duração entre 0,4 e 0,6 segundos, representando 65,51% do total. Já no caso do Galaxy 5 (b), nota-se maior número de amostras com valores entre 0,01 e 0,04 segundos, representando 59,37% do total.

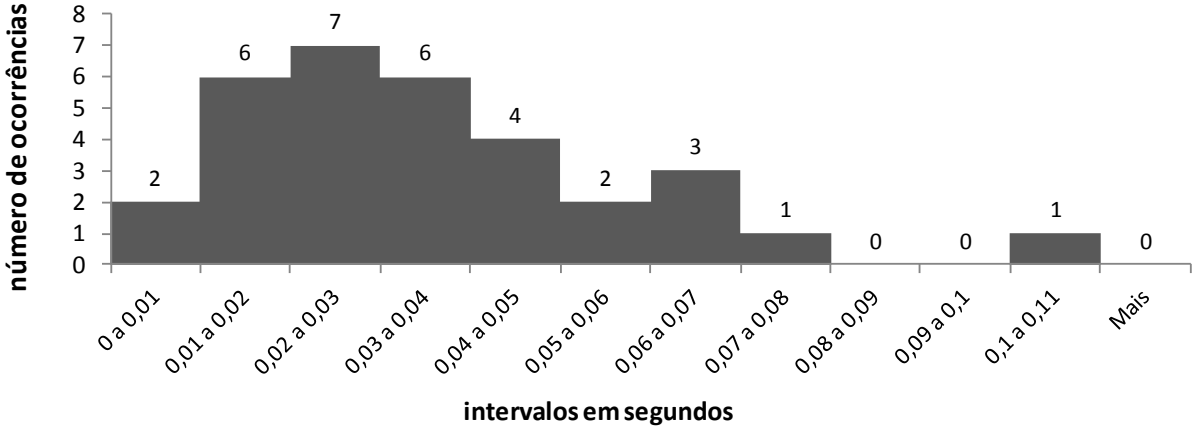
Após realizar testes em rede sem fio com segurança desabilitada, novos testes foram

realizados em uma nova rede com segurança WPA2 Enterprise, buscando avaliar o tempo necessário para a autenticação do cliente. A rede utilizada foi a rede piloto instalada na UFF, que possui 22 pontos de acesso, entretanto, como os testes foram executados apenas em dois andares do prédio da engenharia, apenas 5 deles foram utilizados. Nestes testes, o cliente utilizado foi o celular Galaxy 5.

O comportamento do cliente Galaxy 5 na rede com segurança habilitada foi semelhante ao da rede sem segurança até o momento da reassociação. Após a recepção do quadro *Reassociation Response*, o cliente troca diversas mensagens EAP-TTLS com o ponto de acesso e quatro mensagens EAPOL, referentes ao processo de autenticação [85]. Após a última mensagem EAPOL, que é enviada do cliente ao AP, o cliente volta a trocar tráfego de dados com o AP normalmente.



a) número de amostras de tempo de handoff por intervalo de tempo obtidas nos testes com o cliente Laptop IBM em rede com autenticação desabilitada.



b) número de amostras de tempo de handoff por intervalo de tempo obtidas nos testes com o cliente Galay 5 em rede com autenticação desabilitada.

Figura 56. Histograma contendo amostras de tempo de *handoff* para os clientes IBM (a) e Galaxy 5 (b) em rede com segurança desabilitada.

Esta fase de autenticação, por necessitar da troca de muitos quadros, pode ocasionar aumento expressivo no tempo total necessário para a realização do *handoff*. A Figura 57 mostra o gráfico contendo as médias da duração das fases de *probe*, reassociação, autenticação e tempo total do *handoff* obtidos neste teste, nos quais 40 amostras de cada intervalo foram coletadas. A duração das fases de *probe* e reassociação foram definidas como no teste anterior. A duração da fase de autenticação foi definida como o intervalo de tempo entre o quadro de reassociação (*Reassociation Response*) enviado do AP ao cliente, e a última mensagem EAPOL (*EAP over LANs*) enviada do cliente ao AP. As barras de erros são dadas pelo intervalo de confiança de 95%.

Comparando-se os tempos de *handoff* obtidos nos testes realizados em rede com e sem segurança habilitada, verificamos que a introdução do método de autenticação WPA2 Enterprise aumentou o a média do tempo de *handoff* de 0,035875 segundos para 0,325188 segundos, o que representa um aumento de 806,44%.

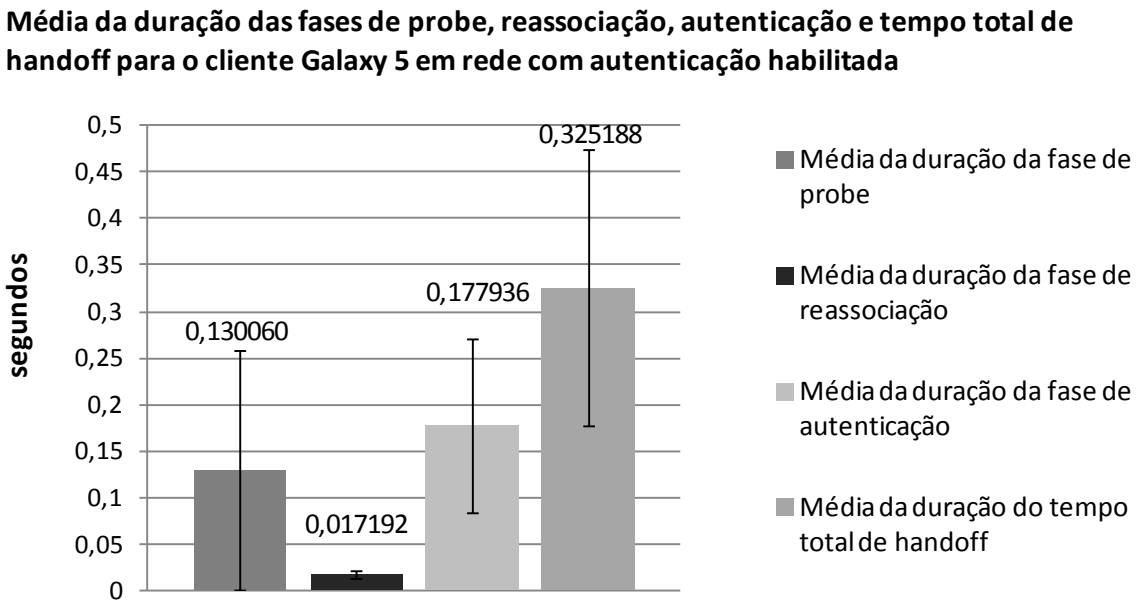


Figura 57. Média da duração do processo de *handoff* e suas etapas para o clientes Galaxy 5 em rede com segurança habilitada.

Da mesma forma como ocorreu no teste anterior, dentre os intervalos obtidos alguns se destacaram pela maior amplitude e pelos mesmos motivos observados, ou seja, pela baixa qualidade de comunicação entre o novo AP e o cliente ou pela existência de muitos quadros gerados por outras redes, ocasionando congestionamento no canal. Em certos casos, a baixa qualidade do sinal causou retransmissão de quadros durante a fase de autenticação, tornando este processo mais longo. Nos casos em que foi observado falha na primeira tentativa de

handoff, o cliente realizou nova fase de *probe* em busca por um novo AP para se associar. Entretanto, como nesta rede de testes mais APs foram utilizados, mais quadros de *probe* foram enviados pelo Galaxy 5, tornando o processo mais longo do que o ocorrido no teste anterior.

A Figura 58 mostra o histograma das amostras de tempo total de *handoff* obtidas no teste com segurança habilitada para o cliente Galaxy 5 . Analisando-se os resultados, verifica-se maior número de intervalos de *handoff* com duração entre 0,04 e 0,07 segundos, representando 57,5% do total.

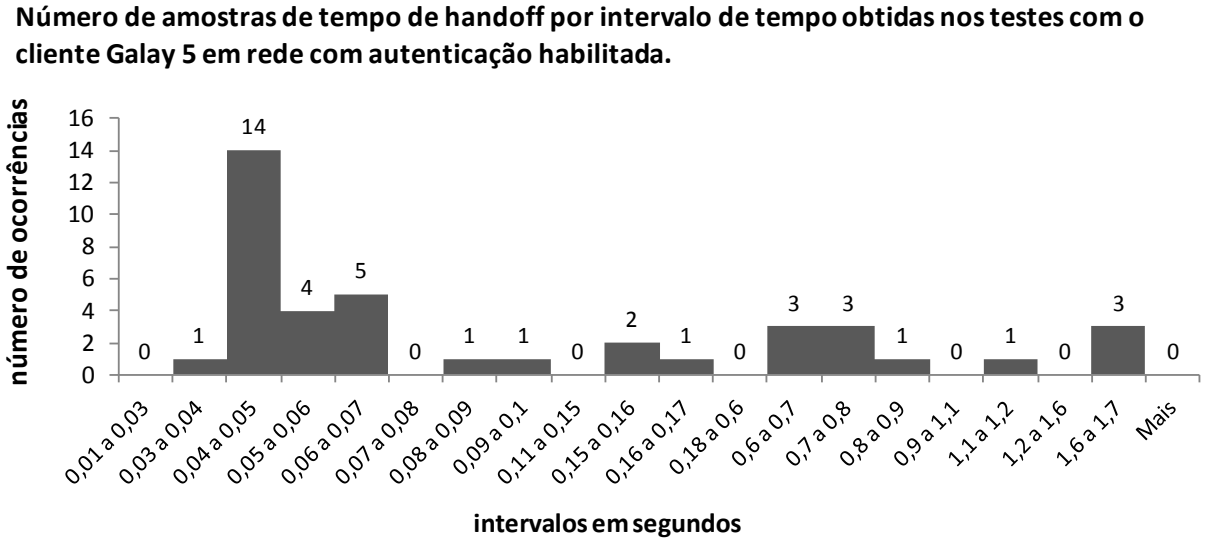


Figura 58. Histograma contendo amostras de tempo de *handoff* para o cliente Galaxy 5 em rede com segurança habilitada.

Após realizados os testes quantitativos, um teste qualitativo foi realizado para avaliar se o processo de *handoff* ocorre entre dois APs que operam em canais diferentes. O teste realizado com o cliente Galaxy 5 na rede operando com segurança WPA2 Enterprise mostrou resultado positivo, ou seja, o *handoff* ocorreu normalmente entre APs com canais distintos. Nos testes anteriores, os pontos de acesso foram configurados com o mesmo canal para facilitar o processo de captura sem fio.

Um segundo teste qualitativo foi realizado nesta mesma rede, no qual o cliente Galaxy 5 foi conectado a um dos pontos de acesso e o aplicativo *Skype* [83] foi utilizado para realizar uma chamada de voz em tempo real entre o cliente e um dispositivo localizado em outra rede. A seguir o cliente foi deslocado para forçar a ocorrência do *handoff*. O teste revelou que, ao final do processo, a comunicação voltou ao normal sem a necessidade de realização de nova chamada de voz, apenas sendo verificado um período de silêncio durante a troca de AP.

5.2.5.6. Conclusões

Através da realização dos testes de *handoff* verificamos que a arquitetura implementada na rede piloto do SCIFI possibilitou que processo fosse realizado com sucesso pelos clientes.

Após a realização dos testes com diferentes dispositivos clientes, verificamos diferentes comportamentos de suas interfaces sem fio, das quais duas se destacam. A primeira delas revela que o cliente Galaxy 5, após se desassociar do AP de origem e escolher um novo AP pertencente à mesma rede para se associar, realiza Reassociação, enquanto o *laptop* IBM realiza uma nova associação. A segunda delas revela que, como o cliente Galaxy 5 envia menor número de quadros de *probe* durante o período do *handoff* em que está desassociado, é capaz de realizar o processo em um intervalo de tempo menor em relação ao IBM ThinkPad, obtendo duração média de 0,03 segundos para o tempo total de *handoff* em rede com segurança desabilitada, em comparação aos 0,78 segundos obtidos para o IBM.

Após a realização dos testes em rede com segurança WPA2 Enterprise habilitada, verificamos que o processo de autenticação ocasiona grande impacto no tempo total de *handoff*. O cliente Galaxy 5 levou em média, 0,32 segundos para realizar o processo incluindo a autenticação, o que significa um aumento de mais de 806% em relação ao resultado obtido em rede sem segurança. Verificamos também que a duração da fase de *probe* para este cliente foi maior, devido ao maior número de pontos de acesso na rede.

Os testes qualitativos mostraram que o *handoff* ocorre normalmente entre APs que operam em canais diferentes na rede com segurança habilitada. Além disso, os testes que envolveram a realização de chamada de voz através do aplicativo *Skype*, mostraram que, apesar da haver desconexão do cliente no momento do *handoff*, a chamada não foi finalizada durante a realização do processo, e apenas um momento de silêncio foi observado.

6. CONCLUSÕES

Este trabalho mostrou todo o estudo realizado para a elaboração do Sistema de Controle Inteligente para Redes sem Fio (SCIFI), bem como sua arquitetura, algoritmos, e testes de avaliação. O SCIFI é um sistema de controle automático e dinâmico para redes 802.11 infraestruturadas que surgiu a partir da necessidade de uma ferramenta voltada para a configuração automática de pontos de acesso de baixo custo, que atualmente carecem deste tipo de solução. Seus principais objetivos são facilitar o processo de configuração e reduzir a interferência entre pontos de acesso da rede através da escolha automática e dinâmica dos canais e potências de transmissão, que é realizada com base em informações de interferência do ambiente. O sistema, que foi desenvolvido em JAVA e pode ser executado em um PC comum, é capaz de operar com pontos de acesso de diversos fabricantes, desde que suportem a instalação de *firmware* baseado em Linux, como o OpenWRT. O SCIFI foi desenvolvido na Universidade Federal Fluminense (UFF) com apoio da Rede Nacional de Ensino e Pesquisa (RNP) e se mostra como uma alternativa aos caros sistemas de controle comerciais que existem no mercado atualmente, e que operam apenas com APs e *switches* específicos.

O sistema foi criado com os requisitos de não depender de características específicas de dispositivos clientes da rede nem necessitar de alterações profundas no padrão 802.11 atual. Antes de realizar a escolha dos canais e potências, o controlador ordena que os pontos de acesso executem determinadas tarefas, que são a coleta do número de clientes associados e dados sobre interferência de pontos de acesso vizinhos. A seguir, executa seus algoritmos para escolher os parâmetros de canal e potência a serem utilizados pelos APs.

A comunicação entre o controlador e os pontos de acesso é realizada por SSH (*Secure Shell*) e informações são transferidas ao controlador através de SCP (*Secure Copy Protocol*). As tarefas são executadas nos pontos de acesso através de *scripts* que utilizam ferramentas Linux previamente instaladas, como iw, iwlist, iwconfig, entre outras. A utilização de *scripts* e ferramentas de código aberto permite que o sistema possa ser adaptado para diversos modelos de pontos de acesso.

O sistema possui um banco de dados, no qual as informações sobre interferência, clientes associados e pontos de acesso são armazenadas. Além disso possui um Servidor de Aplicações que provê acesso à interface Web Administrativa, através da qual o administrador da rede pode realizar configurações, adicionar ou excluir pontos de acesso controlados na base de dados, e visualizar informações sobre os APs, como seus endereços MAC, IP, canal, potência, vizinhos interferentes, entre outras. Todas as tarefas de controle são executadas com intervalos definidos pelo administrador através da interface Web. Desta forma, as configurações de canal e potência são adaptadas de acordo com as informações de interferência atual do ambiente. Além destas funções principais, o controlador também disponibiliza, através de uma página web, a informação de carga em cada ponto de acesso da rede, possibilitando que os clientes (usuários da rede) possam escolher a região de menor carga caso experimentem dificuldade ou baixa qualidade no acesso. A métrica de carga utilizada pelo sistema é o número de clientes associados a cada AP.

O algoritmo de alocação de canais utilizado pelo SCIFI modela a rede em um grafo de interferências, no qual os vértices representam APs e arestas unidirecionais ponderadas que os interligam representam a interferência entre eles. Desta forma, o problema da alocação de canais pode ser tratado como um problema de coloração dos vértices do grafo, no qual as cores representam os possíveis canais a serem utilizados. Como este problema é NP Difícil, uma heurística foi utilizada para que a alocação pudesse ser realizada em tempo viável e de forma dinâmica. A heurística do SCIFI se baseia na heurística DSATUR [24], que utiliza o número de cores adjacentes a cada vértice, ou grau de saturação do vértice, para determinar a prioridade na coloração dos vértices, de forma que o que possuir maior grau deve ser colorido primeiro com a primeira cor disponível.

No SCIFI esta heurística foi aperfeiçoada de acordo com os requisitos definidos para o sistema. Primeiramente, o algoritmo foi modelado para operar de forma centralizada. Outra alteração foi a consideração da interferência ocasionada por pontos de acesso que não pertencem ao mesmo domínio administrativo. Estes APs são inseridos no grafo de

interferências como vértices de cores fixas. Outra diferença é que, no algoritmo do SCIFI, a escolha das cores é realizada com base na qualidade do sinal interferente recebido de outros APs, de forma a reduzir a área de interferência entre pontos de acesso. Além disso, no caso em que mais de um AP possua o mesmo grau de saturação, o que obtiver o maior número de clientes terá prioridade na escolha do canal. Caso novo empate ocorra, o número IP do ponto de acesso deve ser utilizado, de forma que o que possuir o menor IP deve ganhar prioridade.

Após a definição dos canais, dada a grande densidade de pontos de acesso, alguns deles podem vir a operar no mesmo canal, mesmo no caso de estarem em proximidade. Buscando reduzir a área de interferência entre eles, o controlador configura as potências dos pontos de acesso. O algoritmo de controle de potência do SCIFI possui duas etapas, uma que se encarrega da redução e outra que se encarrega do aumento das potências. A redução ocorre quando um ponto de acesso ou mais interferem em outros da rede. Caso isso ocorra, cada AP interferente deve reduzir sua potência em passos até que nenhum outro seja interferido por ele ou até que uma potência mínima determinada pelo administrador seja atingida. O aumento da potência deve ocorrer quando um AP deixa de ser interferente. Caso nenhum outro AP da rede receba seu sinal, ele deve aumentar sua potência em um passo e caso ele seja o único em seu canal, ele deve aumentar a potência para a máxima determinada.

Os testes de avaliação dos algoritmos do SCIFI mostraram que o algoritmo de alocação de canais é capaz de propiciar boa distribuição de canais entre APs que interagem em um ambiente, mesmo com alguns deles não sendo controlados, e a utilização do algoritmo de controle de potência favorece ainda mais a redução da interferência. Como consequência, a rede como um todo é beneficiada com o aumento de sua vazão. No cenário de testes apresentado, a utilização do algoritmo de alocação de canais foi capaz de propiciar um aumento 29,4% da vazão agregada na rede como um todo, sendo que 63,04% deste aumento se deu na vazão agregada da rede gerenciada, enquanto 36,96% se deu na vazão agregada da rede não gerenciada. Ao aplicar o algoritmo de controle de potência, a vazão agregada da rede obteve mais um pequeno ganho de 1,48%.

Além dos testes de avaliação dos algoritmos, testes de avaliação geral do sistema foram executados, buscando verificar o quanto a execução da varredura espectral nos pontos de acesso e a troca de canal poderiam ser prejudiciais aos clientes da rede. Através dos resultados pode-se notar que diferentes dispositivos clientes possuem diferentes comportamentos, de forma que alguns podem ser prejudicados durante a varredura espectral por sofrer desconexão enquanto outros não. Foi verificado que aumentando o intervalo entre a

emissão de *beacons* do ponto de acesso, o cliente que antes sofria desconexão passou a não sofrer mais. No caso da troca de canal é inevitável que o cliente sofra desconexão. Desta forma este processo se mostrou mais prejudicial em relação à varredura espectral e deve ser executado com parcimônia.

Outros testes foram realizados para avaliar a duração das tarefas de controle do SCIFI, incluindo as tarefas de coleta de dados e execução dos algoritmos. Através destes testes foi estimado um valor máximo de pontos de acesso que podem pertencer a uma mesma região de controle. A tarefa que se mostrou de maior preocupação foi a de coleta de dados de varredura espectral (*scan*). Tendo em vista que no momento da realização da varredura os APs cessam a transmissão de *beacons*, apenas um AP pode executar esta tarefa por vez, já que caso todos executassem ao mesmo tempo, nenhum deles receberia *beacons* dos outros. Desta forma, aumentado-se o número de pontos de acesso na rede, o intervalo para execução desta tarefa cresce proporcionalmente. Após esta constatação, o número de pontos de acesso foi estimado com base no intervalo padrão entre execuções da tarefa de *scan*, que é de 500 segundos, de forma que a duração da tarefa para o determinado número máximo de APs não ultrapassasse 50% deste intervalo. De acordo com a Equação 2, que foi a equação obtida para a duração da tarefa de *scan* em relação ao número de APs, o número máximo de pontos de acesso por região de controle obtido foi 40.

Uma avaliação do *overhead* do controlador também foi realizada, mostrando que a tarefa de coleta de dados de número de usuários, por ser executada mais vezes ao dia por padrão, é capaz de gerar um maior *overhead* na rede. Somando-se o *overhead* obtido para cada tarefa de controle, a Equação 3 foi criada para o cálculo do *overhead* em relação ao número de pontos de acesso (N). De acordo com esta equação, uma rede com 20 APs gera um *overhead* médio na rede cabeada de 9,5 Kbytes por segundo, o que é um valor baixo considerando a taxa nominal de 1 Gbps do enlace.

Por fim testes de *handoff* foram realizados buscando avaliar este processo na rede piloto do SCIFI implantada na UFF, que atualmente possui 28 pontos de acesso e utiliza segurança WPA2 Enterprise. Através deste teste verificamos que o *handoff* foi possível e que diferentes clientes possuem diferentes comportamentos. Além disso foi verificado que a utilização da segurança inseriu um aumento de 806% no tempo médio necessário para o *handoff* em relação ao tempo obtido em rede com segurança desabilitada (aberta). Os valores médios de duração do *handoff* obtidos para a rede sem e com segurança habilitada foi de aproximadamente 0,03 e 0,32 segundos, respectivamente.

O projeto SCIFI é importante porque é uma alternativa simples e barata aos sistemas de controle de redes sem fio IEEE 802.11 proprietários existentes no mercado atualmente, de custo elevado. O SCIFI, em sua versão atual, não oferece todas as funcionalidades encontradas em sistemas comerciais. Ele faz principalmente o controle de RF, não tendo, por exemplo, detecção de intrusão. No entanto, diferente de seus concorrentes, o SCIFI é uma plataforma aberta que permite a adição de novas funcionalidades, e pode futuramente ser extendido para ter todas as funcionalidades desejadas. Como um sistema de código aberto, ele também permite auditoria do seu código, o que é mais seguro do que simplesmente confiar nos fornecedores.

O SCIFI vem a atender um nicho de mercado - instituições que precisam de redes sem fio grandes o suficiente para necessitar de gerenciamento centralizado mas que não possuem recursos para adotar as soluções de mercado. Após a disponibilização de uma primeira versão ao público, diversas instituições, além da UFF, optaram por utilizar o sistema devido aos seus benefícios, como a Universidade Federal de Ouro Preto, Universidade Federal de Viçosa, Centro de Análises de Sistemas Navais, entre outras.

Como trabalho futuro, pretendemos implementar algumas funcionalidades para aumentar a facilidade de utilização do sistema, como o cadastramento automático de APs para controle. Além disso, pretendemos realizar testes em larga escala na rede piloto que foi instalada na UFF. Em relação aos algoritmos, pretendemos verificar outras possibilidades para a execução do balanceamento de carga e verificar mais a fundo as vantagens e desvantagens da utilização do mecanismo de controle de potência. Atualmente, duas adições estão sendo feitas à rede piloto implantada na UFF, que são: a construção de uma plataforma de monitoramento, que auxiliará o desenvolvimento futuro; e a criação de ferramentas para a operação da rede, já que o SCIFI foi escolhido como tecnologia para a implantação da rede sem fio da UFF em Niterói.

REFERÊNCIAS

[1] "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, Março 2012.

[2] G. Conradi, "Fat vs. Thin vs. Fit APs," 2010. [Online]. Available: http://www.cse.wustl.edu/~jain/cse574-10/ftp/capwap/index.html#2.2. [Acesso em maio 2012].

[3] "OpenWrt," [Online]. Available: https://openwrt.org/. [Acesso em Outubro 2012].

[4] M. S. Gast, 802.11 Wireless Networks: the Definitive Guide, 2nd Edition, O`REILLY, 2005.

[5] ITU-T, *Recommendation X.200 : Information technology - Open Systems Interconnection - Basic Reference Model: The basic model,* 1994.

[6] "Wi-Fi Alliance," [Online]. Available: https://www.wi-fi.org/. [Acesso em Novembro 2012].

[7] J. F. Kurose e K. W. Ross, Redes de Computadores e a Internet: Uma abordagem top-down, 3a ed., Pearson, 2006.

[8] J. L. Sobrinho, R. D. Haan e J. M. Brázio, "Why RTS-CTS is not your ideal wireless LAN multiple access protocol," *IEEE Wireless Communications and Networking Conference, WCNC,* pp. 81-87, Março 2005.

[9] S. Chieochan, E. Hossain e J. Diamond, "Channel assignment schemes for infrastructure-based 802.11 WLANs: A survey," *Communications Surveys & Tutorials, IEEE,* pp. 124 - 136, 17 Fevereiro 2010.

[10] M. Achanta, "Method and apparatus for least congested channel scan for wireless access points". EUA Patente 0072602, Abril 2006.

[11] R. Akl e A. Arepally, "Dynamic Channel Assignment in IEEE 802.11 Networks," *2007 IEEE International Conference on Portable Information Devices,* pp. 1-5, Maio 2007.

[12] M. Bernaschi, F. Cacace, A. Davoli, D. Guerri, M. Latini e L. Vollero, “A CAPWAP-based solution for frequency planning in large scale networks of WiFi Hot-Spots,” em *Comput. Commun.*, Amsterdam, Holanda, 2011.

[13] J. Riihijarvi, M. Petrova and P. Mahonen, "Frequency Allocation for WLANs Using Graph Colouring Techniques," *Second Annual Conference on Wireless On-demand Network Systems and Services - WONS,* vol. 3, pp. 216-222, Janeiro 2005.

[14] J. Riihijarvi, M. Petrova, P. Mahonen e J. Barbosa, “Performance Evaluation of Automatic Channel Assignment Mechanism for IEEE 802.11 Based on Graph Colouring,” *IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications,* pp. 1-5, Setembro 2006.

[15] K. Leung e B.-J. Kim, “Frequency Assignment for IEEE 802.11 Wireless Networks,” *2003 IEEE 58th Vehicular Technology Conference,* vol. 3, pp. 1422-1426, Outubro 2003.

[16] P. Mahonen, J. Riihijarvi e M. Petrova, “Automatic channel allocation for small wireless local area networks using graph colouring algorithm approach,” em *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004.*, 2004.

[17] A. Mishra, V. Brik, S. Banerjee, A. Srinivasan e W. Arbaugh, “A client-driven approach for channel management in wireless LANs,” *INFOCOM 2006. 25th IEEE International Conference on Computer Communications,* pp. 1-12, Abril 2006.

[18] A. Mishra, S. Banerjee e W. Arbaugh, “Weighted coloring based channel assignment for WLANs,” *SIGMOBILE Mob. Comput. Commun. Rev.,* pp. 19--31, Julho 2005.

[19] M. Haidar, R. Ghimire, H. Al-Rizzo, R. Akl e Y. C. Yupo Chan, “Channel assignment in an IEEE 802.11 WLAN based on Signal-To-Interference Ratio,” *2008 Canadian Conference on Electrical and Computer Engineering,* pp. 1169-1174, Maio 2008.

[20] “IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs,” *IEEE Std 802.11k-2008 (Amendment to IEEE Std 802.11-2007),* pp. 1-244, Dezembro 2008.

[21] A. Hills, “Large-Scale Wireless LAN Design,” *IEEE Communications Magazine,* pp. 98-104, Novembro 2001.

[22] M. W. R. d. Silva e J. F. d. Rezende, “A Dynamic Channel Allocation Mechanism for IEEE 802.11 Networks,” em *VI International Telecommunications Symposium (ITS 2006)*, Fortaleza- CE, Brazil, 2006.

[23] A. Mishra, E. Rozner, S. Banerjee and W. Arbaugh, "Exploiting partially overlapping channels in wireless networks: turning a peril into an advantage," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, Berkeley, CA, USENIX Association, 2005, pp. 29-29.

[24] D. Brèlaz, “New methods to color the vertices of a graph,” *Commun. ACM,* pp. vol. 22, pp. 251-256, 1979.

[25] A. Pires, J. de Rezende e C. Cordeiro, “Protecting Transmissions when Using Power Control on 802.11 Ad Hoc Networks,” em *Challenges in Ad Hoc Networking*, Springer Boston, 2006, pp. 41-50.

[26] A. Sheth e R. Han, “SHUSH: reactive transmit power control for wireless MAC protocols,” em *First International Conference on Wireless Internet*, 2005.

[27] J. Monks, V. Bharghavan e W.-M. Hwu, “A power controlled multiple access protocol for wireless packet networks,” em *IEEE INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies.*, 2001.

[28] D. Qiao, S. Choi, A. Jain e K. Shin, “Adaptive transmit power control in IEEE 802.11a wireless LANs,” em *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, 2003.

[29] A. Akella, G. Judd, S. Seshan e P. Steenkiste, “Self-Management in Chaotic Wireless Deployments,” em *ACM MobiCom*, 2005, pp. 185-199.

[30] V. P. Mhatre, K. Papagiannaki e F. Baccelli, “Interference Mitigation through Power Control in High Density 802.11 WLANs,” em *IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, 2007.

[31] V. Shrivastava, D. Agrawal, A. Mishra, S. Banerjee e T. Nadeem, “Understanding the limitations of transmit power control for indoor wlans,” em *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, San Diego, California, USA, 2007.

[32] I. Papanikos e M. Logothetis, “A study on dynamic load balance for IEEE 802.11b wireless LAN,” em *VIII International conference on advances in communication and control*, 2001.

[33] L.-H. Yen, T.-T. Yeh e K.-H. Chi, “Load Balancing in IEEE 802.11 Networks,” *IEEE Internet Computing,* vol. 13, n. 1, 2009.

[34] H. Salah, S. Adel e T. Rached, “Experimental Performances Analysis of Load Balancing Algorithms in IEEE 802.11,” *International Journal of Computer Science and Information Security,* vol. 4, 2009.

[35] S.-T. Sheu e C.-C. Wu, “Dynamic Load Balance Algorithm (DLBA) for IEEE 802.11 Wireless LAN,” *Tamkang Journal of Science and Engineering, vol. 2, No. 1,* pp. 45-52, 1999.

[36] H. Velayos, V. Aleo e G. Karlsson, “Load balancing in overlapping wireless LAN cells,” em *IEEE International Conference on Communications*, 2004.

[37] A. Dhananjay e L. Ruan, “PigWin: Meaningful Load Estimation in IEEE 802.11 Based Wireless LANs,” em *IEEE International Conference on Communications*, 2008.

[38] B. Kauffmann, F. Baccelli, A. Chaintreau, V. Mhatre, K. Papagiannaki e C. Diot, “Measurement-Based Self Organization of Interfering 802.11 Wireless Access Networks,” *INFOCOM 2007. 26th IEEE International Conference on Computer Communications,* pp. 1451-1459, 2007.

[39] M. T. Lee, L. Lai e D. Lai, “Enhanced Algorithm for initial ap selection and roaming”. EUA Patente

0039817, Fevereiro 2004.

[40] G. Wu e T.-c. Chiueh, “Passive and accurate traffic load estimation for infrastructure-mode wireless lan,” *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems,* pp. 109--116, 2007.

[41] R. Daher e D. Tavangarian, “Load Observation and Control Model for Load Balancing with QoS in WLAN,” em *XIV IST Mobile & Wireless Communication Summit*, Dresden, 2005.

[42] E. Garcia, R. Vidal e J. Paradells, “Cooperative load balancing in IEEE 802.11 networks with cell breathing,” em *IEEE Symposium on Computers and Communications* , 2008.

[43] Motorola, “Soluções Sem Fio Motorola,” [Online]. Available: http://www.motorola.com/Business/XL-PT/Produtos+e+Servicos+para+Empresas/Solucoes+de+Redes+Sem+Fio. [Acesso em Maio 2012].

[44] Motorola, “Manual do Controlador RFS7000,” [Online]. Available: https://docs.symbol.com/manuals/12469001a.pdf?pLibItem=1&localeId=33. [Acesso em Maio 2012].

[45] “IEEE Std for Information Technology - Telecom. and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN MAC and PHY Specifications Amendment 8: MAC Quality of Service Enhancements,” *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003),* pp. 1-189, 2005.

[46] Cisco, “Soluções Sem fio Cisco,” [Online]. Available: http://www.cisco.com/en/US/products/hw/wireless/products.html. [Acesso em Maio 2012].

[47] Cisco, “FAQ sobre controladores da Cisco,” [Online]. Available: http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml. [Acesso em Maio 2012].

[48] Cisco, “Cisco RRM,” [Online]. Available: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml#intro. [Acesso em Maio 2012].

[49] Aruba, “Aruba - Mobility Management System,” [Online]. Available: http://www.globalforte.com/download00034678/Aruba/Products/Mobility_Management_System.pdf. [Acesso em Maio 2012].

[50] Aruba, “ArubaOS,” [Online]. Available: http://www.arubanetworks.com/pdf/products/DS_AOS.pdf. [Acesso em Maio 2012].

[51] Aruba, “Aruba - ARM,” [Online]. Available: http://www.arubanetworks.com/pdf/solutions/TB_ARM.pdf. [Acesso em Maio 2012].

[52] Aruba, “RFProtect,” [Online]. Available: http://www.arubanetworks.com/products/arubaos/rfprotect-spectrum-analyzer/. [Acesso em Maio

2012].

[53] Aruba, “ARM White Paper,” [Online]. Available: http://www.arubanetworks.com/pdf/technology/whitepapers/wp_ARM_EnterpriseWLAN.pdf. [Acesso em Maio 2012].

[54] “Wireless Access Point Utilites for Unix,” [Online]. Available: http://ap-utils.polesye.net/. [Acesso em Maio 2012].

[55] I. T. Union, “ITU-T X.711,” [Online]. Available: http://www.itu.int/rec/T-REC-X.711/en/. [Acesso em Maio 2012].

[56] “RFC 1157 - SNMP,” [Online]. Available: http://tools.ietf.org/html/rfc1157. [Acesso em Maio 2012].

[57] “RFC 1155 - SMI,” [Online]. Available: http://tools.ietf.org/html/rfc1155. [Acesso em Maio 2012].

[58] “RFC 6241 - NETCONF,” [Online]. Available: http://tools.ietf.org/html/rfc6241. [Acesso em Maio 2012].

[59] “RFC 5412 - LWAPP,” [Online]. Available: http://tools.ietf.org/html/rfc5412. [Acesso em Maio 2012].

[60] “RFC 5415 - CAPWAP,” [Online]. Available: http://tools.ietf.org/html/rfc5415. [Acesso em Maio 2012].

[61] “RFC 6347 - DTLS,” [Online]. Available: http://tools.ietf.org/html/rfc6347. [Acesso em Maio 2012].

[62] “RFC 5416 - CAPWAP Binding for IEEE 802.11,” [Online]. Available: http://tools.ietf.org/html/rfc5416. [Acesso em Maio 2012].

[63] Aruba, “Posicionamento em relação ao CAPWAP,” [Online]. Available: http://community.arubanetworks.com/aruba/attachments/aruba/115/422/1/CAPWAP+Position.pdf. [Acesso em Maio 2012].

[64] Aruba, “Airwave Wireless Management Suite,” [Online]. Available: http://www.arubanetworks.com/pdf/products/DS_AW.pdf. [Acesso em Maio 2012].

[65] Motorola, “Release Notes: RFS-7000 v1.0.0.0-357R,” [Online]. Available: https://docs.symbol.com/ReleaseNotes/RFS-7000_v1.0_ReleaseNotes.htm.

[66] “RFC 4253 - SSH,” [Online]. Available: http://tools.ietf.org/html/rfc4253. [Acesso em Maio 2012].

[67] L. R. D. Nascimento, H. D. Balbi, N. C. Fernandes, R. C. Carrano, D. C. M. Saade, C. V. N. D. Albuquerque e L. C. S. Magalhães, “Sistema de controle inteligente para redes 802.11 infra-estruturadas de baixo custo,” *VI Workshop de TIC das IFES, WTICIFES,* Maio 2012.

[68] NoCat, “NoCatAuth,” [Online]. Available: http://nocat.net/.

[69] Java, “JavaServer Faces,” [Online]. Available: http://javaserverfaces.java.net/.

[70] JBoss, “JBoss Application Server,” [Online]. Available: http://www.jboss.org/jbossas. [Acesso em Maio 2012].

[71] H. D. Balbi, F. R. e. Souza, R. C. Carrano, D. C. M. Saade, C. V. N. d. Albuquerque e L. C. S. Magalhães, “Algoritmo de seleção de canais centralizado para redes IEEE 802.11 com controlador,” *II Workshop de Redes de Acesso em Banda Larga (WRA), XXX SBRC,* pp. 73-86, Maio 2012.

[72] H. Balbi, N. Fernandes, F. Souza, R. Carrano, C. Albuquerque, D. Muchaluat-Saade e L. Magalhães, “Centralized channel allocation algorithm for IEEE 802.11 networks,” *The 4th Global Information Infrastructure and Networking Symposium GIIS,* Dezembro 2012.

[73] “OLPC XO,” [Online]. Available: http://laptop.org/en/laptop/index.shtml.

[74] “AirMax,” Ubiquiti, [Online]. Available: http://www.ubnt.com/airmax. [Acesso em Agosto 2012].

[75] “PicoStation 2,” [Online]. Available: http://www.ubnt.com/picostation.

[76] “MadWifi Project,” [Online]. Available: http://madwifi-project.org/wiki.

[77] “RSSI,” [Online]. Available: http://madwifi-project.org/wiki/UserDocs/RSSI. [Acesso em 27 02 2012].

[78] “Iperf,” [Online]. Available: http://iperf.sourceforge.net/.

[79] “RFC 792 - ICMP,” [Online]. Available: http://tools.ietf.org/html/rfc792. [Acesso em 10 2012].

[80] “Ping,” [Online]. Available: http://linux.die.net/man/8/ping. [Acesso em Julho 2012].

[81] “Galaxy 5,” Samsung, [Online]. Available: http://www.samsung.com/br/support/detail/supportPrdDetail.do?menu=SP00&prd_ia_cd&prd_mdl_cd=GT-I5500YKBZ1O. [Acesso em Agosto 2012].

[82] “AirPcap Nx,” [Online]. Available: http://www.cacetech.com/documents/AirPcap%20Nx%20Datasheet.pdf. [Acesso em Junho 2012].

[83] “Skype,” [Online]. Available: http://www.skype.com/intl/pt-br/get-skype/. [Acesso em junho 2012].

[84] Ubiquiti, “Ubiquiti Networks,” [Online]. Available: http://www.ubnt.com/. [Acesso em Agosto 2012].

[85] “ISO/IEC International Std. - Information Technology Telecommunications and Information Exchange Between Systems LAN and MAN Specific Requirements Part 11: Wireless LAN MAC and PHY Specifications Amendment 6: MAC Security Enhancements,” *ISO/IEC 8802-11, Second edition: 2005/Amendment 6 2006: IEEE STD 802.11i-2004 (Amendment to IEEE Std 802.11-1999),* pp. 1-178, 2004.

[86] “IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control,” *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004),* pp. 1-205, 2012.

[87] “RFC 3748 - EAP,” [Online]. Available: http://tools.ietf.org/html/rfc3748. [Acesso em 10 2012].