Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Rolando Oscar Castro Soliz

REDES SEM FIO:
Projeto de uma Rede Corporativa

Rio de Janeiro

2010

Rolando Oscar Castro Soliz

REDES SEM FIO:
Projeto de uma Rede Corporativa

Monografia apresentada para obtenção do titulo de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE –UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2010

Rolando Oscar Castro Soliz

REDES SEM FIO:
Projeto de uma Rede Corporativa

Monografia apresentada para obtenção do titulo de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE –UFRJ.

Aprovada em maio de 2010

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Dedico este trabalho aos meus professores que tem repassado seu conhecimento e incentivando a continuar trilhando este caminho de constante estudo, técnica.

AGRADECIMENTOS

Gostaria de agradecer a todas as pessoas que contribuíram na montagem da infra-estrutura de rede sem fio, site survey e instalação de ativos de rede, em especial ao técnico em Redes Nelson Costa Pinheiro.

RESUMO

SOLIZ, Rolando Oscar Castro. **REDES SEM FIO: Projeto de uma Rede Corporativa**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

As redes IEEE 802.11 se tornaram uma realidade pelo fato de oferecerem varias facilidades na sua instalação, como, por exemplo, baixo custo, rapidez na implantação e necessidade de pouco conhecimento devido à grande quantidade de equipamentos que vêm pré-configurados de fábrica.

Todos estes fatores provocaram o aumento de uso dos recursos de rede por parte dos usuários e provocaram uma série de problemas como a grande concentração de usuários em pontos de acesso sobrecarregados, assim como problemas na hora de controlar uma grande quantidade de Pontos de Acesso distantes das áreas de gerência.

Os maiores problemas das redes sem fio são gerência e segurança. Pela sua própria natureza estas redes trafegam num meio físico susceptível a ataques de usuários maliciosos, e as implantações para prover segurança e gerência necessárias não têm sido feitas na velocidade requerida ou falta de conhecimento dos administradores.

O objetivo deste trabalho é apresentar uma proposta de metodologia de configuração e implantação para redes sem fio corporativas, de tal forma que possa servir como guia para novas instalações.

ABSTRACT

SOLIZ, Rolando Oscar Castro. **REDES SEM FIO: Projeto de uma Rede Corporativa**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

IEEE 802.11 networks became a reality because of the many advantages they offer for installation, for example, low cost, speed of implementation and the fact that minimal specialist knowledge is required because most of the equipment comes pre-configured from the factory

All these factors have led to increased use of network resources and have caused a series of problems, such as a large concentration of users at overloaded access points or problems when controlling a large number of access points which are distant from the management areas.

The greatest problems of wireless networks are management and security. Due to their nature, these networks travel in a physical environment which is susceptible to attacks from malicious users, and the necessary action to provide sufficient security and management have not been carried out quickly enough or the administrators have lacked the knowledge to do so.

The aim of this paper is to present a proposal of a configuration and implementation methodology for corporative wireless networks that can serve as a guide for new installations.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AAA	Authentication Authorization and Accounting
AODV	Ad hoc On-Demand Distance Vector Routing
AP	Access Point
AWP	Adaptative Wireless Path
BSA	Basic Service Area
BSS	Basic Service Set
CCK	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
dBm	Decibel miliwatt
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DFT	Discrete Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DIFS	DCF Inter Frame Space
DNS	Domain Name System
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Inter Frame Space
ESA	Extended Service Area
ESS	Extended Service Set
FHSS	Frecuency Hopping Spread Spectrum
FSK	Frequency Shift Keying
GPS	Global Position System
IDFT	Inverse Discrete Fourier Transform
IEEE	Institute of Electrical and Electronic Engineers
IFS	Inter Frame Space
IPHAN	Instituto do Patrimônio Histórico e Artístico Nacional
LAN	Local Área Network
LANMAR	Routing for Large Scale Wireless AdHoc Networks with Group Mobility
LAR	Location Aided Routing
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
LWAP	Lightweight Acces Point
LWAPP	Lightweight Acces Point Protocol
LWR	Load aWare Routing
MAC	Médium Access Control
MACA	Multiple Access with Collision Avoidance
MANET	Móbile Ad-hoc Networks Working Group
MIB	Management Information Base
MIMO	Multiple-input multiple-output
MPDUs	MAC Protocol Data Units
NAV	Network allocation Vector
OFDM	Orthogonal Frequency-Division Multiplexing

OSI	Open System Interconnection
PCF	Point Coordination Function
PIFS	PCF Inter Frame Space
PLCP	Physical Layer Convergence Protocol
PMD	Polarization Mode Dispersion
PoE	Power over Ethernet
RDMAR	Bandwidth Efficient Routing for Mobile AdHoc Networks
RF	Radio Frequency
RMM	Radio Resource Management
RTS	Request to Send
SIFS	Short Inter Frame Space
SSID	Service Set Identifier
TDM	Time Division Multiplexing
TTL	Time To Live
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLC	Wireless LAN Controller

SUMÁRIO

1 INTRODUÇÃO

Em se tratando de acesso à recursos computacionais via rede, nos últimos tempos tem se notado um grande crescimento das redes sem fio. Isto se tornou possível pela facilidade de implementação destas redes, que na sua grande maioria usam equipamentos simples (*Light APs*) que já vêm pré-configurados e sem uso de segurança, além do custo que tem se mostrado cada vez mais atraente.

As facilidades que as redes IEEE 802.11 trazem são óbvias. Mobilidade, fazendo com que os usuários destas redes possam ter acesso a recursos a partir de qualquer ponto onde a rede tenha cobertura, o que se traduz em maior produtividade para o caso de uma empresa. Custos, o simples fato de colocar uma unidade transmissor-receptora (*Access Point*) conectada a uma LAN já permite o acesso dos usuários aos recursos da rede. Se fosse necessário implantar esta mesma estrutura numa rede cabeada a situação seria muito mais complicada pelo fato de ter que fazer passagem de cabos e obras civis como instalação de dutos, calhas, trabalho em pisos falso e outros. Isso sem considerar os custos de infra-estrutura que, em termos de projeto de uma rede, leva grande parte dos recursos econômicos e também gera a grande maioria dos problemas de acesso.

Todos os motivos mencionados tornaram as redes sem fio tão populares que hoje a demanda dos usuários pelo uso dos recursos com maior banda e segurança tem se tornado um grande desafio para os desenvolvedores de soluções de hardware e software. O uso não controlado do mesmo espectro de banda não licenciada 2.4 GHz e 5Ghz gera mais ruído e interferência. Além disso, o conhecimento dos usuários das características das redes sem fio vem crescendo de tal forma que hoje varias vulnerabilidades vêm sendo exploradas por estes para permitir acesso não autorizado aos recursos destas redes. Outro fator que também

tem que ser considerado é que uma rede sem fio funciona num ambiente não comutado, isso significa que alguns usuários podem simplesmente ficar com grande parte dos recursos disponibilizados.

Outro complicador é o fato, no caso de redes sem fio corporativas, de não se ter informações dinâmicas do uso da rede, o que impede que os clientes possam se adaptar ao meio em constante mudança. Além disso, os administradores não conhecerem realmente qual é o perfil dos usuários destas redes e a real necessidade do uso das mesmas, dificultando a aplicação de algumas normas que permitam ter um nível de segurança razoável para as suas redes.

1.1 OBJETIVO DO TRABALHO

O objetivo deste trabalho é descrever os padrões, protocolos e arquitetura de redes sem fio com o intuito de se estabelecer uma base de conhecimento para definir um modelo de projeto, configuração e implantação de redes sem fio em grande escala, podendo ser aplicada a redes corporativas, redes acadêmicas ou redes públicas em comunidades.

1.2 ORGANIZAÇÃO DA MONOGRAFIA

A presente monografia está estruturada em 4 capítulos. O capitulo 2 apresenta conceitos básicos dos principais padrões para redes sem fio, dando ênfase ao padrão IEEE 802.11, mecanismos para implementação de segurança e modelos de gerência. No capitulo 3 é apresentada uma visão geral dos principais fabricantes de dispositivos para redes sem fio em escala media e grande, assim como alguns modelos de equipamentos. O capítulo 4 apresenta estruturação, dimensionamento de um projeto de rede sem fio, sua implantação, e sugestões para trabalhos futuros.

2 CONCEITOS BÁSICOS

Este capítulo apresenta os conceitos básicos do padrão IEEE 802.11 e os mecanismos de segurança implementados no padrão, assim como estruturas de gerência de redes sem fio. Estes conceitos são fundamentais para permitir uma compreensão do funcionamento de uma rede sem fio e suas vulnerabilidades. O capítulo foi dividido em 3 seções. A seção 2.1 apresenta uma visão do padrão IEEE 802.11; a seção 2.2 apresenta os mecanismos implementados no protocolo; e a seção 2.3 apresenta algumas estruturas de gerencia de redes sem fio.

2.1 PADRÃO 802.11

O padrão IEEE 802.11 foi criado em 1999. Este padrão basicamente especifica as camadas física e a sub-camada de controle de acesso ao meio (MAC). O padrão IEEE 802.11 sofreu varias extensões para poder implementar melhorias, estas extensões são listadas embaixo.

- 801.11 Oferece uma taxa de 1 ou 2 Mbps na banda de 2.4 Ghz. Uso de FHSS e DSSS;
- 802.11a - Oferece uma taxa de 54 Mbps na banda de 5 Ghz. Uso de OFDM;
- 802.11b - Oferece uma taxa de 11 Mbps na banda de 2.4 Ghz. Uso de DSSS;
- 802.11g - Oferece uma taxa de 54 Mbps na banda de 2.4 Ghz. Uso de DSSS e OFDM. Compatível com 802.11b;
- 802.11n - Oferece uma taxa de 65 a 600 Mbps nas bandas de 2.4 Ghz e/ou 5 Ghz. Uso de MIMO-OFDM.

2.1.1 Arquitetura

O padrão IEEE 802.11 define áreas de cobertura que são divididas em células.

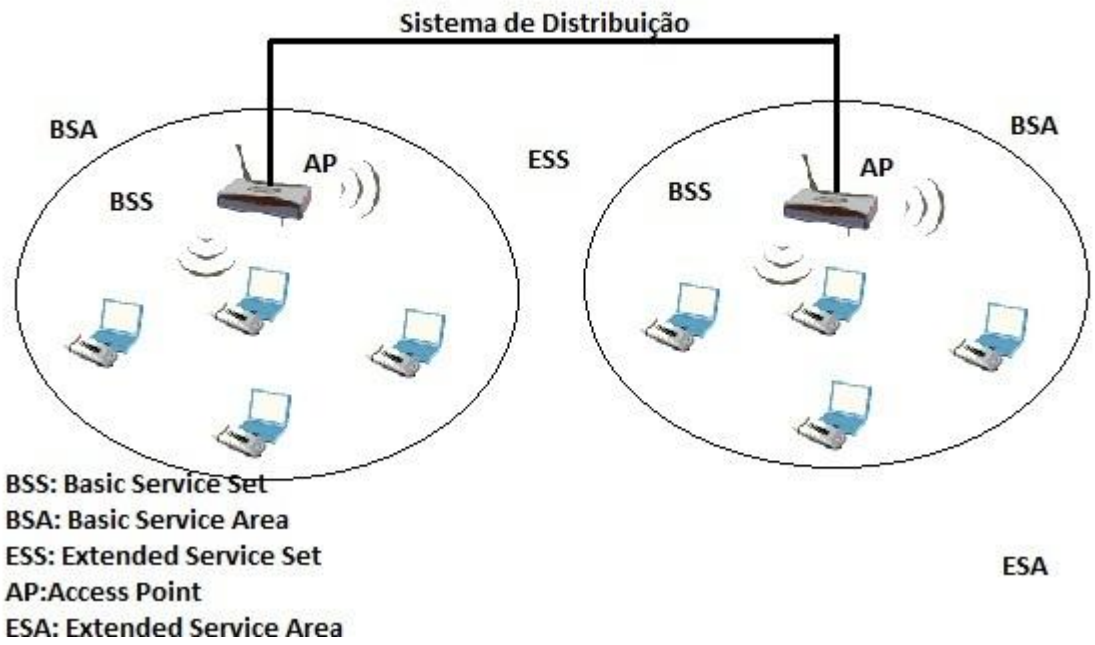


Figura 1- Arquitetura da Rede

BSA (*Basic Service Area*) são as células onde acontece a comunicação entre o conjunto de dispositivos sem fio conhecido como BSS (*Basic Service Set*). O tamanho destas células varia dependendo das características do meio e do hardware dos dispositivos responsáveis pela transmissão e recepção de informações. O BSS possui um identificador BSS-ID.

A interligação entre as BSAs é realizada através de distribuição conhecido como DS (*Distribution System)*, que permite também comunicação com redes cabeadas.

O AP (*Access Point*) é responsável pela conexão das BSAs ao sistema de distribuição, permitindo desta forma o acesso dos usuários a ele.

ESA (*Extended Service Area*) é o conjunto das BSAs interligadas por um DS através dos APs, compreende a área total de cobertura.

ESS (*Extended Service Set*) conjunto de estações formado pelos diversos BSSs e conectados através de um DS. Assim como o BSS, possui um identificador ESS-ID permitindo que as estações se movimentem entre os BSS de forma transparente (*roamming*).

2.1.2 Camada Física

A camada física proporciona vários serviços para a subcamada MAC, basicamente a camada se reduz a dois protocolos:

- O sistema PMD (*Polarization Mode Dispersion*), cuja função define as características e o meio de transmitir e receber através de um meio sem fio entre duas ou mais estações;
- O PLCP (*Physical Layer Convergence Protocol*), que define uma forma de mapear MPDUS (*MAC Protocol Data Units*) no formato de quadros passíveis de serem transmitidos ou recebidos entre diferentes estações através da camada PMD.

A comunicação entre MACs de diferentes estações se realiza através da camada física por meio de uma série de pontos de acesso ao serviço, onde a camada MAC invoca as primitivas de serviço.

Além destas camadas, pode-se notar a camada física de gerência. Nesta camada distingue-se a estrutura da MIB que contém as variáveis de gestão, os atributos, as ações e as notificações requeridas para gerenciar uma estação.

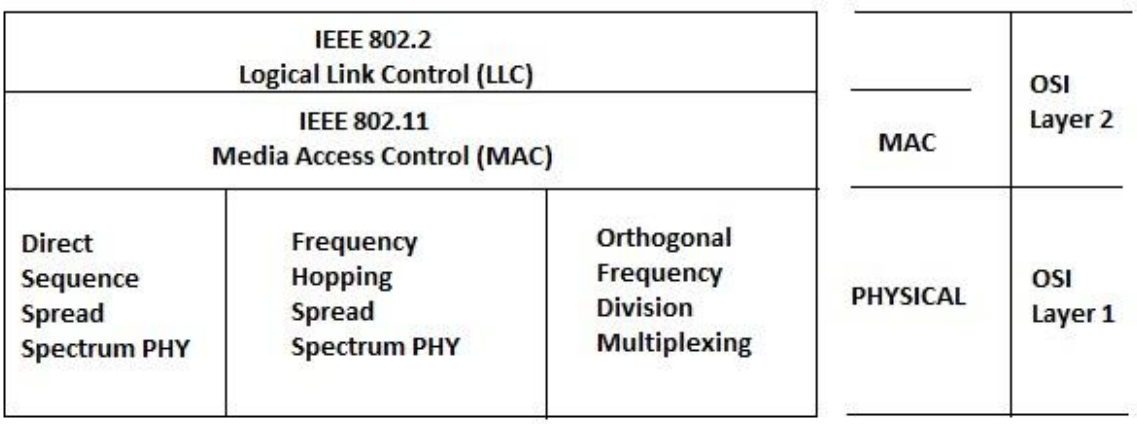


Figura 2 – Arquitetura IEEE 802.11

No padrão IEEE 802.11 vemos que três técnicas são amplamente usadas para transmissão de dados e sinalização de controle na camada física, que são: DSSS (802.11b), FHSS (802.11) e OFDM (802.11a, 802.11g e 802.11n). Cada uma delas apresenta características diferenciadas de robustez, atenuação e uso do espectro.

2.1.2.1 *Direct Sequence Spread Spectrum* (DSSS)

Esta técnica consiste na geração de um padrão de bits redundantes, chamado *sinal de chip*, para cada um dos bits que compõem o sinal de informação, e a posterior modulação do sinal redundante por meio de uma portadora de RF. Na recepção é necessário realizar o processo inverso para obter o sinal de informação original.

A sequência de bits utilizada para modular cada um dos bits de informação é a chamada sequência de *Barker*.

DSSS define dois tipos de modulação a serem aplicados no sinal de informação uma vez se sobrepõe o *sinal de chip* tal e como especifica o padrão IEEE 802.11: a modulação DBPSK (*Differential Binary Phase Shift Keying*) e a

modulação DQPSK (*Differential Quadrature Phase Shift Keying*) proporcionando velocidades de transferência de 1 e 2 Mbps respectivamente.

Nos Estados Unidos e na Europa a tecnologia DSSS opera na faixa de 2.4 GHz até 2.4835 GHz, quer dizer, uma largura de banda disponível de 83.5 MHz. Esta largura de banda total divide-se em 14 canais com uma largura de banda por canal de 5 MHz, dos quais cada país utiliza um subconjunto dos mesmos segundo suas normas reguladoras.

Em topologias de rede que contenham várias células adjacentes ou sobrepostas, os canais podem operar simultaneamente sem interferência quando a separação entre as frequências for de no mínimo 30 MHz. Isso significa que dos 83.5 MHz de largura de banda disponível, pode-se obter um total de 3 canais independentes que podem operar simultaneamente numa determinada zona geográfica sem interferência.

2.1.2.2 *Frequency Hopping Spread Spectrum* (FHSS)

Esta tecnologia consiste em transmitir uma parte da informação numa determinada frequência em um intervalo de tempo chamado *dwell time* que é inferior a 400 ms. Após este tempo muda-se a frequência e a transmissão continua. Desta forma cada quadro de informação é transmitido numa frequência distinta durante um intervalo muito curto de tempo.

Cada uma das transmissões numa frequência realiza-se utilizando uma portadora de banda estreita que vai mudando ao longo do tempo. Este procedimento é equivalente a realizar uma partição da informação no domínio do tempo.

A ordem dos saltos de frequência que o emissor deve realizar vem determinada segundo uma sequência pseudo-aleatória que se encontra definida em

tabelas conhecidas tanto pelo emissor como pelo receptor. A grande vantagem deste sistema com relação ao sistema DSSS é que, com esta tecnologia, pode-se ter mais de uma rede na mesma zona geográfica sem que existam interferências, isso considerando que não existam duas comunicações distintas utilizando a mesma frequência portadora num mesmo instante de tempo.

Se mantiver uma correta sincronização dos saltos entre os dois extremos da comunicação, o efeito global é manter um canal lógico através do qual se desenvolve a comunicação, embora os canais físicos estejam mudando.

O padrão IEEE 802.11 descreve esta tecnologia por meio da modulação em frequência FSK (*Frequency Shift Keying*), e com uma velocidade de transferência de 1 a 2 Mbps.

2.1.2.3 *Orthogonal Frequency Division Multiplexing* (OFDM)

É um tipo de transmissão que envia informações num conjunto de portadoras de diferentes frequências (multi-portadoras), quer dizer, divide um fluxo digital de alta taxa de bits em um esquema de múltiplos fluxos de baixa taxa de bits em paralelo. A geração contínua e a detecção de uma grande quantidade de portadoras que mantêm espaçamento apropriado para satisfazer a ortogonalidade de uma modulação OFDM (de forma a não gerar interferências entre os canais muito próximos), trás uma série de problemas que são resolvidos através de modulação e demodulação em tempos discretos mediante IDFT (*Inverse Discrete Fourier Transform*) e DFT (*Discrete Fourier Transform*).

Uma das grandes vantagens da modulação OFDM é a sua robustez com relação aos caminhos múltiplos, característica dos canais de radio difusão, com relação à atenuação e com relação à interferência de RF.

Este tipo de modulação consegue recuperar informações entre sinais com distintos retardos e amplitudes que chegam ao receptor.

2.1.3 Protocolo CSMA/CA

Como visto anteriormente, uma BSS é um agrupamento de dispositivos que se comunicam através de um meio sem fio dentro de uma BSA. Uma rede deste tipo trás uma serie de problemas no que se refere ao controle de acesso ao meio. Todos os dispositivos podem ouvir o meio. Isso, então, não é necessariamente uma vantagem se for considerado que um dispositivo poderia estar transmitindo ininterruptamente (que impediria outros dispositivos de transmitir). Outros problemas se referem à natureza das transmissões, que são omnidirecionais, e às colisões, que acontecem no rádio do receptor, pois não é prático usar uma frequência de rádio para transmitir e outra para receber. Finalmente, considerando-se que os dispositivos são moveis e têm que ficar ouvindo o meio o tempo todo, não sobraria muita carga nas suas baterias (alto consumo de energia).

A figura 3 pode ser usada para analisar esta situação. Tem-se 4 estações separadas em linha por distâncias de 100 metros entre elas. A potência dos rádios é suficiente para um alcance de 120 metros, e o protocolo de transmissão usado é o CSMA (as estações ouvem o canal antes de transmitir).

- Primeiro caso: estação escondida:
    - **A** deseja transmitir dados para **B** e, ao detectar o meio livre, inicia a transmissão;
    - **A** está transmitindo dados para **B** e agora **C** deseja transmitir para **B**;
    - **B** detecta o meio livre, pois **C** não escuta **A** porque está a uma distância de 200 m, e então começa a transmitir;

- O resultado é uma colisão em **B** que não é detectada por **A** nem por **C**;
- Esta situação é conhecida como problema da **estação escondida** (item b da figura 3).

- Segundo caso: estação exposta:
  - **B** deseja transmitir dados para **A** e, ao detectar o meio livre, inicia a transmissão;
  - **B** está transmitindo dados para **A** e agora **C** deseja transmitir para **D**;
  - **D** detecta que **B** está transmitindo para **A** e, assim, espera finalizar a transmissão para evitar uma colisão;
  - O resultado é que se poderia ter uma transmissão adicional sem interferência, porque **A** não pode ouvir **C** e **D** não poderia ouvir **B**, mas isso não acontece, reduzindo a eficiência do sistema;
  - Esta situação é conhecida como problema da **estação exposta** (item c da figura 3).

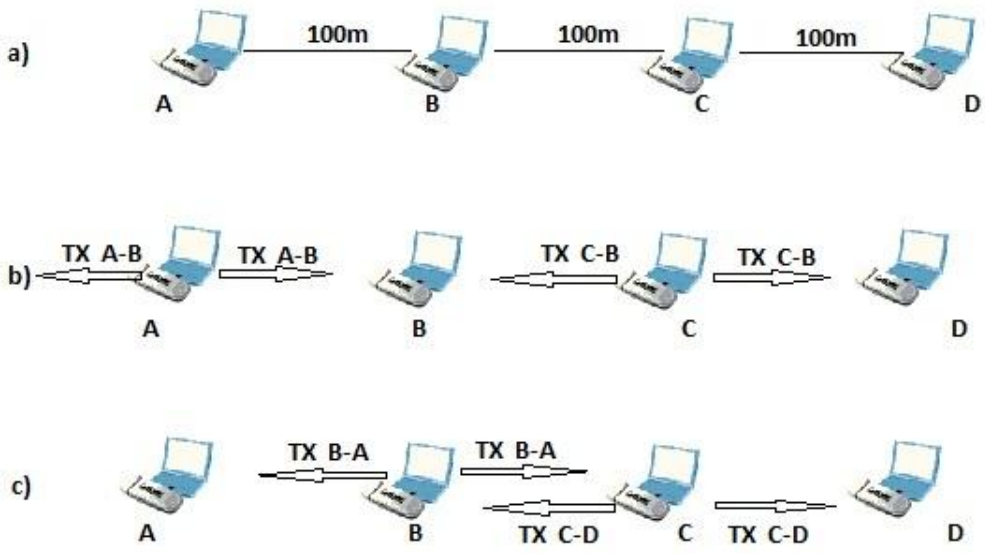


Figura 3 – Transmissão sem fio

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) é um protocolo que ouve o canal antes de iniciar uma transferência, e, se ele está ocupado, usa um algoritmo de *backoff* para ouvir novamente o canal até encontrá-lo livre. Uma vez que o canal está livre, resolve os problemas mencionados pelo uso de sinais de *handshaking*: envio de RTS (*Request To Send*) pelo transmissor, resposta com CTS (*Clear To Send*) pelo receptor, antes do envio dos dados pelo transmissor. RTS e CTS são pequenos quadros que têm a informação de quais são as estações transmissora e receptora, e quanto tempo durará a transmissão.

No caso da estação escondida, **A** ouve o canal e, se estiver livre, envia RTS para **B** indicando o comprimento do *frame* que deseja transmitir. **B** responde com CTS que também especifica o tamanho do quadro para receber. Neste ponto **C** captura a resposta de **B**, percebendo que vai haver uma transferência em que **B** atua como receptor. Assim, **C** permanece em silêncio durante a transmissão, pois sabe quanto tempo vai durar essa transmissão, uma vez que o tamanho do quadro e a velocidade da rede são conhecidos. Com isso, **A** envia dados para **B** e **C** pode transmitir para **B** quando terminar o tempo esperado para durar a comunicação.

No caso da estação exposta, **B** transmite um RTS para **A** indicando que quer enviar dados. Neste momento **C** descobre as intenções de **B** e **A** devolve para **B** um CTS. Enquanto isso, **C** captura o RTS mas não pode se comunicar com **D**, nem transmitir os dados porque primeiro deve enviar um RTS, mas o canal está ocupado pois ele deve esperar até **B** terminar. Embora o problema da estação escondida seja resolvido, ouvir o meio faz com que o problema não se resolva de forma eficiente.

2.1.4 Subcamada MAC

A arquitetura MAC do padrão IEEE 802.11 compõe-se de duas funcionalidades básicas: PCF (*Point Coordination Function*) e DCF (*Distributed Coordination Funtion*).

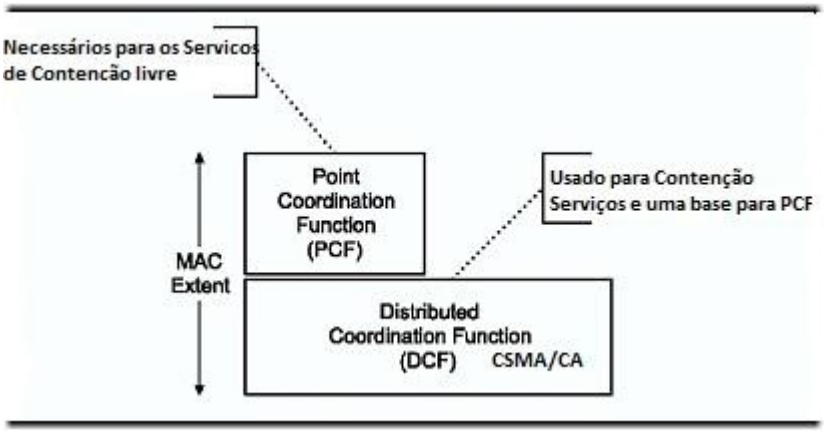


Figura 4 – Descrição funcional subcamada MAC

Na transmissão dos quadros existe um esquema de prioridade de acesso controlado pelo *Inter Frame Space* (IFS). Se o quadro for ACK, CTS ou fragmentos (a partir do segundo) usa um *Short IFS* (SIFS=28µs). Estações que operam segundo PCF usam *PCF IFS* (PIFS=78µs) que tem prioridade sobre MAC operando por DCF. Estações que operam segundo DCF usam *DCF IFS* (DIFS=128µs). Finalmente, quando uma transição não é bem sucedida o DCF usa *Extended IFS* (EIFS).

2.1.4.1 *Distributed Coordination Function* (DCF)

Dentro de um conjunto de BSS (*Basic Service Set*) a DCF determina quando uma estação pode transmitir e/ou receber unidades de dados de protocolo a nível MAC através do meio sem fio. No nível inferior da subcamada MAC encontra-se a DCF e seu funcionamento se baseia em técnicas de acesso aleatório por contingência ao meio.

O tráfego que se transmite sob esta funcionalidade é de caráter assíncrono porque esta técnica de contingência introduz retardos aleatórios e não tolerados pelos serviços síncronos.

O uso destas características pode ser resumido nos seguintes pontos:

- Utiliza MACA (CSMA/CA com RTS/CTS) como protocolo de acesso ao meio;
- Necessário reconhecimento de ACKs, provocando retransmissões no caso de não receber confirmação;
- Usa o campo duração que contém o tempo de reserva para transmissão e ACK, significando que todos os nós poderão ouvir quando o canal voltar a ficar livre;
- Implementa fragmentação de dados;
- Concede prioridade a quadros por meio do espaçamento entre quadros (IFS);
- Suporta Broadcast e Multicast sem ACKs.

2.1.4.2 *Point Coordination Function* (PCF)

Esta função é associada às transmissões livres de contenção que utilizam técnicas de acesso determinístico. O padrão IEEE 802.11 define uma técnica de interrogação circular desde o ponto de acesso até este nível. Esta funcionalidade foi pensada para serviços do tipo síncrono que não toleram retardos aleatórios no acesso ao meio.

O DCF e o PCF podem operar conjuntamente dentro de uma mesma célula ou conjunto básico de serviços dentro de uma estrutura chamada super quadro. Uma parte deste super quadro se adiciona ao período de contenção, permitindo ao subconjunto de estações que o requeiram transmitirem sob mecanismos aleatórios. Uma vez finalizado este período o AP se apodera do meio e inicia-se um período

livre de contenção que permite que as estações que utilizam técnicas determinísticas possam transmitir.

É importante ressaltar que o PCF é totalmente compatível com o DCF, do ponto de vista das estações o funcionamento é totalmente transparente. Desta forma uma estação se associará de modo que possa atuar no período PCF, declarando-se como *CF-Pollable*, ou, pelo contrário, situará seu NAV (*Network allocation Vector*) segundo as indicações do PCF.

Existe um nó organizador ou diretor, chamado ponto de coordenação ou PC. Este nó toma o controle por meio do método PIFS e envia um *CF-Poll* a cada estação que queira transmitir em PCF, permitindo-lhe a transmissão de um quadro. O PC manterá uma lista *Pollable* onde terá todos os dados das estações que se conectaram no modo *CP-Pollable*.

O nó utilizará um quadro para a configuração do super quadro, chamado *Beacon*, onde estabelecerá uma *CFRate* ou taxa de períodos de contenção. Porem este período de contenção poderá sofrer atraso por causa do meio estar ocupado.

2.2 MECANISMOS DE SEGURANÇA

Basicamente o padrão IEEE 802.11 estabelece 3 mecanismos de segurança:

- SSID (*Service Set Identifier*)
- MAC (*Media Access Control*)
- WEP (*Wired Equivalent Privacy*)

2.2.1 *Service Set Identifier* (SSID)

Permite identificar a rede sem fio. Na realidade este identificador tem como principal funcionalidade a segmentação da rede e não sua segurança.

O SSID tem que ser configurado em cada cliente sem fio. O procedimento mais comum é habilitar o SSID para anúncios da rede no formato Broadcast, desta forma o cliente sem fio através de um *scan* encontra a rede e se associa a ela. Do ponto de vista de segurança esta operação é uma vulnerabilidade, já que a rede está anunciando ao mundo que existe, o que pode permitir ataques direcionados.

2.2.2 *Media Access Control* (MAC)

O controle de acesso ao meio é outro mecanismo que permite a filtragem de clientes sem fio à rede. O processo cadastra os endereços MAC da camada 2 do modelo OSI na base de dados dos APs. Em uma estrutura de rede sem fio corporativa pode ser utilizado outro mecanismo de armazenamento centralizado, por exemplo, um Servidor Radius que faria a verificação destes endereços e permitiria o acesso aos recursos da rede. Estes mecanismos também têm falhas, alguns usuários maliciosos poderiam farejar a rede sem fio em modo promíscuo para detectar o endereço MAC e fazer o acesso utilizando o mesmo endereço (clonagem).

2.2.3 *Wired Equivalent Privacy* (WEP)

Outro mecanismo utilizado é o da criptografia, através de uso de chaves simétricas (compartilhadas). Através do uso destas chaves é possível prover autenticação e transmissão de dados segura. Este método também não se mostra muito seguro já que foram divulgadas varias falhas de segurança na implementação do algoritmo de criptografia.

2.3 ESTRUTURA DE GERÊNCIA

Em uma rede infra-estruturada sem fio, um cliente se associa a um AP dentro de uma BSS baseado na função de coordenação distribuída (DCF) que é um mecanismo de acesso ao meio que não garante a melhor utilização da rede.

Com relação a gerência, normalmente clientes fazem a escolha de conexão ao AP que tem o sinal mais forte mas que, às vezes, não é a melhor escolha. Pode acontecer de existir uma grande quantidade de clientes em torno desse AP, fazendo com que todos os usuários se conectem a ele. Assim a banda dividida entre todos os usuários ligados a esse AP será bem menor do que ficar conectado a outro AP com o sinal um pouco menor, mas com poucos usuários conectados (uso ineficiente de recursos). Para evitar este tipo de problema o cliente teria que fazer o controle da carga do sistema, ou outra entidade poderia monitorar esta situação. O IEEE criou um grupo de trabalho 802.11k para definir padrões de RMM (*Radio Resource Management* - Gerência de Recursos de Radio). O problema está em definir quem fará isso, o cliente ou o AP ou outro elemento de monitoração.

2.4 PROTOCOLOS DE ROTEAMENTO

Interligar conjuntos de Access Points (APs) numa única grande rede traz alguns complicadores como instalação de APs em pontos distantes da infra-estrutura (rede cabeada). Isso significa que tem que ser criada uma estrutura que permita usar os próprios APs como salto para chegar até um gateway comum da rede. Vários grupos no IEEE vêm trabalhando em soluções de protocolos de roteamento para redes sem fio, interligando ponto-a-ponto seus backbones (*adhoc*). Os mais importantes são listados a seguir.

2.4.1 *Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility* (LANMAR)

LANMAR [14] explora o fato de não ter sido estudado um método sistemático para a descoberta de grupos em movimento, partindo do principio de que grupos não são conhecidos com antecedência e que os nós se movimentam em grupos.

No caso dos nós mudarem de grupo, o reagrupamento é feito pela camada de aplicação que não necessariamente informa à camada de rede, desta forma a camada 3 tem que descobrir os grupos.

O protocolo propõe um esquema de descoberta dinâmica de grupos móveis afins, e usa essa informação de grupos para roteamento. Os grupos recém formados podem usar um esquema de roteamento local, e o roteamento entre os grupos pode usar um esquema de roteamento sob-demanda como *Ad hoc On-Demand Distance Vector Routing* (AODV) ou *Dynamic Source Routing* (DSR).

A descoberta dos grupos é baseada em observações do movimento relativo entre nós vizinhos, as mensagens são propagadas a uma distância de N saltos o que vai definir o tamanho dos grupos afins.

As informações de nós vizinhos ou companheiros de viagem (TCs) são armazenados numa tabela de roteamento local e identificados a cada nó durante uma Janela de Tempo.

Tendo informações da vizinhança atual, um grupo em movimento é estabelecido e é feito um acordo para a escolha do líder. Cada nó decide o vencedor da eleição segundo uma regra de decisão universal. O ID do líder eleito é reconhecido como o único ID do Grupo lógico formado. Se tiver uma mudança de líder, isto provoca também uma mudança do ID do Grupo.

Os líderes anunciam periodicamente informações das eleições de escolha de líderes juntamente com as rotas para eles. Não está definido o protocolo a ser usado para roteamento entre líderes, podendo ser um protocolo pró-ativo ou reativo.

2.4.2 *Load aWare Routing* (LWR) *Based on Local Information*

O roteamento ciente de carga é um protocolo de roteamento reativo. A principal preocupação deste protocolo é a interferência entre vizinhos. Para resolver o problema o protocolo propõe diminuir as transmissões redundantes e tenta usar as melhores rotas considerando informações locais como tamanho da fila e utilização do canal.

LWR [28] propõe derrubar pedidos de rota a nós fortemente carregados executando um controle de admissão de chamada, reduzindo assim o tráfego de rede redundante.

O estado do canal numa rede *Ad Hoc* pode ser definido como: INATIVO, TRANSMITINDO, RECEBENDO e COLISÃO. O LWR implementa algumas medidas de utilização do canal. Camada MAC monitora mudanças de status, e sempre que uma mudança acontece é acumulado o status prévio de duração do canal para cada um dos 4 estados. Desta forma é calculada periodicamente a utilização do canal em um determinado nó por unidade de tempo.

O canal é considerado ocupado quando sua utilização ultrapassar um limiar (determinado em pesquisa prévia dentro do desempenho padrão do IEEE 802.11) ou quando a probabilidade de colisão é grande.

Sob alta carga, alguns nós tendem a usar o canal compartilhado por um tempo maior que a sua fração justa (*Round Robin*). Este esquema tenta manter a utilização do canal igual entre todos os vizinhos.

O protocolo LWR baseia sua solução na fase de solicitação de rota, onde a lista de vizinhos é atualizada a cada chegada de pacotes. O nó intermediário recebe pacotes de requisição de rota e reenvia ou descarta o pacote baseado em *Time To Live* (TTL) e no nível corrente de carga. No caso de descarte do pacote isto é feito só quando a TTL expira ou quando o nível de carga é mais alto que um limiar.

Outra forma de descarte de pacotes de requerimento de rota é quando o nível de carga atinge um valor próximo do máximo. Este nível de carga é associado com a utilização do canal, tamanho de fila atual, número de vizinhos ativos e valor do tempo de *backoff*, O tempo de *backoff* representa o número de falhas na transmissão de pacotes de dados, estando relacionado à probabilidade de colisão.

2.4.3 *Location-Aided Routing* (LAR) *in Mobile Ad Hoc Networks*

O LAR [12] é um protocolo de roteamento reativo que sugere uma aproximação dos nós para diminuir o *overhead* na descoberta de rotas, utilizando informações de localização para os hosts móveis. Informações de localização usadas pelo LAR podem ser providas por Sistemas de Posicionamento Global (GPS). Em [12] assume-se que cada host conhece sua localização atual.

O protocolo implementa o roteamento através de dois algoritmos: Zona Esperada e Zona de Requisição.

- **Zona Esperada**

  Neste algoritmo o nó origem (O) sabe que o nó destino (D) está em um local L no tempo t0 e que o tempo atual é t1. Desta forma o nó O pode determinar a zona esperada se sabe que o nó D viaja numa velocidade media v. Assim, o nó O assume a zona com raio v(t1-t0) centrado em L (Figura 5-a).

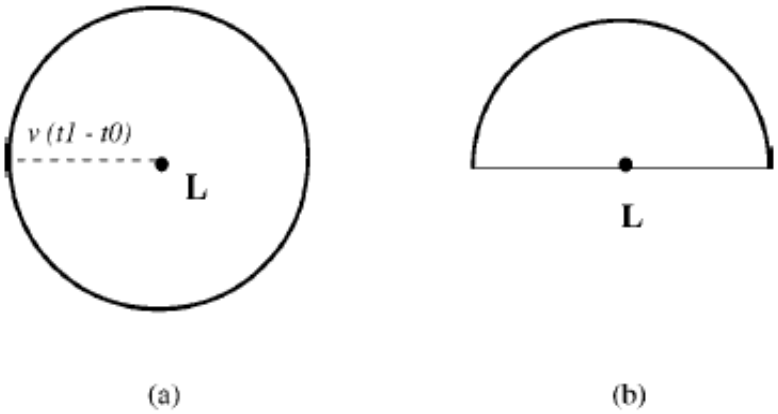


Figura 5 – Zonas esperadas

Se o nó O não conhece previamente a localização do nó D, ele assume toda a região como Zona Esperada. Se o nó O sabe que o destino está se movimentando numa direção, pode diminuir a expectativa de zona (Figura 5-b).

- **Zona de Requisição**

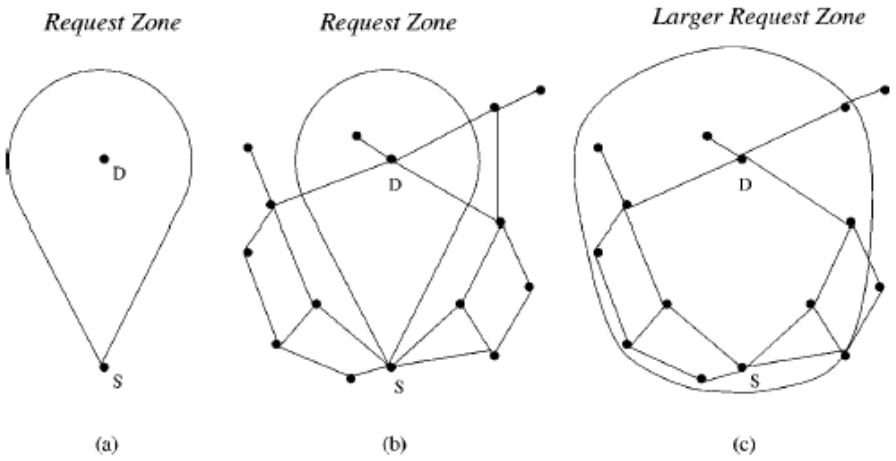


Figura 6 – Zonas de Requisição

Neste caso o nó origem (O) faz inundação definindo (implícita ou explicitamente) uma zona de requisição de rota (Figura 6-a). O nó O só faz requerimento de rota se pertencer à zona de requisição. Para aumentar a probabilidade da requisição de rota alcançar o nó D, a Zona de Requisição deveria incluir a Zona Esperada. Adicionalmente a zona de requisição também pode incluir outras regiões ao redor da zona de requisição.

Há duas razões para a requisição de rotas incluírem outras regiões: quando a Zona Esperada não inclui o nó O, um caminho do nó O para o nó D tem que incluir os nós fora da Zona Esperada (Figura 6-b); se uma rota não é descoberta no intervalo satisfatório, o protocolo pode fazer a requisição numa Zona de Requisição Expandida (Figura 6-c).

2.4.4 Bandwidth-Efficient Routing Protocol for Mobile Ad Hoc Networks (RDMAR)

RDMAR [13] é um protocolo de roteamento reativo concebido a partir de críticas a protocolos como AODV, DSR, TORA, ZRP e protocolos baseados em GPS. Introduz a chamada de Micro-Descoberta de Distância Relativa (RDM) com o objetivo de ter um roteamento com baixo *overhead* e alto *throughput*.

O protocolo usa um mecanismo que limita o alcance de busca de rota em favor do custo de mensagens de requerimento de rota por inundação em toda a área da rede sem fio. Isto é alcançado estimando a distância relativa entre a origem e a busca de rota do destino, assim restringindo o alcance do descobrimento de rota dentro da área centrada no descobrimento de rota do nó de origem e com raio máximo, o qual é igual à distância relativa estimada.

Para manutenção de caminhos ativos é proposto um algoritmo distribuído onde duas heurísticas são consideradas: se a distância relativa do nó chamado é menor ou igual que a do nó chamador, então RDM será aplicado para localizar o reparo da rota com falha na região da rede onde a falha aconteceu; caso contrário o nó informa ao nó chamador sobre a falha na entrega de chamada por este caminho.

Chamadas são roteadas entre as estações da rede usando as tabelas de roteamento armazenadas em cada estação, onde cada nó é tratado como host e como nó de armazenamento e envio. Cada tabela de roteamento lista todos os

destinos alcançáveis e também informações adicionais de roteamento sobre cada destino.

Basicamente, o RDMAR possui dois algoritmos principais: algoritmo de descoberta de rota e algoritmo de manutenção de rota.

- **Descoberta de Rota (RDisc)**

  Pode se inundar toda a rede com um pedido de rota ou limitar o pedido numa região local desde que se tenha um bom modelo de previsão. Se na resposta ao pedido, uma nova rota para o destino chegar à origem, compara-se o número de saltos e sua Distancia Relativa com a rota na tabela de roteamento. Se a nova Distância Relativa for menor a nova rota é selecionada. Se não existia uma rota para esse destino, a nova rota é aceita cegamente.

- **Manutenção de rotas**

  Um nó intermediário, sob recepção de pacotes de dados, primeiro processa os cabeçalhos de roteamento e então reenvia os pacotes para o próximo salto. Se um nó intermediário não pode enviar pacotes por algum problema, tenta várias retransmissões até um número máximo. Se o fracasso persiste o nó intermediário inicia uma fase de RDM com alcance de propagação mínimo. Se o nó intermediário está perto do destino inicia um RDM como acima, e se está perto da origem envia uma Notificação de Fracasso (NF).

  Durante a fase de NF cada nó intermediário que recebe um pacote para reenvio mantém uma lista de todos os vizinhos que usam este nó como rota para alcançar o destino. Esta lista, que é chamada Lista de Dependentes, é importante porque a necessidade de difusão é eliminada enviando NF só para os nós que de fato usam este caminho falho, assim eles podem remover esta rota de sua tabela de roteamento.

2.4.5 *Adaptive Wireless Path* (AWP)

Embora este protocolo de roteamento apareça como proprietário da Cisco [2], se encontra na linha de trabalho do IEEE como norma 802.11s. Ele permite que um conjunto de dispositivos sem fio estabeleçam entre si uma rede sem fio *multi-hop* com capacidade de auto configuração. Estas redes que têm uma topologia em malha, são conhecidas como *Redes Wireless Mesh* e usam o mesmo principio das redes MANET (*Móbile Ad-hoc Networks Working Group*). A diferença é que ao invés de IP usam como endereço o número MAC da camada 2 do modelo OSI.

A descoberta de caminhos pelo protocolo IEEE 802.11s é feita através da adaptação de protocolos de roteamento *ad-hoc*, podendo também se interligar a redes estruturadas através de *gateways*. A vantagem deste protocolo é que permite a cobertura de grandes áreas onde um conjunto simultâneo de usuários pode usar sempre a melhor rota para envio e recepção de dados.

Outra vantagem do protocolo é a grande mobilidade, permitindo o acesso à Internet para dispositivos padrões Wi-Fi em áreas abertas como grandes corporações ou Universidades, assim como segurança de Campi Universitário interligando câmeras Wi-Fi.

3 PROPOSTA DE CONFIGURAÇÃO

Para permitir formular uma proposta de configuração confiável de uma rede IEEE 802.11 serão analisados estudos de caso com redes corporativas e domiciliares. Alguns pesquisadores já questionaram a fragilidade de mecanismos de segurança utilizados em redes sem fio [1], estas situações têm que ser consideradas num estudo de configurações sujeitas à falha.

Existem vários fabricantes de dispositivos que desenvolvem soluções para redes corporativas, entre eles podemos mencionar: Cisco, Alvarion, 3com, Arubanetworks, Nortel, Avaya e outros.

Numa segunda instancia será avaliada a experiência de alguns administradores de rede com vivencia em redes sem fio e as metodologias utilizadas para implementação de segurança e gerencia.

As coletas destas variantes aplicadas em campo permitirão validar ou não uma proposta de configuração se não segura pelo menos com um alto grau de confiabilidade em redes IEEE 802.11.

4 IMPLANTAÇÃO

A seguir coloca-se o roteiro seguido para a implantação da Rede Wireless *Mesh* no Campus Praia Vermelha da UFRJ.

4.1 MOTIVAÇÃO

O principal motivador para a implantação da Rede sem fio no Campus Praia Vermelha da UFRJ foi a impossibilidade de ampliar a rede cabeada em varias áreas por problemas de dutos saturados, além da dificuldade da passagem de nova infra estrutura devido à antiguidade dos prédios que são considerados pelo IPHAN (Instituto do Patrimônio Histórico e Artístico Nacional) patrimônio histórico e, por tanto, tombados, o que não permitem abrir ou furar paredes. Soma-se a isto a iniciativa tomada por várias unidades de instalar APs com segurança fraca, e na grande maioria, sem segurança quando instalados por usuários dentro das salas e sem o conhecimento da administração local, o que trouxe vários problemas de acesso não autorizado às redes internas.

Um projeto de rede sem fio para o Campus com administração centralizada apresenta facilidade e rapidez de implantação, além de permitir uma cobertura de rede em todas as áreas do campus para professores, alunos, funcionários e visitantes. A maior característica da rede sem fio é a sua escalabilidade, o que permite, uma vez instalada, seu crescimento sem maiores complicações, além do baixo custo de implantação e flexibilidade de conexão, permitindo chegar com sinal onde uma estrutura cabeada não consegue.

Uma das características singulares do campus é que permite a instalação de APs externos para prover uma maior cobertura de rede em campo aberto (em torno de 116.085m^2), por outro lado existem vários prédios antigos nos quais a cobertura

da rede através de APs externos é limitada por vários fatores como paredes grosas que chegam a quase 1m de espessura.

Todas estas limitações e impedimentos fizeram com que o Projeto Wireless *Mesh* Campus Praia Vermelha fosse um grande desafio.

4.2 ARQUITETURA DA REDE

Como visto anteriormente, as vantagens do uso de uma rede sem fio com gerência centralizada são inúmeras. Seguindo essa linha de raciocínio, o projeto do campus Praia Vermelha foi baseado no padrão IEEE 802.11 a/b/g com gerência centralizada. Foi usado um controlador de rede local sem fio, WLC (*Wireless LAN Controller*) e APs com capacidades limitadas denominados LWAP (*Lightweight Acces Point*) que não permitem o seu uso sem o WLC.

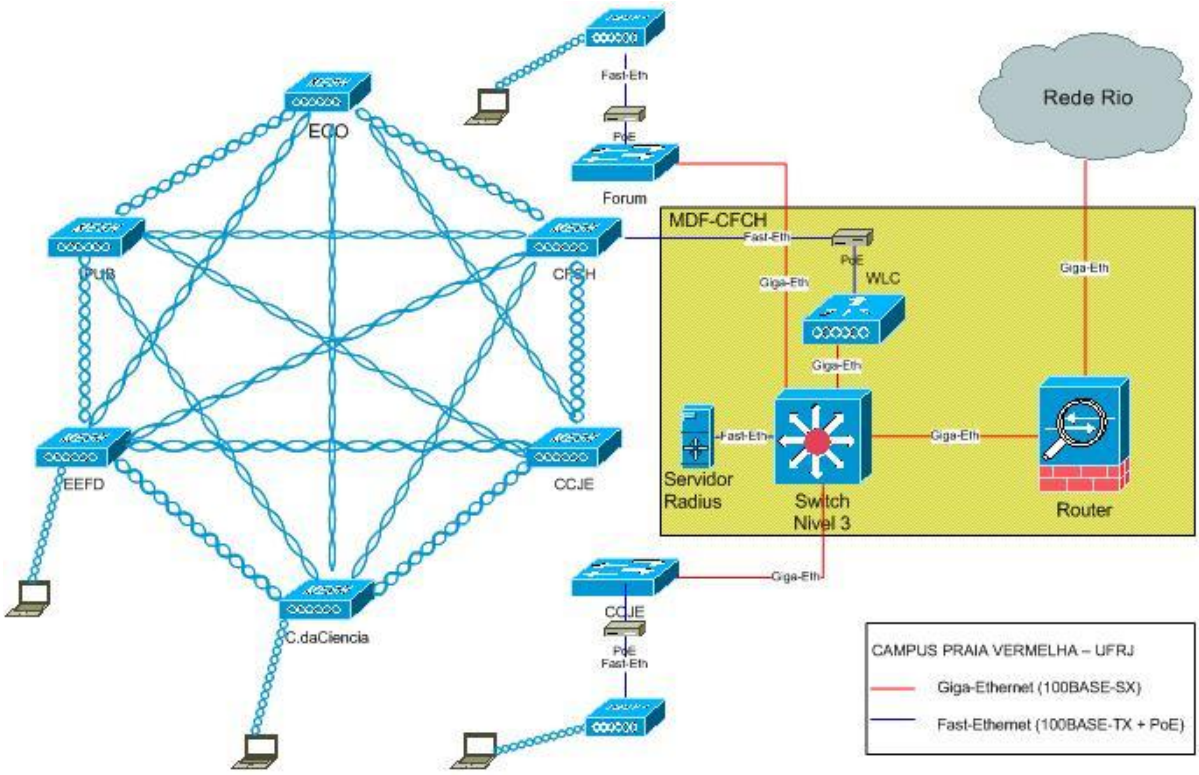


Figura 7 - Topologia da Rede

Os modelos de APs escolhidos atendem aos seguintes requisitos:

- potência, resistência e capacidade de associação em malha,
- suporte a PoE (*Power over Ethernet*),
- segurança,
- características que permitam aos equipamentos passar desapercebidos em áreas com limitações de arquitetura, como no Palácio Universitário (prédio tombado).

Os equipamentos da rede sem fio projetada para o Campus Praia Vermelha foram:

- controladores de rede local sem fio (WLC)
  - WLCs redundantes: no caso de falha de um dos controladores o outro assume a gerencia da rede;
  - foi instalado também um mecanismo de fonte redundante nos WLCs para superar problemas de surto de energia ou pane elétrica no equipamento;
  - as características de gerencia e segurança deste equipamento será abordado mais à frente.
- servidor de nomes (DNS) e Servidor para autenticação, autorização e contabilidade (AAA) para permitir um acesso controlado e seguro à rede
  - estes servidores são baseados no Sistema Operacional Linux.
- pontos de acesso com capacidades limitadas (LWAPs) distribuídos interna e externamente segundo diretivas de projeto.

4.2.1 CONTROLADORES DE REDE LOCAL SEM FIO (WLC)

O WLC foi desenvolvido para gerenciar redes sem fio corporativas. Este equipamento permite criar e implementar políticas de segurança e prevenção contra

intrusos, tanto por via direta dos clientes ou através de outros APs estranhos à rede (*rogue* APs).

Permite gerencia de RF automática, de tal forma que pode aumentar ou diminuir a potência dos LWAPs segundo necessidades que podem ser: distância de outros pontos de acesso; saturação das áreas de cobertura (células) dos APs, permitindo fazer um balanceamento de carga transferindo os usuários para outros APs menos sobrecarregados; ou simplesmente no caso de falha de um dos LWAPs.

Podem ser implementadas políticas de qualidade de serviço (QoS) permitindo dar prioridade ao tráfego diferenciado, como voz no caso de uso com VoIP, vídeo, ou simplesmente para grupos de usuários considerados prioritários. A integração e comunicação em grande escala com os LWAPs são feitas de forma simples, podendo usar protocolos de camada 2 (ethernet) ou 3 (IP) do modelo OSI, através de LWAPP (*Lightweight Acces Point Protocol*) visto anteriormente.

O modelo de WLC escolhido para o projeto possui 2 portas Gigabit Ethernet (IEEE 802.3ae) e permite controlar os APs via LWAPP. Além do equipamento possuir um software de gerência de recursos de radio (RRM). Este software usa um algoritmo que permite detectar e adaptar a rede às mudanças em tempo real, conseguindo, assim , corrigir, otimizar e criar suas próprias configurações.

4.2.2 CARACTERÍSTICAS DOS EQUIPAMENTOS

(A) Access Point Cisco Aironet 1500 Series

Este equipamento tem uma arquitetura Wireless LAN centralizada e foi desenvolvido para uso externo, permitindo a sua operação em áreas com temperatura de até 55^{o}C, assim como suporte a intempéries (IP66) e corrosão

(NEMA4). Suporta topologia *Wireless Mesh*, ponte ponto-a-ponto ou ponte ponto-a-multiponto. Vem com duas antenas externas:

- Antena Omnidirecional operando na frequência de 2,4 GHz, 5,5dBi com tecnologia IEEE 802.11b/g e capacidade de enlace para acesso dos clientes a uma distância de 90 a 150m. No modo ponte recomenda-se até 4 saltos entre o AP mais distante e o ponto de concentração estruturado.

Figura 8 - Access Point 1500AG Series

- Antena Omnidirecional operando na frequência de 5 GHz, 7,5dBi com tecnologia IEEE 802.11a para enlaces de *Backbone Wireless* com capacidade de atingir distâncias entre 300 e 1200m. Neste caso recomenda-se um salto entre o AP mais distante e o ponto de concentração estruturado.

(B) Access Point Cisco Aironet 1130 Series

Este equipamento tem uma arquitetura Wireless LAN centralizada, mas, diferentemente do AP 1500 Series, também pode trabalhar no modo autônomo. Foi desenvolvido para uso interno suportando temperaturas de ate 40^{o}C, permitindo operação simultânea com duas antenas embutidas:

Figura 9 - Access Point 1131AG Series

- Antena Omnidirecional operando na frequência de 2,4 GHz, 3,0dBi com tecnologia IEEE 802.11b/g (modulação CCK e OFDM) e capacidade de enlace para acesso dos clientes a uma distância de 30m com 54 Mbps. Pode operar com 11 canais sendo 3 não sobrepostos. Possui uma porta para Uplink 10/100 BaseT Ethernet.
- Antena Omnidirecional operando na frequência de 5 GHz, 4,5dBi com tecnologia IEEE 802.11a (modulação OFDM) e capacidade de enlace para acesso dos clientes a uma distância de 24m com 54 Mbps. Pode operar com 12 canais sendo que pode ter acima de 19 não sobrepostos. Possui uma porta para Uplink 10/100 BaseT Ethernet.

(C) Access Point Cisco Aironet 1240 Series

Este equipamento tem uma arquitetura Wireless LAN centralizada, como o modelo 1130AG, pode trabalhar no modo autônomo, podendo ser configurado também como ponte. Foi desenvolvido para uso interno suportando temperaturas de até 55^{o}C. Permite operação simultânea com quatro antenas externas 2,4 GHz com conector dual e 5 GHz com conector dual:

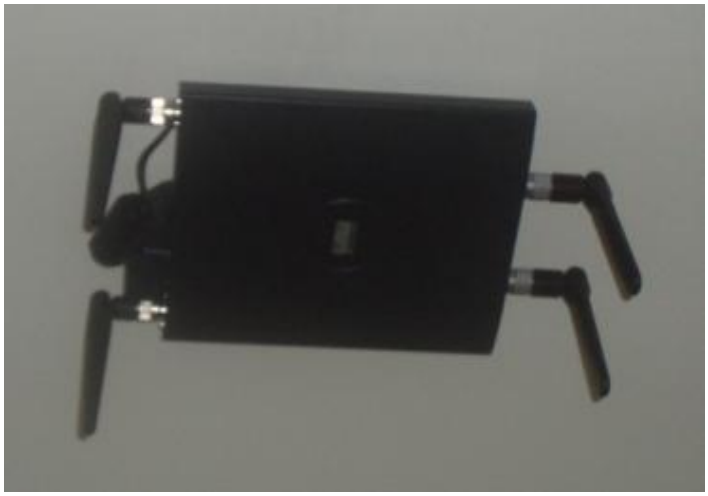


Figura 10 – Access Point 1240AG Series

- Antena Omnidirecional operando na frequência de 2,4 GHz, 2,2dBi dipolar com tecnologia IEEE 802.11b/g (modulação CCK e OFDM) e capacidade de enlace para acesso dos clientes a uma distância de 32m com 54 Mbps. Pode operar com 11 canais sendo 3 não sobrepostos. Possui uma porta para Uplink 10/100 BaseT Ethernet.
- Antena Omnidirecional operando na frequência de 5 GHz, 3,5dBi dipolar com tecnologia IEEE 802.11a (modulação OFDM) e capacidade de enlace para acesso dos clientes a uma distância de 26m com 54 Mbps. Pode operar com 12 canais sendo 12 não sobrepostos. Possui uma porta para Uplink 10/100 BaseT Ethernet.

Todos os APs podem ser alimentados com PoE (IEEE 802.3af) de 48 VDC; possuem capacidade de suportar taxa de dados em IEEE 802.11a de 6, 9, 12, 18, 24, 36, 48 e 54 Mbps; em IEEE 802.11b/g de 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 e 54 Mbps. A configuração padrão dos APs foi feita no modo LWAP, todos com suporte a LWAPP para comunicação com o dispositivo de gerência centralizada.

(D) Wireless LAN Controller 4400 Series (WLC)

Este equipamento permite uma gerência centralizada e automática com comunicação em tempo real entre os LWAPs e o controlador. Possui também um sistema de prevenção contra intrusos (IPS), além de capacidade de gerência de RF, que permite controlar a potência dos LWAPs segundo as necessidades. Dependendo do modelo de cada controlador pode suportar de 12 até 100 LWAPs, além da capacidade de empilhamento entre controladores. Pode ser usada redundância de fonte de alimentação e de controlador.

O modelo adotado no Projeto *Wireless Mesh* Praia Vermelha possui duas portas Uplink 1000Base-X. Por ser um equipamento para ambiente interno, suporta temperaturas de até 40^{o}C, permindo gerência via Web (HTTP/HTTPS) e também através da interface de linhas de comando (telnet, SSH e porta serial), assim como SNMP. É possível criar contas de usuários no próprio controlador para autenticação baseada na Web, mas o verdadeiro potencial está na capacidade AAA que pode ser feita através de *Radius* e todas suas extensões. Outra grande vantagem é a atualização automática de todos os LWAPs feita assim que o controlador é atualizado.

Figura 11 – Wireless LAN Controller 4400 Series

4.2.3 DIMENSIONAMENTO DA REDE

Neste projeto foram considerados 2 tipos de dimensionamento baseados em testes de acesso aos recursos da rede: foi considerado um sinal mínimo de 70 dBm para transmissão e recepção de dados e um número médio de 20 usuários por AP.

- Áreas Externas: A área externa do Campus Praia Vermelha tem em torno de 116.085m^2. Foi definido para esta área o uso de 6 (seis) **Access Point 1500AG Series** pela sua característica de uso em ambientes externos, potência de sinal e resistência a fatores como corrosão e calor. Desse total 4 estão instalados e funcionais.
- Áreas Internas: Neste caso foram consideradas as áreas com maior concentração de usuários e sem cobertura externa. Na utilização dos APs foi definido o uso dos modelos **Access Point 1131AG Series** com características decorativas em áreas tombadas pelo IPHAN (Palácio Universitário). Nos prédios mais novos foram usados os modelos **Access Point 1240AG Series**. Do total de 20 APs internos foram instalados 4, sendo 3 APs modelo 1130AG no Palácio Universitário e 1 AP modelo 1240AG no prédio do Instituto de Psicologia.

4.2.4 POSICIONAMENTO DOS APs

Assim que foi definido o perímetro do Campus, foram definidas áreas de cobertura externa com interseção entre células de 20%. Nas áreas internas foi considerado o mesmo padrão. Foi definido para os usuários o uso da banda de frequência de 2,4GHz e para o *backbone* o uso da frequência de 5GHz.

O posicionamento dos APs com sua área de atuação pode ser visto na figura 12.

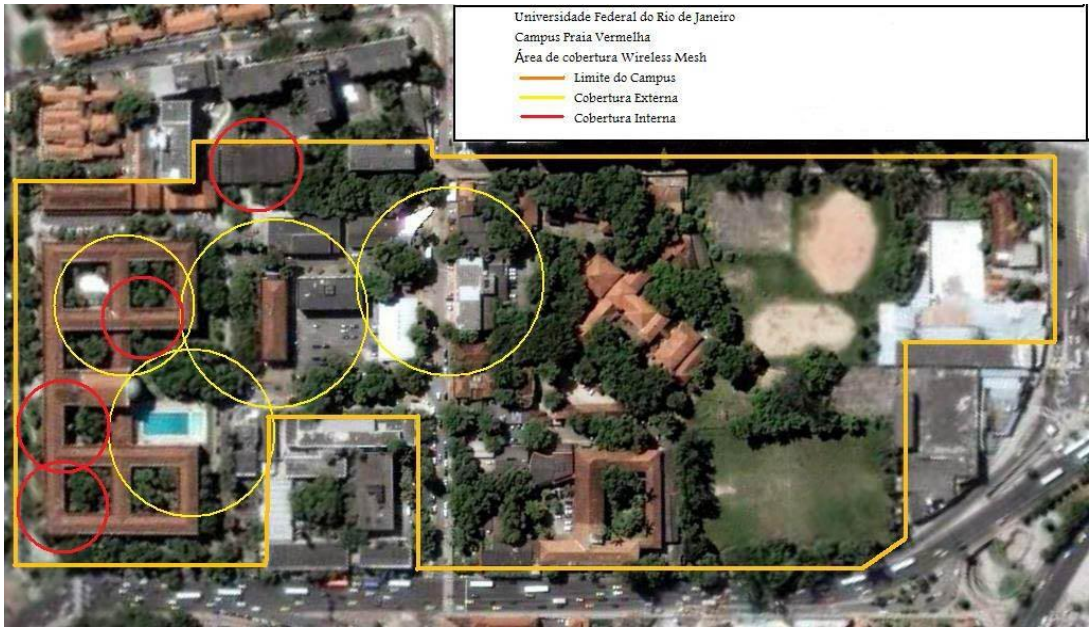


Figura 12 – Posicionamento dos APs

Na figura 12, os círculos amarelos representam a área de cobertura externa com uso dos APs modelo 1500AG, os círculos vermelhos representam a área interna com uso dos APs modelos 1131AG e 1242AG. Ainda está prevista a instalação de mais 16 APs em áreas internas do Campus.

4.2.5 MOBILIDADE

Pelas suas características (rede *wireless mesh*) os APs, assim como os usuários da rede, são monitorados através de uma estrutura centralizada. Em caso de pane em algum AP a gerência centralizada aumenta a potência do sinal no AP mais próximo para conseguir absorver os usuários do AP parado, permitindo, desta forma, uma redundância de cobertura. Embora a maioria dos usuários se conecte à rede em lugares fixos, é possível que usuários em movimento permaneçam conectados à rede através do uso de *roamming* implementado por esta solução.

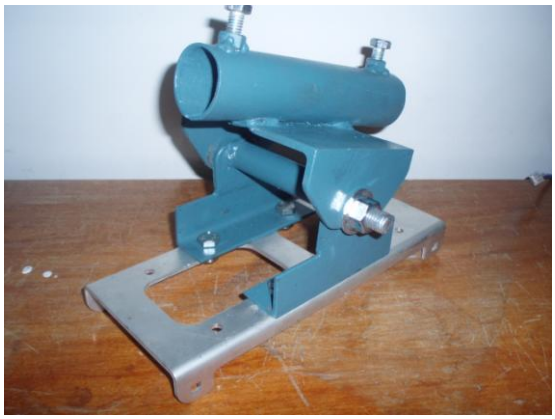
4.2.6 SEGURANÇA

Numa primeira fase foi definida a criação genérica de contas de usuários no próprio WLAN *Controller*, permitindo a autenticação com a mesma conta e senha de até 8 usuários simultaneamente. O usuário consegue se conectar à rede sem fio sem autenticação previa, recebendo endereço IP do Servidor DHCP. Na primeira tentativa de acesso à internet o usuário é redirecionado para uma pagina Web onde é solicitada a sua autenticação. Uma vez validada a senha o acesso aos recursos da rede é liberado.

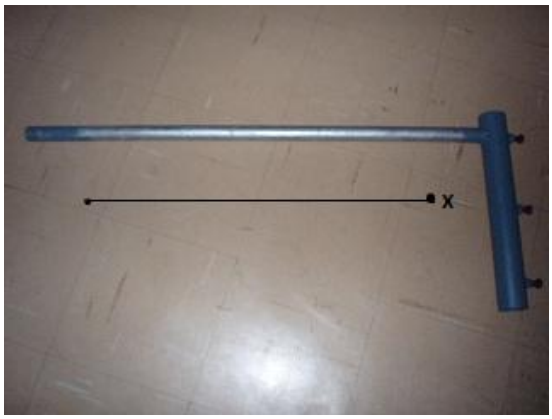
Numa segunda fase pretende-se deixar a autenticação a cargo dos administradores das redes locais, via protocolos como LDAP e aplicações de software livre e de código aberto baseadas em Unix, como o *Freeradius*.

4.2.7 INSTALAÇÃO DE ANTENAS

Pelas dificuldades observadas na realização do *Site Survey*, principalmente com relação ao posicionamento ou altura exata das antenas, projetou-se uma solução de postes modulares que permitissem a instalação das antenas numa área com base fixa, mas que permitisse movimentar os APs nos eixos XYZ (acima, abaixo e aos lados).



(a)



(b)

(c)

(d)

Figura 13 – Instalação de Antenas

Foi projetado um mecanismo (figura 13-a) que pudesse segurar o AP modelo 1500AG e ao mesmo tempo permitir a movimentação no eixo x em relação ao primeiro módulo do poste (figura 13-b). A figura 13-c mostra os dois primeiros módulos já montados. A figura 13-d mostra a estrutura completa já montada, incluindo o AP 1500AG.

5 CONCLUSÕES

Embora o IEEE seja responsável pela padronização de normas que são implementadas nas redes sem fio, na grande maioria dos casos é o mercado que de fato sai na frente na aplicação de soluções para redes sem fio. Isso ocorre pelas próprias necessidades do mercado que não pode esperar por formalizações.

Viu-se que a solução implementada para as redes sem fio consideradas como corporativas ou Campus (onde existe uma grande quantidade de usuários) passa necessariamente por uma estrutura de gerência centralizada. Só desta forma é possível acompanhar todas as variáveis que acompanham uma solução deste porte.

A propagação em larga escala de redes sem fio em frequências abertas trouxe uma série de problemas que irão simplesmente piorar com o tempo, como a interferência entre elas. Desta forma, embora redes sem fio se apresentem como solução aos problemas enfrentados em infra-estrutura, não se pode considerar esta como um substituto às redes cabeadas, mas como uma alternativa para contornar problemas que impeçam o uso da mesma.

6 REFERÊNCIAS

[1] Borisov, N., Goldberg, I., Wagner, D. (2001) “Intercepting mobile communications: The insecurity of 802.11”, In Proceedings of MOBICOM 2001.

[2] Cisco Sistem (2007), http://www.cisco.com, Fevereiro/2007

[3] Crow, B.; “Performance Evaluation of the IEEE802.11 Wireless Local Area Network Protocol”- Cap.2, Msc Thesis, DECE-University of Arizona,1996.

[4] Ergen, Mustafa “IEEE 802.11 Tutorial” ergen@eecs.berkeley.edu University of California Berkeley, June 2002

[5] Estándares IEEE http://standards.ieee.org/db IEEE802.11 Wireless LAN Medium Access (MAC) and Physical Layer (PHY) IEEE802.11b Higher-Speed Physical Layer Extension in the 2.4GHz Band

[6] IEEE Comitê de padronização de LAN (1999) “Information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requerements – IEEE 802.11”, IEEE Computer Society.

[7] Nahrstedt, K., e Steinmetz, R., Resource management in networked multimedia systems. IEEE Computer (maio de 1995), 52_63

[8] Wireless Network Station Connection Policy – The University of Sheffield

[9] WI_FI Alliance (2007), http://www.wi-fi.org, Fevereiro/2007

[10] Dynamic Group Discovery and Routing in Ad Hoc Networks - Xiaoyan Hong ,Mario Gerla - Proceedings of the First Annual Mediterranean Ad Hoc Networking Workshop (Med-hoc-Net 2002), Sardegna, Italy, Sept. 2002 http://www.cs.ucla.edu/NRL/wireless/uploads/med-hoc-net2002-hxy.pdf

[11] A Load aWare Routing (LWR) based on Local information. http://www.cs.ucla.edu/NRL/wireless/uploads/pirmc01.doc

[12] Location-Aided Routing (LAR) in mobile ad hoc networks http://theory.lcs.mit.edu/classes/6.895/fall02/papers/Vaidya/winet-p307-ko.pdf

[13] RDMAR: A bandwidth-efficient Routing Protocol for Mobile Ad hoc ... http://www.ee.surrey.ac.uk/Personal/G.Aggelou/PAPERS/rdmar.pdf

[14] LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility http://www.cs.ucsb.edu/~ravenben/papers/sensors/Lanmar.pdf