# Aplicação de Sistemas Wireless em Sistemas de Supervisão e Controle em Subestações

M. Nakashima, A. R. Figueiredo, S. Gambini, CTEEP, J.A. Jardini, L.C. Magrini e C. A. B. Pariente, USP.

***Resumo*-Este trabalho relata a experiência obtida no desenvolvimento e implementação de um projeto de pesquisa e desenvolvimento visando estudar a aplicação de sistemas de comunicação sem fio em subestações. Foram analisadas as diferentes tecnologias sem fio disponíveis e optou-se pela utilização de equipamentos de padrão IEEE 802.11a/b/g. A aplicação objetivou a substituição dos cabos de comunicação serial entre o edifício de comando e controle diferentes pontos de cole-tas de dados na área energizada de uma subestação de EHV, analisando diversos parâmetros de interesse, como a relação sinal ruído (SNR, do inglês Signal Noise Ratio). Além da análise dos padrões atualmente disponíveis e posterior seleção daquele considerado mais adequado, o projeto procurou ainda identificar condições de interferências e o impacto do volume de dados no desempenho da ligação wireless.**

***Palavras-chave*—wireless, SNR, SL, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.**

## I. Introdução

Este documento descreve a metodologia empregada no desenvolvimento do projeto "Aplicação de Sistemas Wireless em Subestações de HV", o produto final do projeto é um protótipo funcional instalado na SE Cabreúva. A estrutura deste artigo segue as diferentes etapas de implementação do projeto: A seção II trata do "site survey" realizado no campo para avaliar os equipos de comunicação sem fio adequados ao projeto. A seção III é um analise dos padrões IEEE para comunicação wirelles. A seção IV trata dos testes realizados em laboratório. A seção V trata da instalação feita em campo. A seção VI discute quesitos de confiabilidade e controle de acesso. A seção VII apresenta as conclusões do projeto. A seção VIII é dedicada aos agradecimentos e a seção IX é contem as referencias bibliográficas.

## II. Site survey

Depois de estudar os padrões de comunicação sem fio disponíveis e contatar diversos fornecedores no mercado nacional, ficou claro que, para determinar que tipo de equipamentos sem fio poderam serem utilizados numa subestação seria conveniente realizar uma visita de avaliação das condições de operação dos diferentes equipamentos disponíveis no local onde será realizada a instalação; essa visita é denominada "site survey" na área de comunicação sem fio e serve também para identificar a eventual existência de sinais na mesma faixa de freqüência dos equipamentos sendo testados que possam vir a representar possíveis interferências. Especificamente, foi realizado um site Survey da SE Cabreúva, analisando diversos pontos possíveis para instalação dos equipamentos sem fio. A SE Cabreúva foi escolhida pois apresenta três níveis de tensão: 440kV, 230 kV e 138 kV.

### *A. Equipamentos utilizados*

Durante o site survey foram utilizados os seguintes equipamentos:

- Antena Omni direcional de 16dbi
- Antena Yagi direcional de 12dbi
- Access point padrão IEEE 802.11b,
- Placa PCMCIA IEEE 802.11b.
- Dois notebooks.

### *B. Estrategia aplicada e Dados levantados*

Foi instalada a antena Omni direcional numa sacada do primeiro andar do edifício de comando, com visada de 270$^{o}$ para a área energizada da subestação. Essa antena foi ligada, por cabo proprietário, ao Access Point que foi configurado, para trabalhar numa rede sem fio aberta em canal 6, sem criptografia e sem filtragem de endereços MAC. Um dos notebooks foi ligado por cabo cross ethernet com esse Access Point estabelecendo uma rede privada.

A placa PCMCIA foi instalada no outro notebook que foi configurado para agir como estação cliente móvel. Com esse notebook cliente foram visitados 9 locais dentro da área energizada verificando-se, em cada caso, a relação sinal-ruído e o nível do sinal. Nos locais onde foi identificada a pior relação sinal-ruído foi adicionada a antena Yagi direcional ao notebook cliente e foram coletados os tempos de transmissão para 70 megabytes de dados.

A Figura 1, a seguir, apresenta os 9 pontos da SE Cabreúva onde se levantaram dados sobre a relação Sinal-Ruído (SNR, do inglês: Signal Noise Ratio ), do nível do Sinal (SL, do inglês: Signal Level ) e do ruído.

Este trabalho foi realizado com apoio financeiro da verba para P&D da ANEEL.

M. Nakashima, A. R. Figueiredo, e S. Gambini, trabalham na Companhia de Transmissão de Energia Elétrica Paulista (e-mail: {mnakashima, arfigueiredo, sgambini}@cteep.com.br).

L.C. Magrini e C. A. B. Pariente são pesquisadores do Grupo de Automação, Geração, Transmissão e Distribuição da POLI-USP (e-mail: magrini@pea.usp.br, lupus@usp.br).

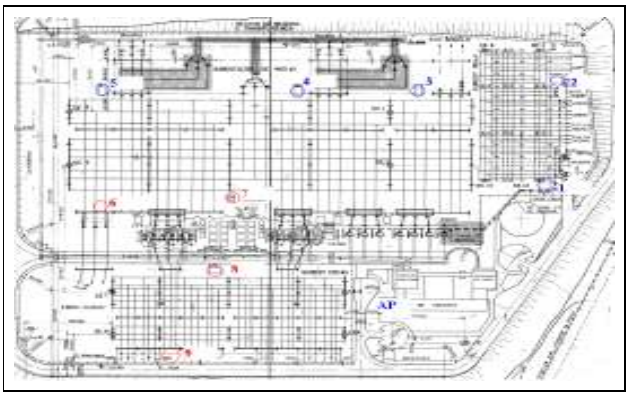

Figura 1. Pontos visitados na SE Cabreúva durante o Site Survey.

Do total de locais visitados foram coletados dados apenas nos últimos cinco, numerados em vermelho na Fig. 1, sendo que o ponto 6 foi visitado duas vezes. Nesses pontos foram coletados dados pelo cliente móvel usando o software que acompanha a placa PCMCIA; esse software permite registrar, valor médio, máximo e mínimo, a cada segundo, dentre as 60 amostras coletadas nesse período. São avaliados os seguintes parâmetros: (a) **SNR**: Signal to Noise Ratio (relação sinal-ruído), (b) **SL**: Signal Level (Nível do sinal), (c) **NL**: Noise Level (Nível do ruído). Esses dados foram reduzidos e plotados para estudar o comportamento do sinal. A Figura 2 apresenta esse comportamento.

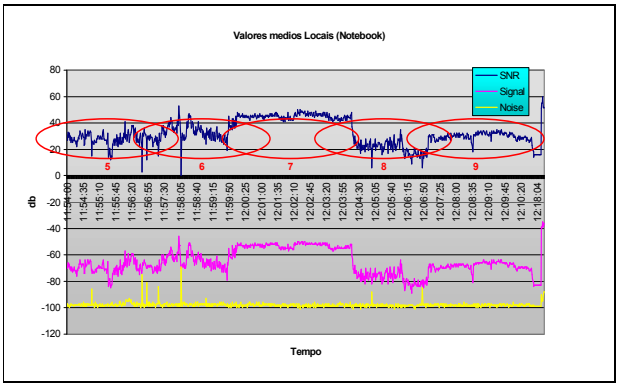


Figura 2. Os parâmetros SNR, SL e NL no notebook.

O tracejado azul representa valores do SNR, o tracejado rosa é o nível do sinal enquanto que o amarelo é o ruído. As curvas apresentadas na figura 2 são representações logarítmicas, em decibéis, da potência do sinal, do ruído e do quociente entre esses valores; a transformação de potência, em Watts, para decibéis é realizada usando a fórmula:

$$\mathbf{P_{db} = 30 + 10.log(P_W)}$$

Dessa forma, o quociente **SNR**, em qualquer instante do tempo no intervalo considerado, é obtido como a diferença entre os valores do sinal e do ruído. Por exemplo: no instante "11:58:01" o valor de **SNR** é 53, que é a diferença entre o valor do sinal, –46, e do ruído, -99. De modo geral, costuma-se considerar que, o valor do parâmetro **SNR** é melhor enquanto é maior (mais positivo) e os valores dos parâmetros **SL** e **NL** são melhores enquanto são menores (mais negativos).

As elipses vermelhas identificam, grosso modo, o intervalo de tempo em que foram coletados os dados na casa correspondente ao número na parte inferior da elipse, também em vermelho. Como os gráficos mostram, os dados começaram a ser gravados no local número 5 prosseguiu-se na seqüência com os locais 6, 7, 8, e 9 (na Fig. 1, os pontos 6 e 7 encontram-se no nível de tensão 440kV e os pontos 8 e 9 no nível de tensão de 230kV), depois do qual voltou-se ao local número 6; porém, devido a um hiato na gravação, não é possível apresentar os dados correspondentes a essa segunda visita ao local 6.

Dos gráficos, pode-se identificar o ponto 6 como aquele com o comportamento mais caótico do parâmetro **SNR**, o ponto 7 com os piores valores de **SNR**, o ponto 8 com os valores globalmente mais baixos e o ponto 9 com os valores mais uniformemente próximos do valor médio; em particular a crista no gráfico do parâmetro **SNR** que se observa o ponto 9, entre 12:08:01 e 12:10:26 corresponde à transmissão, por ftp, de um arquivo de 70 megabytes.

A Tabela I apresenta um resumo estatístico dos dados, expressados em decibéis (db):

TABELA I
RESUMO ESTATÍSTICO DOS PARÂMETROS SNR, SL, NL NO SITE SURVEY

| Parâmetro | Valor médio | Desvio padrão |
|---|---|---|
| **SNR** | 32,37 | 9,51 |
| **SL** | -65,52 | 9,44 |
| **NL** | -97,89 | 1,88 |

Foram realizadas transferências maciças de dados, para testar a velocidade da ligação, desde as casas 9 e 6; especificamente foi transferido um arquivo de 70 megabytes desde o notebook em campo até o notebook ligado no access point. A Tabela II seguinte registra os resultados dessas transferências.

TABELA II
Taxa de transferência para 70Mbdesde os pontos 6 e 9.

| Casa | tempo consumido | Taxa da transferência | Taxa da transferência |
|---|---|---|---|
| 9 | 137 segs | 505,00 Kbytes/seg | 3,94 Mbps |
| 6 | 162 segs | 428,60 Kbytes/seg | 3,34 Mbps |

Como o software registra apenas o tempo decorrido, não foi possível uma obtenção exata da qualidade do sinal em cada uma das casas. A vistoria realizada permitiu identificar a casa numerada com número 6 na Fig. 1, como aquela com as piores condições de enlace enquanto que as demais tiveram uma performance mais ou menos homogênea. Para contornar a queda do sinal foi reposicionada a antena Yagi, um pouco mais distante da casa e a velocidade de transferência registrada na Tabela II para essa nova configuração, foi comparável à dos casos mais favoráveis.

Da figura 2 pode-se considerar que, sem serem os melhores possíveis, os valores:

- **SNR** de 30db ou maior,
- **Nível do sinal (SL)** de –70db ou menor,

podem ser considerados como limiares para o estabelecimento dos enlaces em cada um das casas. A escolha desses valores pode ser justificada da seguinte forma: O valor médio do nível do sinal, calculado numericamente na Tabela I, é -65,52, mas como já foi comentado, os valores desse parâmetro são considerados melhores enquanto são menores; convém então considerar um limiar "um pouco" inferior; para evitar exagerar na diminuição do valor, consideramos a metade do desvio padrão para esse parâmetro (calculado também na Tabela I), ou seja, (9,4410)/2 =4,7205. Assim, chegamos, aproximadamente a –70 ≈= -65,5243 - 4,7205=-70,2448. Por outro, como se trata de gráficos logarítmicos, a correlação entre os dados é linear e, portanto, uma diminuição no nível do sinal implica na mesma diminuição no parâmetro **SNR** o que é favorável pois, como já foi comentado, valores menores de **SNR** são mais favoráveis; porém, como esse parâmetro depende do ruído, que é imprevisível, então consideramos uma diminuição "conservadora" de apenas 2 unidades e, assim, chegamos, aproximadamente, ao valor 30 ≈= 32,3744 - 2,00.

Durante os testes experimentou-se com equipamentos sem fio de diferentes fabricantes e padrões, disponibilizados por um fornecedor brasileiro, e optou-se por um rádio de baixo custo, de padrão IEEE802.11b, com capacidade para ser configurado como Access Point ou como Bridge Ponto-ponto ou ainda como Bridge Ponto-Multiponto. Essa escolha permitiu intercambiar, quando conveniente, os pontos de acesso com os clientes da rede sem fio.

## III. Análise dos padrões wireless do IEEE

O protocolo 802.11 é uma especificação da camada física e de controle de acesso ao meio para redes sem fio de área local, que incluem estações fixas, portáveis e móveis. Esse padrão define o protocolo e as conexões possíveis de equipamentos de comunicação de dados através do "ar", por ondas de radio ou infravermelhas, em uma rede de área local, usando o mecanismo de compartilhamento de meio com detecção de colisão CSMA/CA (do inglês: *carrier sense multiple access with collision avoidance*).

O controle de acesso ao meio (MAC, do inglês: *medium access control*), suporta operação tanto sob controle de um ponto de acesso (*access point*) quanto entre estações independentes. O protocolo inclui autenticação, associação e reassociação de serviços, um procedimento criptográfico opcional, gerenciamento de energia para reduzir consumo de energia em estações movíeis, e uma função de coordenação de ponto para transmissão de dados limitada pelo tempo. O padrão inclui a definição da base de informação de gerenciamento MIB (do inglês *management information base*) usando a Notação Sintática Abstrata ASN.1 (do inglês *Abstract Syntax Notation*) e especifica o protocolo MAC formalmente usando a linguagem de especificação e descrição SDL (do inglês *Specification and Description Language*).

A implementação original em ondas infravermelhas da camada física (PHY) previa uma taxa de transferência de dados teórica de 1Mbps e extensão opcional para 2Mbps. A implementação em ondas de rádio da camada PHY, especificava:

> Espectro de propagação com saltos de freqüência FHSS, (do inglês: *frequency-hopping spread spectrum*) com taxa de transferência teórica de 1 Mbps e, opcionalmente, de 2Mbps

Ou então

> Espectro de propagação de seqüência direta (DSSS, do inglês: *direct sequence spread spectrum*) que suporta taxas de transferência de dados teóricas tanto de 1Mbps quanto 2Mbps.

Cada uma das partes do padrão 802 divide-se em várias subpartes, identificadas com um sufixo alfabético; no caso do padrão 802.11, temos as seguintes subpartes:

### *A. IEEE802.11a: Camada física de alta velocidade na banda de 5GHz.*

Especifica a camada física PHY para um sistema multiplexado de divisão de freqüência ortogonal OFDM (do inglês: *orthogonal frequency division multiplexing*). As rádio-freqüências a serem usadas estão planejadas para ser formadas por bandas: 5,15GHz–5,25 GHz (banda baixa), 5,25GHz–5,35GHz(banda media), e 5,725GHz–5,825GHz (banda alta), que fazem parte da infraestrutura nacional de informação não licenciada UNII (do inglês: unlicenced national information infrastructure) dos Estados Unidos.

O sistema OFDM deve, obrigatoriamente, prover taxas de transferência teóricas de 6, 12 e 24 Mbps e, opcionalmente, de 9, 18, 36, 48 e 54 Mbps. Esta extensão do padrão 802.11 divide a sua banda de transmissão em 12 canais os quais não tem sobreposição; os 4 primeiros pertencem a banda baixa, os seguintes quatro à banda media e os últimos quatro a banda alta.

A Figura 3 mostra um esquema desses canais nas três bandas UNII.

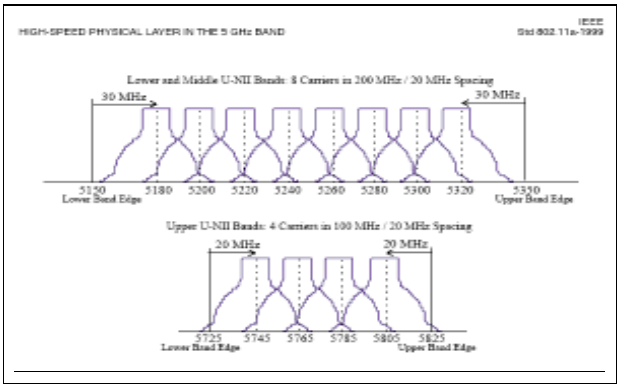


Figura 3. As 12 bandas do padrão 802.11a..

### *B. IEEE802.11b: Extensão de alta velocidade da camada física (PHY) na banda de 2,4 gigahertz*

Este padrão propõe uma extensão do padrão 802.11 para velocidades maiores na banda de 2,4 gigahertz. Especificamente, a taxa de transferência teórica é elevada para 11Mbps. A banda de transmissão é dividida em 11 canais, como mostra a Tabela III.

TABELA III
OS CANAIS DO PADRÃO 802.11B

| Canal | Inicio | Centro | Final | Sobreposição |
|---|---|---|---|---|
| 1 | 2,401 | 2,412 | 2,423 | Sem sobreposição |
| 2 | 2,406 | 2,417 | 2,428 | Com sobreposição |
| 3 | 2,411 | 2,422 | 2,433 | Com sobreposição |
| 4 | 2,416 | 2,427 | 2,438 | Com sobreposição |
| 5 | 2,421 | 2,432 | 2,443 | Com sobreposição |
| 6 | 2,426 | 2,437 | 2,448 | Sem sobreposição |
| 7 | 2,431 | 2,442 | 2,453 | Com sobreposição |
| 8 | 2,436 | 2,447 | 2,458 | Com sobreposição |
| 9 | 2,441 | 2,452 | 2,463 | Com sobreposição |
| 10 | 2,446 | 2,457 | 2,468 | Com sobreposição |
| 11 | 2,451 | 2,462 | 2,473 | Sem sobreposição |

Como a tabela mostra, somente os canais 1, 6 e 11 não possuem sobreposição; deste modo esses canais costumam ser combinados em instalações prediais para fornecer acesso wireles desde diversos pontos de acesso. A Figura 4. mostra uma possível combinação dos canais 1, 6 e 11 num prédio.

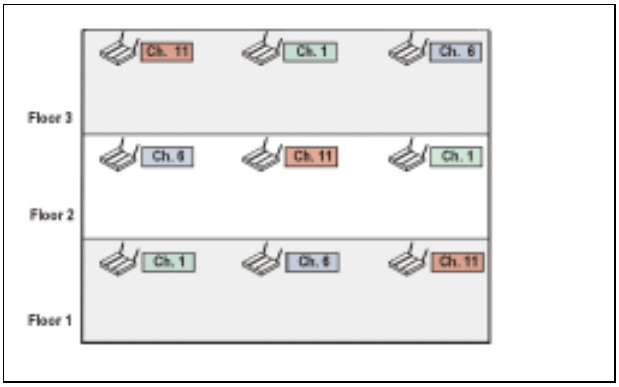


Figura 4. Combinação de canais 1, 6 e 11.

### *C. IEEE802.11g: Mais extensões de alta velocidade da camada física (PHY) na banda de 2,4 gigahertz*

Esta extensão do padrão 802.11 eleva a taxa teórica de transmissão de dados para 54 Mbps, na banda de 2,4 Ghz e mantém compatibilidade com o padrão 802.11b; isto que dizer, para que dispositivos wireless atendam ao padrão 802.11g eles, além de satisfazer os novos requisitos do padrão 802.11g, devem ser capazes de conversar com dispositivos wireless que atendem ao padrão 802.11b.

A segurança foi também levemente melhorada ao ser introduzido o algoritmo opcional "privacidade equivalente a cabos" WEP (do inglês: *Wired Equivalence Privacy*) que prevê chaves criptográficas de 64 e 128 bits. Porem, deve-se observar que, embora esse algoritmo de criptografia seja certamente uma melhora na segurança oferecida pelos padrões wireless, ele é uma solução tida como fraca segundo os padrões atuais de segurança.

### *D. Avaliação dos padrões IEEE 802.11*

Os padrões foram avaliados, comparando as diferentes modulações implementadas nas normas IEEE 802.11a, IEEE 802.11b e IEEE 802.11g, utilizando como métricas a velocidade de transmissão e o alcance do sinal em metros. O padrão IEEE 802.11a foi descartado por trabalhar numa faixa de freqüência diferente dos outros dois; entre os padrões IEEE 802.11b e IEEE 802.11g optou-se pelo 802.11b mesmo sendo o de menor velocidade, pois concluiu-se, da leitura dos padrões que o padrão IEEE 802.11g, atinge as distancias atingidas pelo padrão IEEE 802.11b, usando a mesma modulação do que este último o que os faz equivalentes em distancias maiores a 500 metros.

## IV. TESTES EM LABORATÓRIO

Foram portanto adquiridos equipamentos de padrão IEEE 802.11b, e procedeu-se a realizar testes em laboratório que são descritos a seguir.

### *A. Equipamentos utilizados*

No laboratório foram testados os seguintes equipamentos:
- 4 Access point padrão IEEE 802.11b, 200miliwatts
- Placa PCMCIA IEEE 802.11b.
- Um notebook

### *B. Configuração e Testes realizados*

- Um rádio foi configurado como Access Point para servir de estação base, recebendo um número IP da rede local e sendo ligado, vai cabo ethernet, no HUB da intranet do laboratório
- Os outros três rádios foram configurados como bridges ponto-multiponto e lhes foram designados também números IP da rede local.
- A placa PCMCIA foi instalada no notebook que foi configurado para agir como estação cliente móvel, recebendo também um número IP da rede local.

A Tabela IV apresenta um resumo das configurações mencionadas, sendo que as linhas 3-8 descrevem os parâmetros da estação base detectados por cada cliente e as linhas 10-12 parâmetros associados a cada cliente.

TABELA IV
RESUMO DAS CONFIGURAÇÕES NO LABORATÓRIO

| Parâmetro | Rádio | Rádio | PCMCIA |
|---|---|---|---|
| Informação da estação base visualizada pelos clientes | | | |
| IP AP | b0.b1.b2.58 | b0.b1.b2.58 | b0.b1.b2.58 |
| SSID | GAGTD | GAGTD | GAGTD |
| Canal | 6 | 6 | 6 |
| MAC AP | **00026F354C08** | **00026F354C08** | **00026F354C08** |
| Mbits/s | 11 | 11 | 11 |
| Informação de cada Cliente | | | |
| Quality % | 100 | 100 | 100 |
| MAC Bridge | **0202C3584BE4** | **00026F354FEB** | **00026F354D6E** |
| IP Bridge | b0.b1.b2.59 | b0.b1.b2.66 | b0.b1.b2.67 |

Os rádios adquiridos vêm da fábrica configurados para fazer parte, como clientes, de uma rede sem fio sem nenhum

tipo de filtragem, no canal 6 de comunicação. A configuração do rádio deve ser feita estabelecendo uma rede local com um PC, usando um cabo cross ethernet, e acessando um servidor web embarcado no rádio. Além disso, não é possível desligar a comunicação sem fio do radio deixando a interface ethernet ativa. O radio em questão possui um botão para voltar às configurações de fábrica. A Tabela V apresenta as velocidade e o alcance dos rádios segundo a modulação usada, operando sempre a 23 dBm de potência de saída.

TABELA V
Velocidade e alcance dos rádios segundo modulação

| **Modulação** | **Velocidade** | **Alcançe outdoor** |
|---|---|---|
| CCK | 11.0 Mbps | 300m/ 450m |
| CCK | 5.5 Mbps | 400m/ 600m |
| DQPSK | 2.0 Mbps | 500m/ 750m |
| DBPSK | 1.0 Mbps | 800m/1200m |

As características acima mencionadas originaram um problema de acesso à configuração do rádio, devido a que, pela sua configuração de fábrica os mesmos tendem a se somar a qualquer rede sem fio aberta nas redondezas e ficarem inacessíveis para configuração; de fato, nas proximidades do laboratório encontram-se 3 redes acadêmicas abertas e, para determinar em qual delas os rádios estavam se somando como clientes, foi necessário solicitar que as mesmas fossem desligadas para obter acesso às facilidades de configuração. Mesmo assim, depois de ter configurado em canais diferentes, comprovou-se que um Access Point de padrão IEEE802.11b/g, localizado a aproximadamente 300mts do laboratório, produzia interferência com os rádios sendo testados num facho de, aproximadamente 30º; o problema foi contornado transladando os rádios para um anexo do laboratório fora da área de cobertura do Access Point origem da interferência. Aproveitou-se para analisar a interferência com sinal de telefone celular com modulação GSM, na banda de 2.400 GHz: nenhuma interferência foi detectada. Porém, foi possível identificar que notebooks equipados de placas wireless embarcadas, causam interferência com os rádios testados, quando essas placas embarcadas estão configuradas para detectar automaticamente as redes sem fio nas redondezas.

A Tabela VI apresenta um resumo da força do sinal, em percentual, típica em momentos nos quais os clientes wireless foram utilizados como canais de comunicação para interrogar medidores.

TABELA VI
RESUMO DA FORÇA DO SINAL NOS CLIENTES

| Identificação da rede | | Sinal | | |
|---|---|---|---|---|
| IP | MAC address | Canal | % | Modo |
| b0.b1.b2.59 | 00026F354BE4 | 6 | 79 | AP |
| b0.b1.b2.66 | 00026F354FEB | 6 | 81 | AP |
| b0.b1.b2.67 | 00026F354D6E | 6 | 81 | AP |

Os conflitos com outras redes sem fio, mencionados acima, foram detectados usando o cliente móvel, que recebeu número IP b0.b1.b2.40; em geral o software que a acompanha a placa PCMCIA é flexível o suficiente para identificar todas as redes sem fio na área dos testes, e permite ainda distinguir cada ponto de rede pelo SSID da rede à qual pertencem assim como pelos endereços MAC dos dispositivos de rádio. Outra ferramenta de análise oferecida pelo software que acompanha essa placa permite registrar diversos parâmetros de transmissão, como a relação sinal ruído SNR, a força do sinal, a quantidade de pacotes perdidos, etc. A Tabela VII apresenta o alcance da placa PCMCIA segundo a modulação.

TABELA VII
Velocidade e alcance PCMCIA segundo modulação

| Modulação | *Velocidade* | Alcance Outdoor |
|---|---|---|
| CCK | 11 MBIT/S | 160m |
| CCK | 5.5 MBIT/S | 270m |
| DQPSK | 2 MBIT/S | 400m |
| DBPSK | 1 MBIT/S | 550m |

## V. Instalação em campo

Depois do site survey realizado e dos testes de laboratorio foi instalado um prototipo funcional na SE Cabreúva.

### *A. Equipamentos utilizados*

No campo foram utilizados os seguintes equipamentos:
- 1 Antena Omni direcional de 15dbi
- 3 Antenas Yagi direcionais de 12dbi
- 4 Access point padrão IEEE 802.11b, 200miliwatts
- Placa PCMCIA IEEE 802.11b.
- Um notebook
- 2 conversores RS485 ethernet.
- 2 medidores de energia elétrica, com capacidade de captura e armazenamento de dados de oscilografia
- Um PC configurado com:
  - Software SCADA configurado para acessar os dados dos medidores usando protocolo Modbus TCP;
  - Os softwares proprietários para comunicação com os medidores de energia elétrica.
  - Um aplicativo desenvolvido para adquisição dos dados de eventos transitórios que é executado sob demanda pelo SCADA quando este último lê um registro Modbus que indica a presença desses eventos.

### *B. Configuração e Testes realizados*

- Foi instalada a antena Omni direcional num local do telhado do edifício de comando, com visada de 270º para a área energizada da subestação.

- Essa antena foi ligada, por cabo proprietário, a um rádio configurado como Access Point para servir como estação base, e trabalhar numa rede sem fio aberta em canal 6, sem criptografia mas com filtragem de endereços MAC; além disso esse rádio foi configurado para fazer parte da intranet corporativa e ligado, via cabo ethernet, no hub da rede local.

- Outros dois rádios foram configurados como bridges ponto-multiponto e a eles foram designados também números IP da rede local.

- Cada um de esses dois rádios foram ligados, via cabo cross ethernet, a um conversor RS485, que pela sua vez foi ligado num medidor de energia elétrica, por cabo serial.

- O outro rádio foi configurado como bridge ponto-multiponto e lhe foi designado um número IP da rede local, sendo ligado, via cabo cross ethernet, com o PC no qual reside o sistema SCADA e os softwares proprietários para comunicação com os medidores.
- A placa PCMCIA foi instalada no notebook que foi configurado para agir como estação cliente móvel.

A Figura 5, apresenta uma configuração típica do protótipo instalado.

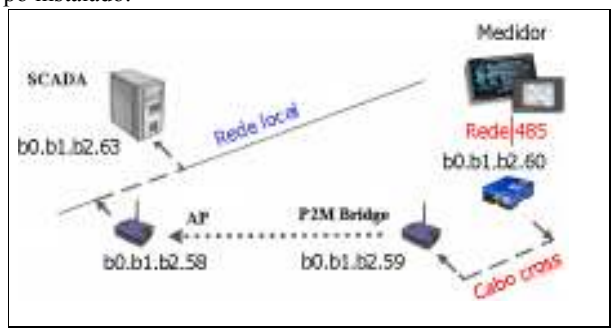


Figura 5. Configuração típica do protótipo.

Os medidores foram configurados para registrar e armazenar dados de corrente e tensão em diferentes níveis de tensão tanto em medições periódicas a cada segundo, quanto para eventos transitórios com duração de poucos ciclos. Os dados assim adquiridos foram transmitidos através dos enlaces sem fio, sendo adquiridos utilizando-se os softwares proprietários de cada medidor, além do SCADA; notou-se porém uma perda de performance, com tendência a gerar um gargalho no canal de comunicação quando o aplicativo desenvolvido para aquisição dos dados de eventos transitórios entra em funcionamento. A solução sugerida neste caso é utilizar medidores que possuam, pelo menos, dois canais de comunicação serial independentes, de modo a usar um de esses canais para a interrogação periódica (a cada segundo) do medidor e o outro canal para a transmissão de dados de eventos transitórios.

Durante o tempo que o protótipo descrito está em operação foram detectadas interferências esporádicas e breves, cuja causa ainda não foi identificada mas que não pode ser associada a eventos na rede da transmissão. Suspeita-se que os mesmos tenham origem no uso de rádios para comunicação de voz entre o pessoal trabalhando na área energizada e o edifício de comando.

## VI. Confiabilidade e Controle de Acesso

Os dispositivos wireless que atendem o padrão 802.11 não podem ser considerados canais de comunicação seguros, devido ao algoritmo de criptografia incluído na sua definição. Mesmo nessa situação, existem algumas medidas que podem ser tomadas para impedir acesso não autorizado a uma rede sem fio, reforçando desse modo a segurança. Vamos discutir os que podem ser aplicados a dispositivos que atendem o padrão 802.11.

### *A. Algoritmo de Wired Equivalence Privacy (WEP)*

O algoritmo WEP é um sistema criptográfico simétrico, isto quer dizer que usa a mesma chave tanto para cifrar mensagens (ou seja, aplicar o algoritmo de criptografia nas mensagens de modo que mesmo que interceptados não possam ser lidos) quanto para decifrar mensagens.

No padrão 802.11g este algoritmo pode ser usado com chaves criptográficas de 64 ou 128 bits, mas existem produtos no mercado que mantendo compatibilidade com o padrão, permitem usar chaves criptográficas de 256 bits e outros algoritmos criptográficos além do WEP.

### *B. Desabilitar Broadcast Service Set ID (SSID)*

Os dispositivos de hardware que servem como pontos de acesso à redes sem fio e que atendem o padrão 802.11 possuem um identificador alfanumérico único, denominado identificador de conjunto de serviço SSID (do inglês: Service Set ID), que pode ter de 1 até 32 bytes. Esse identificador é usado para que os dispositivos clientes possam diferenciar a que rede sem fio a que estão conectados, quando várias dessas redes operam com alcance sobreposto. Para iniciar a comunicação a estação que serve como ponto de acesso para a rede sem fio faz broadcast de seu SSID, permitindo dessa forma, que os possíveis clientes o identifiquem e possam tentar o inicio de uma comunicação.

Alguns aparelhos, trazem o SSID setado na fábrica com um valor padrão, facilitando assim a identificação do ponto de acesso para possíveis invasores. Portanto deve se sempre verificar se os aparelhos em questão trazem essa configuração e, nesse caso, substituir o valor de fábrica.

### *C. Wi-Fi Protect Access (WPA),*

Esta é uma extensão da funcionalidade do algoritmo WEP que possui duas partes, a primeira é destinada a impedir o acesso não autorizado à rede sem fio e a segunda, reforça a criptografia, para que mesmo que um intruso obtenha acesso, lhe seja difícil decodificar as mensagens que transitam pela rede sem fio.

### *D. Autenticação de endereço MAC,*

Essa autenticação implementa-se mantendo no ponto de acesso, uma lista dos endereços MAC autorizados a acessar a rede sem fio.

## VII. Conclusões

O protótipo desenvolvido permitiu demonstrar a viabilidade de substituir cabos de comunicação serial por enlaces sem fio em Sistemas de Supervisão e Controle em Subestações, dentro dos parâmetros de operação escolhidos para o projeto.

A viabilidade econômica de tal substituição deve levar em consideração que, quanto maior o número de pontos remotos sendo interrogados através do enlace sem fio, tem-se ao

mesmo tempo que o custo adicional é incrementado em cada ponto pelo custo de um rádio, e que a banda é dividida entre a quantidade de rádios agindo como clientes na área energizada.

Contrariamente ao que se esperava no inicio do projeto, as interferências não foram originadas pelas linhas de transmissão, mas por outros equipamentos de rádio.

Na data da elaboração deste relatório os testes do enlace durante manobras ainda não tinham sido realizados e, nessa ocasião, seria recomendável registrar o horário de inicio e fim de cada manobra, para poder analisar os parâmetros do sinal com mais precisão. Além disso, falta ainda estudar o impacto do uso de criptografia e do volume de dados na performance do canal de comunicação sem fio.

## VIII. Agradecimentos

Os autores agradecem a colaboração de Peter Laszlo da Turbolink durante o site Survey, do Flavio Correa da firma "Cernet Tecnologia e Sistemas", http://www.cernet.com.br/, pelas informações sobre o formato do arquivo de log [2] do cartão PCMCIA, e do Eng. Hilton Fernandes do LSI-POLI-USP que propicio diversas discussões sobre padrões wireless na USP e indicou diversos contatos de fornecedores de equipamentos sem fio.

## IX. Referências bibliográficas

*Periódicos:*

[1] A. Hills, J. Schlegel, and B. Jenkins, "Estimating Signal Strengths in the Design of an Indoor Wireless Network," *IEEE Trans. On wireless communications*, vol. 3, nro. 1, pp. 17-19, Jan. 2004.

*Livros:*

[2] R. Olexa, *Implementing 802.11, 802.16 and 802.20 Wireless Networks. Plannig, Troubleshooting and Operations*. Newnes - Elsevier, 2005, ISBN: 0-7506-7808-9.

*Artigos em Anais de Conferências (Publicados):*

[3] W. F. Young, "COMMUNICATION VULNERABILITIES AND MITIGATIONS IN WIND POWER SCADA SYSTEMS," in *Proc. of the American Wind Energy Association WINDPOWER 2003 Conf.*, pp. 315-320.

*Normas:*

[4] IEEE Std 802.11, (ISO/IEC 8802-11: 1999), disponível em http://standards.ieee.org/getieee802/portfolio.html.

[5] IEEE 802.11a-1999 (R2003), disponível em http://standards.ieee.org/getieee802/portfolio.html.

[6] IEEE 802.11b-1999 (R2003), disponível em http://standards.ieee.org/getieee802/portfolio.html..

[7] IEEE 802.11g-2003, disponível em http://standards.ieee.org/getieee802/portfolio.html..