XXI SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

Versão 1.0
23 a 26 de Outubro de 2011
Florianópolis - SC

GRUPO –GTM

GRUPO DE ESTUDO DE TRANSFORMADORES, REATORES, MATERIAIS E TECNOLOGIAS EMERGENTES - GTM

APLICAÇÃO DE REDE WIRELESS PARA SISTEMA DE MONITORAMENTO ONLINE NA SUBESTAÇÃO SANTO ÂNGELO DA ELETROBRAS ELETROSUL

CLAYTON S. DURIGUETTO(*) TREETECH
RAFAEL P. FEHLBERG TREETECH
FERNANDO T.DE CARVALHO TREETECH
SANDRO PEIXOTO ELETROBRAS ELETROSUL

RESUMO

Este informe técnico tem por finalidade descrever a tecnologia da rede de comunicação wireless integrada junto ao sistema de monitoramento dentro da SE Santo Ângelo com o objetivo de melhorar o desempenho, customização da rede de comunicação entre o campo e a sala de controle e facilitar implementações futuras sem a utilização de novos cabos e/ou fibras-ópticas.

PALAVRAS-CHAVE

Transformador, Conversor, Monitoração, WLAN, Access Point

1.0 - INTRODUÇÃO

As redes locais sem fio WLAN (Wireless Local Area Network) constituem-se como uma alternativa às redes convencionais com fio, fornecendo as mesmas funcionalidades, mas de forma flexível, de fácil configuração e com boa conectividade em áreas prediais,residenciais ou indústriais.

Redes WLAN viabilizam dessa forma o atendimento de pontos de rede com a mesma eficiência e até mesmo uma melhor relação custo/benefício em relação ao sistema de cabeamento convencional nesses casos.

A instalação de redes wireless e de novos pontos de rede elimina a necessidade de se passar novos cabos, reduzindo o tempo de configuração de novas posições de trabalho e facilitam a construção de estruturas em infra-estrutura. Uma rede wireless proporciona, dessa forma, todas as funcionalidades de uma rede cabeada, porém sem as restrições físicas do cabeamento propriamente dito.

Atualmente a grande maioria das redes wireless permite plena conectividade e atende aos padrões e normas dos orgãos internacionais. Isto significa que, uma vez utilizando equipamentos padronizados, redes wireless podem ser interconectadas com as redes de cabeamento convencional sem maiores problemas, e computadores utilizando dispositivo wireless interagem com computadores da rede cabeada e vice-versa sem qualquer restrição.

Nesta categoria de redes, se permitem definir assim, vários tipos de redes, que são: Redes Locais sem Fio ou WLAN, Redes Metropolitanas sem Fio ou WMAN (Wireless Metropolitan Area Network), Redes de Longa Distância sem Fio ou WWAN (Wireless Wide Area Network), redes WLL (Wireless Local Loop) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (Wireless Personal Area Network).

Sendo assim, as WLAN combinam a mobilidade do usuário com a conectividade a velocidades elevadas de até 155 Mbps, em alguns casos.

(*) Praça Claudino Alves, n° 141 – Centro – CEP 12940-800 Atibaia, SP, – Brasil
Tel: (+55 11) 4413-5787 – Email: clayton.duriguetto@treetech.com.br

Dependendo da tecnologia utilizada, rádio freqüência e do receptor, as rede WLANs podem atingir quilômetros dependendo da potência do equipamento utilizado.

2.0 - COMO FUNCIONAM AS WLAN

Através da utilização portadoras de rádio, as WLAN estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas. Múltiplas portadoras de rádio podem coexistir em um mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Em um ambiente típico, ver Figura 1, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, em um esquema de micro células com roaming semelhante a um sistema de telefonia celular.

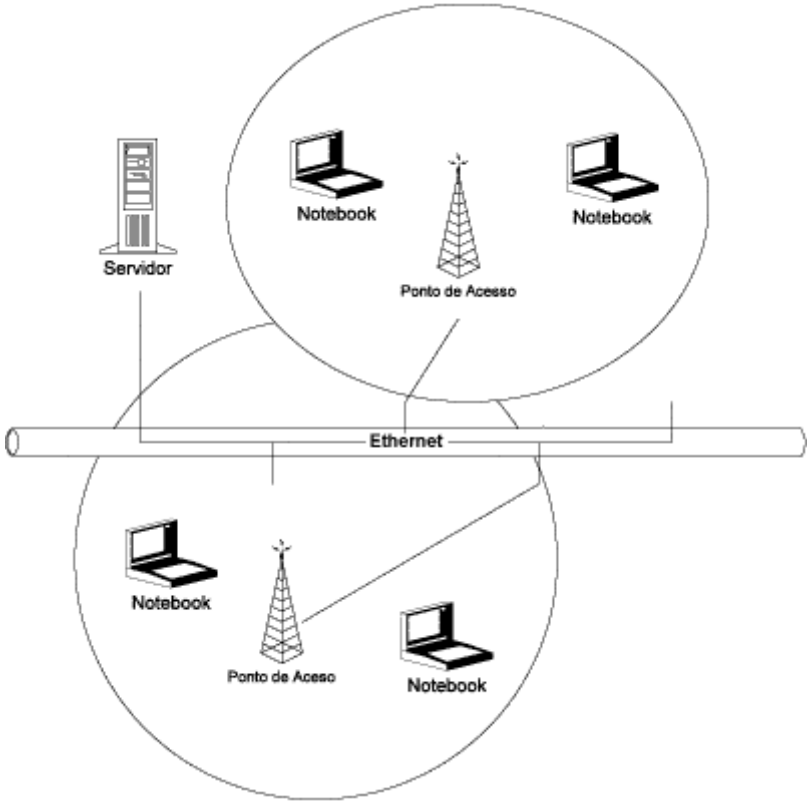

FIGURA 1 – Rede wireless LAN típica

2.1 Topologia

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. Os sistemas Spread Spectrum utilizam a técnica de espalhamento espectral com sinais de rádio freqüência de banda larga, provendo maior segurança, integridade e confiabilidade, em troca de um maior consumo de banda. Há dois tipos de tecnologias spread spectrum: a FHSS, Frequency-Hopping Spread Spectrum e a DSSS, Direct-Sequence Spread Spectrum ver Figura 2.

A FHSS usa uma portadora de faixa estreita que muda a freqüência em um código conhecido pelo transmissor e pelo receptor que, quando devidamente sincronizados, o efeito é a manutenção de um único canal lógico.

A DSSS gera um bit-code (também chamado de chip ou chipping code) redundante para cada bit transmitido. Quanto maior o chip maior será a probabilidade de recuperação da informação original. Contudo, uma maior banda é requerida. Mesmo que um ou mais bits no chip sejam danificados durante a transmissão, técnicas estatísticas embutidas no rádio são capazes de recuperar os dados originais sem a necessidade de retransmissão.

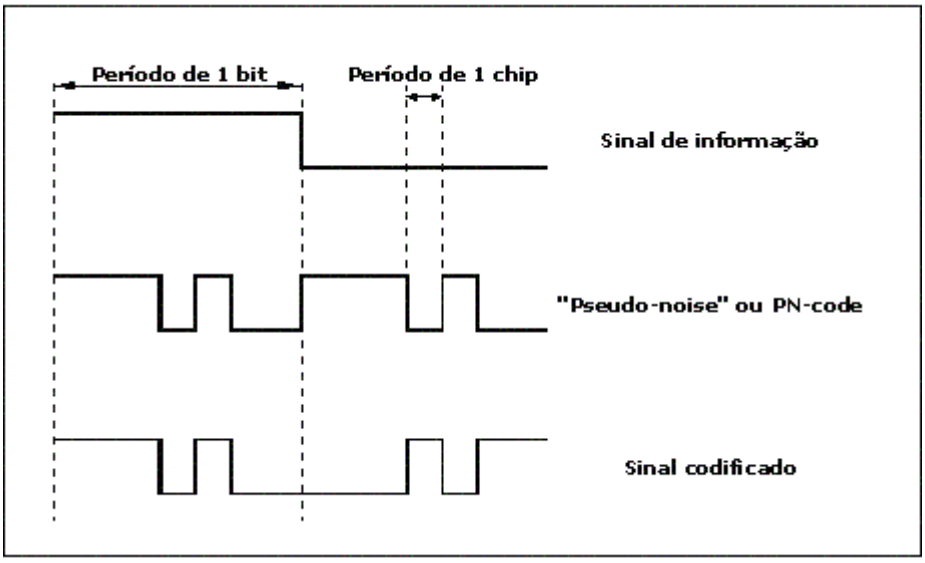

FIGURA 2 – Transmissão Spread Spectrum

2.2.1 IEEE 802.11 Wireless Local Area Network

O padrão IEEE 802.11, ver Figura 3, especifica três camadas físicas (PHY) e apenas uma subcamada MAC (Medium Access Control) provê duas especificações de camadas físicas com opção para rádio, operando na faixa de 2.400 a 2.483,5 mHz (dependendo da regulamentação de cada país), e uma especificação com opção para infravermelho, são elas:

a. Frequency Hopping Spread Spectrum Radio PHY:
Esta camada fornece operação 1 Mbps, com 2 Mbps opcional. A versão de 1 Mbps utiliza 2 níveis da modulação GFSK (Gaussian Frequency Shift Keying), e a de 2 Mbps utiliza 4 níveis da mesma modulação;

b. Direct Sequence Spread Spectrum Radio PHY:
Esta camada provê operação em ambas as velocidades (1 e 2 Mbps). A versão de 1 Mbps utiliza da modulação DBPSK (Differential Binary Phase Shift Keying), enquanto que a de 2 Mbps usa modulação DQPSK (Differential Quadrature Phase Shift Keying);

c. Infrared PHY:
Esta camada fornece operação 1 Mbps, com 2 Mbps opcional. A versão de 1 Mbps usa modulação 16-PPM (Pulse Position Modulation com 16 posições), e a versão de 2 Mbps utiliza modulação 4-PPM.

No lado da estação, a subcamada MAC fornece os seguintes serviços: autenticação, desautenticação, privacidade e transmissão da MADU (MAC Sublayer Data Unit), e no lado do sistema de distribuição: associação, desassociação, distribuição, integração e reassociação. As estações podem operar em duas situações distintas:

a. Configuração Independente:
Cada estação se comunica diretamente entre si, sem a necessidade de instalação de infraestrutura. A operação dessa rede é fácil, mas a desvantagem é que a área de cobertura é limitada. Estações com essa configuração estão no serviço BSS (Basic Service Set);

b. Configuração de Infra-estrutura:
Cada estação se comunica diretamente com o ponto de acesso que faz parte do sistema de distribuição. Um ponto de acesso serve as estações em um BSS, sendo seu conjunto chamado de ESS (Extended Service Set). Além dos serviços acima descritos, o padrão ainda oferece as funcionalidades de roaming dentro de um ESS e gerenciamento de força elétrica (as estações podem desligar seus transceivers para economizar energia). O protocolo da subcamada MAC é o CSMA/CA (Carrier Sense Multiple Access with Collision Avoidence).

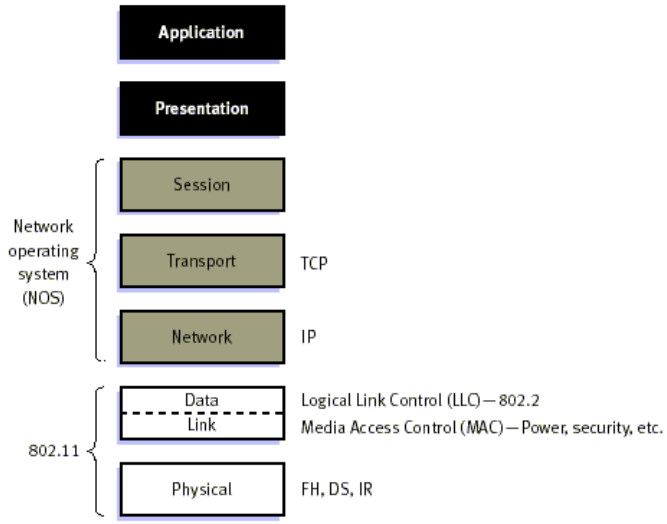

FIGURA 3 – Padrão de comunicação IEEE 802.11

3.0 - SEGURANÇA NA WLAN

O mercado hoje em dia não tem tantas preocupações quanto às implicações associadas à segurança deste tipo de rede. Por outro lado, empresas de grande e médio porte ainda estão bastante preocupadas com o fato de transmitir dados confidenciais pelo ar.

Existem vários tipos de segurança em WLAN 802.11, será descrito o modelo utilizado na SE Santo Ângelo.

3.1 Padrão de segura WPA (WI-FI Protect Access) 802.11

Tendo em vista o grande número de vulnerabilidades encontrada protocolo WEP, o grupo que criou o padrão IEEE 802.11 iniciou pesquisas para o desenvolvimento de um novo padrão de segurança denominado IEEE 802.11i. O intuito primordial era resolver todos os problemas de segurança encontrados no WEP. Enquanto o padrão estava sendo desenvolvido, a Wi-Fi Alliance, para responder às críticas geradas pelo meio corporativo em relação ao WEP, apresentou em 2003 um padrão denominado Wi-Fi Protected Access (WPA). O WPA é baseado no RC4 e em um subconjunto de especificações apresentadas em uma versão preliminar do IEEE 802.11i. O WPA introduz diversos mecanismos para resolver os problemas de segurança associados ao WEP:

- Regras para o IV(Vetor) e IV estendido de 48 bits – Como os 24 bits de IV utilizado pelo WEP permitiam pouco mais de 16 milhões de IV diferentes, facilitando repetições em um curto espaço de tempo, o WPA introduz um IV estendido de 48 bits. Assim, mais de 280 trilhões de IVs diferentes são possíveis. Adicionalmente, o WPA introduz regras para a escolha e verificação de IV´s para tornar ataques de re-injeção de pacotes ineficazes.

- Novo código de verificação de mensagens – O WPA usa um novo campo de 64 bits, o MIC (Message Integrity Code), para verificar se o conteúdo de um quadro de dados possui alterações por erros de transmissão ou manipulação de dados. O MIC é obtido através de um algoritmo conhecido como Michael.

- Distribuição e derivação de chaves – O WPA automaticamente distribui e deriva chaves que serão utilizadas para a criptografia e integridade dos dados. Isto resolve o problema do uso da chave compartilhada estática do WEP.

3.1.1 Autenticação

Existem dois tipos de autenticação no protocolo WPA. Um direcionado para redes corporativas que utiliza um servidor de autenticação 802.1x/EAP, portanto uma infra-estrutura complementar, e outro, mais simples, projetado para pequenas redes em escritórios e redes domésticas (redes SOHO – Small Office/Home Office). Estes dois tipos de autenticação são denominados WPA Corporativo e WPA Pessoal, respectivamente.

- WPA Pessoal – como um usuário comum não é capaz de instalar e fazer a manutenção de um servidor de autenticação criou-se o WPA-PSK (WPA-Pre Shared Key) que é uma passphrase12, previamente compartilhada entre o Access Point e os clientes. Neste caso, autenticação é feita pelo Access Point. A chave é configurada manualmente em cada equipamento pertencente à rede e pode variar de 8 a 63 caracteres ASCII.

- WPA Corporativo – o Access Point não é responsável por nenhuma autenticação. Tanto a autenticação do usuário quanto do dispositivo é feita por um servidor de autenticação. É utilizada uma infra-estrutura complementar formada por um servidor que usa o protocolo de autenticação 802.1x em conjunto com algum tipo de EAP (Extensible Authentication Protocol). O 802.1x é um protocolo de comunicação utilizado entre o Access Point e o servidor de autenticação. Este protocolo já era largamente utilizado em redes cabeadas e se mostrou também adequado quando integrado às redes sem fio. Quando um cliente solicita uma autenticação, o servidor de autenticação verifica em sua base de dados se as credenciais apresentadas pelo solicitante são válidas, em caso positivo o cliente é autenticado e uma chave chamada Master Session Key (MSK) lhe é enviada. Na maioria das vezes, utiliza-se como servidor de autenticação um servidor RADIUS, mas não é obrigatório.

3.1.2 Integridade

A integridade no WPA é composta por dois valores. Além do ICV(Integrity check Value), é adicionada ao quadro uma mensagem de verificação de integridade denominada MIC (Message Integrity Check).

O Michael é uma função hash não linear, diferentemente do CRC-32. O endereço de destino deu origem, a prioridade (definida atualmente como zero), os dados e uma chave de integridade que são inseridos no Michael para produzir o MIC. A saída corresponde a 8 bytes que juntamente com o ICV formam a integridade do protocolo WPA. Portanto a integridade é representada por um total de 12 bytes, 8 gerados pelo Michael e 4 pelo CRC-32, ver Figura 4.

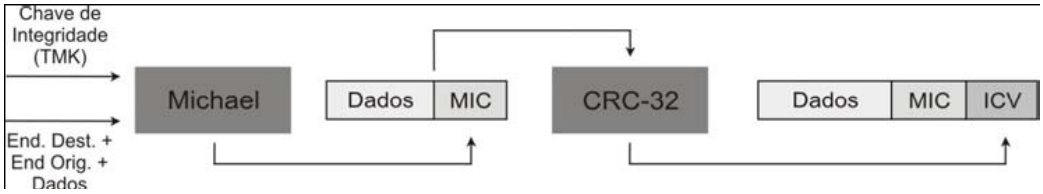

FIGURA 4 – Protocolo de Integridade do WPA

3.1.3 Confidência

O TKIP (Temporal Key Integrity Protocol) soluciona boa parte das vulnerabilidades no protocolo WEP. O TKIP é baseado no conceito de chaves temporais, ou seja, a chave é usada durante certo tempo e depois é substituída dinamicamente.

No WPA o vetor de inicialização possui 48 bits o que torna praticamente impossível haver reutilização de vetores. Na estrutura do cabeçalho 802.11 o campo reservado para o IV só contém 24 bits, devido a isto se criou outro campo chamado IV Extended, que não faz parte da estrutura do cabeçalho 802.11, para alocar o resto do IV. O IV também é utilizado como um contador de quadros (TSC – TKIP Sequence Counter). Quando uma nova chave de criptografia é estabelecida, o TSC é zerado. A cada quadro transmitido, ele é incrementado. Desta forma, quadros com TSC fora de ordem são descartados, evitando-se re-injeções de pacotes.

O processo de codificação do WPA é semelhante ao do WEP. A principal diferença está na chave que irá alimentar o RC4. Esta chave é o resultado de um algoritmo de combinação de chave cuja entrada é o vetor de inicialização, o endereço MAC do transmissor e a chave de criptografia de dados. Ao final, a chave gerada pelo algoritmo de combinação de chave e o IV são passados para o RC4, ver Figura 5.

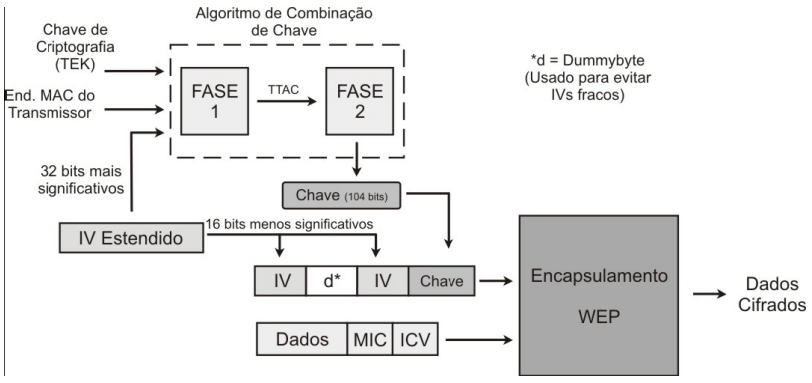

FIGURA 5 – Algoritmo de combinação da chave WPA

4.0 - APLICAÇÃO DA REDE WIRELESS NA SUBESTAÇÃO SANTO ANGELO

O Sistema de Monitoramento para o banco de autotransformadores trifásicos 525/230-13,8kV - 224 MVA da subestação de Santo Ângelo, TF3, têm por objetivo reduzir o risco de ocorrência de falhas catastróficas nesse equipamento ao efetuar o diagnóstico de seu estado atual, detectando problemas que ainda encontra-se em fase inicial de desenvolvimento, bem como o prognóstico de problemas futuros com base na progressão das medições ao longo do tempo. Para isto, o sistema efetua a aquisição e armazenamento das medições de sensores inteligentes instalados no autotransformador via os conversores de rede RS-485/wireless, assim como tratamento desses dados com a finalidade de transformá-los em informações úteis para a manutenção.

4.1 Arquitetura do sistema de monitoramento

O sistema de monitoramento está baseado em uma arquitetura descentralizada, composta basicamente de equipamentos de aquisição de dados, equipamentos de armazenamento e tratamento de dados e do meio de comunicação, que interliga as duas primeiras partes, os equipamentos de aquisição de dados estão no próprio corpo dos autotransformadores e no cubículo comum (QCC), e consistem-se em IEDs, equipamentos eletrônicos baseados em microcontroladores e projetados especificamente para instalação em autotransformadores, adequados, portanto, para operação em temperaturas de no mínimo -40 a +85ºC com até 95% de umidade relativa, sendo imunes também a interferências eletromagnéticas e de rádio-freqüência. Estes IEDs, aquisitam grandezas do tipo temperatura do óleo, temperatura dos enrolamentos, umidade no comutador, capacitância e tangente delta nas buchas condensivas, gases dissolvidos no óleo, membrana no conservador e contatos secos.

4.2 Meio de comunicação de dados

Os equipamentos de aquisição de dados estão interligados por duas redes de comunicação serial padrão RS-485/wireless nos painéis dos autotransformadores e cubículo comum, através de cabo do tipo par trançado blindado. A interligação dos equipamentos de aquisição de dados com o sistema de armazenamento e tratamento de dados localizados na central de monitoramento, no Sertão Maruim, foi efetuada por rede wireless, acrescentando-se os conversores e access point adequados. O acesso remoto é feito através da intranet da Eletrosul via protocolo TCP/IP, ver Figuras 6,7 e 8.

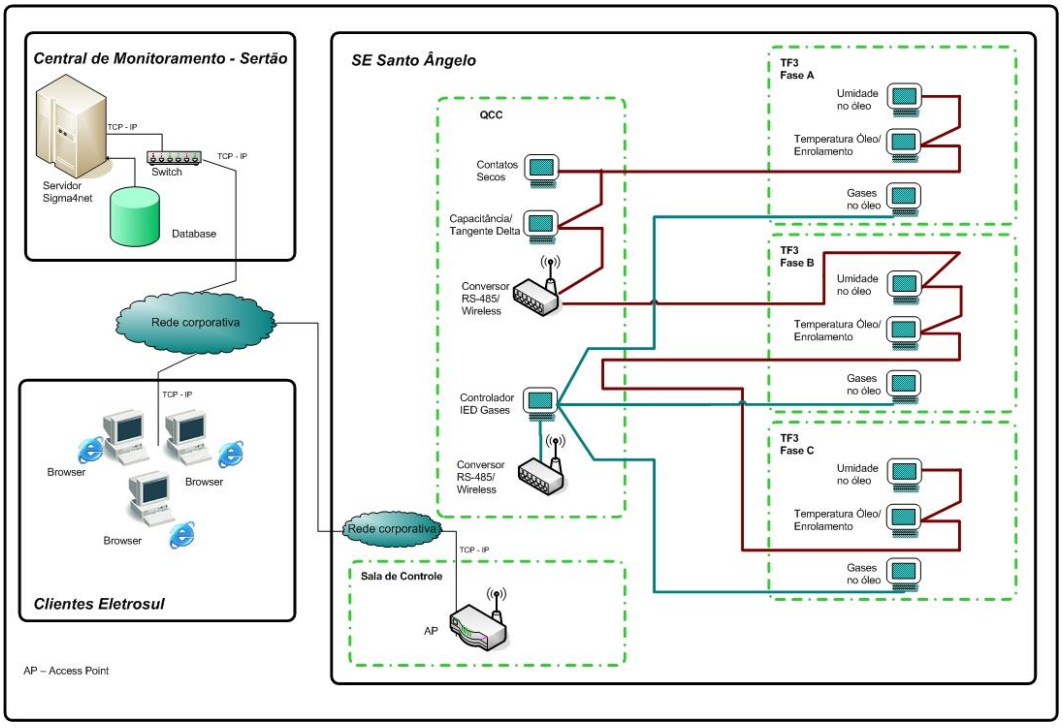

FIGURA 6 – Arquitetura de monitoramento da SE Santo Ângelo.

FIGURA 7 – Painel com conversores RS-485/Wireless

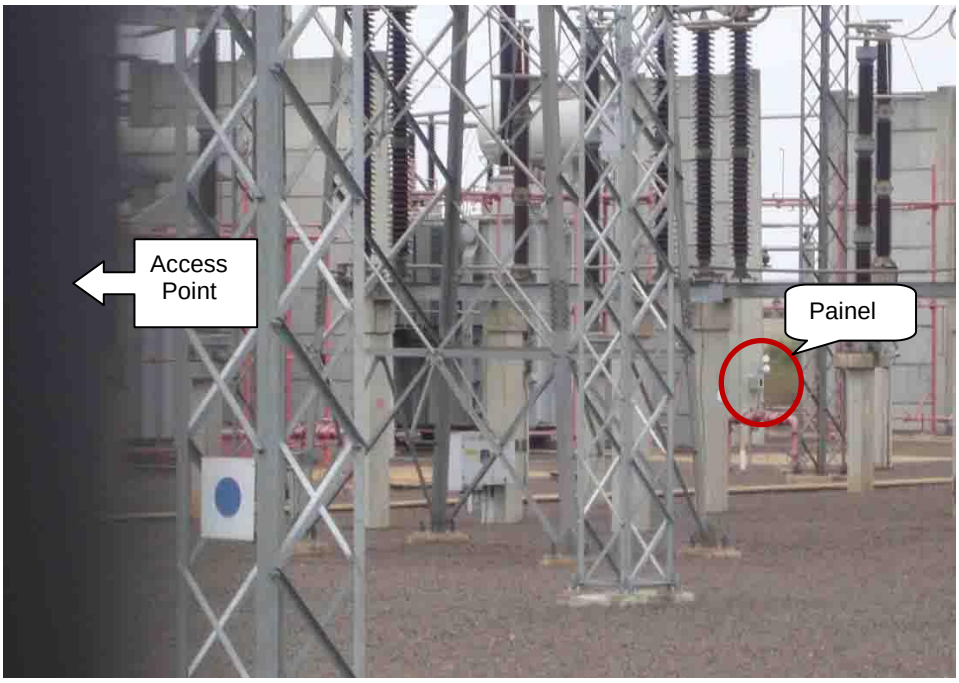

FIGURA 8 – Vista antena do access point e antenas dos conversores

4.3 Segurança

O access point instalado na sala de controle da SE Santo Ângelo possui segurança de autenticação WAP-PSK e método de criptografia TKIP conforme descrito no item 3.0 deste informe técnico, com isso os conversores instalados na parede corta-fogo estão com a mesma configuração. Para tanto, além destas seus endereços físicos de rede estão cadastrados no access point, aumentando ainda mais a segurança das informações.

5.0 - CONCLUSÃO

Desde a instalação do sistema de monitoramento na SE Santo Ângelo em novembro de 2009, esta aplicação de rede wireless, está em pleno funcionamento, podendo ser expandida para outros equipamentos da subestação colocando apenas os IEDs necessários e um conversor RS-485/Wireless, reduzindo o custo na instalação com cabos, fibras-ópticas e até mesmo conversores adicionais.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) Ciampa M., Olenewa J. – Wireless# Guide To Wireless Communications 2006

(2) Haykin S., Moher M. – Sistemas Modernos de Comunicações Wireless 2007

(3) Boland, H.e Mousavi, H. Security issues of the IEEE 802.11b wireless LAN, 2004

7.0 - DADOS BIOGRÁFICOS

Clayton Sperandio Duriguetto - Nascido em Guarulhos, SP, em 09 de agosto de 1983, trabalha com a Treetech Sistemas Digitais desde 2001. Especializado em desenvolvimento de sistemas de monitoramento e controle de transformadores de potência, disjuntores e redes industriais no departamento de Engenharia de Aplicação/Software. Formado em Bacharel Sistemas de Informação pela Faculdade Eniac, Guarulhos – SP em 2009, Técnico em Eletro-eletrônica pela Instituição Senai – Hermenegildo Campos de Almeida em 2000 Guarulhos - SP.

Rafael Prux Fehlberg - Nascido em Porto Alegre, RS, em 13 de agosto de 1981, trabalha com a Treetech Sistemas Digitais desde 2004 com engenharia aplicada a monitoramento de equipamentos de subestações. Formado em Engenharia de controle e automação pela PUC-RS em 2003.

Fernando Temotheo de Carvalho - Nascido em São Paulo, SP, em 04 de janeiro de 1981, trabalha com a Treetech Sistemas Digitais desde 2002. Especializado em desenvolvimento de sistemas de monitoramento e controle de transformadores de potência, disjuntores e redes industriais no departamento de Engenharia de Aplicação/Software. Formado em Ciências da Computação pela Universidade Uninove, São Paulo – SP em 2004.

Sandro Peixoto - Nascido em Florianópolis - SC, trabalha na Eletrobras Eletrosul desde 2001. Especializado em engenharia de sistemas de energia elétrica, sistemas de monitoramento de equipamentos de pátios de subestações de energia elétrica. Formado em Engenharia Elétrica pela UFSC em 2001, Técnico em Eletrônica pela Escola Técnica Federal de Santa Catarina em 1990.