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 ESTUDIO DE TRANSFORMADORES, REACTORES, MATERIALES Y TECNOLOGÍAS EMERGENTES - GTM

APLICACIÓN DE RED WIRELESS PARA SISTEMA DE MONITOREO ONLINE EN LA SUBESTACIÓN SANTO ÁNGELO DE ELETROBRAS ELETROSUL

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

RESUMEN

Este informe técnico tiene por finalidad describir la tecnología de la red de comunicación wireless integrada junto al sistema de monitoreo dentro de la SE Santo Ángelo con el objetivo de mejorar el desempeño, la customización de la red de comunicación entre el campo y la sala de control y facilitar implementaciones futuras sin la utilización de nuevos cables y/o fibras ópticas.

PALABRAS CLAVE: Transformador, Conversor, Monitoreo, WLAN, Access Point.

1.0 - INTRODUCCIÓN

Las redes locales sin cable WLAN (Wireless Local Area Network) se constituyen como una alternativa a las redes convencionales con cable, con las mismas funcionalidades, pero de forma flexible, de fácil configuración y con buena conectividad en áreas prediales, residenciales o industriales.

Redes WLAN posibilitan, de esa forma, atender puntos de red con la misma eficiencia y hasta con una mejor relación costo-beneficio en relación con el sistema de cableado convencional en esos casos.

La instalación de redes wireless y de nuevos puntos de red elimina la necesidad de pasar nuevos cables, reduciendo el tiempo de configuración de nuevas posiciones de trabajo, y facilitan la construcción de estructuras en infraestructura. Una red wireless proporciona, de esa forma, todas las funcionalidades de una red cableada, pero sin las restricciones físicas del cableado propiamente dicho.

Actualmente la gran mayoría de las redes wireless permite plena conectividad y atiende a los patrones y normas de los órganos internacionales. Eso significa que, una vez utilizando equipos estandarizados, redes wireless pueden ser interconectadas con las redes de cableado convencional sin mayores problemas, y computadoras utilizando dispositivo wireless interaccionan con computadoras de la red cableada y viceversa sin cualquier restricción.

En esa categoría se permiten definir así varios tipos de redes, que son: Redes Locales Sin Cable o WLAN, Redes Metropolitanas Sin Cable o WMAN (Wireless Metropolitan Area Network), Redes de Larga Distancia Sin Cable o WWAN (Wireless Wide Area Network), Redes WLL (Wireless Local Loop) y el nuevo concepto de Redes Personales Sin Cable o WPAN (Wireless Personal Area Network).

Siendo así, las WLAN combinan la movilidad del usuario con la conectividad a velocidades elevadas de hasta 155 Mbps, en algunos casos.

Dependiendo de la tecnología utilizada, de la radiofrecuencia y del receptor, las redes WLANs pueden alcanzar

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

kilómetros según la potencia del equipo utilizado.

2.0 - CÓMO FUNCIONAN LAS WLANS

A través de la utilización de portadoras de radio, las WLAN establecen la comunicación de datos entre los puntos de la red. Los datos son modulados en la portadora de radio y transmitidos a través de ondas electromagnéticas. Múltiples portadoras de radio pueden coexistir en un mismo medio, sin que una interfiera en la otra. Para extraer los datos, el receptor sintoniza en una frecuencia específica y rechaza las otras portadoras de frecuencias diferentes.

En un ambiente típico, ver figura 1, el dispositivo transceptor (transmisor/receptor) o punto de acceso (access point) es conectado a una red local ethernet convencional (con cable). Los puntos de acceso no apenas proveen la comunicación con la red convencional, como también intermedian el tránsito con los puntos de acceso vecinos, en un esquema de microcélulas con roaming semejante a un sistema de telefonía celular.

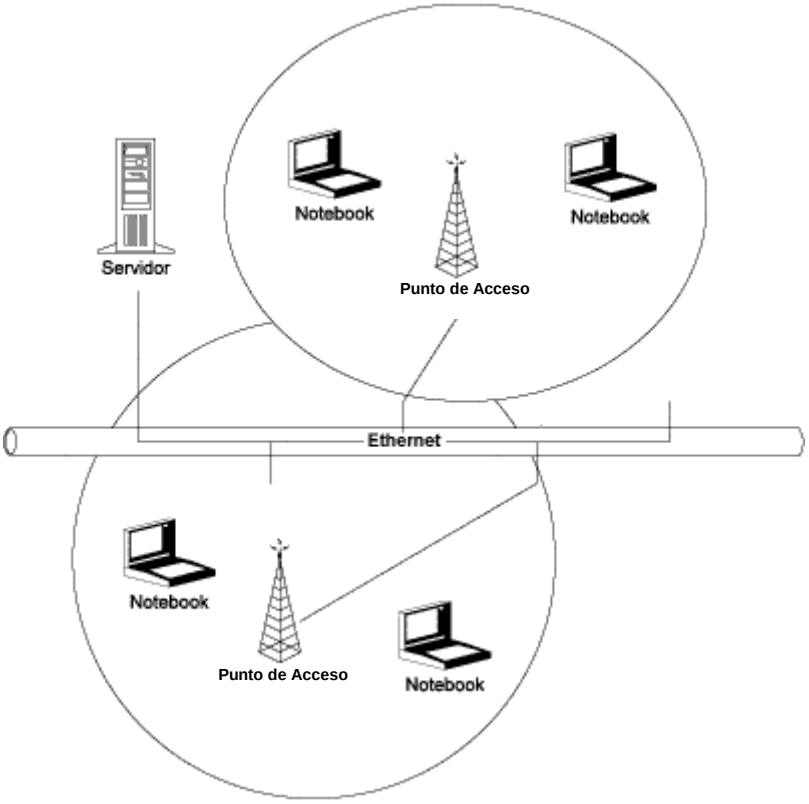

Figura 1 – Red wireless LAN típica.

2.1 Topología

Existen varias tecnologías involucradas en las redes locales sin cable, y cada una tiene sus particularidades, sus limitaciones y sus ventajas. Los sistemas Spread Spectrum utilizan la técnica de esparcimiento espectral con señales de radiofrecuencia de banda larga, brindando mayor seguridad, integridad y confiabilidad, a cambio de un mayor consumo de banda. Existen dos tipos de tecnologías spread spectrum: la FHSS, Frequency-Hopping Spread Spectrum, y la DSSS, Direct-Sequence Spread Spectrum – ver figura 2.

La tecnología FHSS usa una portadora de rango estrecho que muda la frecuencia en un código conocido por el transmisor y por el receptor que, cuando debidamente sincronizados, el efecto es el mantenimiento de un único canal lógico.

La DSSS genera un bit-code (también llamado de chip o chipping code) redundante para cada bit transmitido. Cuanto mayor el chip, mayor será la probabilidad de recuperación de la información original. Aún así, una mayor banda es requerida. Aunque uno o más bits en el chip sean dañados durante la transmisión, técnicas estadísticas embutidas en la radio son capaces de recuperar los datos originales sin la necesidad de retransmisión.

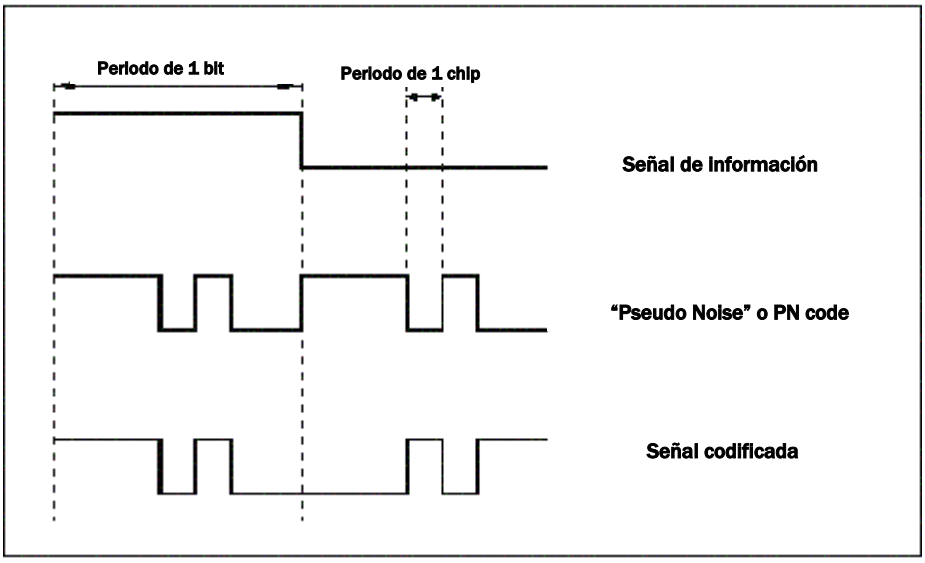

Figura 2 – Transmisión Spread Spectrum.

2.2.1 IEEE 802.11 Wireless Local Area Network

El patrón IEEE 802.11, ver figura 3, especifica tres camadas físicas (PHY) y apenas una subcamada MAC (Medium Access Control) provee dos especificaciones de camadas físicas con opción para radio, operando en el rango de 2.400 a 2.483,5 mHz (dependiendo de la reglamentación de cada país), y una especificación con opción para infrarrojo, son ellas:

a. Frequency Hopping Spread Spectrum Radio PHY
Esa camada brinda operación 1 Mbps, con 2 Mbps opcional. La versión de 1 Mbps utiliza 2 niveles de la modulación GFSK (Gaussian Frequency Shift Keying) y la de 2 Mbps utiliza 4 niveles de la misma modulación.

b. Direct Sequence Spread Spectrum Radio PHY
Esa camada brinda operación en ambas velocidades (1 y 2 Mbps). La versión de 1 Mbps utiliza la modulación DBPSK (Differential Binary Phase Shift Keying), mientras que la de 2 Mbps usa modulación DQPSK (Differential Quadrature Phase Shift Keying).

c. Infrared PHY
Esa camada brinda operación 1 Mbps, con 2 Mbps opcional. La versión de 1 Mbps usa modulación 16-PPM (Pulse Position Modulation con 16 posiciones) y la versión de 2 Mbps utiliza modulación 4-PPM.

En el lado de la estación, la subcamada MAC brinda los siguientes servicios: autenticación, desautenticación, privacidad y transmisión de la MADU (MAC Sublayer Data Unit) y, en el lado del sistema de distribución, asociación, desasociación, distribución, integración y reasociación. Las estaciones pueden operar en dos situaciones distintas:

a. Configuración Independiente
Cada estación se comunica directamente entre sí, sin la necesidad de instalación de infraestructura. La operación de esa red es fácil, pero la desventaja es que el área de cobertura es limitada. Estaciones con esa configuración están en el servicio BSS (Basic Service Set).

b. Configuración de Infraestructura
Cada estación se comunica directamente con el punto de acceso que hace parte del sistema de distribución. Un punto de acceso sirve las estaciones en un BSS, siendo su conjunto llamado de ESS (Extended Service Set). Además de los servicios arriba descritos, el patrón aún ofrece las funcionalidades de roaming dentro de un ESS y administración de fuerza eléctrica (las estaciones pueden desconectar sus transceivers para economizar energía). El protocolo de la subcamada MAC es el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidence).

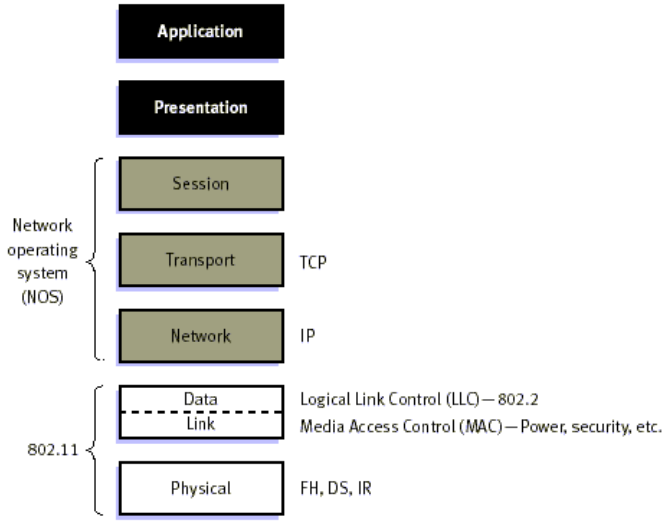

Figura 3 – Patrón de comunicación IEEE 802.11.

3.0 - SEGURIDAD EN LA WLAN

El mercado hoy día no tiene tantas preocupaciones cuanto a las implicaciones asociadas a la seguridad de ese tipo de red. Por otro lado, empresas de grande y medio porte aún están bastante preocupadas con el hecho de transmitir datos confidenciales por el aire.

Existen varios tipos de seguridad en WLAN 802.11. Será descrito el modelo utilizado en la SE Santo Ángelo.

3.1 Patrón de seguridad WPA (WI-FI Protect Access) 802.11

Teniendo en cuenta el gran número de vulnerabilidades encontradas en el protocolo WEP, el grupo que creó el patrón IEEE 802.11 inició pesquisas para el desarrollo de un nuevo patrón de seguridad denominado IEEE 802.11i. El intuito primordial era resolver todos los problemas de seguridad encontrados en el WEP. Mientras el patrón estaba siendo desarrollado, Wi-Fi Alliance, para responder a las críticas generadas por el medio corporativo con relación al WEP, presentó en 2003 un patrón denominado Wi-Fi Protected Access (WPA). El WPA es basado en el RC4 y en un subconjunto de especificaciones presentadas en una versión preliminar del IEEE 802.11i. El WPA introduce diversos mecanismos para resolver los problemas de seguridad asociados al WEP:

- Reglas para el IV (Vector) y IV extendido de 48 bits – Como los 24 bits de IV utilizados por el WEP permitían poco más de 16 millones de IVs diferentes, facilitando repeticiones en un corto espacio de tiempo, el WPA introduce un IV extendido de 48 bits. Así, más de 280 trillones de IVs diferentes son posibles. Adicionalmente, el WPA introduce reglas para la elección y verificación de IVs para tornar ataques de reinyección de paquetes ineficaces.

- Nuevo código de verificación de mensajes – El WPA usa un nuevo campo de 64 bits, el MIC (Message Integrity Code), para verificar si el contenido de un cuadro de datos posee alteraciones por errores de transmisión o manipulación de datos. El MIC es obtenido a través de un algoritmo conocido como Michael.

- Distribución y derivación de llaves – El WPA automáticamente distribuye y deriva llaves que serán utilizadas para la criptografía e integridad de los datos. Eso resuelve el problema del uso de la llave compartida estática del WEP.

3.1.1 Autenticación

Existen dos tipos de autenticación en el protocolo WPA. Uno direccionado para redes corporativas, que utiliza un servidor de autenticación 802.1x/EAP, por lo tanto una infraestructura complementar, y otro, más sencillo, proyectado para pequeñas redes en oficinas y redes domésticas (redes SOHO – Small Office/Home Office). Esos dos tipos de autenticación son denominados WPA Corporativo y WPA Personal, respectivamente.

- WPA Personal – Como un usuario común no es capaz de instalar y hacer el mantenimiento de un servidor de autenticación, fue creado el WPA-PSK (WPA-Pre Shared Key), que es una passphrase12, previamente

compartida entre el Access Point y los clientes. En ese caso, la autenticación es hecha por el Access Point. La llave es configurada manualmente en cada equipo perteneciente a la red y puede variar de 8 a 63 caracteres ASCII.

- WPA Corporativo – El Access Point no es responsable por ninguna autenticación. Tanto la autenticación del usuario cuanto del dispositivo es hecha por un servidor de autenticación. Es utilizada una infraestructura complementar formada por un servidor que usa el protocolo de autenticación 802.1x en conjunto con algún tipo de EAP (Extensible Authentication Protocol). El 802.1x es un protocolo de comunicación utilizado entre el Access Point y el servidor de autenticación. Ese protocolo ya era largamente utilizado en redes cableadas y se mostró también adecuado cuando integrado a las redes sin cable. Cuando un cliente solicita una autenticación, el servidor de autenticación verifica en su base de datos si las credenciales presentadas por el solicitante son válidas, en caso positivo el cliente es autenticado y se le envía una llave llamada Master Session Key (MSK). La mayoría de las veces, se utiliza como servidor de autenticación un servidor RADIUS, pero no es obligatorio.

3.1.2 Integridad

La integridad en el WPA es compuesta por dos valores. Además del ICV (Integrity Check Value), es adicionado al cuadro un mensaje de verificación de integridad denominado MIC (Message Integrity Check).

Michael es una función hash no linear, diferentemente del CRC-32. La dirección de destino dio la prioridad (actualmente fijado en cero), los datos y una clave de integridad que se inserta en Michael para producir el MIC. La salida corresponde a 8 bytes, que juntamente con el ICV forman la integridad del protocolo WPA. Por lo tanto, la integridad es representada por un total de 12 bytes, 8 generados por Michael y 4 por el CRC-32 – ver figura 4.

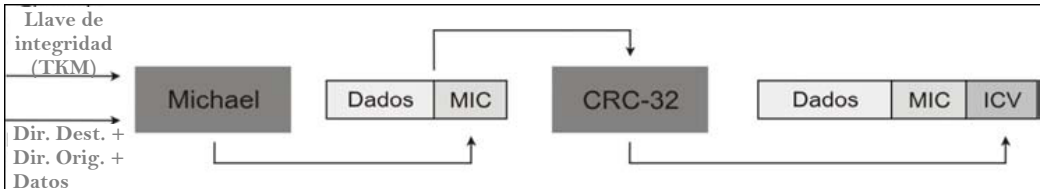

Figura 4 – Protocolo de Integridad del WPA.

3.1.3 Confidencia

El TKIP (Temporal Key Integrity Protocol) soluciona buena parte de las vulnerabilidades en el protocolo WEP. El TKIP es basado en el concepto de llaves temporales, o sea, la llave es usada durante cierto tiempo y después es sustituida dinámicamente.

En el WPA el vector de inicialización posee 48 bits, lo que vuelve prácticamente imposible haber reutilización de vectores. En la estructura del encabezado 802.11, el campo reservado para el IV solo contiene 24 bits, por eso fue creado otro campo llamado IV Extended, que no hace parte de la estructura del encabezado 802.11, para alocar el resto del IV. El IV también es utilizado como un contador de cuadros (TSC – TKIP Sequence Counter). Cuando una nueva llave de criptografía es establecida, el TSC es puesto a cero. A cada cuadro transmitido, él es incrementado. De esa forma, cuadros con TSC fuera de orden son descartados, evitando reinyecciones de paquetes.

El proceso de codificación del WPA es semejante al del WEP. La principal diferencia está en la llave que irá alimentar el RC4. Esa llave es el resultado de un algoritmo de combinación de llave cuya entrada es el vector de inicialización, la dirección MAC del transmisor y la llave de criptografía de datos. Al final, la llave generada por el algoritmo de combinación de llave y el IV son pasados para el RC4 – ver figura 5.

32 bits más significativos
32 bits más significativos

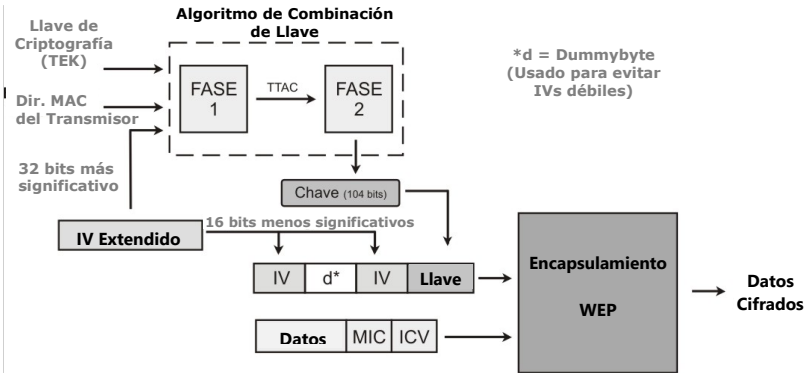

Figura 5 – Algoritmo de combinación de la llave WPA.

4.0 - APLICACIÓN DE LA RED WIRELESS EN LA SUBESTACIÓN SANTO ÁNGELO

El Sistema de Monitoreo para el banco de autotransformadores trifásicos 525/230-13,8kV - 224 MVA de la subestación de Santo Ángelo, TF3, tiene por objetivo reducir el riesgo de fallas catastróficas en ese equipo al efectuar el diagnóstico de su estado actual, detectando problemas que aún se encuentran en fase inicial de desarrollo, así como el pronóstico de problemas futuros con base en la progresión de las mediciones a lo largo del tiempo. Para eso, el sistema efectúa la adquisición y el almacenamiento de las mediciones de sensores inteligentes instalados en el autotransformador vía los conversores de red RS-485/wireless, así como el tratamiento de esos datos con la finalidad de transformarlos en informaciones útiles para el mantenimiento.

4.1 Arquitectura del sistema de monitoreo

El sistema de monitoreo está basado en una arquitectura descentralizada, compuesta básicamente de equipos de adquisición de datos, equipos de almacenamiento y tratamiento de datos y del medio de comunicación, que interconecta las dos primeras partes. Los equipos de adquisición de datos están en el propio cuerpo de los autotransformadores y en el cubículo común (QCC) y consisten en IEDs, equipos electrónicos basados en microcontroladoras y proyectados específicamente para instalación en autotransformadores, adecuados, por lo tanto, para operación en temperaturas de por lo menos -40 a +85ºC con hasta 95% de humedad relativa, siendo inmunes también a interferencias electromagnéticas y de radiofrecuencia. Esos IEDs miden grandezas del tipo temperatura del aceite, temperatura de los devanados, humedad en el conmutador, capacitancia y tangente delta en los bushings condensivos, gases disueltos en el aceite, membrana en el conservador y contactos secos.

4.2 Medio de comunicación de datos

Los equipos de adquisición de datos están interconectados por dos redes de comunicación serial patrón RS-485/wireless en los paneles de los autotransformadores y del cubículo común, a través de cable del tipo par trenzado blindado. La interconexión de los equipos de adquisición de datos con el sistema de almacenamiento y tratamiento de datos localizados en la central de monitoreo, en el Sertao Maruim, fue efectuada por red wireless, acrecentando los conversores y access point adecuados. El acceso remoto es hecho a través de la intranet de Eletrosul vía protocolo TCP/IP – ver figuras 6, 7 y 8.

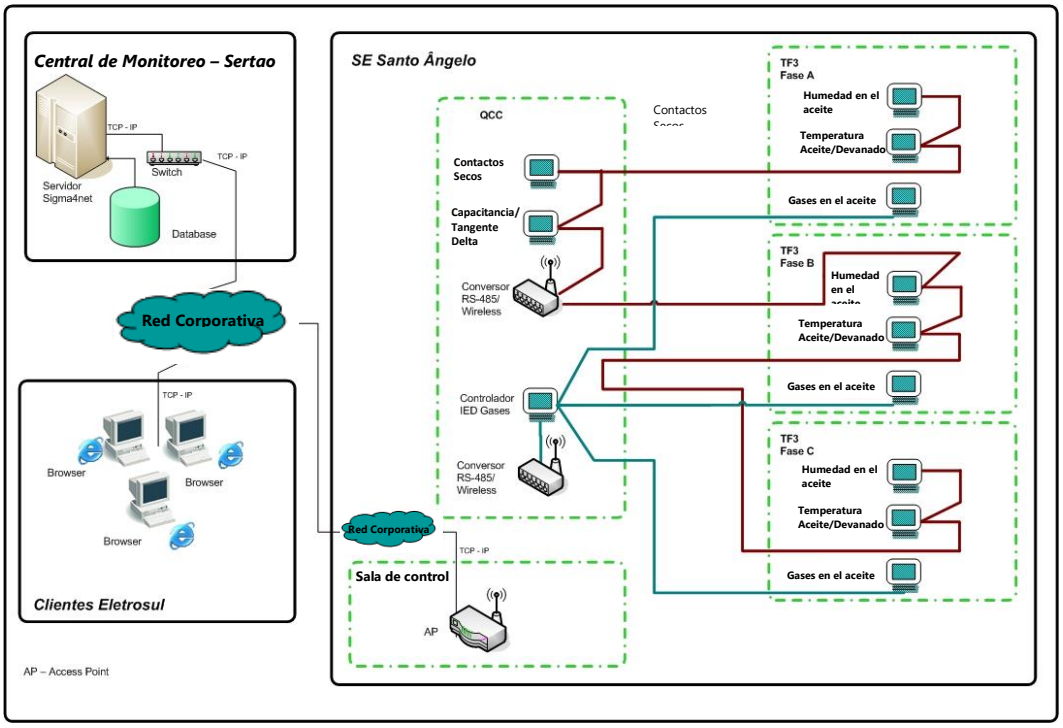

Figura 6 – Arquitectura de monitoreo de la SE Santo Ángelo.

Figura 7 – Panel con conversores RS-485/wireless.

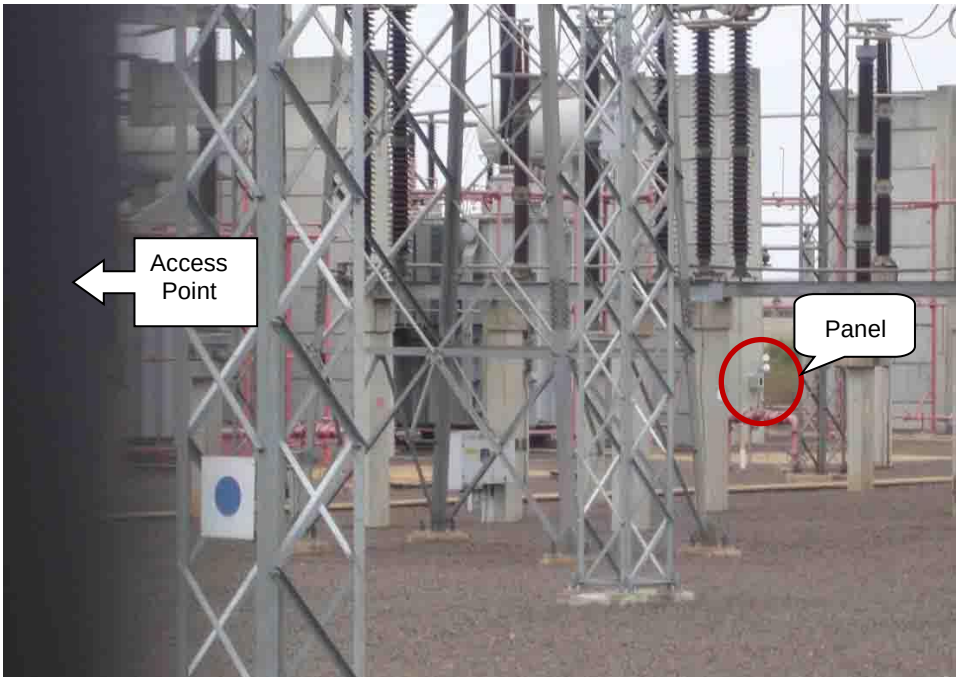

Figura 8 – Vista de la antena del access point y de las antenas de los conversores.

4.3 Seguridad

El access point instalado en la sala de control de la SE Santo Ángelo posee seguridad de autenticación WAP-PSK y método de criptografía TKIP, conforme descrito en el ítem 3.0 de este informe técnico. Así, los conversores instalados en la pared cortafuego están con la misma configuración. Para tanto, además de esas configuraciones, sus direcciones físicas de red están registradas en el access point, aumentando aún más la seguridad de las informaciones.

5.0 - CONCLUSIÓN

Desde la instalación del sistema de monitoreo en la SE Santo Ángelo en noviembre de 2009, esa aplicación de red wireless está en pleno funcionamiento, pudiendo ser expandida para otros equipos de la subestación al ponerle apenas los IEDs necesarios y un conversor RS-485/wireless, reduciendo el costo en la instalación con cables, fibras ópticas y hasta conversores adicionales.

6.0 - REFERENCIAS 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 - DATOS BIOGRÁFICOS

Clayton Sperandio Duriguetto - Nascido en Guarulhos/SP, el 9 de agosto de 1983, trabaja con Treetech Sistemas Digitais desde 2001. Especializado en desarrollo de sistemas de monitoreo y control de transformadores de potencia, disyuntores y redes industriales en el departamento de Ingeniería de Aplicación/Software. Licenciado en Sistemas de Información por la Facultad Eniac, Guarulhos/SP, en 2009, Técnico en Electroelectrónica por el Senai – Hermenegildo Campos de Almeida, en 2000 Guarulhos/SP.

Rafael Prux Fehlberg - Nascido en Porto Alegre/RS, el 13 de agosto de 1981, trabaja con Treetech Sistemas Digitais desde 2004 con ingeniería aplicada al monitoreo de equipos de subestaciones. Graduado en Ingeniería de Control y Automación por la PUC-RS, en 2003.

Fernando Temotheo de Carvalho - Nascido en Sao Paulo/SP, el 4 de enero de 1981, trabaja con Treetech Sistemas Digitais desde 2002. Especializado en desarrollo de sistemas de monitoreo y control de transformadores de potencia, disyuntores y redes industriales en el departamento de Ingeniería de Aplicación/Software. Graduado en Ciencias de la Computación por la Universidad Uninove, Sao Paulo/ SP, en 2004.

Sandro Peixoto - Nascido en Florianópolis/SC, trabaja en Eletrobras Eletrosul desde 2001. Especializado en ingeniería de sistemas de energía eléctrica, sistemas de monitoreo de equipos de patios de subestaciones de energía eléctrica. Graduado en Ingeniería Eléctrica por la UFSC, en 2001. Técnico en Electrónica por la Escuela Técnica Federal de Santa Catarina, en 1990.