Comité Nacional Paraguayo

Unión de Ingenieros de ANDE

X SEMINARIO DEL SECTOR ELECTRICO PARAGUAYO - CIGRÉ
19, 20 y 21 de setiembre de 2012

Elena Villalba[1], Mauricio Menon[2], Hugo Larangeira[2]

CIAC - Parque Tecnológico Itaipu[1], Itaipu Binacional[2]

<villalbaselva@gmail.com>, <menon@itaipu.gov.br>, <hugolas@itaipu.gov.py>

<Seguridad en el entorno IEC 61850: Análisis del PTP - Precision Time Protocol - 2008>

<Paraguay, Brasil>

RESUMEN

La sincronización de los relojes en sistemas distribuidos es una técnica que proporciona precisión a las aplicaciones en tiempo real para la automatización industrial y telecomunicaciones a través de la red Ethernet y mediante la cual, se hace posible que los dispositivos operen bajo una misma base de tiempo. IEEE 1588 *precision time protocol* (PTP) es el protocolo más importante actualmente, debido a que se adapta a las exigencias expuestas en IEC 61850.

En la actualidad se encuentran variadas soluciones para el sincronismo en estos sistemas. Existen soluciones IRIG-B, que requieren de redes dedicadas y separadas de la red Ethernet/IEC 61850 para alcanzar el desempeño temporal adecuado. Existen también soluciones que implementan el protocolo NTP/SNTP, donde la propia red Ethernet sirve de medio físico para la transmisión de mensajes de sincronismo de tiempo, en detrimento del desempeño. Los sistemas de sincronismo PTP presentan las mejores características de las dos soluciones abordadas anteriormente, es decir, utilizan el mismo medio físico de comunicación Ethernet para la transmisión de mensajes de sincronismo (NTP/SNTP) y están al nivel del desempeño alcanzado por las redes dedicadas IRIG-B. Es por este motivo que los sistemas PTP resultan atractivos en un entorno IEC 61850.

Dentro de una red IEC 61850 transitan mensajes con datos para supervisión, control, protección, monitoreo y osciloperturbografía de la subestación. Cada uno de ellos debe operar bajo una misma base de tiempo, de manera a permitir correlacionar eventos y en consecuencia viabilizar la distribución funcional entre los diferentes nodos de la red. El primer paso para la seguridad, es proteger a dicha red y esto incluye el sistema de sincronización de reloj.

La versión 2 del estándar IEEE 1588 (2008) incluye una extensión de seguridad, no solo para prevenir ataques dañinos sino para evitar perturbaciones accidentales o eventos indeseados en la red. Además, se presentan conceptos nuevos tales como el reloj transparente, medidas de retardo punto a punto, mayor tasa de sincronización de mensajes, protocolo de asignación UDP y medidas de seguridad.

Esta medida de seguridad incluye una extensión – anexo K–, que surge con la finalidad de proporcionar métodos para la protección e integridad de mensajes y datos, incluso en entornos abiertos donde los atacantes pueden obtener acceso directo.

Este artículo presenta la implementación de seguridad para envío de paquetes a través de una red Ethernet, efectuando la seguridad en la fuente de autenticación, protección contra ataques dañinos de repetición de los mensajes PTP, man-in-the-middle, integridad de mensajes y evaluar las soluciones adecuadas para cada caso.

PALABRAS CLAVES

PTP, seguridad, precisión, sincronismo, IEC 61850, IEEE 1588 V2.

I. INTRODUCCIÓN

IEEE 1588 define a estos tipos de relojes en un sistema PTP que se pueden clasificar en [1]:

- Reloj GMC (Grand Master Clock): Este reloj sirve de referencia para un dominio PTP, es decir, dicho reloj es la fuente de tiempos para la sincronización con los relojes esclavos. Sólo podemos disponer de un reloj GMC por dominio.
- Reloj M (Master Clock): Este reloj se encarga de proporcionar las referencias de tiempo a los relojes esclavos. Al igual que el reloj GMC, el reloj maestro sólo puede encontrarse uno por dominio.
- Reloj Ordinario / Ordinary Clock (CO): Un reloj ordinario IEEE 1588 es lo que comúnmente se refiere como un PTP cliente. Es el reloj más típico y se aplica a todos los relojes esclavos del sistema, tanto para una aplicación o dispositivo final.
- Reloj de frontera BC (Boundary Clock): Al disponer de varios puertos en un dominio PTP mantiene la escala de tiempo utilizado en el dominio y puede servir como una fuente de tiempo, es decir, ser un maestro, o puede sincronizar con otro reloj, es decir, ser un esclavo. Los relojes de frontera se requieren siempre que hay un cambio de la tecnología de la comunicación u otros elementos de red que bloquean la propagación de los mensajes PTP o siempre que haya un componente de red que inserte un retraso significativo [2]. Existe una alternativa a los relojes de frontera, que es el uso de switches transparentes.

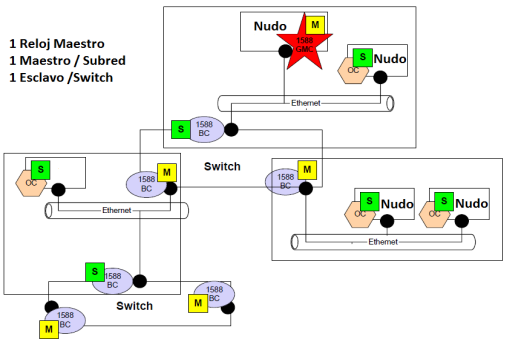

Figura 1. Red PTP

- Reloj Transparente / Transparent Clock (TC): Un switch transparente no se comporta como un nodo dentro del sistema, no obstante altera el contenido de temporización de paquetes PTP para compensar el retraso causado en los nodos, calcula la cantidad de paquetes en tiempo de sincronización y modifica la fecha y hora, por la inmediata.
  El estándar IEEE1588-2008 reconoce dos tipos de relojes transparentes:
  - Reloj Transparente Peer-to-peer (P2P TC): Proporciona el tiempo de tránsito PTP y el evento de la información, además de correcciones para el retraso de la propagación del enlace conectado al puerto de recepción del evento del mensaje PTP.
  - Reloj Transparente End-to-end (E2E TC): El reloj transparente E2E no corrige el retardo de propagación del enlace conectado al puerto.

Para la determinación de la funcionalidad y el tipo de cada uno de los relojes se utiliza el algoritmo BMC (Best Master Clock), que proporciona un mecanismo automatizado para elegir el mejor reloj maestro que hay en un dominio. Este algoritmo utiliza un árbol de decisiones sobre el que se basará diversos parámetros tales como la clase de reloj, la precisión del reloj y la prioridad del usuario. De esta manera si el reloj maestro falla, un segundo reloj maestro se puede seleccionar automáticamente de tal forma que no haya pérdidas de sincronismo en la red.
El protocolo IEEE 1588 incluye varios tipos de mensajes que permiten que el maestro y los relojes esclavos estén sincronizados y mantengan la red en tiempo uniforme y son utilizados por los relojes ordinarios y de frontera, ellos son:

- Mensaje Sync: Este mensaje es enviado por el reloj maestro de forma periódica a los relojes esclavos de la subred, dicho mensaje contiene una estimación del tiempo de cuando fue enviado.
- Mensaje Follow_Up: Un segundo mensaje desde el servidor para corregir errores en la sincronización
- Mensaje Delay_Req: A petición del cliente al servidor para medir el retardo. Cuando este recibe este tipo de mensaje el nodo esclavo envía el correspondiente mensaje Delay_Response, el cual contiene una estimación de tiempo de cuando fue recibido el mensaje Delay_Request.
- Mensaje Delay_Resp: Una respuesta desde el servidor al cliente con la medida del retraso.

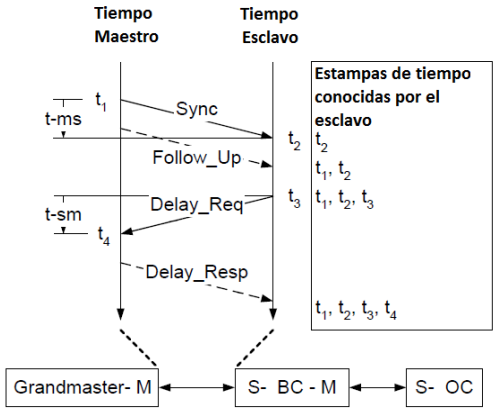

Figura 2. Mensajes en una red PTP

Tambien se distinguen los mensajes de eventos y entidades (tiempo de estampado en la salida de un nodo (reloj) y la entrada de un nodo): sync, delay_req, pdelay_req, pdelay_resp y los mensajes generales PTP, es decir, que no llevan una marca de tiempo son los siguientes: Follow_Up, Pdelay_Resp_Follow_Up, Announce, Management y Signaling. Básicamente estos mensajes proporcionan la información de estado y la transmisión del nodo que gerencia la red y del reloj Maestro. Las decisiones que repercuten de estas informaciones son las que darán la elección para el mejor reloj maestro. Además de servir de "puente" comunicando el valor de tiempo en la recepción de algún mensaje, informando la fecha y hora de envío.

II. MÉTODOS

La seguridad es un aspecto importante para el estándar IEEE 1588, éste debe proporcionar autenticación, protección de la integridad de todos los bytes del mensaje PTP y una autentificación mutua de los nodos. Es por tal motivo que el Estándar en su segunda edición, ha prescripto un anexo K experimental, llamado así porque se consideró que la experiencia debe ser adquirida en su uso [3].
Básicamente se compone de 2 mecanismos:

- Un mecanismo de protección a la integridad, el cuál utiliza un código con mensaje de autenticación para verificar que un mensaje recibido fue transmitido por una fuente autenticada, no fue modificada en el tránsito, y es "nuevo". (Es decir, no es una repetición). La protección contra las repeticiones es implementada usando otros contadores.

- Un mecanismo de respuesta de desafíos, el cuál es usado para afirmar la autenticidad de nuevas fuentes y mantiene "nuevas" las relaciones de confianza.

Con esto podemos concluir que la primera parte abarca la autenticación de los mensajes y la segunda parte se ocupa de la aprobación de la autenticidad de los grupos de origen [3].
Existen diferentes tipos de ataques contra las redes PTP, éstas se pueden organizar dependiendo del tipo de objetivo de la amenaza. Es necesario describir las violaciones que ocasionan fallos en la seguridad del protocolo.
Como primera medida se debe realizar la verificación de los mensajes entrantes a través de una asociación de seguridad (SA) que contiene el contador, un tiempo de vida y una clave de identificación. Por cada mensaje recibido correspondiente a dicha asociación se selecciona un identificador del puerto, dirección de origen, destino y dirección del protocolo.
El mecanismo anterior de por sí no es crítico, pero junto con el cálculo del ICV (Integrity Check Value) se pueden encontrar las vulnerabilidades de seguridad. El estándar IEEE 1588 especifica que el valor ICV se calcula sobre todos los campos del mensaje PTP a partir del primer octeto de la cabecera común y termina incluyendo el último octeto de la autenticación de seguridad TLV (Type Length Value).
Esto se traduce en una vulnerabilidad de seguridad importante ya que el protocolo de direcciones de red utilizado para la seguridad de las asociaciones no está protegido y por lo tanto un atacante puede modificar sin que sea capaz de ser detectado. A continuacion se detallan los análisis de los ataques expuestos contra la IEEE 1588.

1. Asociaciones de seguridad falsas

La asociación de seguridad (SA) contiene una fuente, el destino, la clave, el tiempo de vida del identificador y un contador. Éstas se organizan en tablas.
A la hora de realizar los ataques, los atacantes se basan en la creación de un gemelo a partir de una asociación de seguridad o restablecen una asociación de seguridad ya existente.
Los posibles ataques basados en el uso indebido de las asociaciones de seguridad pueden alterar los campos de los mensajes de sincronización, con esto un atacante puede realizar la adecuación de los mensajes de sincronización lo que causaría que los relojes esclavos se nieguen a sincronizar con el Maestro actual verdadero.
Esto puede causar una denegación de servicio (DoS), sin un genérico sistema de detección de intrusos (IDS) o redes de sensores para detectar el ataque, a menos que el IDS conozca los valores correctos de estos campos.

1.1 Creación de una Asociación de Seguridad Gemela

El funcionamiento normal es que se realice la autenticación mutua entre el reloj maestro y el reloj esclavo estableciéndose así la asociación de seguridad. En la figura 3 [5] se muestra dicho proceso de autenticación, además coloca el contador a 0.
En este caso un atacante se encuentra entre el maestro y el esclavo, este es capaz de modificar, grabar y repetir los paquetes.
Cuando se produce un ataque, el primer paso que se realiza es la modificación del mensaje de sincronización

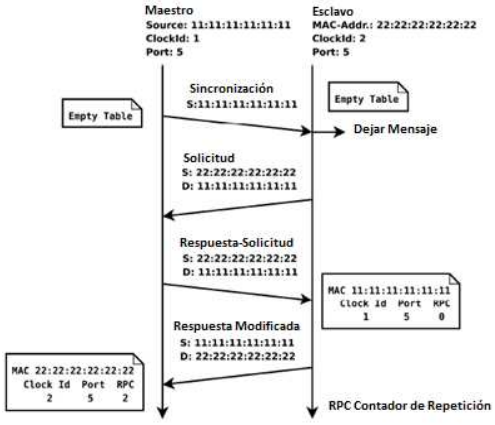

Figura 3. Funcionamiento normal en envio/recibo de mensajes

de tal manera que la dirección de la fuente se cambia a la dirección MAC del atacante (AA: AA: AA: AA: AA: AA). Este mensaje se repite modificado por el atacante y se inicia un nuevo desafío-respuesta de cambio desde la comprobación de ICV y se evalúa positivamente debido al hecho de que la dirección de protocolo no está incluida en el cálculo del ICV. La Figura 4 [5] muestra los detalles sobre cómo el nodo atacante reemplaza la dirección de origen del mensaje, y crea una nueva asociación de seguridad restableciendo el contador al valor inicial.

1.2 Ataque de repetición con una Asociación de Seguridad Gemela

En este ataque, el atacante graba paquetes enviados desde el maestro al esclavo. En este caso lo importante es que el contador del segundo SA se pone a cero cuando se inicializa.
El atacante tiene un mensaje antiguo y cambia la dirección de la fuente de tal manera que coincida con la dirección de la fuente de la segunda asociación de seguridad maliciosa. La repetición y modificación de este último mensaje no es detectado por el sistema de seguridad ya que el cálculo de ICV es correcto y el contador del mensaje es mayor que el contador de repetición de la asociación de seguridad. El objetivo principal de este ataque es cambiar el valor del reloj.

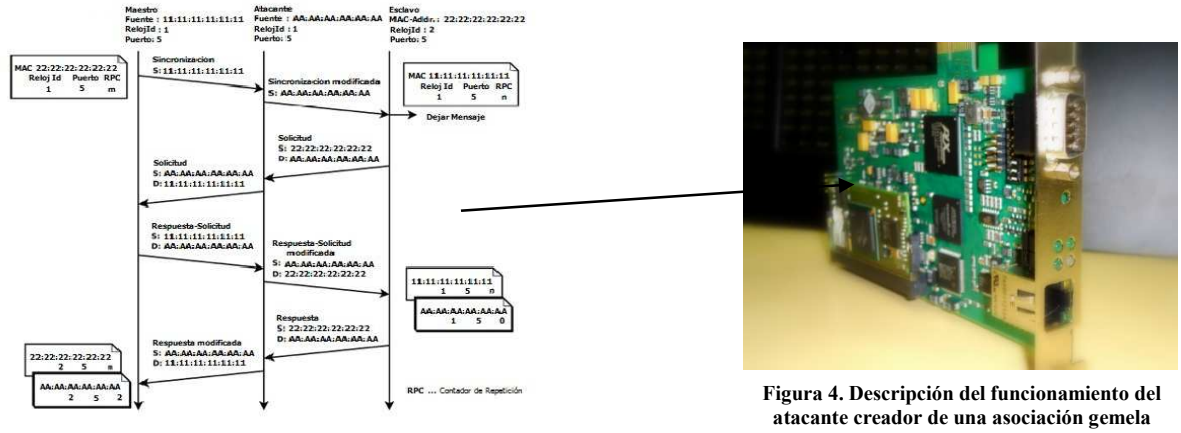

Figura 4. Descripción del funcionamiento del atacante creador de una asociación gemela

1.3 Ataques de repetición utilizando un Reset de la Asociación de Seguridad estática

En este ataque el atacante envía mensajes legítimos entre el maestro y el esclavo. A continuación, restablece la asociación de seguridad estática y el atacante comienza a reproducir los mensajes previamente grabados, mientras que al mismo tiempo suprime los mensajes legítimos del maestro.

2. Ataques Man-in-the-middle (MITM)

Los ataques MITM se basan en forzar a la maquina víctima, o a toda la red, a encaminar el trafico para la maquina del atacante, que por su vez, mantiene el flujo de la red reencaminando los datos, y con esto logra tener acceso a todo el tráfico, sea encriptado o no. Cuando todos los paquetes son atravesados por el atacante, es posible obtener claramente contraseñas de secciones sin codificación, robar secciones seguras, inyectar paquetes en una conexión dada de una víctima, alterar el contenido de los paquetes en circulación, eliminarlos o mismo aumentar la cantidad de datos.

III. Resultados.

La evaluacion de seguridad realizada sugiere que los ataques pasivos y/o activos pueden eliminar, modificar o reproducir mensajes en la transmisión en un supuesto evento, además de producir bloqueo e impedir la sincronización de los esclavos. Estas vulnerabilidades de seguridad están presentes en IEEE 1588 y afectan a todos los relojes maestros y esclavos existentes, así, permiten al atacante cambiar el valor del reloj de los mensajes. Además los mensajes más antiguos pueden ser reproducidos permitiendo la manipulación y la configuración del nodo.
Dentro de los límites de la norma sólo es válido inhabilitar el uso de asociaciones de seguridad dinámicas permitiendo sólo las asociaciones de seguridad estática con las direcciones preconfiguradas. De esta forma se inhibe la creación de asociaciones de seguridad dañinas. Sin embargo, esta solución tiene también un uso limitado, ya que la entrada SA deberá limitarse o de lo contrario el atacante puede secuestrar el segundo SA. Es por tal motivo que es necesario analizar las soluciones dentro de determinados puntos especificos, tal es asi como:

1. Solución para la protección de la dirección de la fuente

La solución es utilizar el campo sourcePortIdentity dentro de la cabecera del PTP para recuperar la dirección de origen o restaurar la dirección de protocolo de la fuente de acuerdo con [2, sección 7.5.2.2.3].
En el primer caso, algunas traducciones de direcciones necesitan ser implementadas. En el segundo caso la longitud de la dirección de red es de 6 bytes. Los protocolos de transporte especificados en la norma pueden causar problemas para las direcciones IPv6 de 16 bytes. La ventaja de la recuperación de la dirección de la fuente origen que ya es utilizado por algunas implementaciones y radica en el hecho de que la traducción no es un proceso necesario.
Los autores del IEEE 1588 han modificado el valor sourcePortIdentity través del campo para la verificación de seguridad. El campo PortIdentity contiene la dirección MAC y esta se utiliza en la tabla de búsqueda del SA.

2. Análisis del reloj transparente.

Dentro del análisis de la Version 2 del Estandar es fundamental tratar la descripción de la modificación de MAC por el reloj transparente. Las modificaciones de los campos de los mensajes son un punto particular, ya que desde el punto de
Ethernet ver una modificación del campo de la corrección es una modificación de la carga, los cambios del campo de la corrección no se permiten en la función relay como se especifica en el estándar IEEE 802.1 [3, cláusula 8.13.2].
Para mapear este comportamiento dentro de la IEEE 802.1 (normas D y Q), un reloj transparente no retransmite el marco que contiene la carga de costo de la IEEE 1588, más bien termina el link entrante y crea un nuevo marco con la dirección de acceso MAC del puerto de salida del puente y del campo de corrección modificado. Esto resulta en un reemplazo de la dirección fuente de los marcos. IEEE 1588 sólo demanda la modificación de “sumas de chequeo y otros campos de contenido relacionado” de una manera explícita. Esto resultó en la creación de una dirección MAC no modificada dentro de muchas implementaciones pero también dentro de la norma [5], en concreto en la aceptación de la tabla maestra, el master cluster y la extensión de seguridad. Aun así, esta especificación no es válida para la IEEE 802.1, la cual interfiere con las funciones de la IEE 1588.

3. Influencia en la seguridad del Protocolo

Las asociaciones de seguridad dependen de direcciones de fuentes protocolarias no modificadas, y, por eso, en caso de transferencia vía Ethernet, la búsqueda de la asociación de seguridad falla o causa comportamientos defectuosos si la dirección MAC es modificada.
En condiciones normales de trabajo la primera parte relevante de la IEEE 1588 que se ve afectada en cuanto a seguridad en la búsqueda de asignaciones de seguridad: una dirección de fuente de protocolo errónea causa un error de búsqueda. Si sólo las de asignaciones de seguridad estáticas están activadas, entonces el paquete está desactivado. Pero, si las de asignaciones de seguridad dinámicas están permitidas, el nodo intenta establecer una nueva SA con el reloj transparente. Ya que el reloj transparente no responde a la respuesta del desafío, el nodo esclavo retiene el modo de desafío y descarta todos los mensajes hasta que el desafío sufre un "time out". Esto puede llegar hasta el TCP timeout o causar infinitos loops. Incluso para timeouts menores que 10 segundos, como sugerido en (4), esto causa ciclos de espera enormes. Esto es un rechazo del servicio en el procesamiento (Challenge Response Cycle) como en los recursos de almacenamiento del nodo (tamaño de la tabla de asignaciones de seguridad).
También existe el caso en el cual un cambio de la dirección MAC causa una elección de otra SA. En esto contexto, un problema más teórico – muy difícil que ocurra en la práctica- es que la dirección MAC se use no sólo para reenviar mensajes PTP, sino también para otros servicios PTP originados por el reloj transparente.
Para la implementación basada en IP, un cambio en la dirección MAC no interfiere en la seguridad, una vez que la seguridad dependa únicamente de la IP.
Exclusivamente en mensajes unidireccionales, puede ser posible crear entradas dobles para las funciones núcleo de la norma.
Por seguridad se requiere la solución que usa el campo fuentePortidentity dentro del título PTP. Esta solución también es recomendada para operación normal.

IV. Conclusiones

El protocolo PTP por sí solo es débil frente a los efectos de ataques de modificación, enmascaramiento, retraso, repetición y/o denegación de servicio, y necesita de mecanismos de seguridad adicionales para proteger dicha red, ya que carece de mecanismos eficaces de seguridad para garantizar la integridad de los mensajes transmitidos y para validar la fiabilidad del remitente. Esto lo vuelve vulnerable y los adversarios pueden usar esta debilidad para realizar ataques genéricos, tales como la saturación de las víctimas y eliminar o modificar los mensajes PTP. Además, un adversario puede montar ataques PTP específicos, que son poco probables de ser detectados por los sistemas genéricos de detección de ataques, sin necesidad de realizar una profunda inspección y el mantenimiento del estado de protocolo.
Debido a que cada reloj PTP elige a su maestro de manera autónoma utilizando el contenido de los mensajes de sincronización de los últimos, una información privilegiada puede ganar fácilmente el algoritmo del mejor reloj maestro a través de la observación del tráfico PTP y la inyección de una sincronización del mensaje con mejor tiempo. Así, el atacante luego de convertirse en un maestro puede controlar a la víctima, siendo capaz de modificar un solo campo en los mensajes de sincronización PTP, además de alterar la jerarquía PTP por la suplantación de identidad en los mensajes de sincronización.
Cabe destacar además, que en el marco de un proceso real de actualización y/o ampliación del sistema de automatización de una subestación co-existen tecnologías de edades diferentes, siendo frecuente el uso de interfaces que permitan integración. El uso de interfaces agrega el problema de seguridad de la red.

La forma más directa contra la mayor parte de las amenazas anteriores es la del uso de los mecanismos de protección de la integridad de mensajes basados en técnicas criptográficas. Desafortunadamente, las técnicas criptográficas pueden introducir retrasos de prohibición o, peor aún, aumentar las fluctuaciones de retardo, lo que podría ser fatal, esencialmente en un entorno IEC 61850 donde la precisión de sub-microsegundos es de suma importancia. Por lo tanto una dirección interesante de estudio es el de validar la viabilidad de medidas criptográficas que se podrían aplicar a PTP.

V. Referencias

[1] Roger Moore, "Time Synchronization with IEEE 1588", PAC World Summer 2009.
[2] Website http://www.IEEE1588.com
[3] IEEE 1588 Version 2. Geoffrey M. Garner, Consultant - September 24, 2008
[4] A. Treytl, G.Gaderer, B.Hirschler and R.Cohen, "Traps and pitfalls in secure clock synchronization" in Proceedings of 2007 International Symposium for Precision Clock Synchronization for Measurement, Control and Communication ISPCS 2007.
[5] Treytl, Albert; Hirschler, Bernd. "Security Flaws and Workarounds for IEEE 1588 (Transparent) Clocks" in Proceedings of 2009 International Symposium for Precision Clock Synchronization for Measurement, Control and Communication ISPCS 2009.
[6] Menon, Mauricio; Habib Igor "Análise de performance do PTP (Precision Time Protocol) en VIII Seminario del Sector Eléctrico Paraguayo – Cigré. SESEP 2010.
[7] IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.
[8] A.Cascaes Pereira, D.Caceres R Perllizzoni. "Automacao de Subestacoes e Usinas – Estado de Arte e Tendencias Utilizando a Norma IEC 61850". Rio de Janeiro – Brasil.
[9] Bennington Jeremy. "The role of Grandmaster, Boundary and Ordinary Clocks in IEEE 1588 Precision Time Protocol (PTP) for frecuency synchronization over packet networks" at publishet in Analogzone.com.
[10] Tsang, Jeanette; Beznosov Konstantin. "A security Analysis of the Precise Time Protocol". Laboratory for Education and Research in Secure Systems Engineering (LERSSE), University of British Columbia. December, 2006.
[11] Loschmidt, Patrick. "On Enhanced Clock Synchronization Performance
Through Dedicated Ethernet Hardware Support". Vienna University of Technology, 2011.

VI. Biografías

Elena Villalba nació en el año 1987 en Ciudad Pte Stroessner, Paraguay. Es Ingeniera Electricista recibida de la Facultad Politécnica - Universidad Nacional del Este. Actualmente desarrolla Investigaciones en el Área de Sincronismo de Tiempo aplicado en Subestaciones y pertenece al Centro de Investigación de la Facultad Politécnica UNE donde se encuentra desarrollando proyectos de estudio de las tecnologías de mediciones fasoriales sincronizadas. Áreas de Interés: Protecciones y Estabilidad de Sistemas Eléctricos, Sincronismo de Tiempo, Sincrofasores, PMU.

Mauricio Menon nació en el año 1981 en Curitiba, Brasil. Es Ingeniero Electricista de la Itaipu Binacional, recibido en la Universidad Tecnológica Federal del Paraná. Especializado en Sincronismo de

Tiempo basado en la Norma IEC 61850 en la Universidad Estadual del Oeste del Paraná. Trabajó en Siemens, Nokia-Siemens y Huawei, entre otras actividades de investigación sobre redes, NGN (voip). Actualmente desarrolla investigaciones en el área de sincronismo de tiempo e IEC 61850.

Hugo Larangeira nació en 1981 en Asunción, Paraguay. Es Ingeniero de Control y Automatización recibido en la Universidad Federal de Santa Catarina. Especializado en Automatización, Control y Supervisión del Proceso Eléctrico basado en la Norma IEC 61850, en la Universidad Estadual del Oeste del Paraná. Actúa en el área de Proyectos de Automatización de Sistemas Eléctricos de Potencia en la Itaipu Binacional. Áreas de Interés: Automatización de Sistemas Eléctricos, Redes de Comunicación, Sincronismo de Tiempo, Osciloperturbografía.