Aspectos básicos de seguridad y QoS en redes de datos sobre Power Line Communications.

Aspectos básicos de seguridad y QoS en redes de datos sobre Power Line Communications.[1]

Basic aspects of security and QoS in data networks on Power Line Communications.

Juan Carlos Vesga Ferreira[2]
[1]Corporación Universitaria de Investigación y Desarrollo, Colombia.

Artículo recibido en el mes de Septiembre de 2013; artículo aceptado en Noviembre de 2013.

Citación del artículo: Vesga, J. C. (2013). Aspectos básicos de seguridad y QoS en redes de datos sobre Power Line Communications. *I+D Revista de Investigaciones*, 2(2), 99-114.

Resumen

Actualmente la seguridad informática es una necesidad, ante la expansión de las redes, para garantizar la disponibilidad, la confidencialidad y la integridad de la información en usuarios públicos y privados. El uso de la red eléctrica como medio físico de transmisión, ha sido considerado como una excelente alternativa en la prestación de servicios de interconexión de última milla. El uso de adaptadores de red basados en *Power Line Communications* (*PLC)* facilitan el diseño de redes *LAN* y comunicaciones de banda ancha a través de la red eléctrica, convirtiendo cualquier tomacorriente en un punto de conexión para el usuario, sin la necesidad de cableados adicionales a los existentes, en donde la seguridad en la red y la calidad de servicio (*QoS / Quality of Service*) se convierten en aspectos de vital importancia a la hora de implementarlas. En este artículo se reflexiona sobre la seguridad en la red y la calidad del servicio (QoS), elementos que juegan un papel importante en la administración y la eficiencia de una red centrada en aplicaciones, utilizando la red eléctrica como medio físico de transmisión desde el análisis simple del estándar *HomePlug* 1.0®.

Palabras clave: OSI, PLC, Seguridad, acceso, QoS.

[1]Artículo de reflexión, de enfoque cualitativo, resultado de un proyecto de investigación, desarrollado en el grupo de investigación GIDSAW de la Corporación Universitaria de Investigación y Desarrollo (UDI) (Colombia). Dirección: Calle 9 No.23-55. PBX. 6352525. La investigación fue financiada por la UDI.

[2]Ingeniero Electrónico, Universidad Industrial de Santander. Ingeniero de Sistemas, Universidad Manuela Beltrán. Magíster en Ingeniería Area Telecomunicaciones, Universidad Pontificia Bolivariana. Docente-investigador del grupo GIDSAW. Corporación Universitaria de Investigación y Desarrollo (UDI) Bucaramanga (Colombia). Dirección; Calle 9 No. 23-55. PBX:6352525.Correo-e: Juancarlos.vesga@udi.edu.co.

Abstract

Currently the information security is necessary because of the expansion of networks and in ensuring the availability, confidentiality and integrity of the private or public user's data. The use of the electric wire cable net as a physical mean to transmission has been regarded as a right choice in the provision of the data inter connection service. The use of the network adapters based on *Power Line Communications* (*PLC)* facilitate the making of *LAN* networks and bandwidth communications through electric wire cable net, converting any outlet into a connection point for user, without any additional wire than those before existing, where the network security and the quality of service provided (*QoS / Quality of Service*) become into important aspects in the implementation process. In this paper a reflection is done about data security in the network and the quality of the service (QoS), elements that plays an important role in the administration and efficiency of a network centered in applications, using the electric wire cable net as a physical mean for transmission from de simple analysis of the *HomePlug* 1.0® standard.

Keywords: OSI, PLC, Security, access, QoS

Introducción

En la era actual, el activo más importante de la gran mayoría de las empresas es la información. Por tal razón, se deben establecer mecanismos de control que ayuden a garantizar la integridad de la misma, y de allí la importancia de elegir e implementar adecuadamente los sistemas y métodos de seguridad más idóneos, que protejan sus redes y sistemas ante eventuales amenazas. La seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones y dispositivos encargados de preservar la integridad, disponibilidad y confiabilidad de la información de un sistema informático y sus usuarios. Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero se pueden asumir medidas de seguridad eficientes que permitan evitar daños y problemas ocasionados por intrusos.

Hoy en día se hace cada vez más imprescindible y necesario un adecuado sistema de protección en los sistemas informáticos, que garantice desde la privacidad de los datos hasta la seguridad en las transacciones de información; y la tecnología PLC no es la excepción. Cualquier computador conectado directa o indirectamente a una red, puede convertirse en una fuente potencial de uso no autorizado a sistemas de información, independientemente de la importancia del servicio que ofrezca o del tipo de información que contenga. Además, las técnicas y metodologías de ataque informático están evolucionando continuamente, al mismo tiempo que evoluciona la complejidad de las redes y los sistemas que las integran.

Por otra parte, la red eléctrica no fue diseñada para realizar procesos de comunicación, sino para el transporte de energía eléctrica. Aunque la red eléctrica no ha sido diseñada para establecer procesos de comunicación a alta frecuencia, actualmente es considerada objeto de estudio, debido a que estaba siendo subutilizada. La red eléctrica es considerada un medio hostil para la transmisión de información, donde se pueden

presentar numerosos problemas en el momento de establecer un proceso de comunicación, aspectos que pueden afectar considerablemente la calidad del servicio (QoS) en la red PLC a la hora de implementar aplicaciones para transmisión de voz, datos o video.

El presente artículo de reflexión, detalla aspectos relacionados con la alternativa antes descrita como opción viable para la seguridad informática.

Seguridad en redes PLC.

La seguridad ha sido un elemento muy crítico en redes cableadas e inalámbricas, y las redes basadas en PLC no son la excepción. Aunque el cableado eléctrico de PLC es también un medio compartido por los diversos dispositivos de red, tal como ocurre en las redes *WLAN*, es mucho más difícil tener acceso a él y representa un peligro importante debido a la presencia de la señal de 110-220 V, 50-60 Hz.

En las redes PLC, al igual que en las redes cableadas, es posible establecer mecanismos de seguridad ante cualquier amenaza mediante la adición de servidores de autenticación o configuración de redes virtuales privadas (en inglés: Virtual Private Networks (VPN)). La seguridad es una cuestión importante para el despliegue de redes de área local en las empresas, donde se sustenta el desarrollo de aplicaciones de telefonía IP. En este contexto, es esencial contar con mecanismos de seguridad fiables para evitar cualquier "escucha" de comunicaciones no autorizadas.

En Colombia, al igual que en diversos países, los hogares obtienen el suministro de energía eléctrica a partir del mismo transformador, por lo cual, el circuito eléctrico que conformaría la red se extiende más allá de los límites de una simple residencia. En vista de lo anterior, el estándar HomePlug 1.0® establece mecanismos de separación entre redes PLC creando redes lógicas por encripción. La privacidad y el esquema de seguridad del estándar HomePlug está basado en el estándar de encripción de datos de 56-bits (DES 56-bit) (Hrasnica, Haidine & Lehnert, 2004).

HomePlug implementa un sistema de red privada de PLC basado en claves de cifrado conocidas por dispositivos autorizados PLC. Este mecanismo corresponde a un registro sencillo, seguro y confiable de los diversos dispositivos PLC que se encuentren en la misma red lógica. Cada estación posee un adaptador PLC, el cual mantiene un cuadro de claves de encripción asociada a una EKS (*Encryption Key Select*). El EKS permite establecer un índice para identificar cada clave de encripción. Cuando se transmite un *frame*, se usa una clave para encriptar el cuerpo del *frame* y otra asociada a un EKS, la cual es incluida en el encabezado del frame. La estación receptora usa la EKS para seleccionar la clave de encripción asociada al mensaje de su cuadro de claves, para desencriptar el cuerpo del frame de manera apropiada (Carcele, 2006). Todas las transmisiones en una red lógica son encriptadas con una clave de encripción de red compartida (NEK, *Network Encryption Key)*. Un aspecto importante es que existe una única NEK, la cual define una red lógica (ver figura 1). Para que una estación pueda formar parte de una red lógica en

particular, esta debe tener el respectivo NEK de la red y la EKS correspondiente (Benyouef, 2003). Una red PLC puede configurarse con un NEK de varias maneras:

(a) a través de la interfaz Ethernet.

Un frame de configuración de la NEK, es enviado en modo broadcast a los dispositivos PLC presentes en la misma red, mediante una herramienta de configuración. Todos los dispositivos PLC conectados por medio de su interfaz Ethernet, recuperan esta configuración.

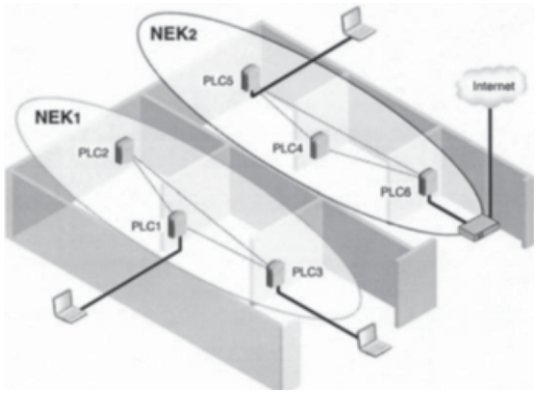
(b) a través de la interfaz eléctrica.

Se envía a través de la red eléctrica a los dispositivos conectados del PLC. Esto sólo es posible si una segunda clave, llamada DEK (Default Encryption Key / Clave de encripción por defecto) es conocida. Esta clave, que es específica para cada dispositivo PLC, se encuentra grabada en la memoria del dispositivo por el fabricante, siguiendo las especificaciones de HomePlug. La DEK es utilizada por dos dispositivos PLC: el dispositivo configuración de la estación y el dispositivo que debe recibir el nuevo NEK para el intercambio cifrado NEK.

(c) Interfaz a través de una Web.

Si los dispositivos PLC son avanzados, las configuraciones de las claves pueden ser administradas mediante una simple interfaz Web.

Figura 1. Redes lógicas PLC con diversos NEK



Fuente: Autor.

La autenticación de un dispositivo PLC consiste en conocer la NEK que identifica la red a la que pertenece. Si un dispositivo PLC no posee la NEK correcta, no puede intercambiar datos con los dispositivos de la red PLC a la que desea conectarse. En HomePlug 1.0® hay dos claves de cifrado, NEK y DEK, almacenadas en un registro específico para cada dispositivo y accesible mediante el parámetro EKS (Encryption Key Select / Clave de encripción seleccionada) (Campista & Costa, 2005). El NEK identifica la red PLC de la misma manera como la *wired equivalent privacy* (WEP) que se utiliza para proteger los datos de una red WLAN, en donde se realizan las siguientes funciones: (a) Creación de varias redes PLC en la misma red eléctrica, (b) Cifrado de los datos que fluyen entre los dispositivos PLC, (c) Autenticación de los dispositivos pertenecientes a la red PLC. En HomePlug®, el valor predeterminado NEK es igual, en ASCII, a 0x46D613E0F84A764C, que es equivalente a la palabra HomePlug®. Si un usuario no entrenado desea implementar una red PLC sin nociones de configuración de red, el precio a pagar es la ausencia total de seguridad, en la medida en que todos los dispositivos tendrán la misma NEK y por ende podrán

intercambiar entre sí toda la información que circule a través del cableado eléctrico (Benyouef, 2003).

Posibles formas de ataque a redes PLC.

El objetivo de un ataque no está restringido solamente a capturar información que circula a través de la red, sino que también puede orientarse a perturbar el óptimo funcionamiento de la red. A continuación se presentan tres tipos de ataques muy posibles en redes basadas en PLC.

Ataques de descifrado.

El objetivo de este ataque consiste en intentar descubrir la NEK de una red PLC para conectarse a ella y acceder a la información que circula a través de ella. Las técnicas que se utilizan para descubrir la NEK en HomePlug 1.0® son las siguientes: (a) Realizar la captura de una gran cantidad de paquetes para su posterior análisis bajo el uso de herramientas software de extracción de contraseñas semejantes al *Backtrack, Wifislax y Wifiway* utilizadas en redes WLAN, (b) Probar todas las combinaciones posibles de NEK para tener acceso a la red. El tiempo que sea necesario para probar todas las combinaciones posibles de NEKs se puede calcular de la siguiente manera:

El NEK se codifica con el algoritmo DES de 56 bits derivado de una contraseña introducida por el usuario de la red PLC, que puede variar de 4 a 24 caracteres. Por lo tanto, es el número máximo de intentos posibles (Benuouef,2003; Campista & Costa,2005):

$$N = 2^{58} \approx 2.88 * 10^{17}$$

Para una trama de Ethernet de 64 bytes con una tarjeta de interfaz de red 100-Mbit/s, es el tiempo de transmisión:

$$T_{frame} = \frac{64 * 8\ bits}{100 * 1024 * 1024} \approx 4.88 * 10^{-6} seg$$

El tiempo total necesario probar todas las combinaciones de entonces es:

$$T_{total} = N * T_{frame} = 2.88 * 10^{17} * 4.88 * 10^{-6} \approx 1.4 * 10^{12} seg \approx 44{,}591\ años$$

En vista de lo anterior, se evidencia que esta técnica requiere demasiado tiempo para utilizarse de forma eficaz.

Ataques de denegación de servicio.

El objetivo de este tipo de ataque consiste en sabotear la red impidiendo su funcionamiento. En redes basadas en PLC, este tipo de ataque se puede implementar mediante el uso de una unidad de radio que opere en la banda de frecuencias de 1 a 30 MHz, generando interferencias y con ello afectando el rendimiento de la red. Este ataque es el más sencillo de implementar. Lamentablemente, también es inmanejable.

Calidad de servicio QoS en redes PLC

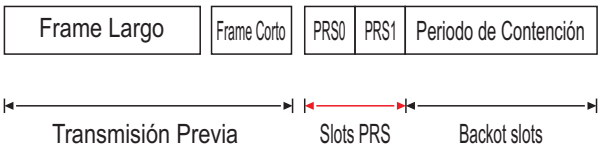
Calidad de servicio o QoS (*Quality of Service*), es un conjunto de requisitos que la red debe cumplir para asegurar un nivel adecuado para la transmisión de la información (voz, datos o video). [12]. Para establecer un adecuado QoS, se fijan niveles de prioridad al tráfico que circula por la red, etiquetando cada una de las tramas y

garantizando un ancho de banda adecuado, permitiendo ofrecer a los usuarios bajos niveles de retardo en la transmisión de datos en una red de extremo a extremo. La red eléctrica es considerada un medio de transmisión hostil para medidas de Calidad de Servicio, debido a su variabilidad con el tiempo (Tang, So, Guanwan & Chen, 2001; European Telecommunications Standards Institute, 2003). A partir de configuraciones definidas por la red eléctrica, la calidad de servicio debe ser analizada por su desempeño en la variación de los siguientes parámetros (Jensen, Slavensky & Kjaersgaard, 2006): (a) Cantidad de usuarios conectados simultáneamente, (b) Tipos de aplicación, (c) Protocolo de transporte, (d) Tamaño del paquete IP (Internet Protocol), (e) Dirección del tráfico (upload y download).

Para ello, los parámetros mínimos que se deben analizar son: (a) Tasa de pérdidas de paquetes, (b) *Throughput,* (c) Prueba de latencia (pertinente para aplicaciones "real equipo"), (d) *Jitter* (variación del atraso) verificación de la priorización del tráfico de servicios, (e) Análisis de priorización de tráfico.

En las redes PLC se establece un mecanismo de resolución de prioridad, el cual proporciona acceso al medio de manera distribuida. Debido a la naturaleza distribuida de este mecanismo, no se requiere de un nodo central para coordinar el acceso al medio. En HomePlug 1.0®, la calidad de servicio se proporciona diferenciando el tipo de tráfico que circula por la red PLC en 4 niveles de prioridad: CA0, CA1, CA2 y CA3. Los dos primeros (CA0 y CA1), son considerados tráfico de baja prioridad y los niveles CA2 y CA3 tienen las prioridades más altas (HomePlug PowerLine Alliance, 2001; Lee, Newman, Latchman, Katar & Yonge, 2003). Como parte fundamental del mecanismo de resolución de prioridad, se encuentra el PRS (Priority Resolution Slot) y las señales de resolución de prioridad. Después del final de cada transmisión, HomePlug 1.0® organiza la resolución de prioridades con el fin de administrar el tráfico mediante dos slots de resolución de prioridad (PRS0 y PRS1) y luego se asigna un periodo de contención donde se debe dar la aprobación al nodo con la más alta prioridad. La figura 2 muestra la ocurrencia de las señales de resolución de prioridad con respecto al final de la transmisión previa y el subsecuente periodo de contención.

Figura 2. Resolución de Prioridad



Fuente: Autor. Tomado de Jung,Chung & Lee (2005)

En el cuadro 1 se ilustra el uso de los slots PRS0 y PRS1, acorde con el tipo de prioridad que poseen sus paquetes para hacer uso de éstos. Estas prioridades se encuentran establecidas según el estándar 802.1D (Lee, Newman, Latchman, Katar & Younge, 2003; Lee & Tripathi, 2007).

Cuadro 1. Prioridades sobre HomePlug 1.0® para administración de tráfico

Prioridad	PRS1	PRS0
CA3	SI	SI
CA2	NO	SI
CA1	SI	NO

Fuente: Autor. Tomado de Lee & Tripathi (2007).

Dentro de las tramas Ethernet IEEE 802.3, existe un campo utilizado para codificar VLANs según la norma IEEE 802.1Q. En el marco de las redes PLC, las cuales operan en el modo *peer-to-peer* (igual a igual), este campo se utiliza para etiquetar las tramas según el valor del nivel de prioridad establecido en los slots PRS. El campo está compuesto por 3 bits, por lo cual es posible obtener hasta ocho valores posibles. En el cuadro siguiente se indican los valores asignados a este campo según el nivel de prioridad (Lee, Newman, Latchman, Katar & Younge, 2003).

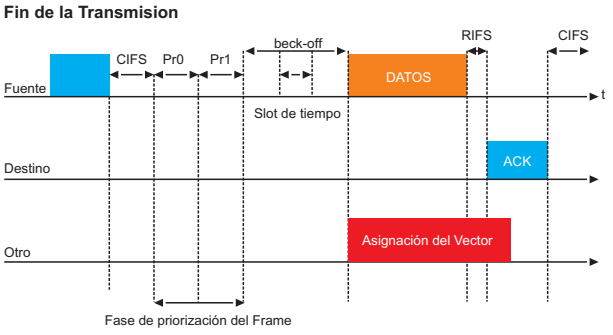
Cuadro 2. Etiquetas según el nivel de prioridad

Prioridad de acceso al canal	Valores de prioridad utilizados como etiqueta VLAN	Tipo de Tráfico
Prioridad 3	7.6	"Voz" - caracterizado por retardos y jitter inferiores a 10ms (ejemplo: VoIP)
Prioridad 2	4.5	"Video" o "audio" caracterizado por retardos inferiores a 100ms
Prioridad 1	0.3	Transferencias masivas y otros tipos de tráfico
Prioridad 0	1.2	La peor condición de tráfico

Fuente: HomePlug 1.0 Specification, HomePlugPowerline Alliance, June 2001.Reproducido con autorización.

Los dos PRS informan a todas las estaciones sobre las prioridades de otras estaciones esperanzadas en acceder al medio, acorde con las políticas para la administración del tráfico. A partir de allí, comienza la disputa entre estaciones por acceder al medio, mediante los procedimientos de *back-off* de azar. En la figura 3 se ilustra el diagrama de Secuencia para envío de datos por HomePlug 1.0®

Figura 3. Diagrama de Secuencia para envío de datos por HomePlug 1.0®



Fuente: Autor. Tomado de Bumler(2003)

Algoritmo de Back-Off

El estándar HomePlug 1.0® utiliza el CSMA/CA como método para controlar el acceso al canal de transmisión. Cuando una estación PLC desea transmitir, debe esperar hasta que el medio está disponible para hacerlo. La estación debe esperar hasta que un IFS (*Inter Frame Spacing* / Espaciado entre tramas) esté libre en un período de tiempo aleatorio denominado "tiempo de back-off" (Carcele, 2006; Guillen, López & Barahona, 2008). El algoritmo de *back-off* define una ventana de contención (CW / Content Window) o ventana de *back-off*. Este parámetro corresponde al número de ranuras de tiempo que pueden ser seleccionadas en el momento de calcular el tiempo de *back-off* de las diversas estaciones en la red PLC, con el fin de que todas tengan la misma probabilidad de acceder al medio.

El algoritmo de *back-off* para HomePlug 1.0® hace uso de tres contadores: Contador de procedimiento de Back-off (BPC), contador de postergación (DC) y contador de *Back-off* (BC). DC permite estimar la cantidad de estaciones que desean establecer comunicación. Cada estación inicia su proceso de contención para el canal, al inicializar a BPC en 0 y escogiendo aleatoriamente a BC entre 0 y CW_{O}-*1,* donde Cw_o representa el tamaño de la ventana de contención inicial. El valor de DC y BC dependen del valor de BPC acorde con el Cuadro 3 (Benyouef,2003; Grote,2007).

Cuadro 3. CW y DC en función de BPC y prioridades.

	CAP: CA3,CA2		CAP: CA1,CA0	
BPC	CW	DC	CW	DC
0	7	0	7	0
1	15	1	15	1
2	15	3	31	3
≥2	31	15	63	15

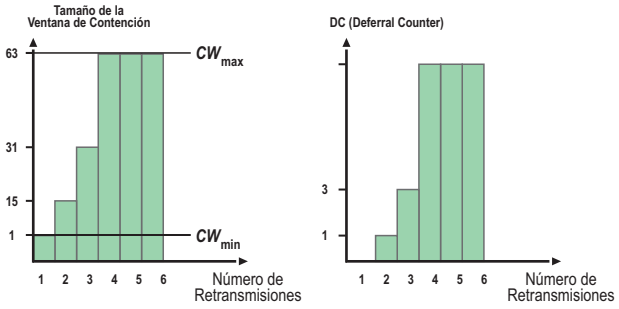
Fuente: Autor. Tomado de Banwell & Galli (2001).

El parámetro *CW* es un parámetro configurable por el administrador de redes, para muchos de los dispositivos comerciales. El valor por defecto es 8 según los valores establecidos en el cuadro anterior. Sin embargo, *CW* puede adoptar los siguientes valores: 8, 16, 32 y 64, bajo el estándar HomePlug 1.0®. Mientras mayor sea el valor de *CW,* disminuye la probabilidad de colisiones de la red PLC, pero por otro lado, aumenta el retardo en el momento de transmitir un frame (Grote, 2007). Aunque HomePlug 1.0® está diseñado para operar con una cantidad pequeña de estaciones, es muy probable que al aumentar la cantidad de estaciones se llegue a afectar considerablemente el acceso a la red. Por tal razón, con el fin de mejorar esta situación, es posible ajustar dinámicamente el valor de CW acorde con el número de estaciones (Andreou, Manitsas & Labridis, 2003).

El valor de la ventana de contención *CW* oscilará entre los valores Cw_{min} y Cw_{max} , los cuales se encuentran predefinidos por el estándar HomePlug. El número de ranuras de tiempo se denomina BC (Back-off Counter), el cual es utilizado por el procedimiento de *Back-off*

cuando el medio esté ocupado, o cuando la estación transmisora no haya recibido el ACK de la estación destino. Tan pronto cuando una estación desea transmitir información, ésta escucha el medio gracias al PCS definido previamente. Si el medio no está ocupado, aplaza su transmisión mientras espera un IFS (Andreou, Manitsas & Labridis, 2003; Grote, 2007).

Figura 4. Variación del tamaño de la ventana de contención acorde con el algoritmo de Back-off



Fuente: HELD Gilbert. Understanding Broadband over Power Line. P.75.Reproducido con autorización.

Cuando el tiempo IFS ha transcurrido y el medio se encuentra libre, es posible iniciar el proceso de transmisión sin necesidad de utilizar el algoritmo de back-off; Por el contrario, ya que el medio se encuentra ocupado por otra estación, la estación deberá esperar hasta que el medio se encuentre nuevamente libre. Vale la pena mencionar que si hay varias estaciones que deseen realizar procesos de transmisión, cada una de ellas calculará un algoritmo de back-off diferente, ignorando la existencia de las demás estaciones presentes dentro de la red. Si dos o más estaciones realizan el mismo cálculo de tiempo de back-off, en el momento en el cual el medio sea liberado, existirá la probabilidad de que éstas inicien su proceso de transmisión presentándose colisiones (Banwell & Galli, 2001; Jensen, Slavensky & KjAersgaard, 2007).

La expresión matemática utilizada para calcular el tiempo de Back-off es la siguiente:

$$T_{Back-off} = Random(0, CW) * time\ slot \quad (Eq.31)$$

La expresión para calcular el valor de CW es el siguiente:

$$CW_{nuevo} = 2 * CW_{actual} + 1 \quad (Eq.32)$$

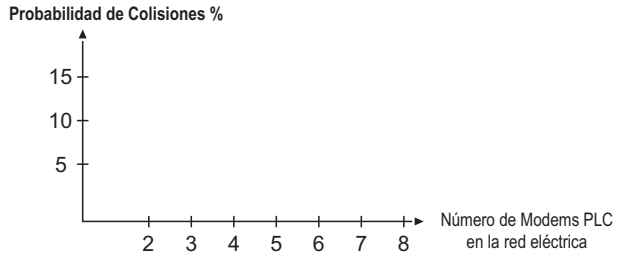
El *Random* (0,CW) es un valor seudoaleatorio que oscila entre [0,CW-1]. De esta forma, el algoritmo genera varios valores de tiempo por cada estación. La figura 4, ilustra la variación de la ventana de contención CW y el contador DC acorde con el número de retransmisiones.

Entre mayor sea el valor de la ventana de contención CW, menor será la probabilidad de que ocurra una colisión. Sin embargo, el hecho de que se aumente el valor de la ventana de contención, provocará que el valor de *Throughput* disminuya (Banwell & Galli, 2001; Grote, 2007). Estos valores cambian desde un valor inicial hasta alcanzar un valor de umbral, que generalmente indica un problema general con la red PLC en la estación que desea transmitir (Grote,2007).

Un aspecto importante que se debe tener en cuenta en las redes PLC, es que el algoritmo de Back-off puede ser utilizado solo cuando no ocurren colisiones. Una estación incrementará el valor de su BPC (back-off procedure counter) tan pronto se detecta una colisión o cuando BPC sea igual a cero (Benyouef, 2003). En la figura 5 se

muestra una gráfica, en donde se relaciona el porcentaje estimado de colisiones que puede ocurrir en una red PLC, según el número de estaciones que forman parte de la red (Benyouef, 2003).

Figura 5. Probabilidad de colisiones vs número de estaciones en la red PLC.



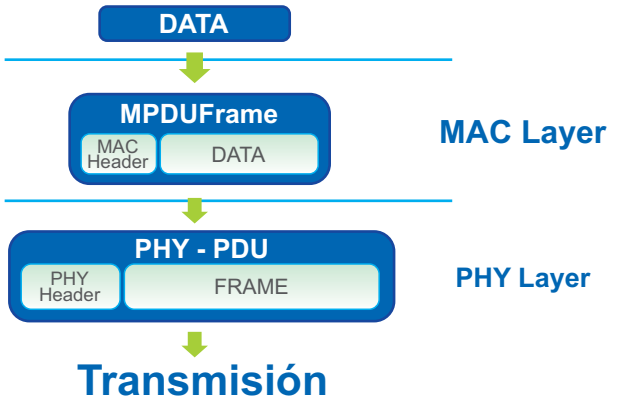
Fuente: HELD Gilbert. Understanding Broadband over Power Line. P. 60

El proceso ARQ (Automatic Repeat Request)

El control de errores es muy importante en cualquier sistema de comunicaciones, el cual indica cómo proceder cuando se pierde información, o ésta sufre algún daño. Dentro de los mecanismos de control de errores, las técnicas ARQ (Automatic Repeat Request) ocupan un papel fundamental. Estas técnicas tienen un papel muy simple: la fuente no volverá a enviar información hasta que no reciba un reconocimiento positivo por parte del otro extremo (ACK, Acknowledgment). En caso contrario, retransmitirá el mismo paquete. La recepción de un reconocimiento negativo (NACK, Negative Acknowledgment) de un paquete, indica que éste ha sido recibido por el destino, pero hay algún error en el paquete. En general existen tres variantes de ARQ: parada y espera, de ventana deslizante y repetición selectiva (Banwell & Galli, 2001; Benyouef, 2003).

Cuando se desea enviar información, cada una de las estaciones debe generar tramas de información. Estos bloques contienen la información bajo un formato específico, el cual depende de la técnica utilizada para acceder al medio físico. Como el medio es compartido, se utiliza una técnica que permite la circulación de múltiples tramas, proveniente de diversas estaciones existentes en la red. Esta estructura de la trama utilizada es enviada sobre la capa física, la cual es completada por una segunda estructura encapsulada sobre la primera.

Figura 6. Arquitectura para transmisión de datos sobre PLC a través de la capa MAC y la capa física PHY.



Fuente: CARCELE, Xavier. Power Line Communications in practice.P.87

La figura 6, ilustra la arquitectura para transmisión de datos sobre PLC a través de la capa MAC y la capa física PHY. La primera capa corresponde a la técnica de acceso al medio. El *frame* generado en esta primera capa se denomina MPDU (MAC Protocol Data Unit). Posteriormente, la trama que proviene de la

MAC es encapsulada en un segundo *frame* a nivel de la capa física, al cual se le denomina PPDU (Physical Protocol Data Unit) (Andreou, Manitsas & Labridis, 2003).

El tamaño de la ventana de contención depende del nivel de prioridad y la estimación del tráfico que circula en la red PLC. Esto ayuda a que se obtenga una mejor eficiencia de la red PLC y un mayor control en la latencia.

Conclusiones

La red eléctrica representa un medio hostil para la transferencia de datos debido a que no ha sido diseñada para transmitir información. PLC al ser una tecnología emergente, se enfrenta a varios inconvenientes tales como: niveles excesivos de ruido, la atenuación de la señal a las frecuencias de interés, discontinuidades en la impedancia característica del canal, efecto *multipath*, entre otros aspectos, afectando considerablemente su óptimo desempeño. Adicionalmente, es muy difícil obtener un modelo significativo de este canal, debido a la constante conexión y desconexión de dispositivos. Aunque el cableado eléctrico de PLC es un medio compartido por los diversos dispositivos de red tal como ocurre en la redes WLAN, no es tan fácil tener acceso a ella, debido al peligro que ésta representa, por la presencia de la señal de 110-220 V, 50-60 Hz.

Como en todo medio de transmisión de acceso compartido, generalmente se presentan problemas de seguridad en la transmisión de datos y la red eléctrica no es la excepción. En vista de lo anterior, el estándar HomePlug 1.0® establece mecanismos de separación entre redes PLC, creando redes lógicas por encripción, soportadas en el estándar de encriptamiento DES 56-bit.

Complementado con el hecho de hacer uso de un sistema de red privada de PLC, basado en claves de cifrado conocidas por dispositivos autorizados PLC, cada estación posee un adaptador PLC, el cual mantiene un cuadro de claves de encripción asociadas a una EKS (Encryption Key Select). Todas las transmisiones en una red lógica, son encriptadas con una clave de encripción de red compartida (NEK, Network Encryption Key). Un aspecto importante es que sólo existe una única NEK, la cual define una red lógica.

En la red PLC, con el fin de mantener una calidad de servicio (QoS) adecuada, se establecen niveles de prioridad al tráfico que circula por la red, etiquetando cada una de las tramas y garantizando un ancho de banda adecuado para los usuarios con bajos niveles de retardo en la transmisión de información de extremo a extremo en la red.

Aunque HomePlug 1.0® está diseñado para operar con una cantidad pequeña de estaciones, es muy probable que al aumentar la cantidad de estaciones se llegue a afectar considerablemente el acceso a la red. Por tal razón, con el fin de mejorar esta situación, es posible ajustar dinámicamente el valor de CW acorde con el número de estaciones, para que oscile entre los valores CW_{min} y CW_{max} los cuales se encuentran predefinidos por el estándar HomePlug®.

Referencias

Andreou, G., Manitsas, E., Labridis, D.(Marzo, 2003). Finite element characterisation of LV power distribution lines for high frequency communications signals. En simposio llevado a cabo en Proceedings of the 7th International Symposium on Power-Line Communications and its Applications (ISPLC), Kyoto, Japan.

Banwell, T. & Galli, S. (Abril, 2001). A new approach to the modelling of the transfer function of the power line channel. En simposio llevado a cabo en Proceedings of the 5th International Symposium on Power-Line Communications and its Applications (ISPLC), Malm¨o, Sweden.

Benyoucef, D. (Marzo, 2003). A new statistical model of the noise power density spectrum for powerline communications. En simposio llevado a cabo en Proceedings of the 7th International Symposium on Power-Line Communications and its Applications (ISPLC), Kyoto, Japan.

Bumiller, G. (Marzo, 2003). System architecture for power-line communication and consequences for modulation and multiple access. En simposio llevado a cabo en 7 th International Symposium on Power-Line Communications and its Applications (ISPLC2003), Kyoto, Japan.

Campista, M. & Costa, L. (2005). *Improving the Data Transmission Throughput over the Home Electrical Wiring*. IEEE Computer Society.

Carcele, X. (2006). *Power Line Communications in practice*. Paris: Artech House.

ETSI, Power Line Telecommunications (PLT) (2003). *Channel Characterization and Measurement Methods*, Technical Report ETSI TR 102 175 v1.1.1 (2003-03), European Telecommunications Standards Institute, 2003. Recuperado de www.etsi.org.

Grote, W. (2007). Fixed or adaptive rate maximum throughput analysis. Ingeniare. *Revista Chilena de Ingeniería*, 15(3), 320-327
Guillen, E., López, J. & Barahona, C.(2008). *Throughput Analysis over Power Line Communication Channel in an Electric Noisy Scenario*. World Academy of Science, Engineering and Technology. Volume 33.

HomePlugPowerline Alliance (2001). HomePlug 1.0® Specification.

Hrasnica, C., Haidine, M. & Lennert, R. (2004). *Broadband Powerline Communications Networks*. NJ USA: John Wiley & Sons Ltd.

Jensen, B., Slavensky, H. & KJÆrsgaard, S. (2006). *Benchmarking and QoS of In-House Powerline Equipment for AV- Streaming Applications*, IEEE Proceedings of ISPLC2006, Orlando.

Jensen, B., Slavensky, H. & KJÆrsgaard, S. (2007) Benchmarking and QoS of In-House Powerline Equipment under Noisy Conditions. IEEE Proceedings of ISPLC2006, Orlando.

Jung, M., Chung, M. & Lee, T. (2005). MAC Throughput Analysis of HomePlug 1.0. *IEEE Communications Letters*, 9(2),184–186.

Lee, J. & Tripathi, K. (Enero,2007). Efficient High Speed Communications over electrical powerlines for a large number of users. En simposio llevado a cabo en Ninth IASTED International Conference Power and Energy System.

Lee, M. K., Newman, R., Latchman, H., Katar, S., Yonge, L. (Mayo, 2003). HomePlug 1.0® Powerline Communication LANs –Protocol Description and Comparative Performance. Results accepted for publication in the Special Issue of the *International Journal on Communication Systems on Powerline Communications*.

Tang, L. T., So P. L., Gunawan, E. & Chen, S. (2001). Characterization of in-house power distribution lines for high-speed data transmission. International Power Engineer. Conference, vol. 1, Singapore.