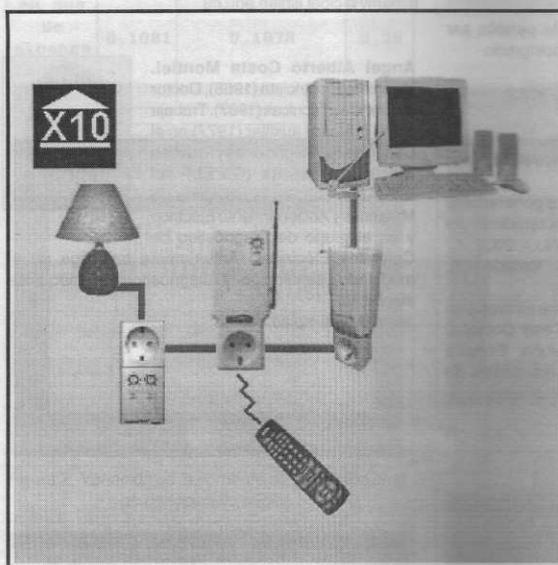


Soluciones domóticas sin instalación

El protocolo X10 más seguro y fiable



□ Juan Carlos C. Martínez, Ing.
Telecomunicaciones,
Universidad de Málaga,
España.

□ Jesús Martínez Cruz, Ing.
Telecomunicaciones,
Universidad de Málaga,
España.

□ Pedro Merino Gómez, Ph.D.
Profesor Titular,
Universidad de Málaga,
España.

Grupo de Informática ETSI
Telecomunicaciones Málaga, España.

RESUMEN

En este artículo se presenta una serie de mejoras para el protocolo domótico X10 destinadas a aumentar su eficiencia, seguridad y versatilidad. Se ha pretendido mantener al máximo la compatibilidad hacia atrás de los equipos. Las modificaciones previstas permiten realizar operaciones rápidas, seguras, eficaces sobre nuevos dispositivos más potentes e inteligentes. Todo esto permite conseguir aplicaciones domóticas más versátiles y útiles. Las propuestas se basan en la experiencia obtenida durante el desarrollo de una aplicación real en la que ya se han incorporado.

PALABRAS CLAVES

Protocolo X10, domótica.

ABSTRACT

This article presents several improvements for the X10 protocol to increase its efficiency, security and versatility. Backward compatibility with old devices has been encouraged in the development of the new features. These changes let make faster, more secure and effective operations on the devices so new versatile and useful domestic applications can be implemented. The extensions have successfully been employed in a real application developed in the University of Málaga.

KEYWORDS

X10 protocol, domotics.

1. INTRODUCCIÓN

El protocolo X10, basado en la transmisión de información a través de la red eléctrica, aporta indudables ventajas. Estas son, por ejemplo, la no necesidad de tender nuevo cableado en una vivienda, así como de disponer de gran variedad de dispositivos a un coste bajo. Sin embargo, tiene una serie de puntos oscuros que lo hacen poco eficaz. La falta de confirmación de que una operación se ha llevado a cabo es una de ellas. A esto se suma la baja velocidad de transmisión y el que no exista una protección de la información. Así, en este artículo se realizará un análisis de estos problemas y se proponen soluciones que se han probado con éxito sobre prototipos. Se pretende que con estas mejoras el protocolo X10 consiga mantenerse en la carrera por imponerse dentro del mercado actual de la domótica siendo buena solución para los hogares ya construidos.

La organización del artículo es la siguiente: en la Sección 2 se introducen las características técnicas de X10, en la Sección 3 se revisan las deficiencias del mismo. Nuestras propuestas de mejora se describen en la Sección 4. Finalmente, se presentan algunas conclusiones.

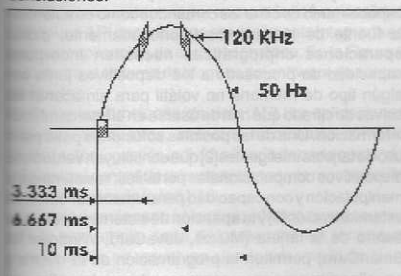


Figura 1. Señales X10 sobre la corriente eléctrica.

2. TECNOLOGÍA X10

La tecnología X10[1] basada en corrientes portadoras, fue desarrollada entre 1.976 y 1.978 por los ingenieros de Pico Electronics Ltd. en Glenrothes, Scotland. X10 surgió de una familia de chips denominada los proyectos X10 (o series X). Esta empresa comenzó a desarrollar este proyecto con la idea de obtener un circuito que pudiera ser insertado en un sistema mayor y controlado remotamente. En colaboración con BSR, una empresa dedicada a los sistemas de audio, comenzaron a construir los dispositivos X10.

El primer módulo podía controlar cualquier dispositivo a través de la red eléctrica doméstica (120 o 220 V y 60 o 50 Hz) modulando pulsos de 120 KHz (0 = sin pulso, 1 = pulso) como se aprecia en la Figura 1. Con un simple protocolo de direccionamiento, podían ser localizados un total de 256 dispositivos en la red. El protocolo soporta 16 grupos de direcciones denominados códigos de casa (desde la 'A' a la 'P'), y otras 16 direcciones para cada código de casa, denominadas códigos de unidad. La comunicación se realizaba por cadenas de control que son sucesiones de unos y ceros que completaban los comandos. En su primera versión tan sólo existían seis operaciones: encender, apagar, aumentar, disminuir, todo apagado y todo encendido. Estas señales son recibidas en todos los módulos pero sólo el módulo con la misma dirección que la indicada en el mensaje de control realizará alguna operación. El mensaje completo tiene 48 bits. Posteriormente, los códigos de operación fueron extendidos a 256 con una cabecera especial, e incluso, la cantidad de información que porta un mensaje puede ser mayor de 48 bits, hasta dos bytes más, si es usado el código de datos extendidos en la cabecera de control del mensaje.

La transmisión X10 está sincronizada con los pasos por cero de la corriente. Un uno binario está representado como un pulso de 120 KHz durante un milisegundo, y un cero como la ausencia de ese pulso. La transmisión completa de un código X10 necesita 11 ciclos de corriente. Los dos primeros ciclos son para el código de inicio de mensaje, 1110. Los cuatro siguientes son el código de casa y los cinco siguientes son el código de unidad o de función. Este bloque completo es transmitido dos veces, separadas cada una por tres ciclos de corriente.

Con todas estas características, lo primero que resalta es la baja tasa de transferencia, reducida a un bit por ciclo de corriente, es decir, a 50 o 60 bps. Sin embargo, la funcionalidad que aporta este protocolo así como la facilidad de su uso e instalación lo han mantenido vivo hasta hoy en día.

3. LIMITACIONES DEL PROTOCOLO X10

A pesar de las indudables ventajas de este protocolo en la actualidad las limitaciones impuestas o no desarrolladas en su diseño limitan su capacidad de expansión dentro del nuevo auge de la domótica.

3.1 Velocidad de transmisión

La velocidad de transmisión es, sin duda, uno de los mayores impedimentos actuales para las aplicaciones que intercambian información. La baja tasa de bit no suponía ningún problema en su nacimiento, ya que, aunque la transferencia por módem vía telefónica podía llegar a los 14.4 Kbps por líneas de cuatro hilos, no estaba apenas extendida. En la actualidad, tecnologías

tales como V.34 y V.90, RDSI, ADSL, DSL, Ethernet, etc., han superado con creces tanto la velocidad de transmisión como su expansión e implantación a pesar de no ser usados en domótica. Si lo son, sin embargo, sus dos más serios competidores en este campo: la tecnología Bluetooth y el bus EIB (European Installation Bus). Frente a la tecnología inalámbrica Bluetooth, X10 pierde la ventaja de no necesitar cableado. La estandarización del bus EIB supondrá la adopción masiva por parte de la industria de esta tecnología en detrimento de las aplicaciones X10. En cualquier caso, el protocolo X10 pierde con ambos en cuanto a velocidad de transmisión.

3.2 Seguridad y privacidad

Sin duda este es el aspecto más oscuro del protocolo X10. Cualquier conexión a la red eléctrica dispone de total acceso a la información X10, así como capacidad de analizarla sin problemas y actuar sobre los dispositivos instalados. En principio esto puede no suponer un problema si se instalan filtros a la entrada de la red eléctrica de la casa, sin embargo, la información sigue estando desprotegida.

3.3 Identificación, corrección y recuperación ante errores

El protocolo X10 incorpora una protección ante errores basada en la duplicidad de la información no en códigos de redundancia. Los bits se envían en un semiciclo con la presencia o ausencia de pulso de 120 KHz y en el siguiente semiciclo se envía el complementario. Además la información se envía dos veces. Esta forma de protección, como puede observarse, es realmente ineficiente y si bien en un principio era una solución que permitía una construcción más simple de los equipos, en la actualidad no es apropiada ya que la red eléctrica de las viviendas cada vez es de mayor calidad.

Otro problema importante es la ausencia de confirmación de que un dispositivo ha aceptado y procesado realmente una orden de control. Debido a este desconocimiento, se hace muy compleja la programación de aplicaciones de control en las que el usuario tenga certeza de la efectividad de su actuación.

4. SOLUCIONES POSIBLES

Al ser X10 un protocolo maduro, son numerosos los tipos de dispositivos y aplicaciones que se han construido. Por lo tanto, no es la intención de este artículo menospreciar las cualidades de este protocolo más aún, se *realizan* sus cualidades, lo cual no impide que se propongan una serie de mejoras que a juicio de los autores daría nueva vida a esta tecnología.

4.1 Velocidad de transmisión

Teniendo presente que las mejoras que en cualquier caso pudieran realizarse, deberían mantener la compatibilidad con los equipos actuales, este es un punto difícil de abordar. Ello se debe a que podría haber dos tipos o más de equipos funcionando a velocidades distintas. Así, la elección de las bandas de transmisión debería seguir las siguientes recomendaciones:

- No ser múltiplos de 120 KHz ni de 50 Hz, para evitar la interferencia de las frecuencias espúreas de orden mayor o igual a 2.
- Evitar que los posibles productos de intermodulación caigan en las frecuencias de 120 KHz y 50 Hz, lo que ocasionaría considerables problemas.
- Usar la sincronización al igual que en la actualidad, con los pasos por cero de la corriente. De esta forma se podrá llevar un mejor control de las transmisiones realizadas a la red por los equipos antiguos.

Para conseguir las mejoras de velocidad tan sólo se deberían usar transmisores y receptores digitales de mayor "bit rate", incidiendo especialmente en su aislamiento de la red para lo que se usarían, en lo posible, equipos aislados ópticamente.

4.2 Seguridad

Sería muy conveniente que los dispositivos X10 fuesen capaces tanto de cifrar los comandos como de autenticar la fuente de los mismos. Infortunadamente, dichas operaciones criptográficas necesitan incorporar capacidad de procesamiento a los dispositivos junto con algún tipo de memoria no volátil para almacenar las claves de cifrado que han de usarse en el intercambio de información. Una de las posibles soluciones pasa por el uso de tarjetas inteligentes[2] que constituyen verdaderos dispositivos computacionales portátiles, resistentes a la manipulación y con capacidad para almacenar datos. La estandarización[3] y la aparición de sistemas operativos dentro de la tarjeta (Multos, JavaCard, Windows for SmartCard) permiten la programación de la misma y aquellas que poseen un coprocesador criptográfico son capaces de generar claves, firmar (autenticar), cifrar y descifrar. Además de incluir estas nuevas extensiones hardware el protocolo debería ser ampliado de forma que la inclusión de nuevas capacidades de seguridad permitiese la compatibilidad hacia atrás. A tal efecto, se podrían usar los bits de mensajes extendidos para encapsular información cifrada sobre la operación.

4.3 Identificación, corrección y recuperación ante errores

La solución a la detección de errores se realiza via software[4,5]. De esta forma se mantiene una compatibilidad total con los dispositivos existentes y se

mitan algunas de las deficiencias. Esto se ha afrontado mediante una API que mejora los servicios de X10.

Para comprender mejor la tarea realizada, se describirá primero el funcionamiento de la interfaz X10 con un PC y posteriormente se explicarán las extensiones propuestas a la norma X10.

4.3.1. API mejorada para X10

En el mercado existen dispositivos que realizan la traducción de señales X10 a código binario sobre RS-232. Esto permite el control de la red de equipos X10 desde un PC o dispositivo similar. Así, cuando se desea actuar sobre un dispositivo se envía su dirección y función a realizar, en transmisiones distintas, previa recepción del código de *READY*, o de aceptación de información. Sin embargo, este código sólo informa que el dispositivo puede recibir otro comando, no que éste se haya realizado correctamente. De esta forma, siempre y cuando se actúe desde un nivel superior de aplicación que no sea la actuación directa de un equipo y seguido de una espera hasta que se realice la función deseada, se podrá incurrir en una colisión de información. Esto provocará que la función anterior, la nueva o ambas no funcionen correctamente. Otra posible solución, en caso de aplicaciones software, es parar la ejecución hasta la recepción del código de *READY*. Pero esta solución es ineficiente ya que no permite una gestión ágil y obliga al usuario a esperas innecesarias.

La mejora propuesta pasa por encapsular la funcionalidad X10 en una API genérica que sea fácilmente integrada en cualquier aplicación de control doméstico. En la Figura 2 se muestra el sistema de bloques del software de control de la interfaz.

Mediante las funciones de esta API las aplicaciones obtienen, entre otros, servicios adicionales como la identificación y gestión individualizada de cada comando solicitado el control de retransmisiones y la recepción de información desde la red X10.

La ventaja de esta capa es la posibilidad de que el usuario solicite una amplia serie de comandos sin tener que esperar a que se resuelvan siendo informado de si un

comando ha sido realizado o no. Se debe tener en cuenta que la confirmación de que un comando se ha realizado es *suave*. Esto significa que al enviarse ese comando no se ha enviado otro antes de recibir la señal de *READY* así como que ésta se ha recibido dentro de un tiempo prudencial. Esta mejora consigue que el acceso a X10 pueda ser usada por aplicaciones superiores, delegando en la API la gestión de los servicios vinculados al nivel físico.

Sin duda, se puede apreciar que, a pesar de esta sensible mejora, X10 sigue adoleciendo de serios problemas a la hora de chequear su funcionamiento.

4.3.2. Confirmación de operación en X10

En el apartado anterior se ha mostrado una solución software al problema de la confirmación de operaciones en X10. Si bien consigue mejoras necesita de algunas ayudas hardware, ausentes en X10, que se propondrán a continuación. La posibilidad más inmediata es diseñar los dispositivos para que siempre sean bidireccionales, es decir, que reciban comandos y envíen información. Así, un interruptor normalmente recibe comandos y un sensor de presencia envía información a una interfaz o consola. Por lo tanto, si un interruptor tuviera ambas funcionalidades podría confirmar que se ha apagado o encendido usando la misma técnica que usa un sensor de presencia. De esta forma, la capa de enlace explicada anteriormente, una vez enviado un comando, esperaría recibir un mensaje del dispositivo al que se solicitó la función. Sin embargo, por el modo de funcionamiento de X10, esta solución ralentiza aún más el proceso ya que cuando un dispositivo quiere transmitir, la interfaz envía al PC una señal de *"polling"* que no cesa hasta que el PC le contesta, enviando seguidamente a la interfaz un bloque de información con todos los dispositivos que han transmitido. Además, la interfaz no asegura que esos dispositivos sean todos los que han transmitido sino sólo los diez últimos. Como se puede ver, esta solución transitoria encuentra un obstáculo en la propia interfaz. Debido a esto, la siguiente modificación propone reformar dicha interfaz para que permita nuevas funciones que proporcionen la confirmación para los dispositivos. Dentro de esta línea estaría que la interfaz almacenara todas las respuestas de los dispositivos y las transmitiera al PC de forma asincrónica, sin esperar una solicitud. Este cambio no afectaría a los otros modos de trabajo manteniendo perfectamente la compatibilidad, necesitando construir nuevos dispositivos que usen técnicas ya implementadas en otros de la familia.

4.3.3. Protección contra errores.

Ya se ha comentado que X10 utiliza la duplicidad de la información para protegerse ante los errores. Esta técnica es muy ineficiente y resulta muy difícil de modificar sin afectar la propia estructura de los dispositivos y del X10. Así, tan sólo se propone el uso de la API descrita en el

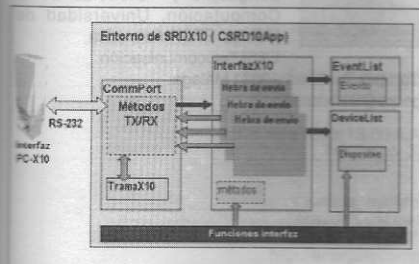


Figura 2. Software de control de la interfaz X10



apartado 4.3.1. si se quiere mantener la compatibilidad hacia atrás. No obstante, debido a la poca cantidad de información que genera X10 junto a la gran calidad de los materiales que soportan la transmisión en la actualidad, la probabilidad de sufrir un error es suficientemente baja como para ocasionar problemas graves. Sin embargo, sí consigue apartar a X10 del campo de la transmisión de datos por la red eléctrica (aunque sea a baja velocidad) ya que no se garantiza la integridad de la información ante un pico de ruido o colisión. Sería la misma información la que debería contener métodos de detección de errores tales como bits de paridad o de checksum.

5. CONCLUSIONES

El protocolo X10 aporta hoy en día, ante el inminente "boom" de la domótica, una solución rápida, versátil y escalable. Su coste es reducido y existe gran variedad de dispositivos en el mercado que resultan suficientes para cubrir las necesidades de un hogar. Si embargo, sus claras deficiencias generadas en su mayor parte por la antigüedad de la especificación, lo ponen en serios aprietos en lo que a todas luces será un duro combate por el mercado. Frente a sus competidores más próximos, Bluetooth y EIB, parte con serias desventajas que, no obstante, pueden subsanarse usando en la mayoría de los casos los mismos dispositivos y variando únicamente las aplicaciones que los controlan o los equipos interfaces. En otros aspectos más dependientes del hardware (velocidad de transmisión o cifrado) se encuentran mayores problemas si se desea mantener la compatibilidad.

Sin embargo y a pesar de todas sus limitaciones, X10 es una tecnología barata frente a las redes de cable y con la necesaria puesta al día podría tener aún opciones en el mercado de la domótica.

6. AGRADECIMIENTOS

Este trabajo ha sido desarrollado en el curso de los proyectos FEDER-TAP-1FD97-1269-C02-02 y CICYT-TIC99-1083-C02-01

7. REFERENCIAS BIBLIOGRÁFICAS

- [1] Patentes de EE. UU. Número: 4 - 189 - 713, 4 - 200 - 862, 4 - 628 - 440, 4 - 638 - 299, 5 - 005 - 187.
- [2] Allen, Catherine A. (ed.). Smart Cards: Sizing Strategic Position Opportunities. Irwin, 1996.
- [3] International Organization for Standardization (ISO). ISO 7816 Integrated Circuit Cards with Electrical Contacts. Part 3: Electronic Signals and Transmission Protocols. Part 4: Protocol Data Unit. <http://www.iso.ch/>

- [4] CUEVAS M. Juan C., MARTÍNEZ C., Jesús, MERINO G., Pedro, El protocolo X10. Una solución antigua a problemas actuales. Simposio de Informática y Telecomunicaciones 2.002 (SIT'02). Sevilla. España. 10 p.
- [5] CUEVAS M., Juan C. Desarrollo de un Entorno Software de Control y Gestión Domótico sobre el protocolo de corrientes portadoras X10. Proyecto Fin de Carrera, Ingeniería de Telecomunicación. Universidad de Málaga. 2.002. 116 p.

AUTORES



Juan Carlos Cuevas Martínez
Ingeniero Técnico de Telecomunicación en la especialidad de Telemática por la Universidad de Jaén, 1.998. Ingeniero de Telecomunicación. Universidad de Málaga, 2.002.

C/ Callejuelas Altas nº 76 1º d.

Mancha Real, C.P. 23100, España.

ccuevas@terra.es

Jesús Martínez Cruz. Ingeniero de Telecomunicación. Departamento de Lenguajes y Ciencias de la computación.

ETSI Telecomunicación, Málaga.

jmcruz@lcc.uma.es



Pedro Merino Gómez. Doctor Ingeniero en Informática por la Universidad de Málaga. Profesor Titular de Universidad. Depto. de Lenguajes y Ciencias de la Computación. Universidad de Málaga. ETSI Informática. ETSI Telecomunicación.

Campus Teatinos. 29071 Málaga.

pedro@lcc.uma.es