

El Protocolo x10: Una solución Antigua a Problemas actuales*

Juan C. Cuevas, Jesús Martínez, Pedro Merino

Dpto. Lenguajes y Ciencias de la Computación
University of Malaga, 29071 Málaga, España
jccuevasm@terra.es, {jmcruz, pedro}@lcc.uma.es

Resumen. En este artículo se describe un sistema software orientado a controlar los dispositivos de una casa desde dentro o fuera de ésta. Las aplicaciones de control son portables, configurables e independientes de la red instalada, gracias a la incorporación de los protocolos TCP/IP y GSM. La solución domótica mostrada no precisa de ningún tipo de infraestructuras adicionales en la casa, al utilizarse la tecnología X10, cuyos dispositivos usan como medio de transmisión la red eléctrica convencional. El acceso al sistema está protegido con recursos de seguridad basados en estándares criptográficos y de tarjetas inteligentes, aportando confidencialidad a las comunicaciones y la posibilidad de una autorización robusta.

1 Introducción

La domótica se define como el área tecnológica que intenta hacer la vida de las personas en sus hogares más fácil, segura y cómoda, usando para ello todo lo que se encuentre a su mano, desde dispositivos electrónicos a los materiales de aislamiento. La domótica surgió como una aplicación de menor entidad a partir de las instalaciones que existían en edificios gubernamentales, sedes de importantes compañías o grandes mansiones. Sin embargo, estos ejemplos son el principal escollo a salvar, ya que asocian un altísimo coste a la instalación y mantenimiento del sistema domótico. Además, la complejidad asociada a su control y gestión ha sido tradicionalmente muy alta. No obstante, en estos últimos años, ha ido adquiriendo mayor importancia, debido principalmente al espectacular avance de la electrónica, telecomunicaciones e informática, que ha generado gran cantidad de nuevos dispositivos y sistemas dedicados al confort y seguridad del hogar, llevando a las grandes compañías de este sector a introducirse de lleno en este terreno casi sin explorar.

En este artículo presentamos una propuesta para solventar estos problemas de gestión de una red domótica de una manera eficiente y robusta, persiguiendo una solución adaptable y escalable a gran cantidad de situaciones y usuarios distintos. La práctica inexistencia de estándares consolidados y de productos comerciales que puedan servir como patrones o ayudas al desarrollo, hacen que este proyecto adquiera

* Trabajo desarrollado en el curso del proyecto 1FD97-1269-C02-02 (Comisión Europea, CICYT)

su carácter especial, precisamente, para esta solución, se ha optado por el uso de un protocolo de comunicaciones que data de la década de los 70, el sistema X10 [1], que usa la red distribución de corriente alterna convencional como medio portador de información, aunque podría haberse elegido otro, ya que el software es independiente de la red que se instale; sin embargo, las características especiales de este protocolo permiten reducir la instalación de los dispositivos del sistema domótico a la simple acción de enchufarlos a una toma de corriente. Otro punto a favor de la tecnología X10 es el gran número de dispositivos [2][3] que existen en el mercado, que dan la posibilidad de adaptarse a casi cualquier necesidad. Por el contrario, no hay tan buenas soluciones [4][5] en una parte esencial del sistema, su inteligencia, la cual debe ser conseguida con el software adecuado. Actualmente las empresas distribuidoras aportan un software anticuado y obsoleto el cual solo aporta acción directa y programación temporal. Este proyecto tiene como objetivo la creación de una arquitectura software que permite considerar al hogar como un completo sistema domótico a través del control remoto de una serie de equipos instalados en la casa, que guardan compatibilidad con X10. Para el acceso remoto se usan las plataformas habituales de comunicación: Internet, y la red de telefonía GSM. Las conexiones remotas tendrán diferentes funcionalidades de control, información y gestión, debido al medio y dispositivos usados en dicha conexión.

A las funciones anteriores hay que añadir la capacidad del sistema de generar sus propios avisos, por lo cual, se pueden recibir mensajes de emergencia desde el hogar del usuario, sin importar donde esté, siempre que se tenga acceso a Internet o a un teléfono GSM. Otro punto a reseñar es la necesidad de seguridad para todo este volumen de información. Este particular es soportado en su mayor parte por una tarjeta inteligente (Smart Card [6][7]) sin la cual no se podrá usar el software cliente ni establecer una sesión con el servidor. Todas las características comentadas serán desplegadas en un entorno gráfico en el que el acceso a la información será rápido e intuitivo, pudiéndose disfrutar de una representación de la casa y de los dispositivos allí instalados. Esta aplicación funcionará bajo Win32 en un PC convencional el puerto serie RS-232 como único interfaz de comunicación con la red X10.

Con todas estas características, el hogar se convertirá en un lugar más seguro y confortable, pudiendo conocer su estado desde cualquier parte, ya sea a través de GSM o Internet. Así, se podrá encender una luz o enviar automáticamente un mensaje de alarma a los bomberos, policía o dueño si se produce un fuego o una intrusión. Además de todo esto será posible realizar una programación temporal para por ejemplo conectar el sistema de riego del jardín, la calefacción o simular presencia de personas en la casa. Incluso, con la estructura abierta del software, existe la posibilidad de crear una red de ordenadores de a través de la red eléctrica, sin necesidad de tarjetas adicionales.

La organización del artículo es la siguiente. En la sección 2 se explican las funciones principales del protocolo X10. La sección 3 describe los requisitos que deben cumplir el sistema y un escenario típico de uso. En la sección 4 aparece la el diseño de la aplicación, donde será descrito con más detalle la arquitectura del sistema y las características especiales del software. Los aspectos de seguridad son tratados en la sección 5. Finalmente la sección 6 da una breve resumen de este artículo y muestra las conclusiones y trabajos futuros.

2 Protocolo 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 X(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). 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 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 con el código de unidad o de función. Este bloque completo es transmitido dos veces, separadas cada una por tres ciclos de corriente.

2.1 Dispositivos X10

Existe una amplia gama de equipos que implementan el protocolo X10, desde interruptores para iluminación a completos paneles de control, emisores y receptores de radiofrecuencias, sensores de movimiento e incluso cámaras. La instalación de casi todos esos dispositivos se reduce a enchufarlos a una toma de corriente convencional de la casa, y para el caso de los dispositivos inalámbricos, su colocación se reduce a fijarlos a una superficie. En este proyecto en concreto, el dispositivo más importante es el interfaz entre el PC y la red eléctrica. La conexión al PC se realiza a través del estándar RS-232, ampliamente difundido y con gran abundancia de soporte hardware y software.

2.2 Software de Control Existente

La mayoría del software comercial usado para tratar con los dispositivos X10 [2][3], tiene características muy limitadas, permitiendo únicamente la programación y activación de algunas funciones a una hora prefijada. En ningún caso existe la posibilidad de interacción entre elementos de la red. Por otro lado, existen diversas aplicaciones de particulares y soluciones a medida, que normalmente adaptan el software existente a una necesidad concreta, pero que no pueden ser consideradas como sistemas completos o arquitecturas orientadas a dar soluciones globales.

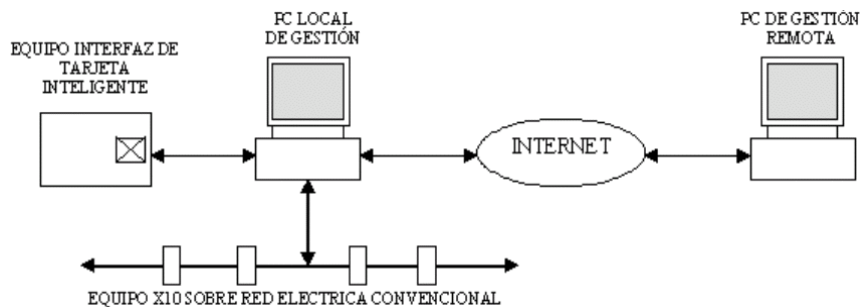


Figura 1. Escenario típico de red doméstica.

3 Requisitos del Sistema y Escenario de Uso

Los requisitos de este sistema, debido a su arquitectura abierta, están principalmente orientados hacia la capacidad de adaptación, configuración y seguridad. Se han considerado:

- ❖ Usar protocolos estándar y de amplia difusión.
- ❖ Lenguaje de programación con posibilidades de alto y bajo nivel, con orientación a objetos.
- ❖ Estructura robusta y configurable, con posibilidad de portabilidad parcial, lo cual se ha afrontado con paradigma cliente-servidor, además del enlace dinámico de funciones.
- ❖ Posibilidad de instalación del sistema en hogares construidos, tanto como en casas de nueva construcción.
- ❖ Conexión con las redes de comunicación convencionales: Internet, línea telefónica convencional o GSM.
- ❖ Un sistema de seguridad fiable para asegurar la privacidad de las comunicaciones del usuario y del control de la aplicación.

Estos requisitos crean el escenario de uso mostrado en la figura 1, que representa el acceso remoto a la red doméstica a través de Internet de la aplicación cliente, asegurando la autenticación y privacidad de las comunicaciones con una tarjeta inteligente.

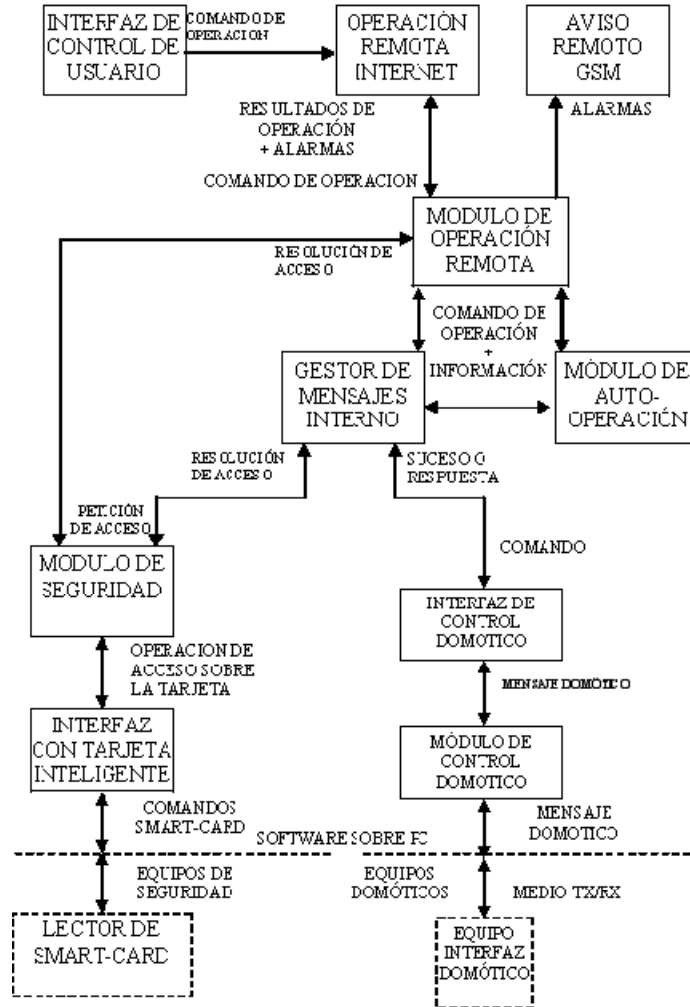


Figura 2. Esquema funcional del sistema.

4 Diseño de la Aplicación

El sistema está compuesto de software y hardware, como se muestra en la figura 2. Este esquema muestra la división funcional del mismo. El módulo de gestión de los mensajes internos es el corazón de la aplicación. Recibe todo el flujo de información, la analiza y despacha la orden correcta al módulo correspondiente, obteniendo una operación resultado en el destino. Este módulo central recibe información desde varias unidades:

Unidades de acceso remoto: Desde estas unidades se recibe información previamente cifrada que se valida en el módulo de seguridad. Después de esto, el núcleo de gestión analiza el paquete de información, extrayendo cualquier comando y realiza las tareas asociadas al mismo. Es importante reseñar que el acceso remoto vía GSM tiene unas capacidades muy limitadas de control.

Interfaz de control de usuario: Las ordenes dadas desde la aplicación cliente, a través del interfaz de usuario, debido a que la aplicación es diseñada según el modelo cliente servidor, usa el mismo tipo de acceso que el destinado a la conexión remota vía Internet, con la diferencia de que en el acceso local la aplicación cliente funciona en el mismo PC que el servidor. De esta manera la arquitectura del software se hace muy adaptable y configurable para posibles ampliaciones posteriores.

Módulo de auto operación: Esta división del software gestiona la programación temporal de tareas y controla los eventos temporizados y las alarmas, procesando la información recibida por el núcleo gestor para llevar esto a cabo. Esta parte controla también las acciones encadenadas que deben ser llevadas a cabo después de que un evento haya sido sucedido. Este módulo usará hilos de funcionamiento a parte para mantener el máximo paralelismo posible y por tanto una mayor eficiencia en el proceso de eventos.

Control de enlace del protocolo X10: En este módulo se montan y se envían los mensajes X10 a través del módulo de comunicaciones serie. Además las tramas X10 recibidas de la red son analizadas y traducidas a comandos internos que son enviados al gestor interno. Este módulo realiza el control de enlace, dejando para el módulo RS-232 tan sólo el trabajo de transmisión y recepción de bits, sin interpretación.

Módulo de seguridad: La seguridad es una característica muy importante para este proyecto, que se explica detenidamente en la sección 5.

El gestor de mensajes interno recibe de todas estas unidades operaciones que deben llevarse a cabo, pero el no toma ninguna iniciativa por sí mismo, tan sólo sirve de puente “inteligente” entre los distintos módulos.

4.1 Diseño del Software

El gráfico anterior muestra la funcionalidad de todo el sistema, aunque la división cliente servidor, organización principal de la aplicación, aparece de forma implícita en los módulos de operación remota

Interfaz entre la Red Domótica y el Programa Servidor

Una parte importante de este software es la independencia de la aplicación de gestión con la red física que realizará las veces de red domótica. Esto se debe a que la comunicación con el módulo de control de enlace de X10 se realiza a través de una serie de funciones definidas en un interfaz común que a través del enlazado dinámico proporcionado por Windows[™] (DLL) permitirá usar cualquier red domótica que siga este interfaz. Esta cualidad es una de las más importantes ya que, debido a la continua expansión que sufre el mundo de la informática y las telecomunicaciones, permitirá estar al día de nuevas redes domóticas con sólo añadir una DLL, manteniendo la interfaz de usuario y toda la funcionalidad del sistema.

Interfaz de Usuario

El interfaz de usuario está dividido en dos partes. La del servidor doméstico, orientado a la configuración y gestión local, da una visión completa de la red y su configuración. La otra parte corresponde con la aplicación cliente, que a través de una conexión TCP/IP mantiene un diálogo con el servidor, requiriendo de este ciertos servicios, como la activación de elementos de la red o variación de la configuración. La idea de usar un esquema de cliente servidor parte de la necesidad de que el software de gestión y control debe poder funcionar sobre una gran variedad de PC (o incluso otras plataformas), además de ser fácilmente configurable, sin la necesidad de portar todo el software completo.

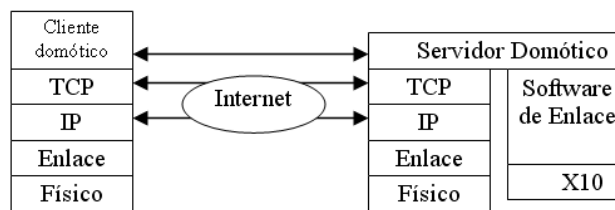


Figura 3. Torres de protocolos del sistema con red doméstica X10.

Unidad de Auto-operación

La unidad de auto-operación u operación automática se encarga de realizar todo el trabajo cuando nadie está manejando la aplicación cliente, simulando la acción humana mediante directivas prefijadas. Estas directivas pueden derivar en gran variedad de tareas de activación temporizada o como consecuencia de alarmas: mandar un mensaje GSM, hacer una llamada con un mensaje pregrabado a la policía. Además, proporciona respuestas ante ciertas lecturas del sistema (la humedad del césped o la temperatura de un pequeño invernadero), junto con la simulación de presencia humana en la casa con eventos pseudo-aleatorios (encendido de luces, bajada o subida de persianas). Muchas de estas tareas serán grabadas por el usuario como macros de actuación.

Así, esta unidad actúa como “cerebro” del sistema, si bien actúa por respuesta a estímulos simples siguiendo directivas fijadas con anterioridad.

5 Seguridad

Los sistemas distribuidos tienen su mayor desafío en la seguridad. La información pasa a través de entornos de baja confianza y que pueden ser fácilmente comprometidos por un intruso. Confidencialidad, autorización e integridad de los datos, son los principales objetivos para la disciplina de la Seguridad de la Información. Por lo tanto, en este proyecto, se debe establecer un mecanismo para asegurar la privacidad de las actuaciones remotas y las respuestas enviadas entre el cliente y el servidor. La autorización o identificación del usuario es otra manera de

proporcionar seguridad al sistema, asegurando que el acceso remoto a los dispositivos X10 sólo es posible para los usuarios con permisos de acceso.

Los sistemas de cifrado asimétricos[9][10] están ampliamente extendidos y son buenas soluciones para los sistemas que requieren confidencialidad y derechos de acceso. De entre ellos, los basados en el uso de claves RSA son los que alcanzan un mayor grado de madurez y confianza. Sin embargo, tanto la generación de las mismas como su uso implican un gran consumo de recursos, aunque algunas propuestas novedosas, como los criptosistemas de curva elíptica[11], consiguen reducirlo.

Las altas necesidades de cómputo de los sistemas de clave pública se traducen además en una ralentización considerable del proceso de comunicación. Para compensar este hecho, habitualmente se separan los conceptos de establecimiento y de sesión, donde se produce el intercambio de datos útiles. En la fase de establecimiento, el esquema de clave pública-privada se utiliza para intercambiar una clave secreta que se usará posteriormente para cifrar y descifrar los datos manejados durante la sesión. Así, en esta fase, todo el proceso de diálogo se establece mediante cifrado simétrico que, en comparación, resulta mucho más sencillo y rápido.

Este modelo es el seguido por protocolos como SSL/TLS[11][12], o Kerberos[13]. Algunas implementaciones de estos estándares están disponibles para uso libre. Una de las librerías más robustas y eficientes es OpenSSL[14], que permite incorporar funciones de seguridad a los proyectos desarrollados en C. Además del protocolo SSL, OpenSSL incorpora funciones de generación de claves RSA, cifrado, descifrado y firma digital, junto con la obtención de resúmenes (hash).

El punto fuerte en la seguridad de los sistemas expuestos con anterioridad, reside en garantizar que la clave privada del usuario autorizado no caerá en manos de ninguna otra persona. Afortunadamente, el uso de un dispositivo criptográfico personal como la tarjeta inteligente, permite salvar esta dificultad: la clave privada se almacena en la tarjeta y no debe abandonarla en ningún caso. Gracias al uso de este dispositivo hardware confiable, se espera el despegue definitivo de las aplicaciones distribuidas cuyos requisitos de seguridad son críticos.

Cada vez más populares, las tarjetas inteligentes incorporan un procesador y un sistema operativo o RunTime (Java, Multos, Basic) [8], lo que permite descargar programas que se ejecuten dentro de la tarjeta, de forma confiable y con acceso a los datos almacenados en ella. Si además incluyen un coprocesador criptográfico, se pueden realizar operaciones criptográficas costosas. Algoritmos tales como SHA-1, DES, 3DES, RSA, o curva elíptica, son ya características habituales ofrecidas por los suministradores. Para las aplicaciones software que requieren la comunicación con la tarjeta, el uso de recomendaciones tales como PC/SC[15] u OpenCard[16], supone la obtención de un medio de acceso homogéneo a cualquier lector registrado o tarjeta. En este proyecto, las aplicaciones usan la implementación que Microsoft hace de PC/SC para operar con la tarjeta inteligente, que a su vez se encarga de las operaciones criptográficas.

5.1 Interfaces de Seguridad del Sistema

Las conexiones de datos establecidas entre los distintos elementos que componen el sistema domótico completo se pueden agrupar en las dos siguientes categorías:

Aplicaciones Cliente/Servidor

El proceso cliente, ejecutado en un PC con soporte de tarjetas inteligentes, introduce su tarjeta personal y su PIN, para desbloquear el acceso a la información sensible. A continuación, se establece la negociación con el servidor mediante el protocolo SSL, adquiriendo una clave temporal de sesión con la que se cifra y descifra la información que se intercambian.

Si el servidor se ejecuta sobre una plataforma confiable, puede sustituirse la tarjeta del lado servidor por un par de claves residentes en disco.

Aplicación cliente GSM

La gestión mediante GSM hace uso del sistema de mensajes cortos SMS que proporciona la plataforma. Aunque la seguridad en la red de telefonía móvil se reduce al cifrado de información establecido en el tramo que va desde el terminal del usuario hasta la estación base, la aplicación servidora (conectada a un módem GSM), almacena un listado de números de teléfono autorizados para realizar consultas. Este método puede considerarse de autenticación ligera, aunque dista de ser una solución tan robusta como la utilizada en las aplicaciones de control remoto a través de Internet.

6 Conclusiones

La domótica es un área que prácticamente acaba de abrir sus puertas al mundo de las tecnologías de la información, sin embargo, en contra de lo que pueda parecer, existen soluciones sencillas, ya estudiadas que pueden proporcionar un muy buen servicio al usuario sin necesidad de desarrollar nuevos sistemas.

Si bien, recientemente se ha conseguido la estandarización del bus EIB (European Installation Bus), para muchos llega tarde, ya que requiere el tendido de cableado, lo cual puede ser imposible o estéticamente inapropiado en edificios con valor histórico-artístico que necesiten de un sistema domótico. Así pues, con el sistema descrito en este artículo se pueden resolver gran cantidad de problemas en la domótica, gracias al uso de dispositivos X10 en la instalación, además de reducir el coste de la misma. Asimismo, es un sistema versátil, gracias a la arquitectura del software diseñado y su orientación cliente servidor independiente de la subred instalada y de su medio físico. El sistema aquí descrito no pretende ser una solución definitiva, pero sí hacer de puente entre la situación actual con una, prácticamente nula, existencia de hogares “inteligentes”, y un futuro no muy lejano de implantación casi total, contando a su vez con la ventaja de poder adaptarse a cualquier red subyacente, lo que le asegura una larga vida como sistema software.

Las mejoras del sistema pasan por la ampliación a futuras de redes de comunicación como GPRS/UMTS y la capacidad del acceso completo al sistema utilizando tan sólo el teléfono móvil. Para conseguir un grado de seguridad equivalente al obtenido mediante el uso de tokens criptográficos, se ha definido la recomendación SimToolkit[17] para terminales móviles, en los que el módulo de identificación personal (SIM) es reemplazado por una tarjeta inteligente. De esta

forma, el modo de operación seguro seleccionado para las aplicaciones de control basadas en TCP/IP, podrá ser implementado sobre plataformas de telefonía móvil.

Actualmente la implementación del prototipo se haya en el proceso de programación del cifrado de las comunicaciones y pruebas finales. Para el desarrollo del sistema y sus pruebas preliminares se están usando los equipos de Power Haus-II de HWG, sobre un sistema operativo Windows[™] 98, que corre en un PC AMD K6-2 350 con 64 Mbytes de RAM. Como conclusión final destacar que en este proyecto se muestra una manera inteligente de aprovechar los conocimientos y tecnología actuales, para aplicarlo a la emergente área de la domótica.

Referencias

1. Patentes de EE.UU. Número: 4 - 189 - 713, 4 - 200 - 862, 4 - 628 - 440, 4 - 638 - 299, 5 - 005 - 187.
2. Distribuidores de equipos y soluciones X10. www.domodesk.com.
3. Distribuidor de equipos y soluciones X10. www.x-10.org.
4. J. Berst. The home of the future - now Pitfalls to avoid on your way to home automation. ZDNET. December 22, 2000.
5. J. Qittner. Watching Your Home From Afair With nifty little X10 modules, you can inexpensively control your home appliances over the Web. Time Dgital, Vol. 5 No 7, November 2000.
6. International Organization for Standardization (ISO). ISO 7816 Integrated Circuit Cards with Electrical Contacts. Part 3: Electronic Signals and Transmision Protocols. Part 4: Protocol Data Unit. <http://www.iso.ch/>
7. Smart Cards Operating System White Paper Abstract. www.microsoft.com/smartcard/. March 2002.
8. W. Diffie, M. Hellman, New directions in Cryptography, IEEE Transactions on Information Theory, IT-22, n. 6 pp 644-654, 1976.
9. R. L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems , Journal of the ACM, 21(2), 120-126, February 1978.
10. A. Jurisic, A., A.J. Menezes, Elliptic curves and cryptography, whitepaper, Certicom Corp., <http://www.certicom.com>, 1997.
11. A. Frier, P. Karlton, P. Kocher, The SSL 3.0 protocol, Netscape Communications Corp., Nov 18, 1996.
12. T. Dierks, C. Allen, The TLS Protocol version 1.0, IETF RFC 2246, January 1999.
13. B. Clifford Neuman and Theodore Ts'o. Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9):33-38. September 1994.
14. Proyecto OpenSSL, disponible en: <http://www.openssl.org>.
15. PC/SC WorkGroup, <http://www.pcscworkgroup.com>.
16. The OpenCard Framework, <http://www.opencard.org>
17. Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface. (GSM 11.14 version 8.3.0 Release 1999). 2000. Disponible en <http://www.etsi.org>.