Diseño de un protocolo RFID propietario para una aplicación específica.

Design of a proprietary RFID protocol for a specific application

JAVIER BATEMAN
Ingeniero electrónico e investigador de la Escuela Colombiana de Ingeniería Julio Garavito. Correo electrónico: bateman@hotmail.com

CRISTIAN CORTES
Ingeniero electrónico e investigador de la Escuela Colombiana de Ingeniería Julio Garavito. Correo electrónico: cristian.cortes@uptc.edu.co

PABLO CRUZ
Ingeniero electrónico e investigador de la Escuela Colombiana de Ingeniería Julio Garavito. Correo electrónico: pablo.cruz@uptc.edu.co

HERNÁN PAZ
Ingeniero electrónico, investigador y docente de la Escuela Colombiana de Ingeniería Julio Garavito. Correo electrónico: hernan.paz@hotmail.com

Clasificación del artículo: investigación (conciencias)

Fecha de recepción: 18 de agosto de 2009 **Fecha de aceptación: 25 de noviembre de 2009**

Palabras clave: comunicación inalámbrica, RFID, control de acceso, lector, etiqueta, protocolo.

Keywords: wireless communication, RFID, access control, reader, tag, protocol

RESUMEN

En la actualidad. las tecnologías en comunicaciones tienden a ser inalámbricas. RFID es una de estas tecnologías, en la cual se identifican etiquetas o Tags en un área de cobertura. Existen tantas aplicaciones RFID como bandas de frecuencias de emisión de la señal; una de ellas es el control de acceso que opera en alta frecuencia (HF).

Generalmente. los procedimientos de acceso de personal a las oficinas o puestos de trabajo en edificios educativos, empresas, instituciones gubernamentales, e industrias son convencionales y se ven afectados por los tiempos que le toma al sistema identificar al personal autorizado, al visitante, y controlar la entrada y salida de activos. Para optimizar estos sistemas de acceso, se diseñó, se construyó y validó un prototipo utilizando tecnología RFID; a través de esta tecnología se minimizaron tiempos y errores; además de facilitar, la trazabilidad del personal autorizado, del visitante y de los activos (equipos valiosos) para la empresa.

Este artículo describe las experiencias que se tuvo en el desarrollo del proyecto de investigación sobre el diseño de un protocolo RFID propietario para control de acceso; esta tecnología puede garantizar acceso confiable a instalaciones en las que se requiera niveles de seguridad altos, sin necesidad de utilizar aparatos sofisticados, ni métodos complejos y con un costo de implementación bajo.

ABSTRACT
At present the communications technologies tend to be wireless. RFID is one of those technologies, in which labels or tags are identified in a coverage area. There are many RFID applications such as emission bands of the signal; one of those is the access control that operates in high frequency (HF).

Generally the procedures of staff access to the office or employment in educational facilities, companies, government institutions and industries are conventional and are affected by the time it takes the system to identify authorized personal, visitors, and entry and exit control of assets. To optimize these access systems, was designed, built and tested a prototype using RFID technology, through this technology the time and errors were minimized, as well as facilitate the traceability of the authorized personnel, of the visitors and the assets (equipment value) of the company.

This article describes the experience in the development of the research project on the design of proprietary RFID protocol for access control; this technology can ensure reliable access to facilities where required high levels of security without need for sophisticated equipment or complex methods, and with a low cost of implementation.

* * *

1. Introducción

Según la Alianza Smart Card que es una asociación multisectorial de industrias sin ánimo de lucro, la adopción de la tecnología RFID en sistemas de control de acceso es la clave para de la seguridad porque facilita la disponibilidad, autenticidad, integridad y privacidad de los mensajes [1]; sin embargo se pueden presentar interferencias, cuando se transmiten simultáneamente los códigos desde varias etiquetas RFID hacia un reader. La función del protocolo es evitar dichas interferencias mediante técnicas de anticolisión, al no permitir las transmisiones simultáneas.

2. Marco teórico

La transmisión de información mediante la tecnología RFID debe cumplir con unos parámetros para garantizar la seguridad y calidad de servicio en los usuarios; uno de ellos es el protocolo que define las reglas, los convenios y las funciones que gobiernan las comunicaciones.
Para la comunicación entre dos entidades situadas en puntos diferentes del sistema, se necesita definir y utilizar un protocolo; los elementos que conforman un protocolo son: 1) la sintaxis: define el formato de los datos y los niveles de señal; 2) la semántica: incluye información de control para la coordinación y manejo de errores; 3) la temporización: incluye la sincronización de velocidades y la secuenciación. Todas estas tareas se subdividen en subtareas y a todo se le da el nombre de arquitectura del protocolo.

3. Características del protocolo en RFID.

En general, se nombrarán algunas características mínimas que debe cumplir todo protocolo RFID para garantizar una comunicación segura y confiable en una aplicación particular:

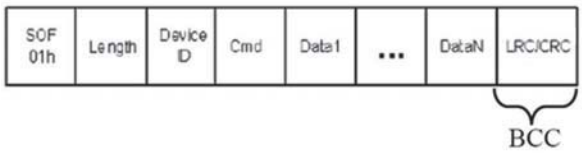

Figura 1. Organizacion de campos para protocolos de comunicación

La trama está conformada por ocho campos, así:

- *SOF (Start Of Frame)*: indica el inicio de la trama. 1 byte.
- *LENGHT (longitud de la trama)*: puede o no incluir la trama de SOF. 1 byte.
- *DEVICE ID*: es el número de identificación del módulo/tarjeta. 1 byte.
- *CMD (Command)*: es el código del comando que indica la operación que se va a realizar. 1 byte.
- *DATA*: en estos campos va la información deseada para la aplicación. 1 hasta 1000 bytes.
- *LRC/CRC*: técnicas aplicadas para control de errores. 1 byte.

A parte de estos campos, se pueden utilizar otros, que sirven para respaldar la transferencia de datos, como por ejemplo:

- *preámbulo*: el cual consiste en una cadena de 20 ceros consecutivos para lograr la sincronización; en la trama se ubica antes del campo SOF. También está
- *EOF (End Of Frame)*: para finalizar la trama. Para reforzar la detección y control de errores se puede agregar bits de paridad de byte y paridad de paridades, adicional a los campos (LRC/CRC)

4. Algunos comandos que se utilizan en la comunicación RFID.

Para comprender la comunicación RFID entre los módulos: tag y reader, es indispensable identificar y conocer las funciones de los siguientes comandos:

- Leer Múltiples Tags: Es un código único, no modificable y creado p or la empresa que es leído cuando la tarjeta está en modo de lectura. Todas las tarjetas poseen un UID (Unique Identification), el cual puede ser utilizado para la construcción de bases de datos de suministros y otros.
- Silenciar o Hablar: activa o desactiva el funcionamiento de las tarjetas para que sean leídas o no por el módulo.
- Leer 1 bloque: lee algún bloque específico de las tarjetas, el cual es requerido para el correcto funcionamiento del proceso.
- Escribir 1 bloque: escribe la información requerida sobre algún bloque específico para ser usado según la aplicación.
- Bloquear/desbloquear 1 bloque: permite/restringe la escritura/lectura de algún bloque en específico de las tarjetas, por seguridad.
- Leer Múltiples Bloques: lee múltiples bloques de una sola tarjeta, de acuerdo con lo que la aplicación requiera.
- Información del sistema: presenta algunas características sobre el funcionamiento de las tarjetas (batería, memoria, entre otras).
- KILL: destruye y desactiva el funcionamiento total de la tarjeta. Sólo en casos en los cuales la tarjeta es desechable.

Algunos de estos comandos y sus funciones se encuentran disponibles en ciertos módulos según la aplicación. Por ejemplo, el comando KILL está disponible en micro-tarjetas y es utilizado en almacenes de cadena, cuyos productos pasan a ser propiedad de los consumidores y, por consiguiente, el Tag debe ser dado de baja.

Todas estas características nombradas están íntimamente relacionados y ligados con la capacidad de la memoria interna con la que cuenta cada tarjeta (EEPROM, EPROM, FLASH).

5. EPC

Definición: Es código de Producto Electrónico que utiliza una cadena de números para identificar al fabricante, el producto y un número de serie exclusivo para cada unidad de artículo. Esta cadena de números se graba en el chip de la etiqueta

RFID.

Función del RFID-EPC: permite hacer un seguimiento preciso de cada producto; de este modo se conoce el movimiento de cada producto a través de lecturas simultáneas de todos los productos transportados y entregados en cada carga o descarga de éstos. Con RFID-EPC es posible mantener la información de los productos actualizada y online; además, evita su daño, debido a que no se requiere manipularlos para llevar su registro y con estas facilidades se gana tiempo, y facilita la trazabilidad total ante contratiempos.

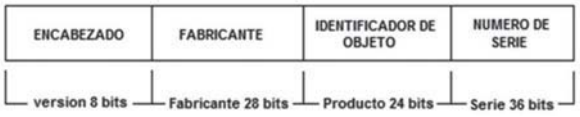

Figura 2. Campos del protocolo EPC

Por medio de esta estructura, implementada en las tarjetas, o microchips, es posible tener toda la información concerniente al producto, por lo cual facilita su seguimiento y organización.

EPC global como ente de estandarización de la tecnología RFID en el uso de la EPC ha constituido las etiquetas en seis clases.

- Clase 0: lectura solamente(la EPC se codifica en el proceso de fabricación)
- Clase 1: lecturas indefinida y escritura una sola vez (la EPC se le incorpora a la etiqueta después del proceso de fabricación.)
- Clase 2: lectura y escritura
- Clase 3: escritura y lectura, más fuente de alimentación que provee una mayor área de cobertura y funciones avanzadas.
- Clase 4: posee las mismas características de la clase 3, más comunicación activa con etiquetas activas.
- Clase 5: posee las mismas características de la clase 4, más comunicación con etiquetas pasivas.

6. Comunicación de campo cercano (NFC)

Comunicaciones de campo cercano son las encargadas de dar soporte a la tecnología RFID, describen la interfaz aérea, la inicialización, la anulación de colisión, el formato de trama y un bloque orientado al protocolo de intercambio de datos con manejo de error; están previstas para permitir la interacción de etiquetas y dispositivos electrónicos a distancias menores a 10 cm; algunos de los estándares seguidos en comunicaciones RFID son: ETSI TS 102.190, ISO 18092, ECMA 340 y NFCIP-1.

ECMA 340: este estándar define los modos de comunicación activo (ambos dispositivos usan sus propios campos de RF) y pasivo para la interfaz entre dispositivos periféricos que tienen acople inductivo y que operan con frecuencia central de 13.56MHz; Además, da algunas especificaciones del protocolo de comunicaciones de campo cercano, a saber: esquema de modulación y demodulación, codificación, tasa de transferencia, formato de marcos para la interfaz de RF, esquemas de inicialización y condiciones requeridas para el control de colisión de datos durante la inicialización. Asi mismo, incluye un protocolo de activación, estructuración e intercambio de datos [2].

NFCIP-1 *Near Field Communication Interface and Protocol*: es un protocolo de interfaz inalámbrica; la comunicación se realiza entre dos entidades (punto a punto): aplicaciones de red y dispositivos electrónicos. Opera en la banda de los 13.56 MHz y tiene un alcance de funcionamiento de 20 centímetros. En este protocolo siempre hay uno que inicia la conversación y éste es el que la monitorizará; éste rol es intercambiable entre las dos partes implicadas.

El pequeño radio de acción de esta tecnología es una gran ventaja por dos motivos: 1) resulta idóneo para atender servicios que impliquen una necesaria privacidad, y 2) al estar tan cerca ambos dispositivos, se evitan los errores en la comunicación y se asegura una mayor eficacia en la transmisión de datos.

El protocolo NFCIP-1 puede funcionar a diversas

velocidades: 106,212 o 424 Kbps, según el entorno en el que se trabaje; las dos partes pueden ponerse de acuerdo con qué velocidad trabajar y reajustar el parámetro en cualquier instante de la comunicación.

La interfaz de Comunicación de Campo Cercano y el Protocolo-2 (NFCIP-2) especifican el mecanismo de selección de modo de comunicación (ECMA 352). Este protocolo distribuye la ubicación de todos los dispositivos NFCIP-1, ISO 14443 e ISO 15693 que operen a 13,56 MHz, pero con diferentes protocolos. Esta especificado en NFCIP-2 que los dispositivos puedan entrar en uno de los tres modos de comunicación y son diseñados para no perturbar otros campos de RF a 13,56 MHz.

NFC no es diseñado para todas las conexiones de redes o la transmisión de grandes cantidades de datos, pero debe permitir un intercambio de datos conveniente entre dispositivos con capacidad de proceso como teléfonos móviles, PDA, PC o lectores de etiquetas. Los protocolos RFID difieren según la aplicación: para RFID en animales se aplica la norma ISO 11784, ISO 11785 e ISO 14223.

Los protocolos ETSI TS 102.190 e ISO 18092 básicamente tratan lo mismo que los estándares mencionados, con la diferencia básica de la organización la cual los publicita y obtienen la licencia respectiva.

6.1. Tipos de tarjetas

1. *Tarjetas de proximidad* (ISO 14443[1]): operan a distancias aproximadas desde el lector de 10 cm; poseen un microprocesador y pueden ser consideradas como transpondedores RFID alto-fin. En ellas se pueden implementar aplicaciones sofisticadas tales como ticketing.

Partes del protocolo ISO/IEC 14443: consta de 4 partes:

Parte 1: define el tamaño y las características físicas de la tarjeta. También provee una lista de diferentes ambientes que la tarjeta tiene que ser capaz de soportar para garantizar su funcionalidad.

Parte 2: describe las características del acople inductivo pasivo, y la comunicación entre la PICC (Proximity integrated circuit(s) card) y el PCD (Proximity coupling device). La frecuencia para hacer la transferencia de energía es 13,56 MHz +/- 7KHz. Asi mismo, especifica los esquemas de modulación empleados: ASK (Amplitude shift keying), BPSK (Binary phase shift keying), y la codificación de línea NRZ (Non-return to zero).

Las tarjetas tipo A, modulan del lector a la tarjeta, en ASK-Manchester con un índice de modulación del 100%. Las tarjetas tipo B, lo hacen en ASK con índice de modulación del 10%, lo cual implica que los datos son codificados con una pequeña reducción de su amplitud normal, lo que le permite a la tarjeta y al lector mantener la alimentación durante el proceso de comunicación, lo cual es mejor que las tarjetas tipo A. Las tarjetas tipo B también utilizan BPSK, lo cual es superior, si se compara con las tarjetas tipo A.

Parte 3: describe los siguientes parámetros: 1) cada tarjeta tiene su propia identificación, 2) el formato de los bytes, 3) los métodos de anticolisión para detectar y comunicarse con una tarjeta en particular cuando hay varias tarjetas en el mismo campo de acción del lector.

Parte 4: especifica un bloque con un protocolo de transmisión half-duplex (T = CL).

El protocolo ISO/IEC 14443: es un estándar internacional que se utiliza en las tarjetas de identificación electrónicas.

Características

- Establece la comunicación estándar y los protocolos de transmisión entre la tarjeta y el lector.
- Opera a 13.56 MHz.

1 Esta norma específica dos estándares tipo A y B para el protocolo de transmisión (inicialización, técnica de anti-colisión e interfaz aérea) en la capa enlace.

- Trabaja a un rango de lectura/escritura hasta 10cm.
- Especifica una velocidad predeterminada de 106kbps, que evita colisiones.
- Seguridad: dispone de mecanismos de autentificación, cuenta con un microprocesador en las tarjetas que les proporciona seguridad; también dispone de "mensajería segura" y "tokens criptográficos" como se describe en la ISO 7816 serie estándar.
- *Tarjetas vecinas* (ISO 15693[2]): tienen un rango superior a 1 m., normalmente incorporan máquinas de estado (condiciones económicas) en lugar de microprocesadores. Estas tarjetas pueden usarse para identificación y control de acceso.

7. Elementos de direccionamiento en RFID

ISO 18000 define la interfaz aérea, los mecanismos de detección de colisión y el protocolo de comunicación para una etiqueta en diferentes bandas de frecuencia. La norma se divide en seis partes: parte 1, describe la referencia de arquitectura, y las partes 2 a 6, especifican las características para las diferentes bandas de frecuencias, así: parte 2, especifica características para etiquetas de bajas frecuencias (<135 KHz.); parte 3.1, características para etiquetas HF (13,56 MHz); Parte 3.2, características de sistemas RFID con anchos de banda superiores a 848 Kbps; parte 4 especifica características para sistemas RFID de 2,45 GHz, en modo 1: sistema back-scattering pasivo, y en modo 2: sistema de alta tasa de datos, mayor alcance y con etiquetas activas. Parte 5 para la banda de 5,8 GHz está actualmente retirado. Parte 6 define un sistema de backscatter pasivo aproximadamente de 900 MHz (la banda sólo es parcialmente disponible en Europa). Parte 7 especifica un sistema RFID con transpondedores activos y mucho tiempo en la banda de 433 MHz.

Interfaz RS485: una interfaz adecuada para manejar las comunicaciones entre lectores es el RS485, ya que ofrece control de error y manejo de colisiones; además, puede transmitir a 9600, 19200, 38400 y 76800 bps; esta última tasa de bit facilita el manejo de hasta 8 módulos a 9.600 bps cada uno. Adicionalmente, cada chip de esta interfaz es capaz de manejar hasta 32 estaciones a distancias de hasta 1.200 metros, lo cual lo hace una interfaz adecuada para el manejo de esta tecnología.

Sistemas de acceso: es un sistema electrónico a través del cual controlamos entradas y salidas y que nos permite conocer quién entra, cuándo entra y a dónde entra cada individuo.

8. Diseño e implementación del prototipo para control de acceso

El protocolo del aplicativo basado en la tecnología RFID, está conformados por las siguientes partes:

- *Header*: tiene una longitud de 16 bits; es la cabecera de la información que puede ser utilizada por otros tipos de protocolos en el futuro.

- *Compañía*: este espacio identifica la empresa que solicitó el servicio, el código es único e intransferible. 32 Bits.

- *Referencia sujeto*: este campo de 3 bits, clasifica el tipo de persona u objeto que se le asigna a cada tag, por ejemplo: empleado, visitante, cliente, activo, etc.

- *Sujeto*: es el código que identifica al sujeto que posee la tarjeta; éste tiene un código único que es personal e intransferible. 13 Bits.

- *Password*: es el número de encriptación del tag, así se puede asegurar que la tarjeta no pueda ser leída por alguna persona que no sea autorizada; su longitud es de 96 a 192 Bits.

2 El estándar describe el protocolo de transmisión, la técnica de anti-colisión y la interfaz aérea en la capa enlace.

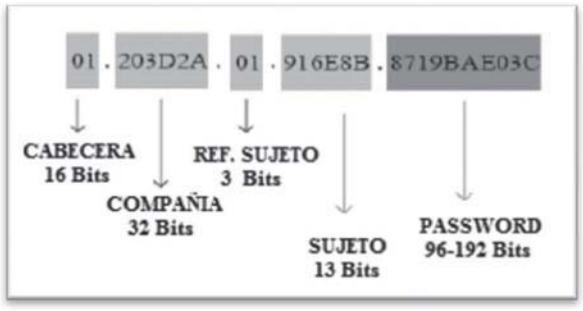

Figura 3. Organización de campos en el protocolo de modelo propuesto

Para el diseño e implementación del prototipo utilizamos un kit de desarrollo de RFID que tiene las siguientes especificaciones:

- Fabricante: PLINTEC
- Banda de Frecuencia: 13,56 MHz
- Protocolo de Comunicación: ISO 15693
- Distancia máx. de operación: 30 cm.
- Tipo de tarjetas: tag pasivo
- Voltaje de alimentación: 5 Vdc

Como se puede apreciar en la siguiente figura, para la comunicación entre los readers, se utilizó la conexión tipo bus en configuración maestro-esclavo [3].

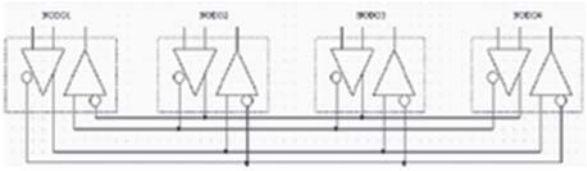

Figura 4. Topología Maestro-Esclavo

Para la conversión de RS232 que suministra el computador que para el ejemplo será el maestro y los Readers los esclavos a RS485 que maneja la línea de transmisión, se utilizó el integrado SN75176 por su bajo costo en el mercado. La siguiente figura es el modelo del circuito para la transmisión y recepción del computador en configuración maestro [3].

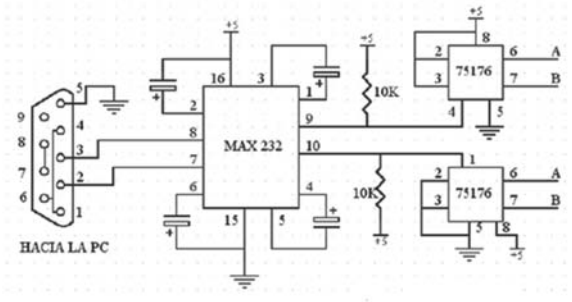

Figura 5. Circuito utilizado para acceso a la red del procesador central

9. Análisis

El control de acceso es una aplicación RFID en la cual se pueden presentar varios dispositivos operando en la misma frecuencia y simultáneamente en espacios cercanos; este hecho puede desencadenar algunos problemas, como lo siguiente:

9.1. Interferencia mutua

Se presenta cuando dos o más readers se traslapan e interfieren al comunicarse con los tags. Esto genera que 2 readers reporten la presencia de una tarjeta a la vez, y en tal caso, no se sabría cómo manejar la información proveniente de los readers. Suele ser causado por exceso de potencia por parte de los readers, causando que las zonas de lectura se traslapen entre sí.

Usualmente, este problema, se puede arreglar de varias maneras, como por ejemplo, muchos módulos tienen la opción de graduar la potencia de radiación, de tal manera que la zona de lectura quede limitada dentro de la zona que realmente se desea sensar, y no se vea la necesidad de traslape con otros readers. Otra posible solución, es ubicar una pantalla conductora en los límites de lectura deseada y, a veces, esta pantalla, o una malla, puede ser suficiente para limitar la zona de lectura, gracias a que a estas frecuencias (UHF) y estas pantallas suelen funcionar.

9.2. Interferencia

Se presenta en las ocasiones en las cuales hay dos o más tarjetas dentro del campo de lectura de un reader simultáneamente. El problema no es realmente éste, ya que es posible que esta situación se presente; el problema es que esto puede llegar a causar ciertos problemas de procesamiento por parte de los readers, por tanto, se vuelve una situación molesta al trabajar con estos módulos. Los nuevos circuitos integrados de Atmel utilizan un algoritmo determinístico de anticolisión, para evitar interferencias.

Las soluciones que se plantean para este problema, tienen la complejidad que deben cambiar todo el sistema, pero tiene muy buenas probabilidades de que este problema no exista. Una posible solución, es dotar tanto a reader como a tarjeta, de la opción de poder trabajar en múltiples frecuencias, de tal manera que pseudo-aleatoriamente, se transmite en cualquier frecuencia de 50 disponibles (según la FCC, con 50 frecuencias distintas es suficiente). De acuerdo con la estadística, hay una posibilidad del 0,04% de que 2 tarjetas transmitan al tiempo y su información interfiera. Es una solución muy óptima, pero es más costosa, ya que se requieren equipos y módulos, capaces de trabajar en variadas frecuencias, lo que los hace más complejos y costosos.

La solución europea es menos eficiente en realidad, pero no conlleva gastos adicionales. Esta solución consiste en activar los módulos de lectura por un tiempo, corto en realidad, pero que sea suficiente para realizar la lectura de las tarjetas. El problema radica cuando se desactiva un módulo que estaba realizando una lectura; esta información se pierde y es prácticamente irrecuperable. Por supuesto, esta solución presenta altas tasas de error y problemas de comunicaciones, por lo cual, en realidad, no es muy aconsejable.

Como punto a parte, también es bueno mencionar, que en algunas ocasiones, y trabajando con ciertas frecuencias, hay muchos materiales que empiezan a generar obstáculos en las señales, como por ejemplo el agua, las maderas, los metales, y otros varios; pero la mejor solución que se puede plantear en estos casos, es estudiar correctamente la frecuencia a la cual se planea trabajar y explicar cuáles son las limitantes y problemas que dicha frecuencia puede presentar y trabajar de acuerdo con estos limitantes [4].

10. Soluciones técnicas

En la aplicación, fue necesario utilizar una comunicación full dúplex con doble hilo de transmisión y recepción. La comunicación full dúplex se implementó, con la intención de separar los hilos de recepción y transmisión, y evitar problemas de colisión, al tener módulos que no son capaces de interpretar el estado de la red. Si la recepción se encuentra separada de la transmisión, es posible que exista información por los dos hilos y no presente ningún problema de procesamiento o colisión.

La razón por la cual se utilizan 2 hilos para recepción y 2 hilos para transmisión, es debido a la funcionalidad del protocolo RS485, el cual estabiliza la red, al hacerla balanceada; esto es útil a la hora de necesitar que la información viaje grandes distancias sin pérdidas considerables de potencia.

Un problema en la aplicación particular consiste en que, si al encontrarse los módulos en modo transmisión, estos presentan baja impedancia, por lo cual, una transmisión desde un módulo encuentra varias terminales con baja impedancia y la señal eventualmente puede no llegar al maestro. Por tal motivo, fue necesario implementar para cada módulo un habilitador de transmisión, por medio de la configuración monoestable de un temporizador 555, de tal manera que los módulos presenten alta impedancia y el único que presenta baja impedancia es el maestro. Este monoestable entra a la habilitación de transmisión del conversor TTL/ RS485 que encadena los datos con la red armada, pero ya en dicha red, al estar todos en modo de alta impedancia, se asegura que la potencia es suficiente para llegar al maestro y poder ser analizados correctamente.

11. Conclusiones

El hecho de que la tecnología RFID se encuentre disponible para bandas abiertas, presenta una

gran ventaja, ya que se pueden realizar estudios y aplicaciones más complejas de manera más económica, sin preocuparse por el uso del espectro frecuencial. Esto es una ventaja para universidades y centros de investigación.

Gracias a que en la actualidad existe gran variedad de protocolos para lograr un correcto funcionamiento de la información, bandas en frecuencia y comunicaciones, es que, para nuestro caso, podemos apropiarnos de dichos protocolos para formular un nuevo protocolo, aplicado a seguridad, haciendo uso de los espacios de datos en dichos protocolos. Aunque no es un protocolo netamente propio, sólo se utilizan los campos que establecen la comunicación entre módulos.

En el protocolo utilizado, se cuenta con un nivel de seguridad alto, ya que se tienen entre 96 y 192 bits de password, creando aproximadamente $6x10^{57}$ posibilidades de código, siendo prácticamente imposible de quebrantar, incluso por métodos informáticos, que tomarían bastante tiempo y recursos poder descifrar. Ventaja que ofrece una tecnología con espacios de memoria para libre uso, útil para aplicaciones en seguridad.

Referencias

[1] http://www.rfidmagazine.com/noticias/detalle.php?id=78. [Consultado 10/10/08].

[2] ECMA INTERNATIONAL. Near Field Communication Interface and Protocol (NFCIP-1). Standard ECMA-340. 2° Edición. Diciembre 2004.

[3] http://www.elperiodico.com/default.asp?idpublicacio_PK=46&idioma=CAS&idnoticia_PK=412197&idseccio_PK=1021&h. [Consultado 19/11/08].

[4] ttp://www.i-micro.com/pdf/articulos/rs-485.pdf. [Consultado 18/09/08].

[5] Clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/TRABAJOS/T1/Seguridad%20RFID.doc

[6] International Standard Organization ISO. Identification cards-Contactless integrated circuit cards-Vicinity cards. ISO/IEC 15693-2. Second Edition 2006-12-15.

[7] Low_Power, Slew-Rate-Limited RS-486/RS-422 Transceivers, Maxim Integrated Products, 19-0122; Rev 7; 6/03.

[8] Robert F. Coughlin, Frederick F. Driscoll, Operational amplifiers and linear integrated circuits, Pearson Education, 08/09/2000.

[9] A. Albright, RFID Tag Placement [online]. USA, California: Frontline Solutions. 2004. Disponible en: http://www.frontlinetoday.com/frontline/article/articleDetail.jsp?id=98552. [Consultado 09/12/08].

[10] Council on Wireless Technology Impacts. 2005. CWTI website [online]. USA. Disponible en: http://www.energyfields.org/. [Consultado 03/11/08].

[11] J. Collins. HP Expands Tagging, Plans 'Noisy Lab' [online]. USA. RFID Journal. 2005. Disponible en: http://www.rfidjournal.com/article/articleview/1341/1/1/. [Consultado 06/12/08].

[12] ES310 Introduction to Naval Weapons Engineering. 2005. Propagation of Waves [online]. USA. Disponible en: http://www.fas.org/man/dod-101/navy/docs/es310/propagat/Propagat.htm. [Consultado 01/10/08].

[13] Korteks. Portola Read Only Disc Packages [online]. USA, California, 2001.

Disponible en: http://www.korteks.com/Products/Passive_Tags/portola_read_only_discs_product.htm. [Consultado 06/12/08].

[14] J. D. Lindsay & W. Reade. Cascading RFID Tags [online]. Jeff Lindsay, 2003. Disponible en: http://www.jefflindsay.com/rfid3.shtml. [Consultado 15/12/08].

[15] Mobile Operators Association. What is a radio wave [online]. UK, 2005. Disponible en: http://www.mobilemastinfo.com/information/radiowaves_and_health/radiowaves.htm. [Consultado 24/09/08].

[16] RFID Journal, 10 Questions to Ask RFID Vendors [online]. USA, 2005. Disponible en: http://www.rfidjournal.com/article/articleview/1330/1/129/. [Consultado 21/09/08].

[17] RFID Journal. FCC Certifies Ubisense's UWB [online]. USA, 2004. Disponible en: http://www.rfidjournal.com/article/articleview/1285/1/1/. [Consultado 11/10/08].

[18] RFID Journal. U.S. Army Tests WhereNet System [online]. USA, 2005 Disponible en: http://www.rfidjournal.com/article/articleview/1316/1/138/. [Consultado 02/12/08].

[19] Savi.com. Spectrum Characteristics for RFID [online]. USA, 2001. Disponible en: http://members.surfbest.net/eaglesnest/rfidspct.htm. [Consultado 21/11/08].