Sistema Empotrado Distribuido para el Control de Accesos - RFIDoors

Daniel García Moreno, Iván Aguilera Calle, Alberto A. Del Barrio, Guillermo Botella

Departamento de Arquitectura de Computadores y Automática, Facultad de Informática
Universidad Complutense de Madrid
Madrid, España
{daniel10, ivanag01, abarriog, gbotella}@ucm.es

Resumen. Con el paso del tiempo se ha ido ampliando la utilización de sistemas con identificación por radiofrecuencia (RFID) en los distintos ámbitos de la sociedad actual. En este trabajo se presenta la implementación de un sistema empotrado distribuido compuesto por elementos de fácil adquisición y de bajo coste como la Raspberry Pi, los módulos RFID o los sensores de ultrasonidos, cuyo objetivo es controlar y gestionar un sistema de autenticación para la apertura y cierre de puertas. Como complemento, este sistema consta además de un servidor y una aplicación para la parte administrativa y operativa del sistema.

Palabras Clave: RFID, Sistema Empotrado Distribuido, Bajo Coste, UART, Accesos, Raspberry Pi.

Abstract. Nowadays, the use of the systems with radio frequency identification (RFID) is becoming widespread in different scenarios of society. This paper presents the implementation of a Distributed Embedded System composed of low-cost components such as Raspberry Pi, RFID modules, ultrasound sensors and others, whose objective is to manage an authentication system for the opening and closing of doors. Furthermore, this system incorporates a server and an application for the administrative and operative part of the system.

Keywords: RFID, Distributed Embedded System, Low Cost, UART, Access, Raspberry Pi.

1 Introducción

La asignatura Sistemas Empotrados Distribuidos (SED) es una materia que se ubica en el Máster de Ingeniería Informática de la Universidad Complutense de Madrid (UCM) [1], implantado desde el curso 2013/2014. Con el fin de potenciar las habilidades en el ámbito laboral, la asignatura de SED basa gran parte de su nota en la realización de múltiples prácticas y proyectos que permitan a los alumnos mejorar sus capacidades en el área de la *Computación Ubícua* y el *Internet of Things* (IoT) [2-7].

En este artículo se describe la implementación de un sistema empotrado distribuido cuyo objetivo es controlar el acceso a una sala a partir de una puerta motorizada. El control de accesos se realiza a partir de llaves electrónicas, empleando para ello la tecnología Radio Frequency Identification (RFID). El sistema desarrollado también permite llevar un control de las personas que han accedido por la puerta.

El resto del artículo se organiza de la siguiente manera: la Sección 2 presenta un estudio de diversos sistemas de control de acceso y de la tecnología RFID; en la Sección 3 se presenta la arquitectura del proyecto y en la 4 la maqueta realizada para implementar la propuesta; la Sección 5 ofrece nuestras conclusiones y posibles líneas de trabajo futuro.

2 Estado del Arte

La tecnología RFID permite identificar o reconocer una etiqueta, aka *tag*, la cual se puede encontrar ubicada en cualquier sitio, como por ejemplo: en la ropa, en un vehículo, en productos de una fábrica o almacén o incluso en las propias personas o animales. La tecnología RFID [17-20] se ha ido expandiendo en los últimos años, debido principalmente a su bajo coste de económico y a la flexibilidad e información y características que pueden aportar frente a los sistemas de control de acceso convencionales como son las tarjetas con bandas magnéticas, códigos de barras, o el reconocimiento basado en vídeo [8-11], redes neuronales [12-13] u otros filtros con mayor complejidad [14-16].

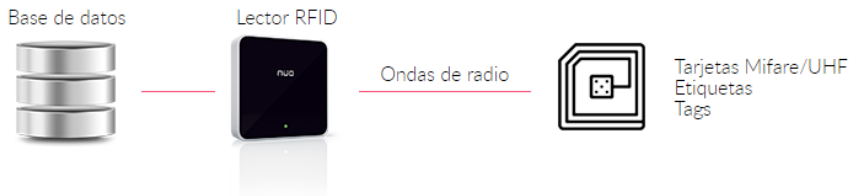


Figura 1. Sistema RFID [20].

Un sistema genérico que utilice la tecnología RFID de forma básica debe tener al menos la infraestructura mostrada en la Figura 1. Las etiquetas RFID tienen integrado un chip, el cual es capaz de responder o de emitir una señal como respuesta a las peticiones que realiza la antena o lector RFID. Por último, el lector RFID suele

consultar y/o realizar modificaciones sobre una Base de Datos del sistema con el fin de dotar de información y/o lógica a la funcionalidad del sistema.

Las etiquetas RFID se encargan de almacenar la información de identificación mediante un código único que se implanta en el chip durante la fabricación [17-19]. Los tags tienen un chip y una antena impresa, los cuales sirven para enviar la información al lector, como se puede apreciar en la Figura 2.

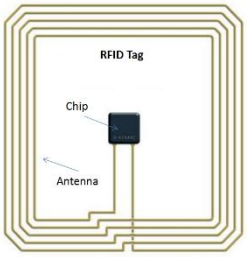
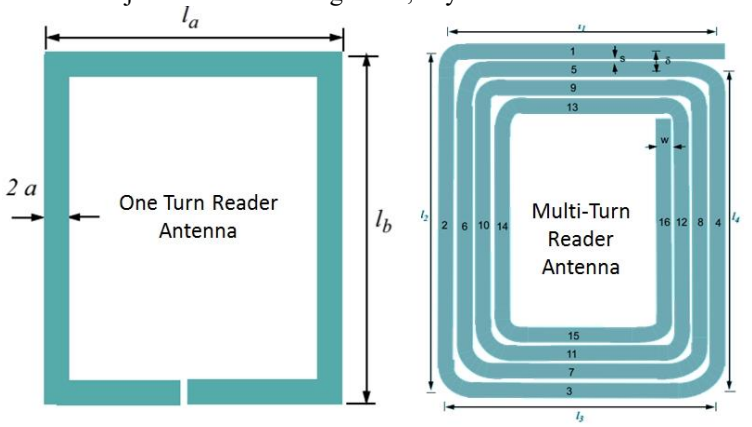


Figura 2. Esquema Tag RFID [17].

La antena del tag recoge la energía transmitida por el lector RFID y la canaliza al chip, por lo que cuanto mayor es el área de la antena de la etiqueta, mayor es la energía que transmite al chip, y también mayor es la distancia o alcance. En la Figura 3, se puede observar el cálculo de la inductancia de la antena del tag y su relación con las dimensiones de la etiqueta. La inductancia es la magnitud física que indica la capacidad para generar un flujo de inducción magnética, cuya unidad de medida es el Henry, *L*.



$$L = 4\left\{l_b \ln\left(\frac{2A}{a(l_b+l_c)}\right) + l_a \ln\left(\frac{2A}{a(l_a+l_c)}\right) + 2\left[a + l_c - (l_a+l_b)\right]\right\} \quad (nH)$$

Figura 3. Calcula de Inductancia tag RFID [17].

2.2 Casos de uso de la tecnología RFID

La forma y los tamaños de los tags varían según cual sea el entorno en el que se estén utilizando, por lo que existe una diversidad abundante de formas y materiales de tags RFID, como puede observarse en la Figura 4.

Figura 4. Tipos de tags RFID [21].

Algunos de los sistemas de identificación mediante tecnología RFID más utilizados son los siguientes:

- Identificación de animales con tecnología RFID: se fabrican con materiales que no sean tóxicos y se comprime la etiqueta en una cápsula que no sea nociva para el organismo, ya que normalmente suelen insertarse en la parte inferior de la piel o incluso en el estómago. Los *Ear Tag* son muy utilizados en este contexto, por ejemplo.
- Sistemas de control de accesos de empleados. Los *Pocket Tag* y los *Key Tag* son muy utilizados en este entorno, por ejemplo.
- Sistemas de control de accesos a las habitaciones de hoteles. En este caso frecuentemente se encuentran tarjetas de plástico con RFID, que son un caso particular de *Pocket Tag*.

3 Arquitectura del Sistema

Como puede observarse en la Figura 5, los componentes principales del proyecto RFIDoors son dos Raspberry Pi conectadas vía UART. El papel que juega cada una de las placas está muy diferenciado:

- En primer lugar tenemos una Raspberry Pi 2 modelo B, que se encarga del control de los diferentes componentes del sistema que provocan el control de las puertas (motores, sensores de ultrasonido, lector de tarjetas, leds…). En otras palabras, esta placa interactuará de manera directa con el usuario.
- En segundo lugar, disponemos de una Raspberry Pi 3 modelo B, cuya función es contener la base de datos que contiene a los usuarios y al servidor. Esta placa estará constantemente a la escucha de las peticiones que vía UART le solicite la otra placa. Esta placa interactuará de manera más directa con el administrador del sistema, disponiendo de otro lector de tarjetas de uso restringido únicamente al administrador, cuyo objetivo es el poder dar de alta nuevas tarjetas. Además, funcionará como servidor para poder ejecutar la aplicación web con la que el administrador podrá dar de alta, de baja y consultar usuarios y accesos.

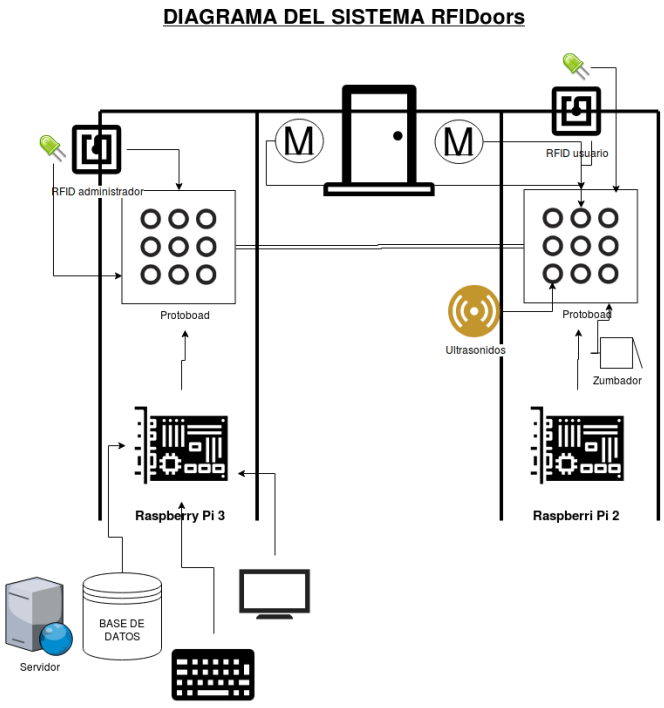


Figura 5. Arquitectura del sistema.

El funcionamiento básico del sistema es el siguiente:

- Las llaves electrónicas llevarán almacenadas un ID, el cual es único para cada tarjeta RFID. Para leer las tarjetas, hemos utilizado dos chips RFID RC522,

puesto que no necesitamos detectar tarjetas a más de dos o tres centímetros. Uno de los lectores será para el usuario y el otro para el administrador.

- Al acercar una tarjeta RFID al lector, este ID se envía de la Raspberry que está conectada con el lector RFID y a la Raspberry administrativa, con el objetivo de consultar su existencia en la base de datos. Si este identificador existe, la placa que ha recibido la solicitud de consulta respondería a la placa que ha obtenido el ID, para posteriormente proceder a la apertura de las puertas.

Una vez comprobada la validez de las tarjetas en la base de datos, el objetivo es que las puertas se abran y cierren de manera automática. Para tal fin, se ha utilizado dos servomotores (se trata de una puerta doble) SG90. Un servomotor rota los grados que se le indiquen mediante modulación del ancho de pulso (PWM). En el caso de estos servomotores, tienen un campo de acción de 180º, pero dado la estructura de la maqueta desarrollada para este proyecto y la ligereza de los materiales utilizados, solo se requiere giros de 90º, y este modelo de servo nos lo permite hacer con la suficiente fuerza como para poder abrir y cerrar las puertas. Los motores están conectados a la Raspberry Pi 2, encargada del control de todos los componentes.

Dado que los motores se encargan de abrir las puertas, es deseable que se cierren automáticamente, ya sea porque la persona que quería entrar ya ha pasado, o porque ha transcurrido un periodo de seguridad en el que nadie ha accedido (en nuestro sistema esto está configurado a 15 segundos). Para poder implementar esta funcionalidad, se ha utilizado un sensor de ultrasonidos, en concreto el modelo HC-SR04. El lector de ultrasonidos está formado por dos cilindros metálicos. Uno de ellos emite una señal que al rebotar en una pared es captada por el otro cilindro. Partiendo de este funcionamiento, lo que se ha hecho es capturar el instante de tiempo en el que la señal es lanzada por el sensor y el instante de tiempo en la misma ha sido recogida. Una vez obtenidos estos tiempos a partir de la fórmula matemática que indica que la distancia recorrida es igual al tiempo transcurrido por la velocidad entre dos (D = T*V/2), calculamos la distancia sobre la que está el sensor de una pared. Si una puerta está colocada sobre un pasillo, el uso de este sensor nos ofrece la funcionalidad de permitir detectar el paso personas por delante de él. En cuanto se detecte una distancia inferior a la longitud del pasillo, la Raspberry Pi 2 enviaría a los motores una orden para cerrar las puertas. El rango de funcionamiento del sensor abarca desde los 2 cm hasta los 3 metros, por lo que para una maqueta pequeña el sensor es totalmente válido.

Para mejorar la usabilidad del sistema de cara al usuario, se han utilizado leds de colores colocados sobre el lector de tarjeta con el objetivo de que el usuario conozca si la tarjeta acercada es válida para poder acceder (led verde), o por el contrario, no es válida para acceder (led rojo). Acompañando a los leds, se ha utilizado un zumbador para poder emitir secuencias de pitidos en caso de acercar una tarjeta no válida o un pitido largo para avisar de que la tarjeta es válida y se va a proceder a la apertura de las puertas.

4 Prueba de Concepto

Para comprobar el correcto funcionamiento del proyecto, se construyó una maqueta a partir de tablones de contrachapado que simulan una puerta, y tras ella, un pasillo. De forma paralela, se han construyeron dos pasillos ocultos que contienen toda la maquinaria del proyecto. En la Figura 6 podemos ver cómo sería la maqueta, así como la disposición final de los elementos anteriormente mostrados en la Figura 5. Como se puede observar, el pasillo central se encuentra tras atravesar la puerta. Los dos pasillos ocultos pueden apreciarse en la vista cenital mostrada en la Figura 6.

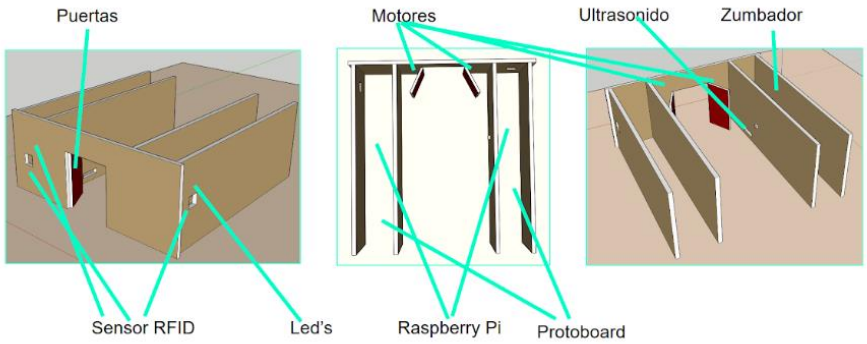


Figura 6. Boceto maqueta RFIDoors.

En el pasillo de la izquierda se encuentra la Raspberry Pi 3, es decir, la placa que contiene la base de datos, que actúa como servidor para mover la aplicación web de gestión del administrador, y que escuchará las peticiones que vía UART reciba de la otra placa para realizar consultas en la base de datos. Además, hay que recordar que gestiona un lector RFID para dar de alta nuevas tarjetas o consultar la información de otras, acompañado de los leds correspondientes que avisan del funcionamiento del lector.

En el pasillo de la derecha, se encuentra localizada la Raspberry Pi 2, la cual se encarga del control de los componentes que interactuarán con el usuario. Entre el pasillo de la derecha y el pasillo central se encuentra un agujero en la pared tras la puerta, donde se encuentra localizado el sensor de ultrasonido, de tal modo que nada más atravesar la puerta, el sensor capta el acceso para posteriormente cerrar la puerta. Los servomotores se encuentran en el pasillo central encima de las puertas, y se conectan a la Raspberry Pi 2 a través de un agujero en la pared del pasillo derecho. La UART conecta las dos placas, y su cableado transcurre por encima de las puertas. Las protoboard se encuentran una en cada pasillo lateral, con el objetivo de poder tener los cables de conexión de los componentes más ordenados, y realizar una conexión con las Raspberry más limpia. Finalmente, en la Figura 7 pueden verse un par de vistas de la maqueta con los dispositivos embebidos, así como una de las funcionalidades de la aplicación web del administrador.

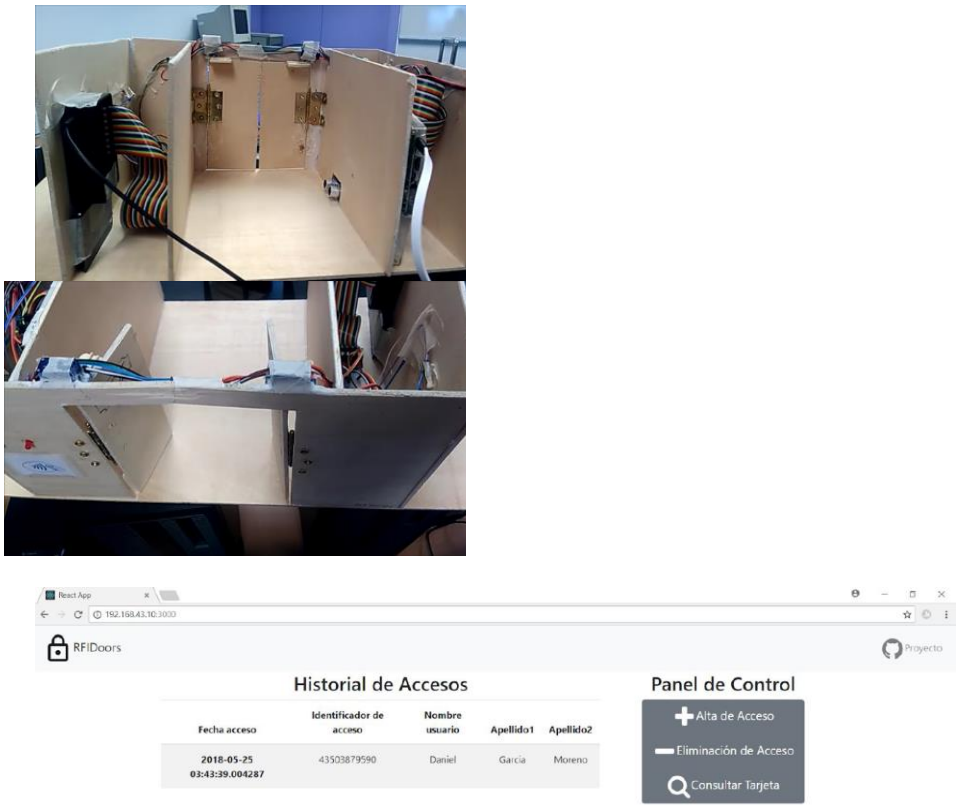


Figura 7. Maqueta RFIDoors y aplicación web del administrador.

5 Conclusiones

En este artículo se ha presentado RFIDoors, un sistema empotrado distribuido para gestionar el acceso a una habitación por medio de tarjetas basadas en la tecnología RFID. Por medio de componentes de bajo coste y alta accesibilidad, como las placas Raspberry Pi, sensores de ultrasonido, servomotores, etc. se ha construido una maqueta como prueba de concepto y con resultado altamente satisfactorio. Además de gestionar el acceso, se ha conseguido el cierre automático de las puertas y se ha desarrollado una aplicación que permite a un administrador gestionar el acceso.

Como líneas de trabajo futuras, el futuro el prototipo planteado podría escalarse con más nodos e incluso pensar en la utilización de placas de más bajo coste y rendimiento para la gestión de los sensores, como puede ser la Raspberry Pi Zero o incluso NodeMCU.

Referencias

1. Máster en Ingeniería Informática de la Universidad Complutense de Madrid, http://informatica.ucm.es/estudios/2018-19/master-ingenieriainformatica
2. D. Lora et al., "Sistema de Seguridad Basado en una Plataforma Heterogénea Distribuida", *Enseñanza y Aprendizaje de Ingeniería de Computadores*, 5: 29-38 (2015).
3. F. Parrales et al. "Una Orquesta Sinfónica como Ejemplo de Aplicación de un Sistema Empotrado Distribuido", *Enseñanza y Aprendizaje de Ingeniería de Computadores*, 5: 115-124 (2015).
4. I.M. Laclaustra et al. "Sistema Domótico Distribuido para Controlar el Riego y el Aire Acondicionado en el Hogar", *Enseñanza y Aprendizaje de Ingeniería de Computadores*, 6: 87-102 (2016).
5. H. Ivanov et al. "Bomberman modo multijugador", *Enseñanza y Aprendizaje de Ingeniería de Computadores*, 7: 53-68 (2017).
6. J. Martín et al., 2016. "A distributed HW-SW platform for fireworks", *Proceedings of the Summer Computer Simulation Conference*. Montreal (Canada), article 17, 7 pages.
7. M. Hernández et al. "Clúster de Computación Científica de Bajo Coste y Consumo", *Enseñanza y Aprendizaje de Ingeniería de Computadores*, 8: 85-95 (2018).
8. D.G. Fernández et al., "HEVC optimization based on human perception for real-time environments", *Multimed Tools Appl* (2018). https://doi.org/10.1007/s11042-018-7033-y
9. D. G. Fernández et al., "Complexity reduction in the HEVC/H265 standard based on smooth region classification. *Digital Signal Processing,* 73: 24-39 (2018).
10. D. Rodríguez et al. 2018. "Data hiding algorithm for HEVC using intra-coded frames", *Proceedings of the 50th Computer Simulation Conference*. Society for Computer Simulation International, Bordeaux (France), Article 2, 12 pages.
11. D. Rodríguez et al. "Intra-Steganography: Hiding Data in High-Resolution Videos," *2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, Madrid, 2018, pp. 1-8.
12. M. S. Kim et al., "Efficient Mitchell's Approximate Log Multipliers for Convolutional Neural Networks", *IEEE Trans. Computers 68(5)*: 660-675 (2019).
13. Min Soo Kim et al., "Low-power implementation of Mitchell's approximate logarithmic multiplication for convolutional neural networks", ASP-DAC 2018: 617-622.
14. A. A. Del Barrio et al., "A Distributed Clustered Architecture to Tackle Delay Variations in Datapath Synthesis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 3, pp. 419-432, 2016.
15. A. A. Del Barrio et al., "A Partial Carry-Save On-the-Fly Correction Multispeculative Multiplier," *IEEE Transactions on Computers*, vol. 65, no. 11, pp. 3251-3264, 2016.
16. A. A. Del Barrio et al., "A Combined Arithmetic-High-Level Synthesis Solution to Deploy Partial Carry-Save Radix-8 Booth Multipliers in Datapaths," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 2, pp. 742-755, Feb. 2019.
17. A. Kalnoskas, "How do RFID tags and reader antennas work?," Analog IC Tips, 25-Apr-2017. [Online]. Available: https://www.analogictips.com/rfid-tag-and-reader-antennas/.
18. D. P. Rose et al., "Adhesive RFID Sensor Patch for Monitoring of Sweat Electrolytes," in *IEEE Transactions on Biomedical Engineering*, vol. 62, no. 6, pp. 1457-1465, June 2015.
19. D. He et al., "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," in *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 72-83, Feb. 2015.
20. A. Donaire and R. Tan, "Sistema de identificación por radiofrecuencia para competiciones deportivas", 2018. [Online]. Available: https://eprints.ucm.es/54982/
21. J.D. Irawan et al., "RFID and IOT for Attendance Monitoring System", *MATEC Web of Conferences* 164, 01020 (2018).