UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

Diseño de un módulo pasarela de ModBUS/RS485 a RF en las bandas ISM orientado a IoT

Antonio Calonge Prados

Tutor: Jorge Daniel Martínez Pérez

Cotutor: Javier Escalera Casillas

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2017-18

Valencia, 24 de julio de 2014

Resumen

En este trabajo final de grado, se pretende diseñar un módulo que actúe como pasarela de comunicaciones vía Modbus/RS485 y radiofrecuencia orientado al internet de las cosas y destinado a expandir los equipos de la empresa Datakorum. Este estudio y diseño viene motivado por el ahorro de costes que supone una instalación cableada y el ahorro de múltiples tarifas de datos móviles que en según qué casos pueden no necesitarse. El desarrollo del proyecto consta de definición de requisitos observando instalaciones reales, estudio de tecnologías de radiofrecuencia e integración y su elección, y finalmente el desarrollo de un prototipo capaz de cumplir con los requisitos definidos. Tanto a nivel de especificaciones físicas como capacidad de integración con los equipos de Datakorum y los servicios de IoT y nube ofrecidos por esta. Para cerrar el trabajo se definirán las líneas futuras de desarrollo y profesionalización a la que se destina el producto final.

Resum

En aquest treball final de grau, es pretén dissenyar un mòdul que actuï com passarel·la de comunicacions via Modbus / RS485 i radiofreqüència orientat a l'internet de les coses i destinat a expandir els equips de l'empresa Datakorum. Aquest estudi i disseny ve motivat per l'estalvi de costos que suposa una instal·lació cablejada i l'estalvi de múltiples tarifes de dades mòbils que en segons quins casos poden no necessitar-. El desenvolupament del projecte consta de definició de requisits observant instal·lacions reals, estudi de tecnologies de radiofreqüència i integració i la seva elecció, i finalment el desenvolupament d'un prototip capaç de complir amb els requisits definits. Tant a nivell d'especificacions físiques com capacitat d'integració amb els equips de Datakorum i els serveis de IOT i núvol oferts per aquesta. Per tancar el treball es definiran les línies futures de desenvolupament i professionalització a la qual es destina el producte final.a memoria del TFG comença amb un breu resum d’entre 150 i 200 paraules, escrit en castellà, valencià i anglès. Aquestes pàgines van sense numerar.

Abstract

In this final degree project, we intend to design a module that acts as a communications gateway via Modbus / RS485 and radio frequency oriented to the internet of things and destined to expand the equipment of the company Datakorum. This study and design is motivated by the cost savings of a wired installation and the saving of multiple mobile data rates that, depending on the cases, may not be needed. The development of the project consists of definition of requirements observing real installations, study of radiofrequency and integration technologies and their choice, and finally the development of a prototype able to meet the defined requirements. Both at the level of physical specifications and the ability to integrate with the Datakorum equipment and the IoT and cloud services offered by it. To close the work, future lines of development and professionalization to which the final product is destined will be defined.

Índice

Capítulo 1. Introducción 3
1.1 Escenario IoT [1] 3
1.1.1 Diferencias entre IoT, Domótica e Industria 4.0 3
1.1.2 IoT en España 4
1.2 DATAKORUM 4
1.3 Motivación 5
Capítulo 2. Requisitos 6
2.1 Criterios de diseño 6
2.1.1 Funcionalidades: 6
2.1.2 Requisitos físicos 6
2.1.3 Características técnicas. 6
2.2 Posibles usos 6
2.2.1 Comunicación RF de maestro a esclavo (extremo maestro). 6
2.2.2 Comunicación RF de maestro a esclavo (extremo esclavo). 6
2.2.3 Comunicación RF de maestro a sensor externo (extremo maestro). 7
2.2.4 Comunicación RF de maestro a sensor externo (extremo esclavo). 7
2.3 Riesgos 7
Capítulo 3. Estudio de mercado 8
3.1 Tecnologías existentes 8
3.1.1 Soluciones basadas en Arduino 8
3.1.2 Soluciones basadas en Raspberry pi 8
3.1.3 Wemos [2] 8
3.2 Tecnologías RF existentes 9
3.2.1 Z-Wave [3] 9
3.2.2 ZigBee [5] 11
3.2.3 6LowPAN [7] 18
3.2.4 Sigfox [8] 20
3.2.5 LoRa [9] 21
3.3 Sensores disponibles 25
Capítulo 4. Desarrollo Práctico 26
4.1 Elección de la tecnología 26
4.2 Elección del módulo LoRa para la realización de pruebas 26
4.2.1 Módulo RN2483 de Microchip [11] 26
4.2.2 Módulo WM-SG-SM-42 de USI [12] 27

4.2.3 Módulo Ra-01 y Ra-02 de AI-Thinker [14] 28
4.3 Diseño del test 28
4.4 Prototipado 29
4.5 Pruebas de conexión y desarrollo 31
4.5.1 Comunicación entre equipos 32
4.5.2 Comunicación dúplex 33
4.5.3 Envío de un String de 100 bytes 34
4.5.4 Analizar SNR y RSSI en dB y dBm al realizar envíos de 100 bytes. 34
4.5.5 Observar como varían los parámetros anteriores en relación con la distancia entre los equipos y encontrar distancias máximas de comunicación 35
4.5.6 Implementar redes de tres equipos o más basándonos en maestro-esclavo 43
4.5.7 Integración de Modbus en los equipos que conforman la red 46
4.5.8 Implementación y compatibilidad con los equipos de Datakorum 48
Capítulo 5. Conclusiones 52
5.1 Cumplimiento de objetivos 52
5.2 Líneas futuras de actuación 52
Bibliografía. 54

Capítulo 1. Introducción

En colaboración con la empresa Datakorum S.L. y dentro del marco del internet de las cosas orientado a *smartcities* se pretende desarrollar un módulo de expansión integrable en los equipos de dicha empresa orientado a redes maestro esclavo. El módulo en cuestión tiene como objetivo recoger las tramas de datos transmitidas a través del protocolo Modbus basado en RS485 y enviarlas a través de las bandas ISM (*Industrial, Scientific and Medical*) y viceversa a fin de lograr la interconexión punto a punto mediante radiofrecuencia entre dispositivos.

La finalidad del proyecto es poder comunicar internamente la red de dispositivos en entornos abiertos donde resulta demasiado costoso instalar una red cableada y/o se presentan problemas de cobertura en el lugar donde se desea emplazar alguno de los equipos de la red, evitando así que cada equipo tenga que conectarse a internet mediante 3G para enviar los datos directamente a la nube desde la que son gestionados. Este módulo permitirá que solo sea necesario comunicar a internet el o los maestros de la red de equipos.

1.1 Escenario IoT [1]

De acuerdo con la mayoría de los analistas de las tecnologías de la información y comunicación (TIC), el internet de las cosas (IoT, *Internet of Things*) es la siguiente gran tendencia que revolucionará no solo a las empresas, sino al mundo entero (especialmente emparejada con la analítica). Esto es porque permite crear un mundo donde todas las cosas están conectadas y producen billones de datos que pueden capturarse, analizarse y utilizarse.

El IoT trae consigo grandes posibilidades en industrias entre las que se encuentran la medicina, la manufactura, la automoción, las ciudades inteligentes y la agricultura, por mencionar algunas. Pero también conlleva riesgos importantes ya que el acceso a los datos puede ser vulnerado y los controles remotos pueden fallar.

En resumen, es un paradigma tecnológico que define la dotación de conectividad a Internet a cualquier objeto sobre el que se pueda medir parámetros físicos o actuar, así como las aplicaciones y tratamiento de datos inteligentes relativos a los mismos, aunque la definición de IoT, como concepto, es bastante amplio y todavía no está consensuado o con un estándar aceptado universalmente que lo desarrolle.

Es uno de los fenómenos tecnológicos más potentes de la actualidad. Y seguirá siendo uno de los fenómenos tecnológicos más potentes de los próximos años. Los expertos calculan que moverá 1,4 billones de euros en 2020, y, en los próximos años, habrá entre 20.800 y 50.000 millones de cosas conectadas en todo el mundo.

La motivación para el IoT viene de la idea de que, si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa, utilizando datos recolectados sin intervención humana, seríamos capaces de hacer un seguimiento detallado de todo cuanto nos rodea, y de esta manera ser capaces de reducir de forma importante los costes y malos usos de una gran cantidad de útiles. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El Internet de las Cosas tiene el potencial de cambiar el mundo como ya lo hizo Internet.

1.1.1 Diferencias entre IoT, Domótica e Industria 4.0

Aunque no es sencillo distinguir términos altamente interrelacionados entre sí, la diferencia entre estos conceptos viene dada por las áreas que cubren. Por ejemplo, la domótica tiene más recorrido histórico. Es un término popularizado desde hace varios lustros y se refiere a la automatización aplicada a entornos domésticos: calderas programables, neveras que saben lo que se consume, hornos que se descargan recetas, regadíos que se lanzan cuando el terreno se seca y otras soluciones similares. Mientras que el concepto de Internet de las Cosas es mucho más amplio en cuanto al espectro de aplicación e interconectividad.

En el caso de la comparación del IoT con la Industria 4.0, IoT es una de las tecnologías habilitadoras de la misma. Inicialmente hay que entender que la Industria 4.0 se presenta como una evolución estructurada que parte de la Primera Revolución Industrial, la que permitió el aumento drástico de la producción gracias a la adopción de la energía del vapor y que ha ido quemando etapas sucesivas. Tras esa primera fase llegó la Segunda Revolución, la que acarreó la producción en masa gracias al uso de la energía eléctrica, y luego fue el turno de la Tercera Revolución o revolución digital, La cual estuvo marcada por el uso de la electrónica y las tecnologías de la información para introducir la automatización en la industria. La Industria 4.0 sería lo mismo que mentar a la Cuarta Revolución, aquella que ya está en marcha.

En su caso, se caracteriza por la introducción masiva de los sistemas "ciber-físicos" (objetos industriales conectados con sensores y actuadores), la interconexión entre industrias, los interfaces abiertos para los servicios, la ciberseguridad y la aplicación de una serie de nuevas tecnologías y metodologías. Y el Internet de las Cosas aquí no sería más que uno de los factores que propicia este nuevo período. El resto son el Big Data, la robótica autónoma y colaborativa, la simulación, la integración entre sistemas tanto de forma horizontal como vertical, la ciberseguridad, el *cloud computing*, la fabricación aditiva y la realidad aumentada. Así que la Industria 4.0 incluye el IoT en su vertiente industrial, pero también cubre muchos más conceptos.

1.1.2 IoT en España

España está bien posicionada dentro del sector del Internet de las Cosas. Ha sabido colocarse en buen lugar al principio de su existencia. No debe pensarse que en comparación con otros países no esté tan avanzada, sin mucho que aportar a la evolución del IoT. España ha sido pionero en IoT y es uno de los países en los que mejor se ha entendido la cadena de valor completa desde un punto de vista tecnológico. Hay países que últimamente han ganado más tracción que el nuestro en estas cuestiones, por ejemplo, Estados Unidos. Pero también se encuentran representantes europeos como la vecina Francia o Alemania y Reino Unido. Todos ellos destacan por sus niveles de emprendimiento. En cuanto al ámbito de mejora para no perder influencia, el problema de España viene de la mano del crecimiento y de la internacionalización de nuestras empresas e iniciativas, nuestras administraciones avanzan y van apostando por estos habilitadores tecnológicos, pero aún estamos lejos de ecosistemas público-privados o puramente privados como se pueden encontrar en Francia, Alemania, Reino Unido o Estados Unidos. Y ése es un punto de referencia al que no hay que perderle la pista. Para avanzar, para favorecer el despegue de este tipo de tecnologías habilitadoras como puede ser el IoT dentro de España, es vital la colaboración público-privada.

Aparte de la financiación, la colaboración entre estamentos y la necesidad de internacionalización, el IoT se enfrenta a otros obstáculos para su crecimiento. Desde la falta de unos estándares claros y definidos, que permanezcan en el tiempo, hasta el déficit de perfiles con conocimiento sectorial, las dificultades para identificar oportunidades de negocio o la búsqueda de razones que motiven la inversión y devuelvan beneficios. También hay que tener en cuenta el tema de la seguridad, especialmente por el gran volumen de datos que lleva aparejado el uso de dispositivos conectados y la amenaza de los ciberdelincuentes. En España también se recomienda a las Administraciones que den visibilidad a los casos de éxito, que impartan formación, que asesoren, que creen comisiones y lancen incentivos con los que atraer talento a nuestro territorio, que apoyen a las aceleradoras de *startups* y que propicien la transferencia tecnológica.

1.2 DATAKORUM

Datakorum es una compañía que desarrolla dispositivos electrónicos WiFi/M2M adaptados al concepto de internet de las cosas (IoT) para ofrecer servicios *Smart City*. Destaca especialmente en el ámbito de iluminación, pero también crea soluciones basadas en *smartgreed* y telemetría para recabar datos en entornos urbanos como por ejemplo los mercados donde la temperatura y humedad relativa, el ruido ambiente o el aforo son datos que pueden ayudar a mejorar la eficiencia del lugar. Otras soluciones como la creación de parkings públicos o la detección de robo de cable

en redes de iluminación urbana también están al alcance de la compañía, además de todo el trabajo que se realiza para expandirse hacia áreas como la agricultura y la industria.

Cuando se crea una solución para un cliente, se evalúa cuál es la instalación óptima para este, y una vez esta está en marcha, el cliente es capaz de interactuar con los equipos y ver todos los datos que estos recaban mediante un *cloud* al que pueden acceder con un usuario, dicho *cloud* será accesible mediante aplicación web o móvil, la cual puede ser personalizada para las necesidades de los clientes.

1.3 Motivación

La motivación para este proyecto en colaboración con Datakorum viene del deseo de la compañía en mejorar las soluciones que se ofrecen. Para ello se ha analizado soluciones actualmente existentes y se ha buscado puntos de mejora que permitan ahorrar costes y mejorar la eficiencia.

Se ha puesto como ejemplo una instalación de parking público con múltiples entradas y salidas, cada una de las entradas o salidas está sensorizada para detectar si hay un vehículo entrante o saliente. Los sensores están asociados a equipos, que son los encargados de enviar el dato al *cloud*, el cual, gestionará dicho dato y podrá mostrar a los ciudadanos cuantas plazas del total hay ocupadas a través de paneles informativos o aplicaciones móviles. Además, ayudará a los gestores del parking a conocer datos sobre la afluencia a dicho parking, cuáles son las horas de máxima y mínima ocupación y otros datos relevantes para futuras mejoras.

Los puntos de mejora para dicha instalación se basaron, en primera instancia, en evitar que cada sensor estuviera asociado a un equipo que comunicase con el *cloud*, el objetivo es reducir costes de conectividad y evitar que la escasa cobertura de la red móvil en ciertos puntos impidiese emplazar los equipos en el lugar que facilitan el buen funcionamiento de la solución.

Una posible solución se basa en crear una red maestro esclavo mediante protocolo Modbus. Con ello se pretende que el número de equipos que se conectan al *cloud* sea el mínimo posible, aprovechando para que estos sean aquellos que se encuentran en mejor posición en cuanto a cobertura. La desventaja de este tipo de solución, pese a su buen funcionamiento en la práctica, es que para crear esa red Modbus, en la mayoría de los casos unas entradas o salidas estarán bastante alejadas las unas de las otras. Esto se traduce en mayores costes de instalación ya que las largas longitudes de cable, en la mayoría de los casos, estarán enterrados, lo cual generará mayor tiempo de instalación y mayores costes.

Sabiendo que en este tipo de instalaciones el modelo maestro-esclavo funciona bien, y puede ser extrapolable a otro tipo de soluciones, se ha propuesto implementar este modelo de solución a través de radiofrecuencia, concretamente, se pretende utilizar la banda libre ISM. Con esto se pretende que las tramas Modbus se traduzcan a algún protocolo en RF y que se transmitan por medio aéreo entre nuestros equipos. Poder interconectar los equipos ya sea bien vía Modbus o RF solventará muchos de los problemas y costes de instalación como los ya mencionados en el caso del parking.

Capítulo 2. Requisitos

2.1 Criterios de diseño

2.1.1 Funcionalidades:

Para Realizar el diseño y saber qué aspectos deben tenerse en cuenta, es necesario conocer como se desea que este funcione.

El módulo debe ser capaz de leer y retransmitir tramas de datos, tanto leídas desde equipos como desde sensores independientes. Deben ser capaces de leer datos por Modbus o puerto serie y transmitir vía RF y viceversa.

Los equipos deben poder configurarse para comunicarse entre sí y sensores externos. Entre ellos deben ser capaces de gestionar redes propias, entre otras, redes maestro esclavo. En el caso de las redes maestro esclavo, será preferible que aquel que actúe como maestro esté asociado directamente (o integrado) en un equipo que tenga conexión directa con internet.

2.1.2 Requisitos físicos

En cuanto a aspectos físicos, como principal premisa, se requiere la compatibilidad total con los equipos que actualmente existen en Datakorum, es decir, que el módulo que se pretende diseñar sea integrable dentro de los mismos, por lo que el tamaño no debe exceder de una superficie de 80 cm^2 ni de una altura de 2 cm, además debe tener compatibilidad de pines.

No solo la integración dentro de un equipo debe ser requisito, sino que también se pretende que este módulo pueda funcionar fuera de los equipos, así puede resultar más sencillo aprovechar sensores existentes sin necesidad de darle un equipo para que lea de él. En caso de estar aislado, se diseñará un emplazamiento en una carcasa específica.

2.1.3 Características técnicas.

Como primer esbozo de las características técnicas, se pretende que el equipo se alimente a 12 voltios VDC, ya que así facilitamos la compatibilidad con los equipos de Datakorum. También debe estar orientado a alimentarse mediante baterías a 12 voltios VDC, aunque la capacidad de esta aún está por determinar.

En cuanto al alcance en RF, se pretende que el alcance mínimo sea de 100 metros, ya que se ha visto en determinadas instalaciones que es una distancia común que cubrir. Se pretende que trabaje sobre la banda ISM, preferiblemente en alguna banda de operación permitida en Europa.

2.2 Posibles usos

2.2.1 Comunicación RF de maestro a esclavo (extremo maestro).

En la comunicación de maestro esclavo, donde la comunicación la inicia el esclavo, debe tenerse en cuenta que sigue siendo el maestro el que maneja la red. Los esclavos iniciaran la comunicación debido a un evento o una programación horaria tipo baliza.

Los eventos que motivarían que iniciase la comunicación el esclavo estarían asociados a la sonorización o alertas de la instalación. Los sensores podrían activar el evento debido a valores críticos o escalones de valor programados para ser comunicados.

En el caso del balizado, cada cierto tiempo o a ciertas horas, los equipos enviarían el dato o los datos programados.

2.2.2 Comunicación RF de maestro a esclavo (extremo esclavo).

Esta es la configuración más sencilla de manejar, ya que es el maestro el que controla cuando y como recibe información de los esclavos. Este ordena a los esclavos que le arrojen los datos que haya solicitado, además es capaz de ejercer control sobre los equipos asociados a los esclavos.

Esta clase de comunicación será normalmente bajo demanda, es decir, el usuario a través de su aplicación solicitará la toma de datos o la actuación. También es posible una programación para adquisición de datos ordenada desde el maestro.

También es posible que se generen eventos en el maestro que provoquen que este deba actuar sobre el resto de los esclavos. Otra posibilidad es que un evento generado por algún esclavo haya sido comunicado al maestro, en consecuencia, este deberá actuar sobre el resto de los esclavos.

2.2.3 Comunicación RF de maestro a sensor externo (extremo maestro).

Este caso es similar al 2.2.1, pero más simple, ya que no es un equipo que trate de notificar eventos o alarmas. El sensor podrá enviar el dato continuamente y sería el maestro el que activase la ventana de recepción.

Otra posibilidad es dotar al sensor de un controlador capaz de asemejar más el uso al apartado ya citado, permitiendo el balizado y la generación de eventos que deberán ser notificados para la gestión de la red de equipos.

2.2.4 Comunicación RF de maestro a sensor externo (extremo esclavo).

Este caso se parece al punto 2.2.2, pero al igual que antes, bastante más simple. La aplicación mas sencilla es que el maestro demande el envió de datos para gestionar la cantidad de envíos de la red.

También es posible programar el maestro para decidir cómo y cuándo se piden los datos.

2.3 Riesgos

Los riesgos que pueden presentarse son diversos, deben destacarse los que pueden derivar de la manera en la que los equipos se interconectan, es decir, que los equipos puedan tener una calidad de conexión insuficiente afecta directamente al funcionamiento de la red.

A la hora de crear la red, es importante definir bien las direcciones de cada equipo, ya que, si se comenten errores en este paso, puede que más de un equipo esté recibiendo datos u ordenes que no son para él o el caso contrario, que enviemos órdenes a un equipo pero que este, en realidad, no pertenezca a la red.

El hecho de que los equipos trabajen sobre la banda libre ISM, la cual es ampliamente utilizada por una diversa variedad de protocolos, favorece que se puedan recibir interferencias, porque es bastante importante proteger la calidad de la señal. A su vez, esto abre la posibilidad de que, al ser bandas abiertas, individuos ajenos a los equipos puedan recopilar información o tratar de actuar sobre estos, por lo que será necesario cifrar las comunicaciones.

Capítulo 3. Estudio de mercado

3.1 Tecnologías existentes

Hoy día, el IoT cubre la mayoría de los artículos de foros en internet que tratan sobre tecnología centrados en la electrónica y las comunicaciones, están copados de artículos y tutoriales en los que te explican en qué se basa el IoT y como poder ponerlo en práctica.

3.1.1 Soluciones basadas en Arduino

La plataforma de hardware libre de Arduino se ha visto muy enriquecida gracias a ello. Es muy fácil comprar módulos para comunicar los objetos cotidianos y otros no tan cotidianos a internet y a su vez entre sí. Incluso desde el mismo arduino.cc ofrecen placas de Arduino especialmente diseñadas para IoT y *Werables* (objetos "ponibles" como ropa o accesorios capaces de comunicarse con nuestros *Smartphones* y a su vez a internet). Internet está plagado de soluciones a estos conceptos de una manera "casera" y sencilla.

También existen soluciones profesionales basadas en Arduino o cuyo hardware es compatible con el mismo para dotar de IoT tanto a los elementos del hogar, como a edificios corporativos o plantas industriales. Además, la facilidad con la que Arduino es capaz de integrar tecnologías IoT es muy beneficiosa en entornos de investigación donde el presupuesto es escaso y se quiere sensorizar lugares u objetos a los que se tiene difícil acceso o se necesita estar en dos o más lugares a la vez.

3.1.2 Soluciones basadas en Raspberry pi

Raspberry pi ofrece otras posibilidades. Si bien es verdad que es más complicado de aprender a utilizar y a integrar el hardware en ella, es más potente y ofrece capacidad de procesado.

Una de las principales ventajas de Raspberry pi es que permite de manera eficiente la creación de pequeños servidores de internet en los que almacenar datos y generar plataformas web sencillas para interoperar estos. Al estar basado en Linux permite, no solo adquirir los datos que se desea o manejar aquello que se quiera, si no también tratar los datos, procesarlos para mejorar la información que estos ofrecen.

Al igual que en el caso de Arduino, existen multitud de foros y webs donde te explican como poder crear tus propias soluciones y descargar sistemas operativos dedicados a IoT. Grandes compañías como Microsoft o IBM han lanzado sus propios cores para Raspberry pi destinados a IoT, lo que demuestra el alto potencial de este tipo de soluciones no solo para el aficionado sino también para temas de estudio e investigación en IoT y aplicaciones corporativas.

Cabe destacar, que tanto Arduino como Raspberry pi pueden ser muy buenos amigos y ser capaces de trabajar juntos de manera altamente sinérgica, ya que, si bien Raspberry pi nos ofrece capacidades de procesado, análisis y gestión de datos, Arduino complementa muy bien la parte de adquisición de datos, intercomunicación y gestión del hardware, por lo que estas dos herramientas juntas son capaces de hacer grandes cosas.

3.1.3 Wemos [2]

Wemos es (entre otras muchas similares) una compañía que ha aprovechado el éxito de Arduino y ha creado sus propias placas de microcontroladores orientados a IoT basados en este. Poseen diferentes diseños orientados a diferentes tipos de comunicaciones y además se han centrado en la conexión de sus placas a internet con los populares chips ESP826.

Wemos es un ejemplo como otros tantos de la cantidad de hardware que se crea orientado a IoT donde prima la sencillez de aplicación y la manera en la que facilitan la creación de proyectos para este nuevo concepto más potente.

3.2 Tecnologías RF existentes

3.2.1 Z-Wave [3]

La tecnología Z-Wave está orientada a domótica y se basa en una red mallada que utiliza ondas de radio de baja energía para comunicarse de un electrodoméstico a otro.

un sistema de automatización Z-Wave puede controlarse a través de Internet desde un mando inalámbrico, un teclado montado en la pared smartphones, tabletas u ordenadores, con una puerta de enlace Z-Wave o un dispositivo de control centralizado que sirve como mando central y puerto de salida.

Proporciona interoperabilidad entre los sistemas de control del hogar de diferentes fabricantes que forman parte de su alianza (La Z-Wave Alliance está unida en su apoyo a Z-Wave como la tecnología habilitadora para la era del control y monitoreo inalámbrico en cualquier lugar o lugares. Los miembros de la Z-Wave Alliance lideran el mercado de controles domésticos, proporcionando sistemas que brindan mayor comodidad, conveniencia y seguridad. En el ecosistema Z-Wave [4]).

Figura 1. Alguns de las empresas que conformar la Z-Wave Alliance

Z-Wave proporciona una capa de interoperabilidad que asegura que los dispositivos puedan compartir información y permita que todo el hardware y software trabaje en conjunto. Su tecnología de red de malla inalámbrica permite a cualquier nodo comunicarse, directa o indirectamente, con nodos adyacentes, controlando cualquier nodo adicional. Los nodos que están dentro del rango se comunican entre sí directamente. Si no están dentro del rango, pueden vincularse con otro nodo que esté dentro del alcance de ambos para acceder e intercambiar información.

Ciertas partes de la tecnología Z-Wave se publicaron abiertamente cuando Sigma Designs lanzó una versión pública de la capa de interoperabilidad, agregando software a la biblioteca de código abierto de Z-Wave. La disponibilidad de código abierto permite a los desarrolladores de software integrar esta tecnología en dispositivos con menos restricciones. La seguridad S2 de Z-Wave, Z / IP para transportar señales Z-Wave a través de redes IP, y el middleware Z-Ware son todos de código abierto desde 2016.

- ***Características técnicas***
    - RF

Z-Wave está diseñado para proporcionar una transmisión fiable y de baja latencia de pequeños paquetes de datos a velocidades de hasta 100 kbit/s. El rendimiento es de 40 kbit/s (9,6 kbit/s con chips antiguos) y es adecuado para aplicaciones de control y sensorización. La distancia de comunicación entre dos nodos es de aproximadamente 30 metros (40 metros con un chip de la serie 500), y con la capacidad de que un mensaje pueda saltar hasta cuatro veces entre nodos,

brinda suficiente cobertura para la mayoría de los hogares o lugares residenciales. La modulación empleada se basa en la codificación mánchester.

Z-Wave utiliza la banda industrial, científica y médica (ISM) sin licencia de la Parte 15. Funciona a 868,42 MHz en Europa, a 908,42 MHz en Norteamérica y utiliza otras frecuencias en otros países, según sus reglamentos. Esta banda compite con algunos teléfonos inalámbricos y otros dispositivos electrónicos de consumo, pero evita la interferencia con Wi-Fi, Bluetooth y otros sistemas que operan en la abarrotada banda de 2,4 GHz. Las capas inferiores, MAC y PHY, están descritas por ITU-T G.9959 y son totalmente compatibles con versiones anteriores a esta. En 2012, la Unión Internacional de Telecomunicaciones (ITU) incluyó las capas Z-Wave PHY y MAC como una opción en su estándar G.9959 para dispositivos inalámbricos de menos de 1 GHz. Las velocidades de datos incluyen 9600 bps y 40 kbps, con una potencia de salida de 1 mW o 0 dBm. Los chips del transceptor Z-Wave son suministrados por Sigma Designs y Mitsumi.

- Configuración de red, topología y enrutamiento

Z-Wave usa una arquitectura de red de malla enrutada por origen. Las redes de malla también se conocen como redes inalámbricas ad hoc. En tales redes, los dispositivos usan el canal inalámbrico para enviar mensajes de control que luego son transmitidos por dispositivos vecinos en forma de onda. El dispositivo de origen que desea transmitir se conoce, por lo tanto, como el iniciador.

Los dispositivos se pueden comunicar entre ellos mediante el uso de nodos intermedios para rodear y sortear activamente los obstáculos del hogar o los puntos muertos por radio que pueden aparecer en el entorno multitrayecto de una casa. Un mensaje del nodo A al nodo C puede entregarse con éxito incluso si los dos nodos no están dentro del alcance, siempre que un tercer nodo B pueda comunicarse con los nodos A y C. Si la ruta preferida no está disponible, el creador del mensaje intentará otras rutas hasta que se encuentre una ruta al nodo C. Por lo tanto, una red Z-Wave puede abarcar mucho más que el rango de radio de un solo equipo; sin embargo, con varios de estos saltos se puede introducir un ligero retraso entre el comando de control y el resultado deseado.

La red más simple es un único dispositivo controlable y un controlador principal. Se pueden agregar dispositivos adicionales en cualquier momento, al igual que controladores secundarios, incluidos los controladores de mando tradicionales, los controladores de llavero, los controladores de interruptor de pared y las aplicaciones de PC diseñadas para la administración y el control de una red Z-Wave. Una red Z-Wave puede constar de hasta 232 dispositivos, con la opción de conectar redes si se requieren más dispositivos.

Un dispositivo debe estar "incluido" en la red Z-Wave antes de que pueda controlarse a través de esta. Este proceso (también conocido como "emparejamiento" y "adición") generalmente se logra presionando una secuencia de botones en el controlador y en el dispositivo que se agrega a la red. Esta secuencia solo debe realizarse una vez, después de lo cual el dispositivo siempre es reconocido por el controlador. Los dispositivos se pueden eliminar de la red Z-Wave mediante un proceso similar. El controlador aprende la intensidad de la señal entre los dispositivos durante el proceso de inclusión, por lo que la arquitectura espera que los dispositivos estén en su ubicación final prevista antes de que se agreguen al sistema. Por lo general, el controlador tiene una pequeña batería de respaldo interna, lo que permite que se desenchufe temporalmente y pueda ser llevado a la ubicación de un nuevo dispositivo para el emparejamiento. El controlador se devuelve a su ubicación normal y se vuelve a conectar.

Cada red Z-Wave se identifica mediante una identificación de red, y cada dispositivo se identifica además mediante una identificación de nodo. La ID de red (también llamada ID de inicio) es la identificación común de todos los nodos que pertenecen a una red Z-Wave lógica. La ID de red tiene una longitud de 4 bytes (32 bits) y el controlador principal se la asigna a cada dispositivo cuando el dispositivo está "incluido" en la red. Los nodos con diferentes ID de red no pueden

comunicarse entre sí. La identificación del nodo es la dirección de un solo nodo en la red. La ID de nodo tiene una longitud de 1 byte (8 bits) y debe ser única en su red.

El chip Z-Wave está optimizado para dispositivos que funcionan con pilas, y la mayoría de las veces permanece en un modo de ahorro de energía para consumir menos energía, despertando solo para realizar su función. Con las redes de malla Z-Wave, cada dispositivo de la casa rebota señales inalámbricas en esta, lo que da como resultado un bajo consumo de energía, lo que permite que los dispositivos funcionen durante años sin necesidad de reemplazar las pilas. Para que las unidades Z-Wave puedan enrutar mensajes no solicitados, no pueden estar en modo de suspensión. Por lo tanto, los dispositivos que funcionan con pilas no están diseñados como unidades repetidoras. Los dispositivos móviles, como los controles remotos, también están excluidos ya que Z-Wave supone que todos los dispositivos en la red permanecen en su posición original detectada.

- Seguridad

Aunque ha habido una serie de investigaciones de seguridad académicas y prácticas en sistemas de domótica basados en protocolos ZigBee y X10, la investigación todavía está en pañales para analizar las capas apiladas del protocolo Z-Wave, que requieren el diseño de un dispositivo de captura de paquetes de radio y software para interceptar las comunicaciones en esta tecnología.

El 17 de noviembre de 2016, la Z-Wave Alliance anunció estándares de seguridad más estrictos para aquellos dispositivos que reciben certificación Z-Wave a partir del 2 de abril de 2017. Conocida como Seguridad 2 (o S2), proporciona seguridad avanzada para dispositivos domésticos inteligentes, puertas de enlace y concentradores. Respalda los estándares de encriptación para transmisiones entre nodos, y exige nuevos procedimientos de vinculación para cada dispositivo, con códigos únicos PIN o QR en cada dispositivo. La nueva capa de autenticación está destinada a evitar que los hackers tomen el control de dispositivos no seguros o poco seguros. Según Z-Wave Alliance, el nuevo estándar de seguridad es la seguridad más avanzada disponible en el mercado para dispositivos y controladores domésticos inteligentes, puertas de enlace y concentradores.

- Hardware

El chip más común para los nodos Z-Wave es el ZW0500, construido alrededor de un microcontrolador Intel MCS-51 con un reloj interno del sistema de 32 MHz. La parte RF del chip contiene un transceptor GisFSK para una frecuencia seleccionable por software. Con una fuente de alimentación de 2.2-3.6 voltios, consume 23 mA en modo de transmisión. Sus características incluyen cifrado AES-128, un canal inalámbrico de 100kbps, escucha simultánea en múltiples canales y soporte USB VCP.

3.2.2 ZigBee [5]

ZigBee es un estándar de red de malla inalámbrica, de bajo coste y baja potencia, destinado a dispositivos alimentados por pilas o batería en aplicaciones de monitoreo y control inalámbrico. ZigBee ofrece comunicación de baja latencia. Los chips generalmente se integran con transceptores de radio y con microcontroladores. ZigBee opera en las bandas de radio industriales, científicas y médicas (ISM): 2,4 GHz en la mayoría de las normativas del mundo; aunque algunos dispositivos también usan 784 MHz en China, 868 MHz en Europa y 915 MHz en los EE.UU. y Australia, sin embargo, incluso esas regiones y países todavía usan 2,4 GHz para la mayoría de los dispositivos comerciales para uso doméstico. Las velocidades de datos varían de 20 kbit/s (banda de 868 MHz) a 250 kbit/s (banda de 2,4 GHz).

ZigBee se basa en la capa física y el control de acceso al medio definido en el estándar IEEE 802.15.4 para redes inalámbricas de área personal (WPAN) de baja velocidad. La especificación incluye cuatro componentes clave adicionales: capa de red, capa de aplicación, objetos de dispositivo ZigBee (ZDO) y objetos de aplicación definidos por el fabricante. Los ZDO son

responsables de algunas tareas, incluido el seguimiento de las funciones del dispositivo, la administración de las solicitudes para unirse a una red, así como la detección y seguridad del dispositivo.

La capa de red de ZigBee admite nativamente tanto redes en estrella como en árbol, y redes de malla genéricas. Cada red debe tener un dispositivo coordinador. Dentro de las redes de estrella, el coordinador debe ser el nodo central. Tanto árboles como mallas permiten el uso de enrutadores ZigBee para extender la comunicación a nivel de red. Otra característica definitoria de la tecnología son las instalaciones para llevar a cabo comunicaciones seguras, protegiendo el establecimiento y transporte de claves criptográficas, marcos cifrados y dispositivos de control. Se basa en el marco de seguridad básico definido en IEEE 802.15.4.

- ***ZigBee Alliance [6]***

La ZigBee Alliance es una alianza, sin ánimo de lucro, de más de 400 compañías y más de 600 productos certificados. La mayoría de las compañías son pertenecen al ámbito de la fabricación de semiconductores, con el objetivo de auspiciar el desarrollo e implementación de una tecnología inalámbrica de bajo coste.

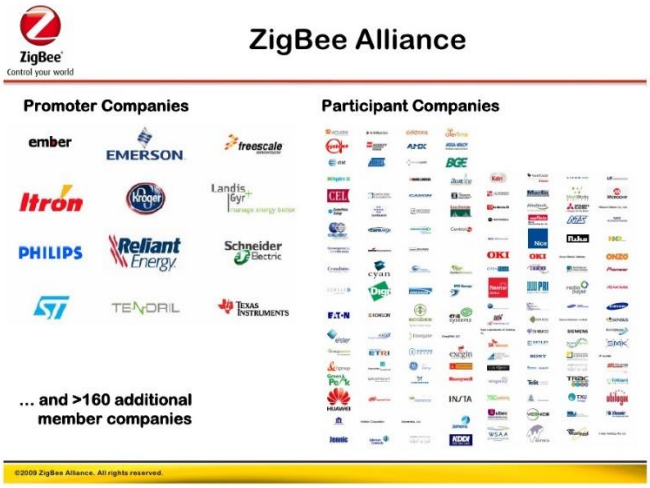


Figura 2. Algunas empresas que conforman la ZigBee alliance.

- ***Características técnicas***

  - ♦ Protocolos

Recientemente se ha estado investigando en los protocolos que gestionan los algoritmos de red (*ad hoc on-demand distance vector*, vector de distancias bajo demanda; neuRFon) con el fin de conformar redes ad-hoc de baja velocidad. Estas redes, en su mayoría, están pensadas para formar un *cluster* de *clusters*. También es posible estructurarlas en forma de malla o simplemente como un único *cluster*. Las actuales características de los protocolos soportan redes que pueden ser utilizadas para facilitar el balizado.

Las redes que no emplean balizas (aquéllas con un grado de balizado igual a 15) tiene acceso al canal mediante CSMA/CA. Los routers tienden a mantenerse activos todo el tiempo, por lo que suelen requerir una alimentación estable. Esto, a cambio, permite redes heterogéneas en las que algunos dispositivos tienen la capacidad de estar transmitiendo datos constantemente, mientras que otros se limitan a transferir información ante la presencia de estímulos externos. El ejemplo típico se basa en la activación inalámbrica: un nodo en una lámpara u otro aparato puede estar recibiendo de manera continua ya que está conectado a la red; sin embargo, un aparato de activación que funcione a pilas debería permanecer dormido hasta que el aparato se activase. En una red de estas características la lámpara sería un router o coordinador, y el elemento activador un dispositivo final.

Si la red emplea balizas, los routers activan estas periódicamente a fin de confirmar su presencia a otros nodos. Los nodos pueden ser desactivados entre las recepciones de balizas para reducir su ciclo de servicio (*duty cycle*). Los intervalos de balizado pueden ir desde 15,36 ms a 15,36 ms * 214 = 251,65824 segundos a 250 kbit/s; de 24 ms a 24 ms * 214 = 393,216 segundos a 40 kbit/s; y de 48 ms a 48 ms * 214 = 786,432 segundos a 20 kbit/s. Sin embargo, largos periodos con ciclos de servicio cortos requieren una temporización precisa, lo que puede ir en contra del principio de bajo coste.

Generalmente, los protocolos ZigBee minimizan el tiempo de actividad de radiofrecuencia para tratar de reducir o evitar el uso de energía. En redes donde existen balizas, los nodos sólo necesitan permanecer despiertos mientras estas transmiten (además de cuando se les asigna temporización para la transmisión). En caso de no incorporar balizas, el consumo es asimétrico repartido entre dispositivos permanentemente activos y otros que sólo lo están esporádicamente.

Los dispositivos ZigBee están obligados a respetar el estándar de WPAN para baja tasa de transmisión especificado en la norma IEEE 802.15.4-2003. En ella se definen los niveles más bajos: el nivel físico (PHY) y el control de acceso al medio (MAC, parte del nivel de enlace de datos, DLL). El estándar trabaja sobre las bandas ISM de uso no regulado. Se definen hasta 16 canales en el rango de 2,4 GHz, cada uno de ellos con un ancho de banda de 5 MHz. La frecuencia central que maneja cada canal puede calcularse como: FC = (2405 + 5*(k-11)) MHz, con k = 11, 12..., 26.

La radiofrecuencia emplea un espectro de dispersión de secuencia directa. Se utiliza BPSK en ambos rangos de frecuencia menores, además de un QPSK ortogonal que transmite dos bits por símbolo en la banda de 2,4 GHz. Esto permite obtener tasas de transmisión en el aire de capaces de alcanzar 250 kbps, mientras que las bandas inferiores se han ampliado tras la última revisión a esta tasa desde los 40 kbps de la primera versión. Los rangos de transmisión oscilan entre los 10 y 75 metros, aunque depende bastante del entorno. La potencia de salida de radio suele ser de 0 dBm (1 mW).

Aunque en general se utiliza CSMA/CA con el fin de evitar colisiones en la transmisión, existen algunas excepciones para su uso: por una parte, las tramas siguen una temporización fija que debe respetarse; y, por otra parte, las confirmaciones de envíos tampoco siguen esta disciplina; finalmente, si se asignan intervalos de tiempo garantizados para una transmisión tampoco es posible que exista contención.

- Hardware

El diseño de radiofrecuencia utilizado por ZigBee tiene pocas etapas analógicas y utiliza circuitos digitales siempre que sea posible.

Pese a la sencillez del hardware, el procedimiento para la certificación de un dispositivo conlleva una validación completa de los requisitos para el nivel físico. Esta revisión intensiva tiene múltiples ventajas, ya que todas las radios que se fabriquen a partir de una misma máscara de semiconductor dispondrán de unas mismas características de radiofrecuencia. De otra manera, un nivel físico mal controlado puede ser perjudicial, no sólo para el propio dispositivo, sino también para el consumo de energía de otros dispositivos dentro de la red. Otros estándares pueden compensar determinados problemas, mientras que ZigBee trabaja en márgenes bastante estrechos de consumo y ancho de banda. Por ello, según el 802.15.4, las radios pasan validaciones ISO 17025. La mayoría de los fabricantes tienen planteado integrar la radio y el microcontrolador en un único chip, lo cual permite crear dispositivos más compactos.

Esta norma especifica el funcionamiento en las bandas ISM sin licencia de 2,4 a 2,4835 GHz (en todo el mundo), de 902 a 928 MHz (en América y Australia) y de 868 a 868,6 MHz (Europa). Dieciséis canales se asignan en la banda de 2,4 GHz, con cada canal espaciado a 5 MHz, aunque utilizando solo 2 MHz de ancho de banda. Las radios usan codificación de espectro ensanchado de secuencia directa, que es administrada por el flujo digital en el modulador. La codificación de desplazamiento de fase binaria (BPSK) se utiliza en las bandas de 868 y 915 MHz, y la

codificación de desplazamiento de fase en cuadratura compensada (OQPSK) que transmite dos bits por símbolo se utiliza en la banda de 2,4 GHz.

La velocidad de datos en el aire sin procesar es de 250 kbit/s por canal en la banda de 2,4 GHz, 40 kbit/s por canal en la banda de 915 MHz y 20 kbit/s en la banda de 868 MHz. El rendimiento de los datos reales será menor que la velocidad de bits máxima especificada debido a la sobrecarga del paquete y los retrasos en el procesamiento. Para aplicaciones en interiores a 2,4 GHz, la distancia de transmisión puede ser de 10-20 m, dependiendo de los materiales de construcción, el número de muros a penetrar y la potencia de salida permitida en esa ubicación geográfica. Al aire libre con línea de visión, el alcance puede ser de hasta 1500 m, dependiendo de la potencia de salida y las características ambientales. La potencia de salida de las radios generalmente es de 0-20 dBm (1-100 mW).

- Dispositivos y modos de operación

  - *ZigBee coordinador (ZC)*

El dispositivo más capaz, el coordinador forma la raíz del árbol de la red y puede tender un puente a otras redes. Hay exactamente un Coordinador ZigBee en cada red, ya que es el dispositivo que inició originalmente la red (la especificación ZigBee LightLink también permite operar sin un Coordinador ZigBee, lo que lo hace más utilizable para productos domésticos disponibles en el mercado). Almacena información sobre la red, incluso actúa como el Centro de confianza y el depósito de claves de seguridad.

  - *ZigBee enrutador (ZR)*

Además de ejecutar una función de aplicación, puede actuar como un enrutador intermedio, transmitiendo datos de otros dispositivos.

  - *Dispositivo ZigBee end (ZED)*

Contiene suficiente funcionalidad para comunicarse con el nodo padre (ya sea el Coordinador o un Enrutador); no puede retransmitir datos de otros dispositivos. Esta relación permite que el nodo esté dormido una cantidad significativa de tiempo, lo que da una larga duración de la batería. Una ZED requiere la menor cantidad de memoria y, por lo tanto, puede ser menos costosa de fabricar que una ZR o ZC.

- Software

El software está diseñado para ser fácil de desarrollar en microprocesadores pequeños y económicos.

  - *Capa de red.*

Las principales funciones de la capa de red son permitir el uso correcto de la subcapa MAC y proporcionar una interfaz adecuada para su uso por la siguiente capa superior, es decir, la capa de aplicación. Sus capacidades y estructura son las típicamente asociadas a tales capas de red, incluido el enrutamiento. La función de la capa de red es exactamente como suena. Se trata de funciones de red como conectar, desconectar y configurar redes. Agregará una red, asignará direcciones y agregará o eliminará ciertos dispositivos. Esta capa utiliza topologías de estrella, malla y árbol. Agrega una interfaz a la capa de aplicación.

Por un lado, la entidad de datos crea y gestiona las unidades de datos de capa de red de la carga útil de la capa de aplicación y realiza el enrutamiento de acuerdo con la topología actual. Por otro lado, está el control de capa, que se utiliza para gestionar la configuración de nuevos dispositivos y establecer nuevas redes: puede determinar si un dispositivo vecino pertenece a la red y descubre nuevos vecinos y enrutadores. El control también puede detectar la presencia de un receptor, lo que permite la comunicación directa y la sincronización MAC.

El protocolo de enrutamiento utilizado por la capa de red es AODV, que tiene propiedades similares al Enrutamiento basado en asociatividad (ABR). A diferencia de AODV, ABR fue un protocolo patentado de enrutamiento inventado en 1994 en la Universidad de Cambridge, Inglaterra. AODV era un borrador de IETF activo, que constantemente agregaba características de una variedad de sugerencias y fuentes a lo largo del tiempo. En AODV, para encontrar el dispositivo de destino, AODV transmite una solicitud de ruta a todos sus vecinos. Luego os vecinos transmiten la solicitud a sus otros vecinos y en adelante hasta que se llegue al destino. Una vez que se llega al destino, envía su respuesta de ruta a través de la transmisión de unidifusión siguiendo la ruta de menor costo de regreso a la fuente. Este enfoque de descubrimiento de ruta es similar al del enrutamiento basado en asociatividad, excepto que ABR no usa números de secuencia o vectores de distancia. Una vez que la fuente recibe la respuesta, actualizará su tabla de enrutamiento para la dirección de destino del próximo salto en la ruta y el costo de la ruta.

- *Capa de aplicación.*

La capa de aplicación es la capa de nivel más alto definida por la especificación y es la interfaz efectiva del sistema ZigBee para sus usuarios finales. Comprende la mayoría de los componentes agregados por la especificación ZigBee: tanto ZDO como sus procedimientos de gestión, junto con los objetos de aplicación definidos por el fabricante, se consideran parte de esta capa. Esta capa vincula tablas, envía mensajes entre dispositivos enlazados, administra direcciones de grupo, reensambla paquetes y también transporta datos. Es responsable de proporcionar servicio a los perfiles de dispositivo de ZigBee.

- *componentes principales.*

El ZDO (*ZigBee Device Object*), un protocolo en la pila de protocolos de ZigBee, es responsable de la administración general del dispositivo, las claves de seguridad y los modos de funcionamiento. Es responsable de definir el rol de un dispositivo como coordinador o dispositivo final, pero también del descubrimiento de nuevos dispositivos (de un solo salto) en la red y la identificación de los servicios que ofrecen. Después de esto, puede establecer enlaces seguros con dispositivos externos y responder a las solicitudes de enlace en consecuencia.

La subcapa de soporte de aplicaciones (APS) es el otro componente estándar principal de la capa y, como tal, ofrece una interfaz bien definida y servicios de control. Funciona como un puente entre la capa de red y los otros elementos de la capa de aplicación: mantiene tablas de enlace actualizadas en forma de una base de datos, que se puede usar para encontrar los dispositivos apropiados según los servicios que se necesitan y aquellos que ofrecen los diferentes dispositivos. Como la unión entre ambas capas especificadas, también enruta los mensajes a través de las capas de la pila de protocolos.

- *Modelo de comunicación.*

Una aplicación puede consistir en comunicar objetos que cooperan para llevar a cabo las tareas deseadas. El objetivo de ZigBee es distribuir el trabajo entre muchos dispositivos diferentes que residen dentro de nodos ZigBee individuales que a su vez forman una red (dicho trabajo será típicamente local para cada dispositivo, por ejemplo, el control de cada electrodoméstico).

La colección de objetos que forma la red se comunica utilizando las facilidades proporcionadas por APS, supervisadas por las interfaces ZDO. El servicio de datos de capa de aplicación sigue una estructura típica de solicitud-confirmación/indicación-respuesta. Dentro de un solo dispositivo, pueden existir hasta 240 objetos de aplicación, numerados en el rango 1-240. 0 está reservado para la interfaz de datos ZDO y 255 para transmisión; el rango 241-254 no está actualmente en uso.

Dos servicios están disponibles para que los objetos de aplicación los usen (en ZigBee 1.0): El servicio de pares clave-valor (KVP) tiene la finalidad de configuración. Permite la descripción, solicitud y modificación del atributo de objeto a través de una interfaz simple basada en *get/set* y primitivas de evento, algunas permiten una solicitud de respuesta. La configuración usa XML comprimido (se puede usar XML completo) para proporcionar una solución adaptable y elegante.

El servicio de mensajes está diseñado para ofrecer un enfoque general del tratamiento de la información, evitando la necesidad de adaptar los protocolos de la aplicación y la posible sobrecarga incurrida por KVP. Permite que las cargas útiles arbitrarias se transmitan a través de tramas APS.

El direccionamiento también es parte de la capa de aplicación. Un nodo de red consiste en un transceptor de radio conforme a 802.15.4 y una o más descripciones de dispositivo (básicamente colecciones de atributos que pueden ser sondeados o configurados, o que pueden ser monitoreados a través de eventos). El transceptor es la base para el direccionamiento, y los dispositivos dentro de un nodo se especifican mediante un identificador de punto final en el rango 1-240.

- *comunicación y descubrimiento de dispositivo.*

Para que las aplicaciones se comuniquen, sus dispositivos integradores deben usar un protocolo de aplicación común (tipos de mensajes, formatos, etc.); estos conjuntos de convenciones están agrupados en perfiles. Además, el enlace se decide al hacer coincidir los identificadores de clúster de entrada y salida, únicos dentro del contexto de un perfil dado y asociados a un flujo de datos entrantes o salientes en un dispositivo. Las tablas de enlace contienen pares de origen y destino.

Dependiendo de la información disponible, el descubrimiento del dispositivo puede seguir diferentes métodos. Cuando se conoce la dirección de red, la dirección IEEE se puede solicitar utilizando la comunicación de unidifusión. Cuando no lo es, las peticiones se transmiten (la dirección IEEE forma parte de la carga de respuesta). Los dispositivos finales simplemente responderán con la dirección solicitada, mientras que un coordinador de red o un enrutador también enviarán las direcciones de todos los dispositivos asociados.

Este protocolo de descubrimiento extendido permite a los dispositivos externos averiguar sobre los dispositivos en una red y los servicios que ofrecen, qué puntos finales pueden informar cuando son consultados por el dispositivo descubridor (que previamente ha obtenido sus direcciones). Los servicios coincidentes también pueden ser utilizados.

El uso de identificadores de clúster impone la unión de entidades complementarias utilizando las tablas de enlace, que mantienen los coordinadores de ZigBee, ya que la tabla siempre debe estar disponible dentro de una red y es muy probable que los coordinadores tengan un suministro de energía permanente. Las copias de seguridad, administradas por capas de nivel superior, pueden ser necesarias en algunas aplicaciones. La vinculación requiere un enlace de comunicación establecido; una vez que existe, se decide si agregar un nuevo nodo a la red, de acuerdo con la aplicación y las políticas de seguridad.

La comunicación puede suceder inmediatamente después de la asociación. El direccionamiento directo utiliza la dirección de radio y el identificador de punto final, mientras que el direccionamiento indirecto utiliza cada campo relevante (dirección, punto final, clúster y atributo) y requiere que se envíen al coordinador de la red, que mantiene asociaciones y traduce las solicitudes de comunicación. El direccionamiento indirecto es particularmente útil para mantener algunos dispositivos muy simples y minimizar su necesidad de almacenamiento. Además de estos dos métodos, está disponible la transmisión a todos los puntos finales en un dispositivo, y el direccionamiento de grupo se utiliza para comunicarse con grupos de puntos finales que pertenecen a un conjunto de dispositivos.

- ***Funcionamiento de la red***

Los protocolos actuales de ZigBee son compatibles con redes habilitadas con baliza y sin baliza. En redes no habilitadas para balizas, se usa un mecanismo de acceso de canal CSMA/CA sin delimitación. En este tipo de red, los enrutadores ZigBee normalmente tienen sus receptores continuamente activos, lo que requiere un suministro de energía más robusto. Sin embargo, esto permite redes heterogéneas en las que algunos dispositivos reciben continuamente mientras que otros solo transmiten cuando se detecta un estímulo externo. El ejemplo típico de una red heterogénea es un interruptor de luz inalámbrico: el nodo ZigBee en la lámpara puede recibir constantemente, ya que está conectado a la fuente de alimentación, mientras que un interruptor

de luz con batería permanecerá dormido hasta que se pulse el interruptor. El interruptor se activa, envía un comando a la lámpara, recibe un acuse de recibo y vuelve a dormir. En una red de este tipo, el nodo de la lámpara será un Enrutador ZigBee, o si no, el Coordinador ZigBee; el nodo de conmutación es típicamente un dispositivo ZigBee End.

En las redes habilitadas para balizas, los nodos enrutadores transmiten balizas periódicas para confirmar su presencia a otros nodos de la red. Los nodos pueden dormir entre balizas, lo que reduce su ciclo de trabajo y prolonga la duración de la batería. Los intervalos de baliza dependen de la velocidad de datos; pueden oscilar entre 15.36 milisegundos y 251.65824 segundos a 250 kbit/s, de 24 milisegundos a 393.216 segundos a 40 kbit/s y de 48 milisegundos a 786.432 segundos a 20 kbit/s. Sin embargo, la operación de bajo ciclo de trabajo con intervalos de baliza largos requiere un tiempo preciso, lo que puede entrar en conflicto con la necesidad de un bajo costo del producto.

En general, los protocolos de ZigBee minimizan el tiempo que la radio está encendida, a fin de reducir el uso de energía. En las redes de balizamiento, los nodos solo necesitan estar activos mientras se está transmitiendo una baliza. En las redes no compatibles con balizas, el consumo de energía es asimétrico: algunos dispositivos siempre están activos, mientras que otros pasan la mayor parte del tiempo durmiendo.

A excepción del Smart Energy Profile 2.0, los dispositivos ZigBee deben cumplir con la norma IEEE 802.15.4-2003 de red de área personal inalámbrica de baja velocidad (LR-WPAN). El estándar especifica las capas de protocolo inferiores: la capa física (PHY) y la parte de control de acceso a medios de la capa de enlace de datos (DLL). El modo de acceso de canal básico es "detección de portadora, acceso múltiple/prevención de colisiones" (CSMA/CA). Es decir, los nodos hablan de la misma manera que los humanos conversan; comprueban brevemente para ver que nadie está hablando antes de que él o ella comience, con tres excepciones notables. Las balizas envían en un horario fijo y no usan CSMA. Los reconocimientos de mensajes tampoco usan CSMA. Finalmente, los dispositivos en redes habilitadas para balizas que tienen requisitos de baja latencia en tiempo real también pueden usar intervalos de tiempo garantizados (GTS), que por definición no usan CSMA.

- ***Servicios de seguridad***

Como una de sus características definitorias, ZigBee proporciona facilidades para llevar a cabo comunicaciones seguras, proteger el establecimiento y el transporte de claves criptográficas, marcos cifrados y dispositivos de control. Se basa en el marco de seguridad básico definido en IEEE 802.15.4. Esta parte de la arquitectura se basa en la gestión correcta de claves simétricas y la correcta implementación de métodos y políticas de seguridad.

- Modelo de seguridad básica

El mecanismo básico para garantizar la confidencialidad es la protección adecuada de todo el material de claves. La confianza debe asumirse en la instalación inicial de las claves, así como en el procesamiento de la información de seguridad. Para que una implementación funcione globalmente, se asume su conformidad general con los comportamientos especificados.

Las claves son la piedra angular de la arquitectura de seguridad; como tal, su protección es de suma importancia, y nunca se supone que las claves se transporten a través de un canal inseguro. Una excepción momentánea a esta regla ocurre durante la fase inicial de la adición a la red de un dispositivo previamente desconfigurado. El modelo de red de ZigBee debe tener especial cuidado con las consideraciones de seguridad, ya que las redes ad hoc pueden ser físicamente accesibles para los dispositivos externos. Además, el estado del entorno de trabajo no puede predecirse.

Dentro de la pila de protocolos, las diferentes capas de red no están separadas criptográficamente, por lo que se necesitan políticas de acceso y se supone el diseño convencional. El modelo de confianza abierta dentro de un dispositivo permite compartir claves, lo que disminuye notablemente el coste de potencia. Sin embargo, la capa que crea un marco es responsable de su seguridad. Si pueden existir dispositivos maliciosos, cada carga útil de la capa de red debe

cifrarse, de modo que el tráfico no autorizado puede cortarse inmediatamente. La excepción, nuevamente, es la transmisión de la clave de red, que confiere una capa de seguridad unificada a la red, a un nuevo dispositivo de conexión.

- Arquitectura de seguridad

ZigBee usa claves de 128 bits para implementar sus mecanismos de seguridad. Una clave se puede asociar a una red, siendo utilizable tanto por las capas ZigBee y la subcapa MAC, como por un enlace, adquirido a través de preinstalación, acuerdo o transporte. El establecimiento de claves de enlace se basa en una clave maestra que controla la correspondencia de la clave de enlace. En última instancia, al menos, la clave maestra inicial se debe obtener a través de un medio seguro (transporte o preinstalación), ya que la seguridad de toda la red depende de ello. Los enlaces y las claves maestras solo son visibles para la capa de aplicación. Los diferentes servicios utilizan diferentes variaciones unidireccionales de la clave de enlace para evitar fugas y riesgos de seguridad.

La distribución de claves es una de las funciones de seguridad más importantes de la red. Una red segura designará un dispositivo especial en el que confían otros dispositivos para la distribución de claves de seguridad: el centro de confianza. Idealmente, los dispositivos tendrán la dirección de confianza del centro y la clave maestra inicial precargadas; si se permite una vulnerabilidad momentánea, se enviará como se describe anteriormente. Las aplicaciones típicas sin necesidades de seguridad especiales utilizarán una clave de red proporcionada por el centro de confianza (a través del canal inicialmente inseguro) para comunicarse.

Por lo tanto, el centro de confianza mantiene tanto la clave de red como la seguridad de punto a punto. Los dispositivos solo aceptarán las comunicaciones que se originen en una clave suministrada por el centro de confianza, a excepción de la clave maestra inicial. La arquitectura de seguridad se distribuye entre las capas de red de la siguiente manera:

La subcapa MAC es capaz de establecer comunicaciones de confianza de un solo salto. Como regla general, el nivel de seguridad que debe usar está especificado por las capas superiores.

La capa de red gestiona el enrutamiento, el procesamiento de los mensajes recibidos y la capacidad de transmitir solicitudes. Los marcos salientes usarán la clave de enlace adecuada de acuerdo con el enrutamiento, si está disponible; de lo contrario, la clave de red se usará para proteger la carga de los dispositivos externos.

La capa de aplicación ofrece servicios de establecimiento de clave y transporte tanto para ZDO como para las aplicaciones.

La infraestructura de niveles de seguridad se basa en CCM, que agrega funciones de cifrado e integridad únicamente a CCM.

3.2.3 6LowPAN [7]

6LoWPAN es un acrónimo de IPv6 orientado a redes inalámbricas de área personal de baja potencia. 6LoWPAN es el nombre que se ha dado a un grupo de trabajo centrado en el área de Internet del IETF.

El concepto 6LoWPAN se originó a partir de la idea de que "el Protocolo de Internet podría y debe aplicarse incluso a los dispositivos más pequeños", y que los dispositivos de baja potencia con capacidades de procesamiento limitadas deberían poder participar en el Internet de las cosas.

El grupo 6LoWPAN es el que define los mecanismos de encapsulado y compresión de encabezado que permiten que los paquetes IPv6 sean enviados y recibidos a través de redes basadas en IEEE 802.15.4. IPv4 e IPv6 son los encargados para la entrega de datos para redes de área local, redes de área metropolitana y redes de área mucho más amplia como Internet. De la misma manera, los dispositivos IEEE 802.15.4 otorgan capacidad de comunicación de detección

en el dominio inalámbrico. Sin embargo, las naturalezas inherentes de las dos redes no son iguales.

La especificación base desarrollada por el grupo 6LoWPAN IETF es RFC 4944 (actualizada por RFC 6282 con compresión de encabezado, y por RFC 6775 con optimizaciones de descubrimiento vecino). El documento de declaración de problema es RFC 4919. IPv6 sobre Bluetooth Low Energy (BLE) se define en RFC 7668.

- ***Áreas de aplicación***

El objetivo de las redes IP para comunicaciones de radio de baja potencia son las aplicaciones que necesitan conectividad inalámbrica a Internet a velocidades de datos más bajas para dispositivos con un factor de forma muy limitado. Un ejemplo son las aplicaciones de automatización y entretenimiento en entornos domésticos, de oficina y de fábrica. Los mecanismos de compresión de encabezado estandarizados en RFC6282 se pueden usar para proporcionar compresión de encabezado de paquetes IPv6 a través de tales redes.

IPv6 también está en uso en la red inteligente, lo que permite que los medidores inteligentes y otros dispositivos creen una red de malla micro antes de enviar los datos al sistema de facturación utilizando la red troncal de IPv6. Algunas de estas redes se ejecutan en radios IEEE 802.15.4 y, por lo tanto, usan la compresión y fragmentación del encabezado según lo especificado por RFC6282.

- ***Funciones***

Al igual que con todas las asignaciones de IP de capa de enlace, RFC4944 proporciona una serie de funciones. Más allá de las diferencias habituales entre las redes L2 y L3, el mapeo desde la red IPv6 a la red IEEE 802.15.4 plantea desafíos de diseño adicionales (ver RFC 4919 para una descripción general).

- Adaptación de los tamaños de paquete de las dos redes

IPv6 requiere que la unidad de transmisión máxima (MTU) sea de al menos 1280 octetos. Por el contrario, el tamaño del paquete estándar de IEEE 802.15.4 es de 127 octetos. Una sobrecarga de trama máxima de 25 octetos ahorra 102 octetos en la capa de control de acceso a medios. Una característica de seguridad opcional pero altamente recomendada en la capa de enlace representa una carga adicional. Por ejemplo, se consumen 21 octetos para AES-CCM-128, dejando solo 81 octetos para las capas superiores.

- resolución del direccionamiento

A los nodos IPv6 se les asignan direcciones IP de 128 bits de forma jerárquica, a través de un prefijo de red de longitud arbitraria. Los dispositivos IEEE 802.15.4 pueden usar direcciones extendidas IEEE de 64 bits o, después de un evento de asociación, direcciones de 16 bits que son únicas dentro de un PAN. También hay una identificación PAN-ID para un grupo de dispositivos IEEE 802.15.4 físicamente ubicados.

- Diseños de dispositivos diferente

Los dispositivos IEEE 802.15.4 están restringidos intencionalmente en factor de forma para reducir costes (permitiendo la red a gran escala de muchos dispositivos), reducir el consumo de energía (permitiendo dispositivos ser alimentados por batería) y permitir flexibilidad de instalación (por ejemplo, pequeños dispositivos para redes corporales) . Por otro lado, los nodos cableados en el dominio de IP no están restringidos de esta manera; pueden ser más grandes y hacer uso de las fuentes de alimentación de la red.

- Enfoque diferente en la optimización de parámetros

Los nodos IPv6 están orientados a alcanzar altas velocidades. Los algoritmos y protocolos implementados en las capas superiores, como el *kernel* TCP de TCP/IP, están optimizados para manejar problemas de red típicos, como la congestión. En los dispositivos compatibles con IEEE 802.15.4, la conservación de la energía y la optimización del tamaño del código siguen siendo prioritarios.

- Capa de adaptación para interoperabilidad y formatos de paquete

Un mecanismo de adaptación para permitir la interoperabilidad entre el dominio IPv6 y el IEEE 802.15.4 se puede ver mejor como un problema de capa. Identificar la funcionalidad de esta capa y definir nuevos formatos de paquete, si es necesario, es un área de investigación atractiva. RFC4944 propone una capa de adaptación para permitir la transmisión de datagramas IPv6 sobre redes IEEE 802.15.4.

- Gestión de los mecanismos de direccionamiento

La administración de direcciones para dispositivos que se comunican entre los dos dominios diferentes de IPv6 e IEEE 802.15.4 es incómoda, si no exhaustivamente compleja.

- Consideraciones de enrutamiento y protocolos para topologías de malla en 6LoWPAN

El enrutamiento per se es un problema de dos fases que se está considerando para redes de IP de baja potencia:

- Enrutamiento de malla en el espacio de la red de área personal (PAN).
- La enrutabilidad de los paquetes entre el dominio IPv6 y el dominio PAN.

Varios protocolos de enrutamiento han sido propuestos por la comunidad 6LoWPAN como LOAD, DYMO-LOW, HI-LOW. Sin embargo, actualmente solo dos protocolos de enrutamiento son legítimos para implementaciones a gran escala: LOADng estandarizado por la ITU según la recomendación UIT-T G.9903 y RPL estandarizados por el grupo de trabajo IETF ROLL.

- Descubrimiento de dispositivo y servicio

Dado que los dispositivos habilitados para IP pueden requerir la formación de redes ad hoc, será necesario conocer el estado actual de los dispositivos vecinos y los servicios alojados por tales dispositivos. Las extensiones de descubrimiento vecino IPv6 es un borrador de Internet propuesto como una contribución en esta área.

- Seguridad

Los nodos IEEE 802.15.4 pueden operar en modo seguro o modo no seguro. En la especificación se definen dos modos de seguridad para lograr diferentes objetivos de seguridad: Lista de control de acceso (ACL) y Modo seguro

3.2.4 Sigfox [8]

Sigfox es una compañía francesa que fue fundada en 2009 y que construye redes inalámbricas orientadas a conectar objetos de bajo consumo de energía, como analizadores de energía o relojes inteligentes, que deben estar continuamente encendidos y transmitiendo pequeñas cantidades de datos.

- ***Tecnología***

Sigfox se vale de una tecnología patentada que otorga la capacidad comunicar datos utilizando la banda de radio ISM Industrial, Científica y Médica que utiliza 868MHz en Europa y 902MHz en los Estados Unidos. Emplea una señal con gran alcance que pasa libremente a través de objetos

sólidos, llamada "banda ultrabaja" y apenas necesita energía, dándose a conocer com "Red de área amplia de baja potencia (LPWAN)". La red está basada en una topología de estrella de un salto y requiere que un operador móvil sea el encargado de transportar el tráfico generado. La señal también puede usarse para cubrir de manera sencilla áreas grandes y para lograr alcanzar objetos subterráneos.

Sigfox se ha asociado con varias empresas de la industria LPWAN tales como el gigante Texas Instruments, Silicon Labs y ON Semiconductor. Las bandas de radio ISM pueden gestionar comunicaciones bidireccionales limitadas. El estándar existente para comunicaciones Sigfox puede admitir hasta 140 mensajes de enlace ascendente por día, cada uno de los cuales puede transportar una carga de 12 bytes (excluyendo el encabezado del mensaje y la información de transmisión) y hasta 4 mensajes de enlace descendente al día, cada uno de ellos puede llevar una carga de 8 Bytes.

3.2.5 LoRa [9]

LoRa está pensado para aplicaciones de baja potencia, de red de área amplia (LPWAN). Tiene un rango de más de 15 kilómetros en condiciones óptimas y una capacidad de hasta 1 millon de nodos. La combinación de baja potencia y largo alcance limita la velocidad de datos máxima a 50 kilobits por segundo (Kbps).

LoRa es una tecnología exclusiva y patentada cuya propiedad pertenece a Semtech Corporation, que funciona en la banda ISM. La asignación de frecuencias y los requisitos reglamentarios para ISM varían según en qué región opere. Dos de las más populares son las frecuencias de 868 megahercios (MHz) utilizada en Europa (incluida España) y 915 MHz utilizada en América del Norte. Otras regiones, especialmente para el caso de Asia, existen otros requisitos.

La capa física LoRa utiliza modulación de espectro ensanchado (SSM) (Figura 3). SSM codifica la señal base con una secuencia de alta frecuencia, que deliberadamente propaga la señal base a través de un ancho de banda mayor, reduce el consumo de energía y aumenta la resistencia frente a interferencias electromagnéticas.

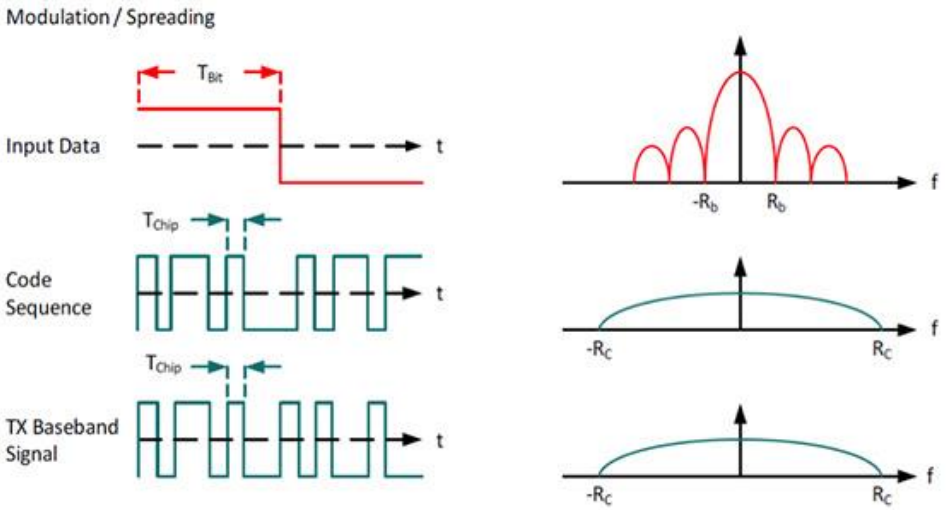


Figura 3. Representación gráfica de la modulación LoRa

El factor de propagación (SF) de la señal base es variable y obedece a una solución de compromiso. Para un ancho de banda disponible, un mayor factor de propagación reduce la tasa de bits, y a su vez reduce la duración de la batería (en caso de tenerla) incrementando el tiempo de transmisión.

Un determinado factor de propagación (SF) y el ancho de banda (BW) darán una tasa de bits definidos por la ecuación (1):

$$\boldsymbol{Bit\ Rate = SF * \frac{BW}{2^{SF}}} \quad (1)$$

LoRa permite seis factores de propagación (SF7 - SF12) y tres diferentes anchos de banda (125 kHz, 250 kHz, 500 kHz). Los factores de propagación y anchos de banda permitidos están definidos por las agencias reguladoras regionales. En el caso de América del Norte, por ejemplo, especifica un ancho de banda de 500 kHz y factores de propagación de 7 a 10.

Debido a la tecnología de espectro de propagación, los mensajes con diferentes velocidades de datos son ortogonales y no interfieren los unos con los otros, creando un conjunto de canales "virtuales", aumentando la capacidad de la puerta de enlace.

El esquema LoRa se basa en una variante de SSM llamada modulación de *chirp spread spectrum* (CSS) (Figura 4). CSS codifica los datos con un "pitido" o *chirp*, que es esencialmente una señal sinusoidal de frecuencia modulada en banda ancha que aumenta o disminuye con el tiempo.

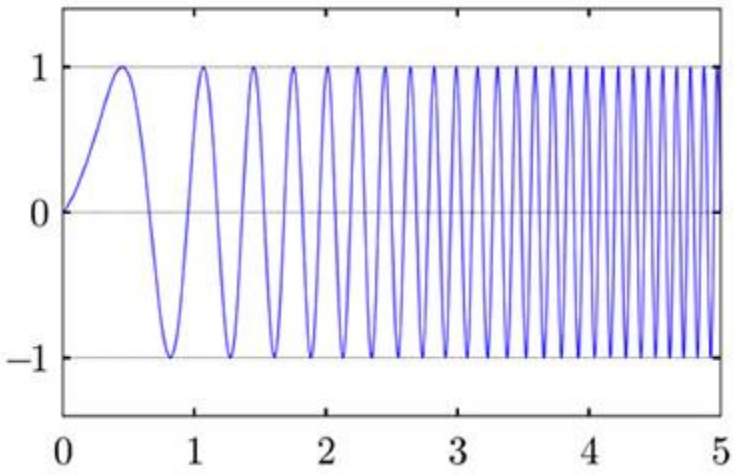


Figura 4. Ejemplo de modulación CSS.

CSS es muy adecuado para aplicaciones de baja velocidad de datos (<1 Mb/s) que requieren un bajo consumo energético. IEEE 802.15.4a, otro estándar de velocidad baja, lo especifica como técnica para su uso en redes de área personal inalámbricas (LR-WPAN). CSS se ha utilizado durante muchos años para proporcionar comunicación sólida de largo alcance en las aplicaciones militares y espaciales, pero LoRa es la primera implementación comercial de bajo costo.

- ***LoRaWAN y arquitectura de red LoRa***

La especificación LoRaWAN define que la capa de control de acceso al medio (MAC) para LPWAN. LoRaWAN se implementa en la parte superior de la capa física LoRa y especifica el protocolo de comunicaciones y la arquitectura de red. Estas funciones tienen un alto grado de influencia sobre varios parámetros de rendimiento, que incluyen:

- La vida útil de la batería de los nodos.
- La capacidad máxima de la red.
- La seguridad que tiene la red.
- Las aplicaciones que se valen del protocolo LoRaWAN.

La arquitectura de red LoRaWAN utiliza una topología de estrella en la que cada nodo final se comunica con varias puertas de enlace, que, a su vez, se comunican con el servidor de red.

LoRa tiene cuatro elementos de red (Figura X):

- Los nodos finales que recopilan datos de los sensores los transmiten *upstream* y *downstream*, y reciben la comunicación desde el servidor de aplicaciones. Los

dispositivos de *Endpoint* usan comunicación inalámbrica *single-hop* con una o varias compuertas.

- El concentrador o compuerta actúa como un puente transparente y retransmite los datos bidireccionales entre los nodos finales y los servidores *upstream*.
- El servidor de red se conecta a varias puertas de enlace a través de una conexión TCP/IP segura, ya sea por cable o vía inalámbrica; elimina los mensajes duplicados; decide qué compuerta debe responder a un mensaje de nodo final; y gestiona el nodo final, las velocidades de transmisión de datos con una velocidad de datos adaptable (ADR), destinadas a maximizar la capacidad de la red y extender la vida útil de la batería del nodo final.
- El servidor de la aplicación recopila y analiza los datos de los nodos finales y determina las acciones que seguirá el nodo final.

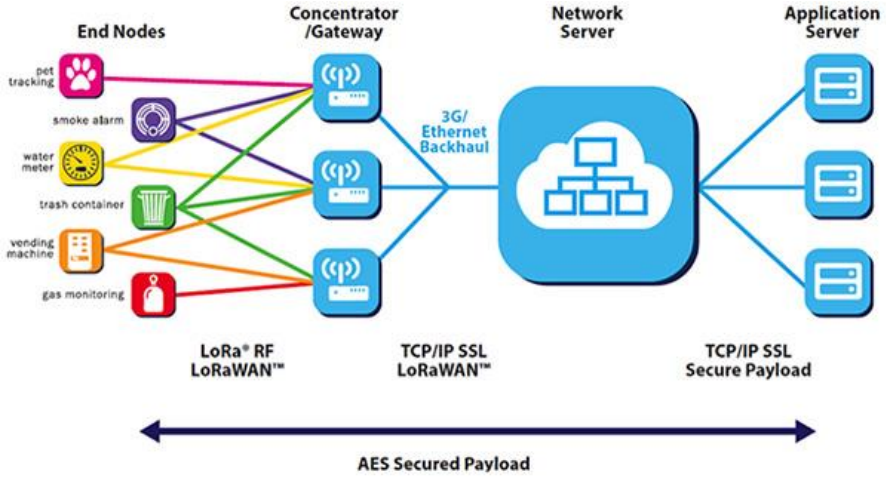


Figura 5. Topología de aplicación LoRaWan.

La comunicación de extremos es normalmente bidireccional, pero LoRa también admite el funcionamiento de multidifusión para funciones tales como actualizaciones de software. Muchos de los protocolos existentes, como por ejemplo ZigBee, emplean una topología de malla en los que cada uno de los nodos finales recibe y retransmite información desde otros nodos finales. Este enfoque aumenta el rango y el tamaño de la celda de la red, pero la sobrecarga de comunicación adicional le añade complejidad, reduce la capacidad de la red y aumenta el consumo de energía de cada uno de los nodos.

- ***Clasificación de los nodos finales LoRa***

Hay tres clases de dispositivos de nodo final. Las tres clases permiten la comunicación bidireccional y puede iniciar una subida a los servidores a través de la puerta de enlace. Difieren en relación con cuándo aceptar mensajes entrantes del servidor.

Un dispositivo LoRaWAN Clase A consume menos energía. Un nodo final sólo permite la comunicación desde el servidor durante dos breves ventanas de recepción, que se abren durante un corto período de tiempo después de una transmisión de enlace ascendente. Los mensajes desde el servidor en cualquier otro momento deben esperar hasta la próxima hora programada de enlace ascendente. Un dispositivo de Clase A es asincrónico. Un extremo comienza una transmisión cuando tiene datos para enviar, entonces espera a una hora preestablecida y espera una respuesta.

Un dispositivo LoRa Clase B ofrece una funcionalidad de clase, pero también abre ventanas de recepción extra a las horas programadas. Para sincronizar con la red, el nodo Clase B recibe un contador sincronizado en tiempo desde la compuerta cada 128 segundos. Se le asigna un espacio de tiempo dentro de 128 segundos que permiten que el servidor sepa cuando el dispositivo final está escuchando.

Un dispositivo LoRa de Clase C proporciona ventanas de recepción casi continuamente abiertas. Las ventanas sólo se cierran durante las transmisiones de punto final. Un dispositivo de Clase C es adecuado donde se requiere una gran cantidad de datos para recibir, en lugar de transmitirse.

- ***Seguridad LoRaWAN***

Una seguridad sólida es un elemento clave de cualquier diseño LPWAN. LoRaWAN utiliza cifrado AES de 128 bits y tiene dos capas independientes de seguridad, una clave de sesión de red (NwkSKey) y una clave de sesión de aplicación (AppSKey) .

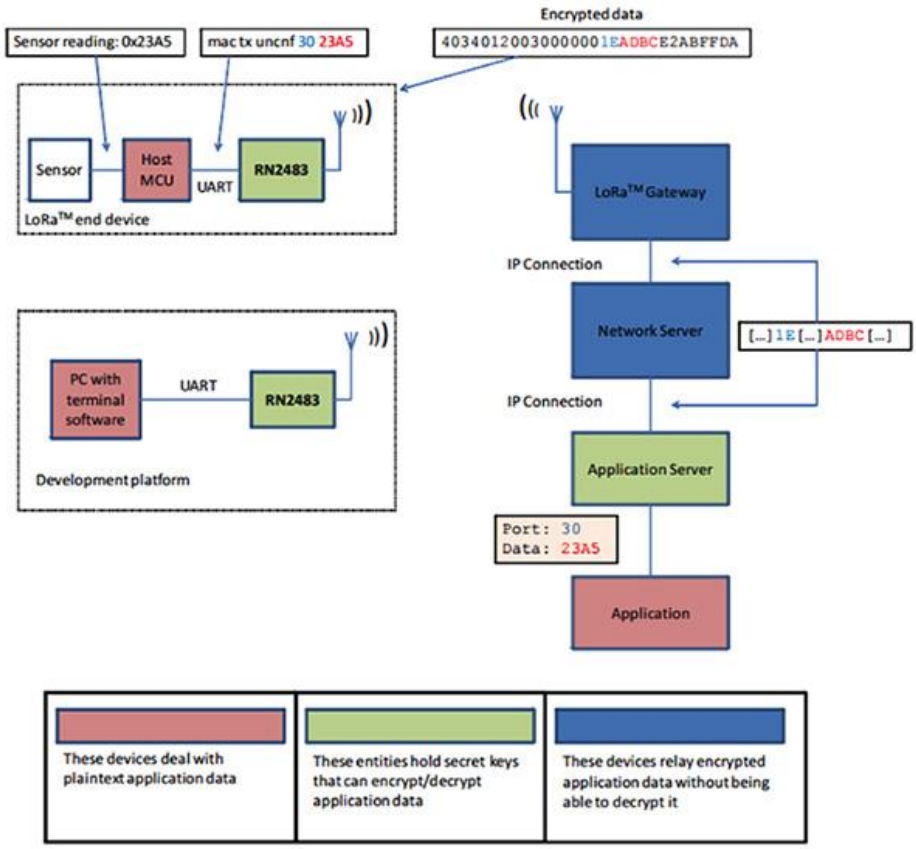


Figura 6. Flujo de datos seguros con LoRaWan.

El nivel de seguridad de red garantiza la autenticidad del nodo en la red, y la aplicación de la capa de seguridad garantiza que el operador de red no tiene acceso a los datos de aplicaciones del usuario final.

Hay dos métodos para implementar las claves:

- Activación mediante personalización (ABP): Aquí, los dispositivos finales LoRaWAN pueden ser programados en fábrica con la información de autenticación para una determinada red LoRaWAN.
- Activación inalámbrica (OTAA): Este utiliza un ID de aplicación, un único ID de dispositivo, y una red de dispositivo asignado para obtener la dirección y NwkSKey AppSKey. Este es el método preferido porque las teclas no están predeterminadas y pueden ser regeneradas.

- ***LoRa Alliance [10]***

Lora Alliance es una asociación abierta, sin fines de lucro, que ha crecido a más de 500 miembros desde su inicio en marzo de 2015, convirtiéndose en la alianza más grande y de más rápido crecimiento en el sector de la tecnología. Sus miembros colaboran estrechamente y comparten experiencias para promover e impulsar el éxito del protocolo LoRaWAN como el estándar global abierto líder para la conectividad IW LPWAN segura y de grado operador. Con la flexibilidad

técnica para abordar una amplia gama de aplicaciones Iot, tanto estáticas como móviles, y un programa de certificación para garantizar la interoperabilidad, LoRaWAN ya ha sido desplegado por los principales operadores de redes móviles a nivel mundial, con amplia expansión en 2018 y más allá.

Su misión y objetivo es apoyar y promover la adopción global del estándar LoRaWAN asegurando la interoperabilidad de todos los productos y tecnologías de LoRaWAN, para permitir que el IoT ofrezca un futuro sostenible.

Sus miembros provienen de organizaciones de todo tipo de todo el mundo que abordan todos los aspectos del ecosistema LoRaWan. Los miembros incluyen empresas multinacionales de telecomunicaciones, fabricantes de equipos, integradores de sistemas, fabricantes de sensores, empresas emprendedoras y compañías de semiconductores. Sus miembros desarrollan, implementan y utilizan la tecnología en países y continentes, impulsando la implementación del Internet de las cosas. LoRa Alliance es una organización con membresía que atiende la necesidad de la compañía individual y está dividida en un patrocinador, colaborador y un nivel de adoptante.

Figura 7. Algunas de las empresas que conforman la LoRa Alliance desde 2015.

3.3 Sensores disponibles

Existe una gran multitud de sensores orientados a IoT que pueden resultar de gran interés. Por ejemplo, en el caso que se quiere estudiar (soluciones para *Smart City*) existen multitud de sensores orientados a analizar a temperatura y la humedad relativa junto con otros parámetros atmosférico, sensores acústicos, sensores para tener información sobre tasas de tráfico o afluencia de gente, sensores de luminosidad y presencia para regular de manera eficiente el alumbrado público o sensores capaces de detectar cuando se deben recoger las basuras de una zona.

La integración de estos sensores suele ser sencilla, y en la mayoría de los casos en los que se desea implementar dentro una de las tecnologías RF vistas, ya existen varias empresas que tienen un sensor adaptado específicamente, siendo el caso más frecuente ZigBee.

Muchos de ellos se pueden adquirir en internet para cualquier tipo de público y ofrecen una instalación sencilla. Otros y en mayoría, en cambio, requieren de especialistas para su instalación de forma óptima a fin de que sean capaces de mostrar datos realmente relevantes o de interés específico orientado a mejorar y optimizar la ciudad, siendo capaces de actuar sobre ciertas soluciones.

Capítulo 4. Desarrollo Práctico

4.1 Elección de la tecnología.

Ahora que ya se han visto diferentes tipos de tecnologías en RF, toca elegir cual es la que más se adecúa a los criterios de diseño y más se distancia de los posibles riesgos.

Por decisión técnica y estratégica de Datakorum, se ha elegido la tecnología LoRa, ya que cubre sobradamente las especificaciones de distancia cubierta y es una tecnología cuyo protocolo de capa física es de código abierto. Otro de los principales motivos de la elección de la tecnología LoRa es que es una nueva tecnología con mucho potencial para IoT y puede ser escalada a LoRaWAN, lo cual abre vías para futuras ampliaciones, o, mejor dicho, mejoras de la tecnología y las plataformas de conectividad. Además, la manera en la que se pueden conformar redes internas o de equipos es muy similar, por no decir prácticamente igual, que las que ofrece una red modbus, las cuales son objeto de réplica y se busca compatibilidad con ellas en este proyecto.

LoRa es capaz de ofrecer bastante sencillez al desarrollo ya que podemos probar algunos de sus módulos certificados con ayuda de un Arduino.

4.2 Elección del módulo LoRa para la realización de pruebas

4.2.1 Módulo RN2483 de Microchip [11]

Este módulo ofrece la pila de protocolo LoRaWAN tipo A integrado. Dada la aplicación que queremos para el proyecto, la pila de protocolo LoRaWAN no es algo que se busque como requisito, pero en caso de serlo, no es interesante el tipo de dispositivo A, ya que necesitamos que sea C debido a que no nos podemos permitir esperar a que un dispositivo final sea el primero en hablar para poder mandar a una petición u orden a este. Esto será un factor de descarte para este módulo.

Para conseguir comunicación punto a punto con este dispositivo es necesario recurrir a los comandos AT y saltarnos la pila de protocolo, lo cual también, aunque no por ello se ha excluido, puede ser incomodo a la hora de trabajar con él.

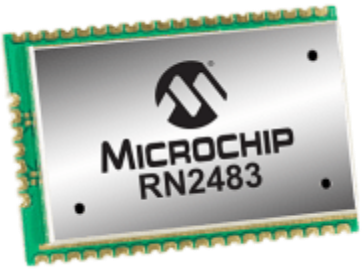


Figura 8. Módulo RN2483 de Microchip.

Otras cualidades del módulo son:

- Interfaz de comandos ASCII sobre UART.
- Tamaño compacto de 17,8 x 26,7 x 3 mm.
- Pads SMT almenados para un montaje fácil y solido sobre la PCB.
- Actualización de firmware mediante UART.
- 4 GPIO para control, estado y ADC.
- Modulo altamente integrado con una unidad microcontroladora, cristal, EUI-64 *Node Identity Serial* EEPROM, transceptor de radio con interfaz análoga y circuitos coincidentes.
- Respetuoso con el medio ambiente, cumple RoHS.
- Evaluado por la directiva europea R&TTE.
- 47 pines.

- Potencia de salida de 14,00 dBm.
- Rango de temperatura de -40 a 85ºC.
- Rango de frecuencias de 434 y 868 MHz.
- Sensibilidad de recepción de -148 dBm.
- Consumo en transmisión de 40 mA (a 14 dBm y 868 MHZ
- Consumo en recepción de 14,2 mA.

4.2.2 Módulo WM-SG-SM-42 de USI [12]

Este módulo se presenta en colaboración con STMicroelectronics con el objetivo de crear una placa de expansión para el núcleo del microcontrolador ST32. Se presenta para desarrollar soluciones basadas en tecnología LoRa y/o FSK/OOK.

Figura 9. Módulo WM-SG-SM-42 de USI.

Este módulo se presenta dentro de la placa I-NUCLEO-LRWAN1 [13], una placa de evaluación compatible tanto con la plataforma Arduino como con las placas de desarrollo electrónico basadas en los microcontroladores de la familia ST32, como la placa NUCLEO-L053.El módulo ofrece la pila de comandos AT para LoRaWAN precargada y se basa en el software I-CUBE-LRWAN, software que ayuda a la configuración del protocolo LoRaWAN.

Este módulo está certificado para operar como dispositivo tipo A en redes LoRaWAN y además permite su utilización como dispositivo tipo C.

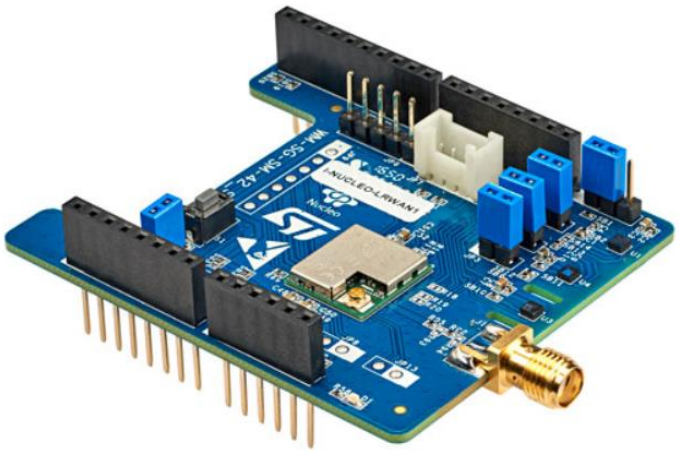


Figura 10. I-NUCLEO-LRWAN1 de ST-Link.

Las principales características de esta placa de evaluación son:

- Unidad microcontrolador STM32L052T8Y6 de ultra bajo consumo ST, Cortex® -M0 + basado en 64 Kbytes de memoria Flash, 8 Kbytes de RAM, 2 Kbytes de EEPROM, T-RNG
- Transceptor de radio Semtech SX1272 compatible con la modulación LoRa®, FSK, GFSK, MSK, GMSK y OOK
- Alta sensibilidad hasta -137 dBm
- Rango de frecuencia de 860 MHz a 1020 MHz
- 14 dBm a 20 dBm de potencia de salida
- Rango de voltaje de 2.0 V a 3.6 V
- Rango de temperatura de -40 ° C a + 85 ° C

- Cristales insertados de 32 kHz y 32 MHz
- Interfaz de comunicación USART
- Sensor de acelerómetro ST y magnetómetro (LSM303AGR)
- Sensor de humedad relativa y temperatura ST (HTS221)
- Sensor de presión ST (LPS22HB)
- Conectores Arduino ™
- Conector SMA

4.2.3 Módulo Ra-01 y Ra-02 de AI-Thinker [14]

Estos módulos están basados en el transceptor SX1278 de SEMTECH y se limitan a la comunicación con la modulación LoRa, con lo que no hay que preocuparse de trabajar dentro de una red LoRaWAN.

Ya que en un principio no se desea trabajar dentro de una red LoRaWAN, y debido a que la empresa Datakorum ya trabaja con otros módulos de comunicación de AI-Thinker, se ha optado por este módulo para el desarrollo del proyecto.

Este módulo ofrece una sensibilidad de más de -148 dBm y ofrece una potencia de salida de +20 dBm. Ofrece comunicaciones fiables a largo alcance. La modulación LoRa ofrece también ventajas de selección de canal y antibloqueo, lo que soluciona problemas típicos de distancia, anti-bloqueo y consumo de energía.

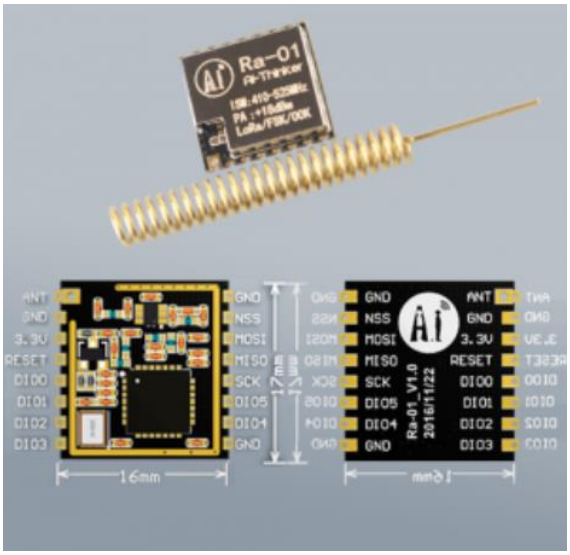


Figura 11. Ra-01 de AI-Thinker.

Como características destacables encontramos las siguientes:

- Admite la modulación FSK, GFSK, MSK, GMSK, LoRa y OOK
- Rango de frecuencias entre 410 y 525 MHz (opera normalmente en 433 MHz)
- Sensibilidad de recepción ultra alta de hasta -141 dBm
- Tiene excelentes propiedades anti-bloqueo
- Admite la detección de preámbulos
- Soporte de comunicación SPI semiduplex
- Paquetes con CRC de hasta 256 bytes
- Paquete de parche de huella de sello de doble cadena de huella pequeña
- Alimentación de 2,5 a 3,7 V (típica 3,3 V)
- Rango de temperatura de -30º hasta 85º C

4.3 Diseño del test

Una Vez se ha elegido el módulo, se puede trazar una hoja de procedimiento. Primero debe realizarse un prototipo adecuado del módulo para trabajar con este, además de encontrar una librería que nos permita hacer pruebas utilizando una placa de Arduino.

El procedimiento puede enumerarse como:

1. Encontrar una librería adecuada para implementar dentro de la plataforma de Arduino
2. Diseñar y construir un prototipo a raíz del módulo Ra-01
3. Lograr la comunicación entre dos equipos
4. Lograr una comunicación dúplex
5. Enviar una cadena de 100 bytes
6. Analizar SNR y RSSI en dB y dBm al realizar envíos de 100 bytes
7. Observar como varían los parámetros anteriores en relación con la distancia entre los equipos y encontrar distancias máximas de comunicación
8. Implementar redes de tres equipos o más basándonos en maestro-esclavo
9. Integración de Modbus en los equipos que conforman la red
10. Implementación y compatibilidad con los equipos de Datakorum

Una vez se haya completado con éxito estos hitos, se podrá profundizar en el desarrollo comercial del producto y evaluar con datos reales las limitaciones de este

4.4 Prototipado

Antes de comenzar a montar un prototipo es necesario saber que librería se va a emplear, ya que de esta depende la cantidad de pines que se va a emplear o las funcionalidades que se van a implementar.

La librería que se va a emplear para utilizar el módulo Ra-01 con una placa Arduino Mega 2560 R3 es la librería LoRa.h [15], la cual está orientada a ser utilizada con los transceptores SX1278, es decir, el transceptor integrado en el módulo Ra-01. Una vez seleccionada la librería, vemos cómo funciona para conocer qué pines debemos conectar. Estos son: GND (masa), 3.3V (alimentación), RESET, DIO0 (pin de entrada salida digital, el 0 tiene funciones específicas como la sincronización de direcciones, el Rssi o la detección de cabecera y la notificación de estar listo para envió y recepción), NSS, MOSI, MISO y SCK (estos 4 últimos pines se emplean para operar sobre el módulo a través de la interfaz SPI).

Se han obtenido 4 módulos para esta etapa de prototipado:

Figura 12. Módulos Ra-01 adquiridos.

Para poder montarlo, es necesario hacerlo sobre una pequeña lamina de baquelita con pads de cobre para poder realizar las soldaduras de los pines

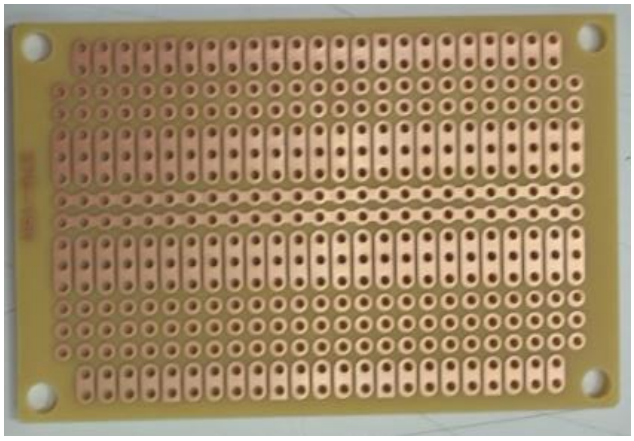


Figura 13. Placa de baquelita.

Es además necesario retirar parte del cobre donde se va a emplazar el módulo para así evitar los posibles cortocircuitos con el cobre, ya que la distancia de los pads almenados es bastante menor a la separación entre vías de cobre:

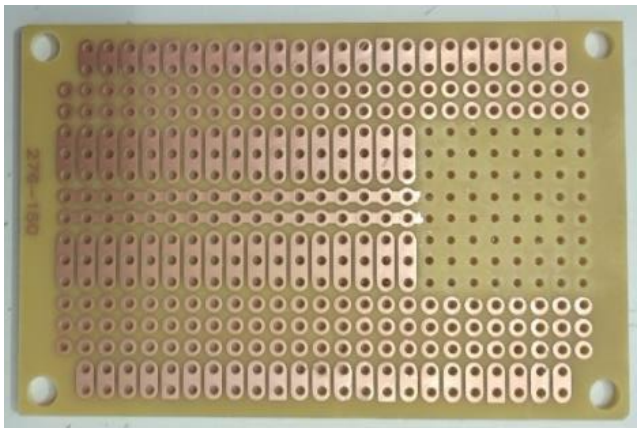


Figura 14. Placa de baquelita tras retirar cobre.

A los extremos de la zona donde se ha retirado el cobre, se suelda una tira de pines con el objetivo de unir estos a los pines del módulo y más tarde poder pinchar este sobre una placa de conexiones:

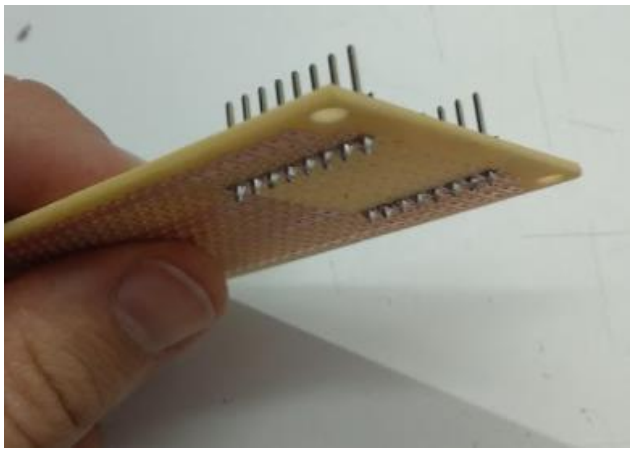


Figura 15. Placa de baquelita tras soldar las tiras de pines.

Finalmente, se pega el módulo a la lámina con cinta de doble cara, se unen los pines soldando pequeños cables y se suelda la antena, para terminar, se recorta la lámina sobrante.

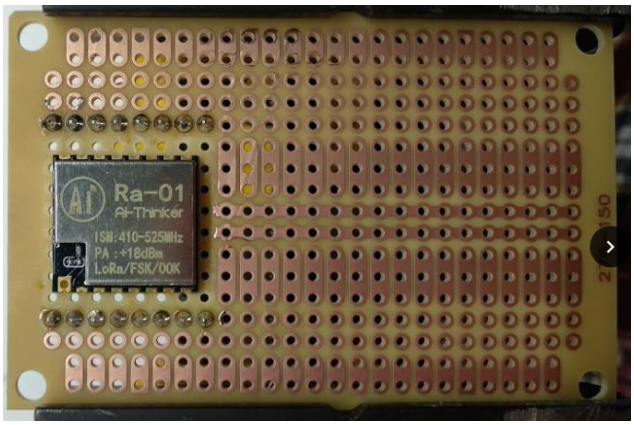


Figura 16. Emplazamiento del módulo Ra-01 en la placa de baquelita.

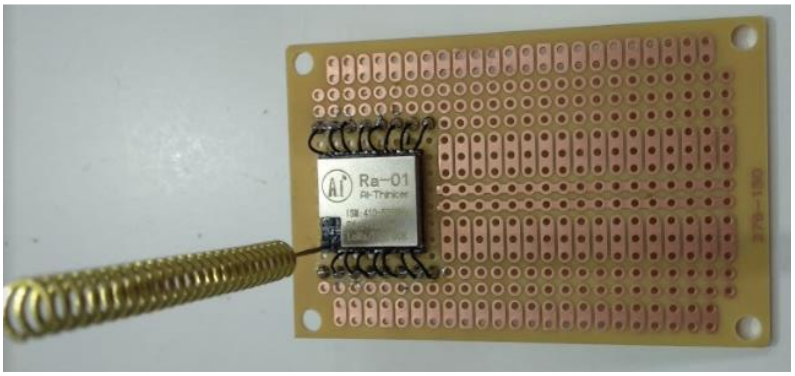


Figura 17. soldadura de los pines y antena.

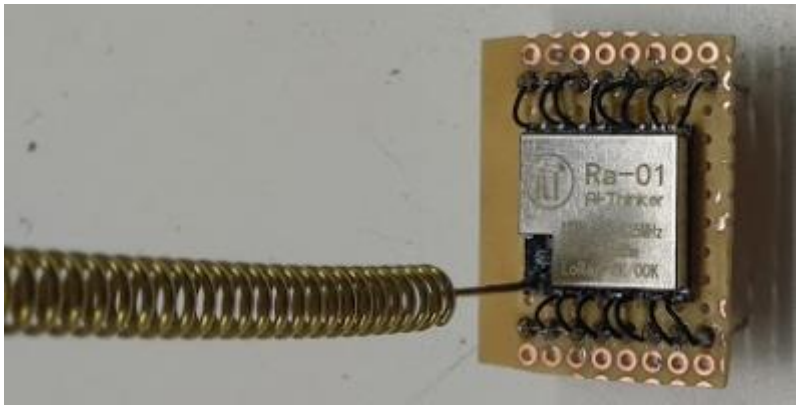


Figura 18. Módulo prototipo integrable.

Una vez se repite este proceso con todos los módulos ya se puede comenzar con las pruebas de conexión y desarrollo.

4.5 Pruebas de conexión y desarrollo

Antes de hacer nada, hay que definir cómo se va a conectar el módulo Ra-01 con la placa Arduino MEGA 2560 R3. Las conexiones inmediatas son las relativas a alimentación, se interconectarán los pines de 3,3 V y se conectará el pin GND del Ra-01 con cualquiera de los pines GND de la placa, en este caso se hará en uno de los relativos a la zona de alimentación (POWER). Si seguimos el API de la librería LoRa.h, los pines DIO0, RESET y NSS están configurados por defecto en los pines digitales 2, 9 y 10 respectivamente. El resto de los pines orientados a la comunicación SPI dependen del modelo de placa Arduino utilizada, además es necesario incluir la librería SPI.h. En el caso de la placa MEGA 2560 R3, los pines MISO, MOSI y SCK se

conectan respectivamente a los pines digitales 50, 51 y 52. Una vez conectado todo a la placa se verá con sus respectivas conexiones como se muestra en la figura 19:

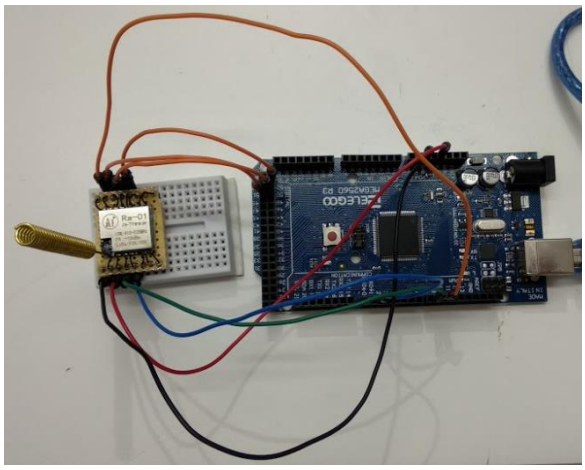


Figura 19. Primer conexionado del prototipo en Arduino MEGA 2560.

Ahora se proceder a implementar los sketches necesarios para realizar las pruebas de comunicación y funcionalidad.

4.5.1 Comunicación entre equipos

Esta es la prueba más simple y sencilla, con esto solo se pretende comprobar que los módulos funcionan, para ello, y de aquí en adelante, se utilizarán por lo menos dos placas Arduino con sus respectivos módulos. Dada la simplicidad de esta prueba, y dado que es una comprobación de que somos capaces de establecer comunicación, nos limitaremos a cargar el ejemplo dado por la librería para un transmisor y un receptor, salvo por algunas modificaciones.

Al sketch que se carga en el emisor se le ha llamado *maester*, y al que se carga en el receptor se le ha llamado *slave*. Entre las modificaciones que han sufrido los sketches se encuentran los ajustes de la banda, que se ha fijado a 433 MHz con un ancho de banda de 62,5 MHz, y también se ha fijado el factor de dispersión a 10. También habilitaremos un CRC para asegurar la recepción de paquetes.

El paquete enviado contendrá el mensaje “HOLA MUNDO” y en el emisor se verá un contador de envío, el mensaje se enviará cada dos segundos y en el receptor se mostrará por pantalla a través del puerto serie.

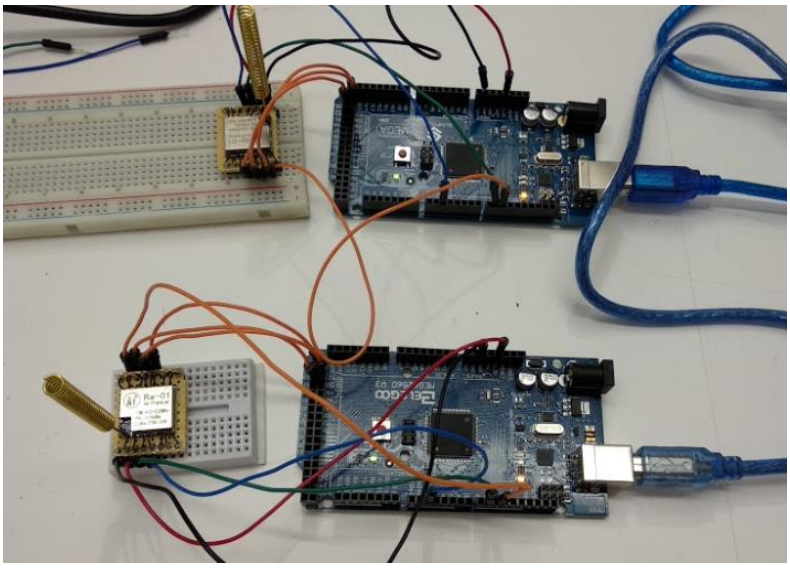


Figura 20. Par de equipos para comunicación LoRa.

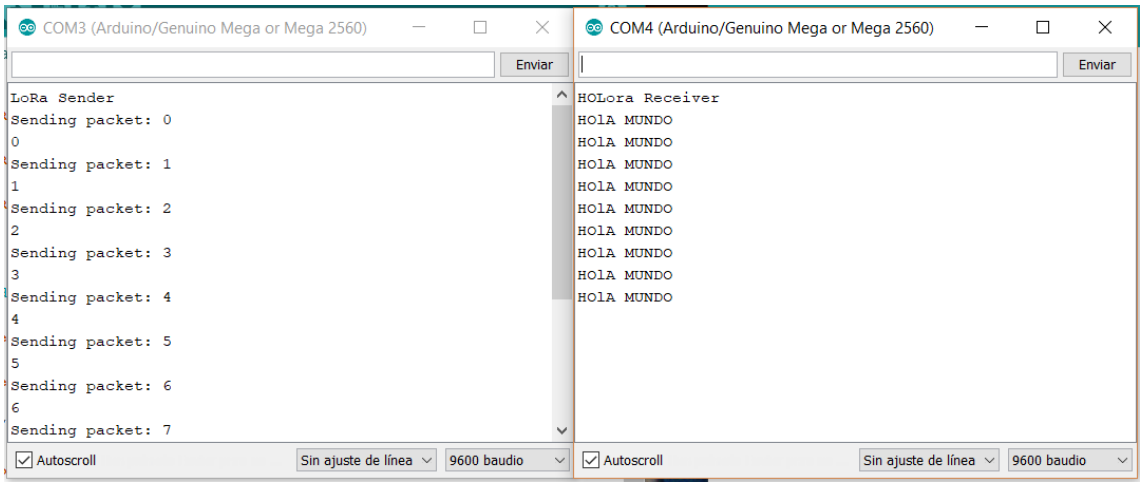


Figura 21. Lectura puerto serie "Hola mundo".

4.5.2 Comunicación dúplex

Para continuar con las pruebas de comunicación, se ha partido de los ejemplos de la librería LoRa.h para comunicación dúplex y se han modificado para crear un chat. Los equipos se identificarán con una dirección en hexadecimal, siendo 0xAA y 0xBB y cuyos sketches se llamarán ChatA y ChatB. Se reserva la dirección 0xFF para broadcast y, de hecho, esta será la dirección a la que enviaremos los mensajes en ambos dispositivos.

En este caso no fijaremos ni el factor de dispersión ni el ancho de banda, que por defecto tienen el valor de 8 MHz para la frecuencia y 7 para el factor de dispersión.

Dentro del bucle principal, se utilizan dos rutinas, la que lee del puerto serie y envía a través de LoRa, y la que está a la espera de recibir mensajes. El modo de funcionamiento de la primera es sencillo, espera a que el puerto serie esté activo, entonces, lee de este y almacena los datos en un buffer limitado a 100 bytes. Cuando el puerto serie deja de estar activo, empaqueta los datos del buffer en un paquete LoRa y los envía, finalmente borra el buffer.

El paquete LoRa se implementa con la subfunción sendMessage(String), a la que se le pasa como argumento el mensaje. El paquete a enviar se construye escribiendo en orden la dirección destino, la dirección local, el identificador del mensaje (un número que indica la cuenta de mensajes que se han enviado), el tamaño del mensaje y el mensaje propiamente.

En recepción se utiliza la subfunción onReceive(int), a la que se le pasa como argumento el tamaño del paquete que se recibe. Lo primero que se hace es comprobar quien es el destinatario, quien es el emisor, el identificador de mensaje y el tamaño del mensaje entrante. Si el tamaño que se ha pasado como argumento no coincide con el tamaño que se ha leído, se lanzará un mensaje de error y se saldrá de la recepción. Si la dirección destino no es la dirección local o de broadcast (0xFF) se lanzará un mensaje y se saldrá de la recepción. Finalmente se escribirá por el puerto serie de quién procede el mensaje, a quien se envía, el identificador, el tamaño y el mensaje propiamente.

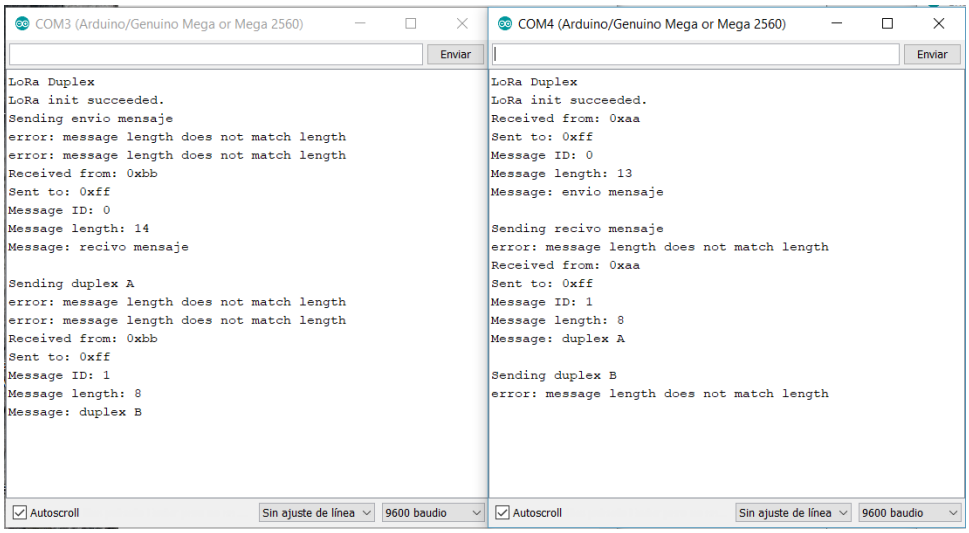


Figura 22. Lectura del puerto serie, "Chat" para comunicación duplex.

4.5.3 Envío de un String de 100 bytes

Esta prueba es una variación de la anterior, solo que en lugar de leer o escribir por el puerto serie, se ha simplificado para enviar 100 bytes conformados por caracteres ASCII, almacenados en una cadena de caracteres que se rellena mediante un bucle *for*, y en lugar esperar a recibir la orden de envío desde el puerto serie, se ha configurado un botón, en el pin digital 2, que, al pulsarse, realizará el envío.

En esta prueba se han modificado los pines por a los que se conecta por defecto dejando libre el pin 2 para el botón. La nueva configuración es el pin 5 para DIO0, el pin 6 para RESET y el pin 7 para NSS.

A través del monitor del puerto serie se puede ir comprobando que se envían y reciben los mensajes, se pueden leer los caracteres ASCII. El resto de funcionamiento del sketch es igual que en el anterior caso, eliminando los bucles que ahora son innecesarios.

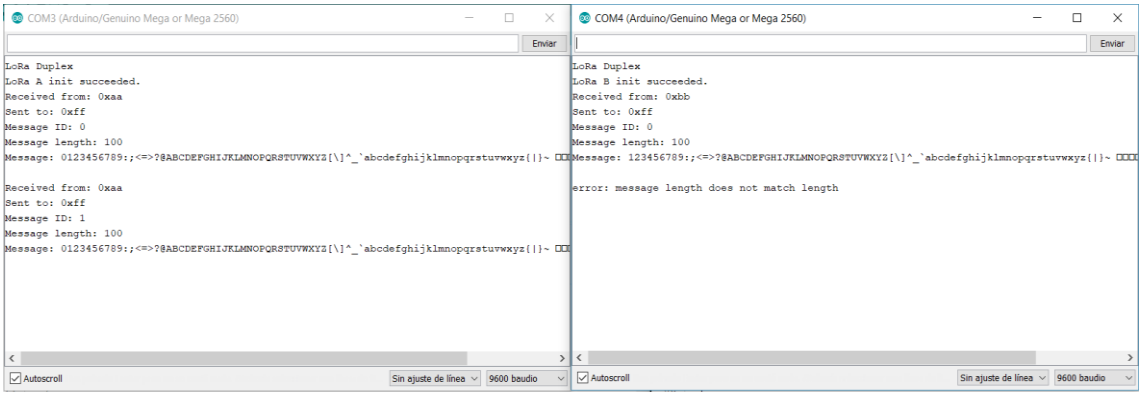


Figura 23. Lectura del puerto serie, envío de 100 bytes.

4.5.4 Analizar SNR y RSSI en dB y dBm al realizar envíos de 100 bytes.

Una vez se es capaz de realizar un envío de un tamaño controlado, se puede analizar este envío. La librería LoRa.h permite visualizar la relación señala a ruido y la potencia de recepción cuando se recibe un mensaje gracias a las funciones LoRa.packetRssi() y LoRa.packetSnr(), ambas devuelven un tipo int con la potencia en dBm y dB respectivamente.

Es necesario aclarar que también se puede elegir la potencia de transmisión mediante la función LoRa.setTxPower(TxPower). Por defecto, y tal como se realizan las pruebas, está fijado a 17 dBm.

Ahora que se sabe la información del paquete a enviar es el mismo que en el caso anterior, se puede eludir todo el contenido sobre el mensaje excepto los dos valores que se espera analizar a la hora de mostrarlo por pantalla.

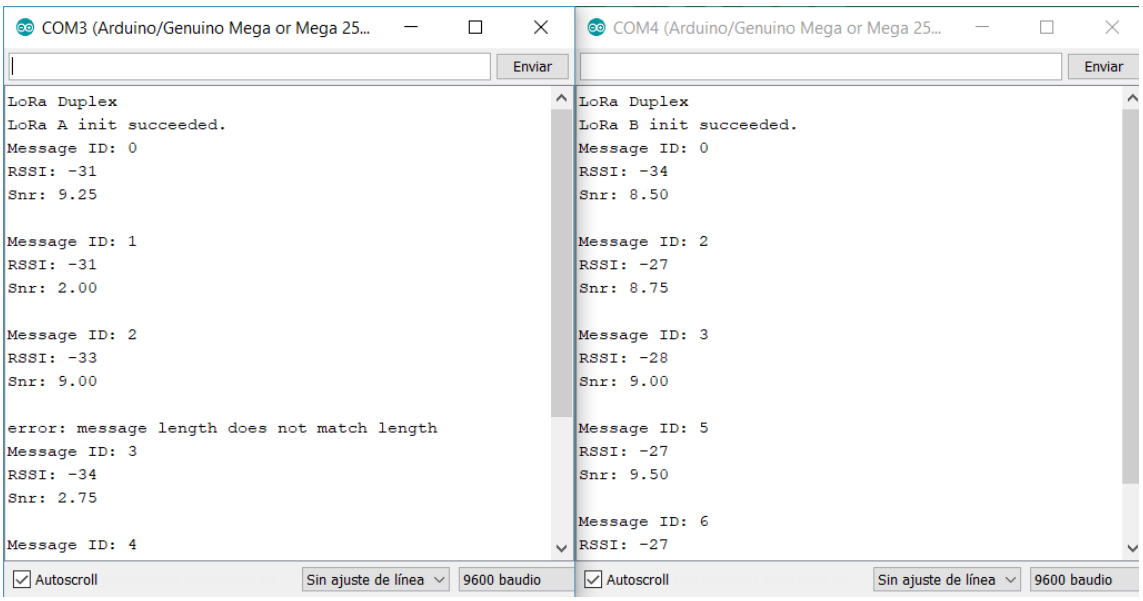


Figura 24. Lectura del puerto serie, visualización de los parámetros de señal.

4.5.5 Observar como varían los parámetros anteriores en relación con la distancia entre los equipos y encontrar distancias máximas de comunicación

Ahora que sabe cómo controlar los envíos y lo que contienen los paquetes transmitidos, podemos analizar como varia la relación señal a ruido y la potencia de recepción con la distancia. Para ver esto se debe analizar una muestra considerable de paquetes enviados en distancias iguales.

La modificación del sketch anterior para adaptar su funcionalidad a esta tarea consiste en implementar un bucle que, una vez se pulse el botón para realizar el envío, se realicen 100 envíos consecutivos.

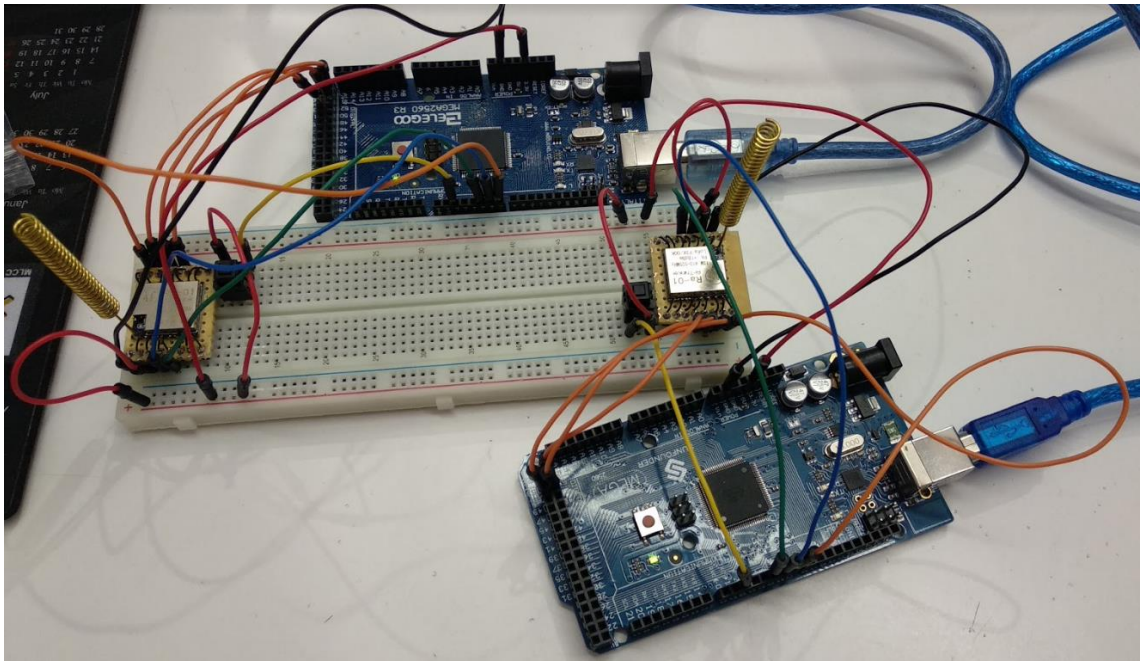


Figura 25. Montaje con botones para realizar el envío.

La primera distancia que se ha tomado ha sido muy próxima, de 16 cm. Los datos se han transferido a una hoja de Excell para graficarlos:

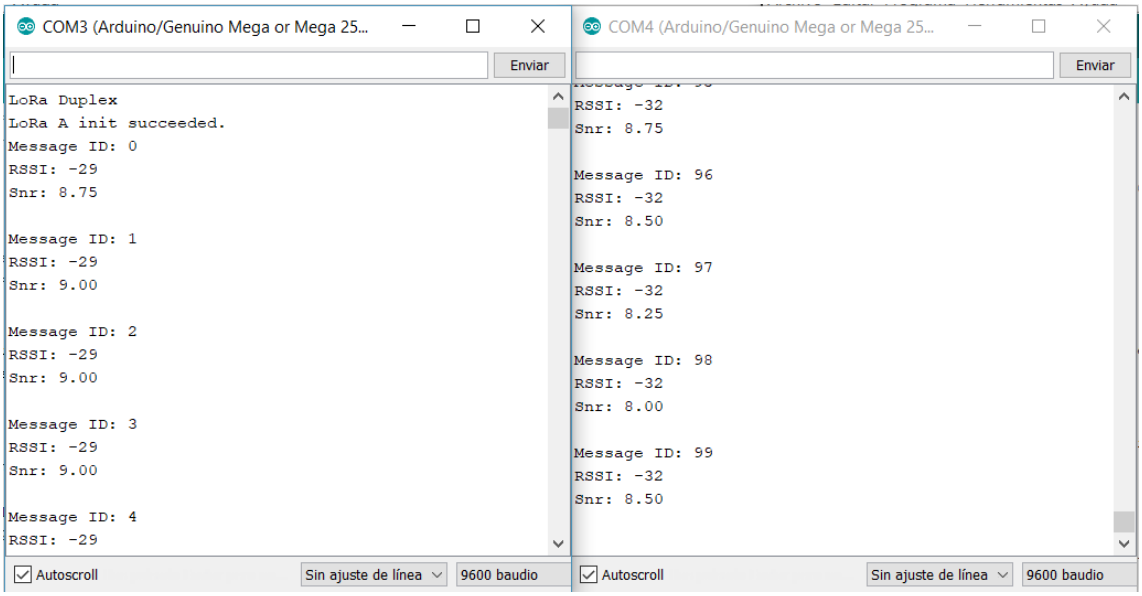
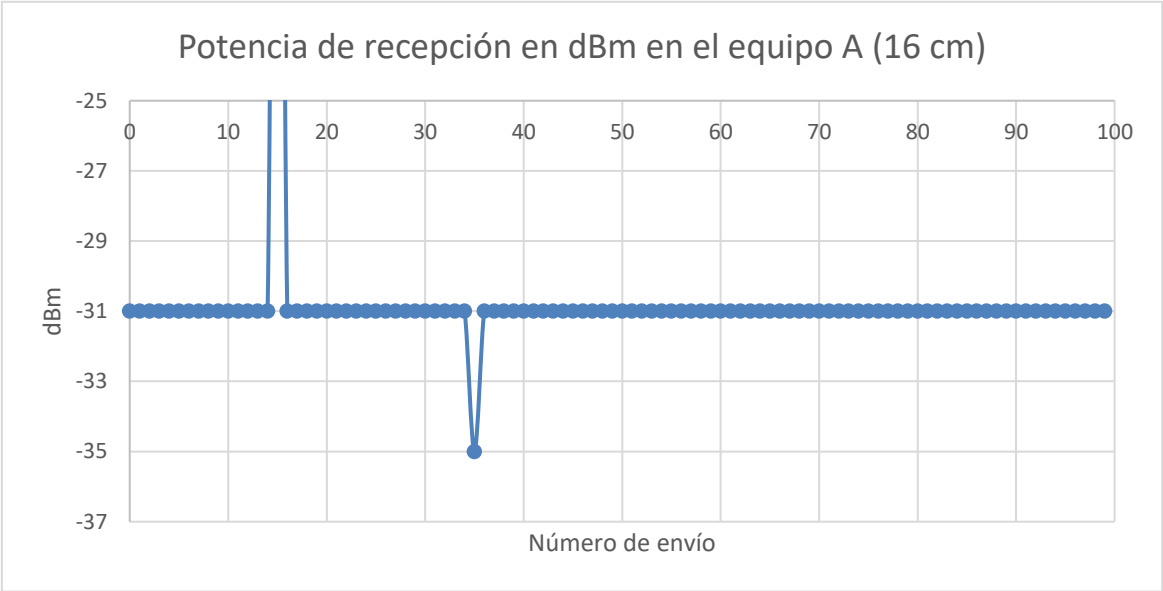
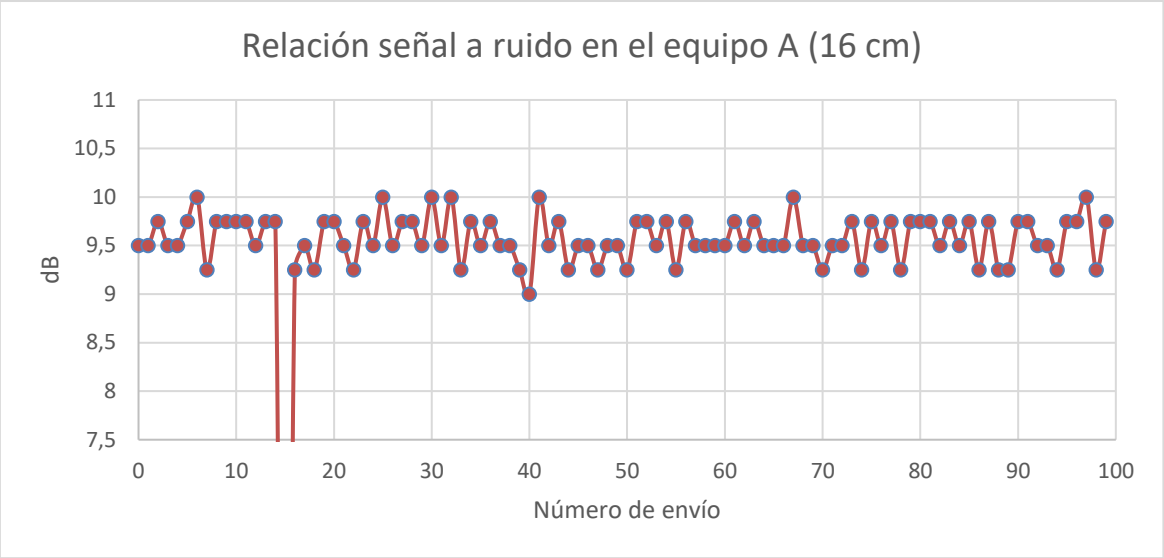
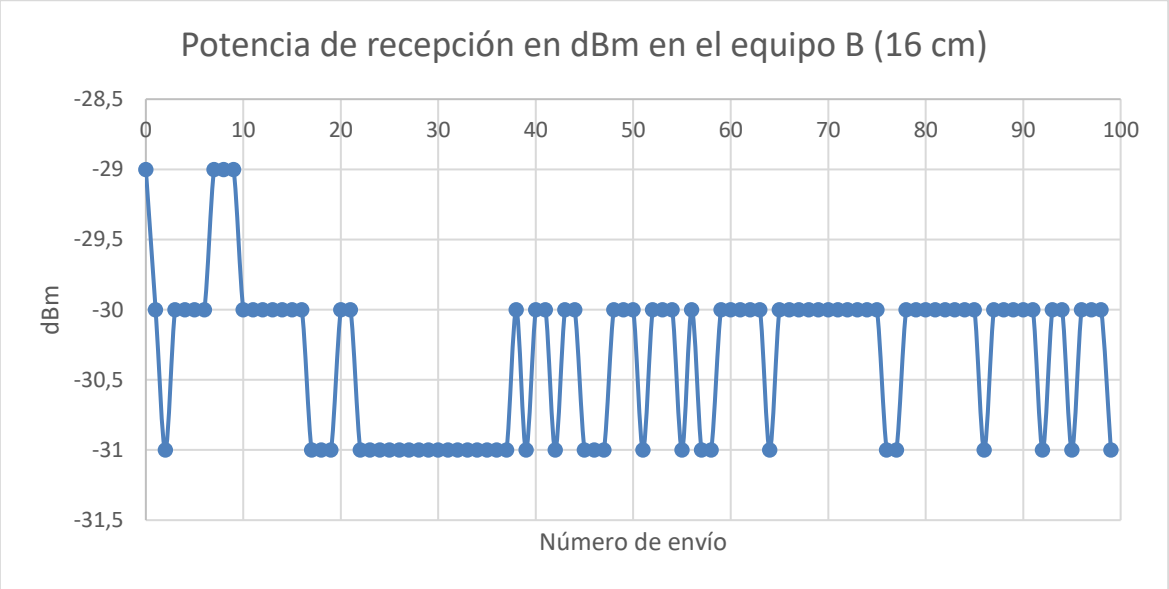


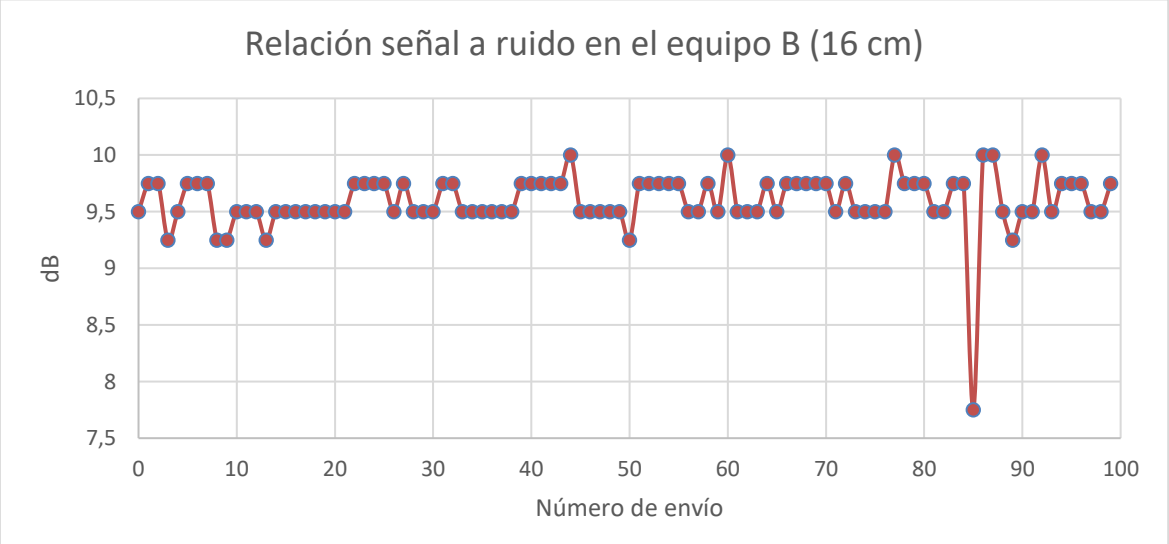
Figura 26. Lectura puerto serie para 16 cm.

En este primer envío se analizan los datos tanto en A como en B y se obtiene:







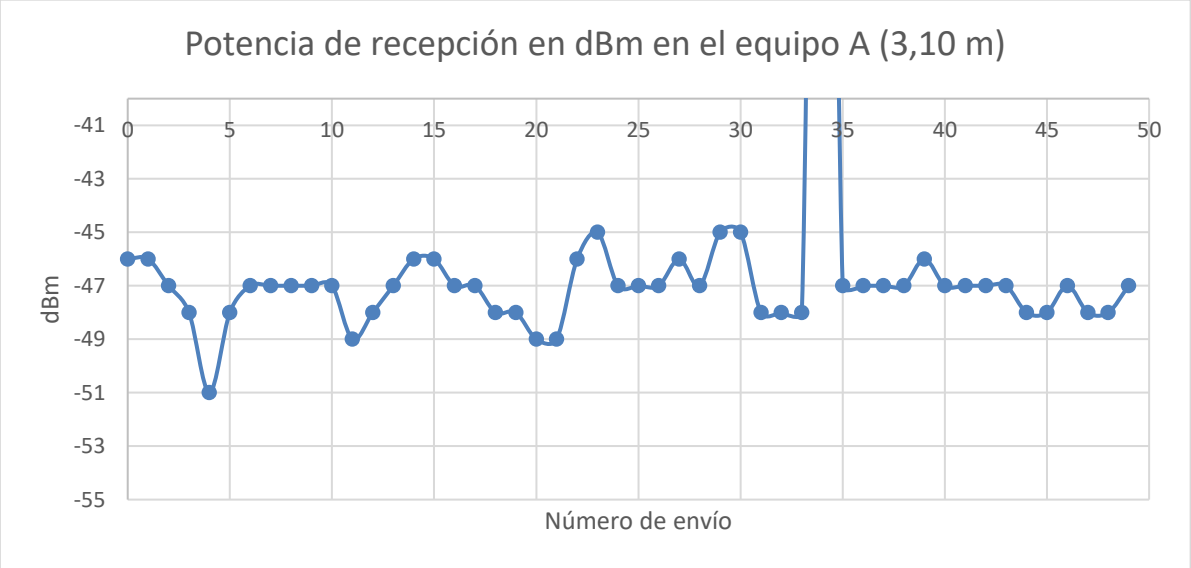


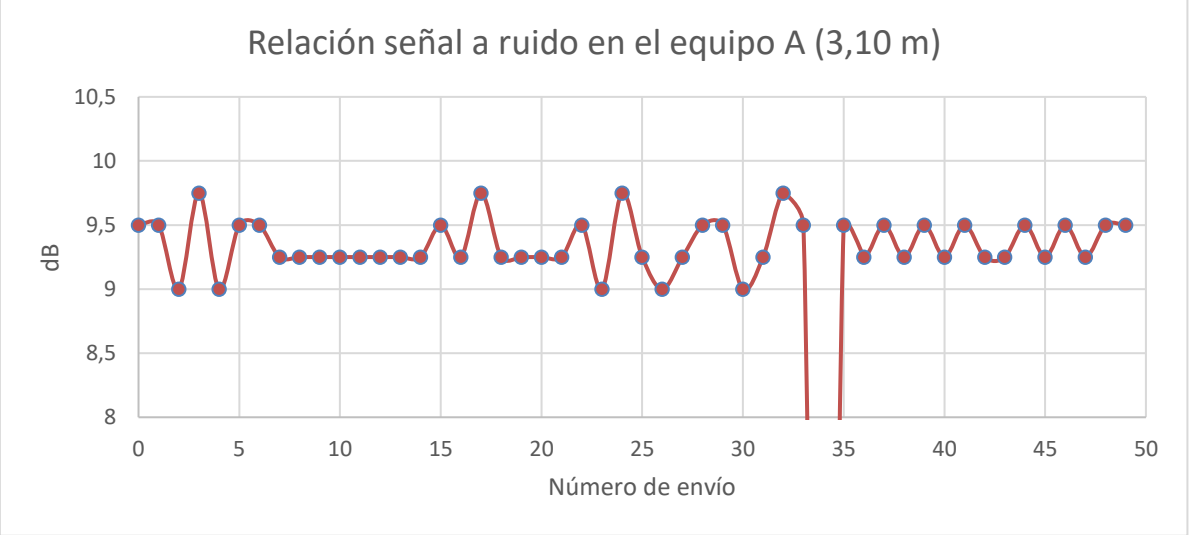
En el caso del equipo A, se ha perdido un envío, pero la potencia de recepción es más estable que en el caso del equipo B. se ha recibido a excepción de un envío una potencia de -31 dBm, siendo la excepción -35dBm. En el caso de la relación señal a ruido, por el momento se puede apreciar

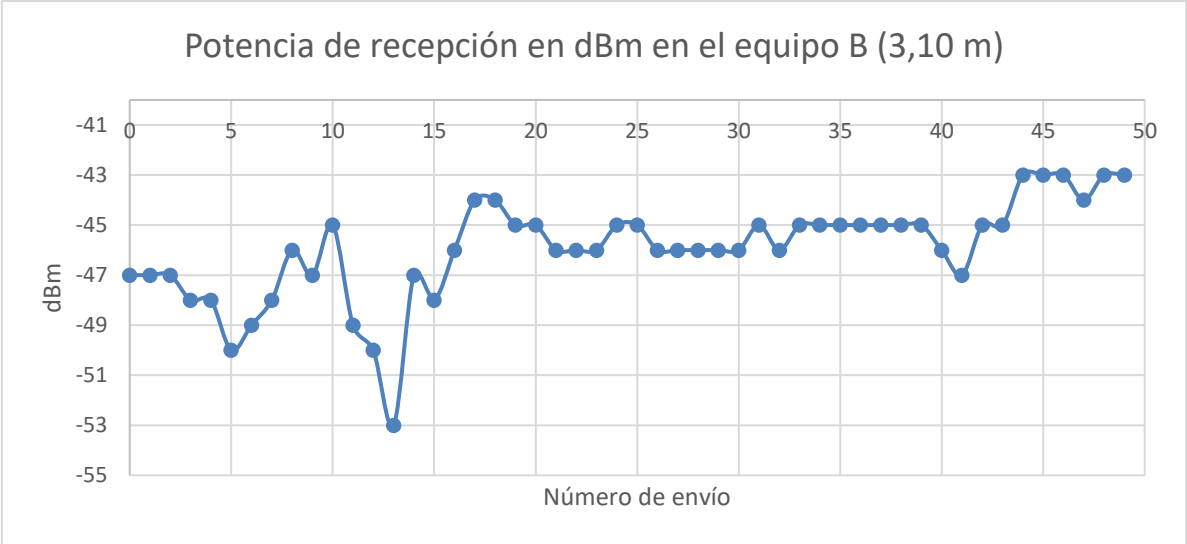
que domina la señal, la cual, ha oscilado entre 9 y 10 dB, la medida oscila en un paso mínimo de 0,25 dB. Esta poca variación y bajo nivel se debe a que no tenemos muchas interferencias dentro de la banda LoRa en el recinto de pruebas.

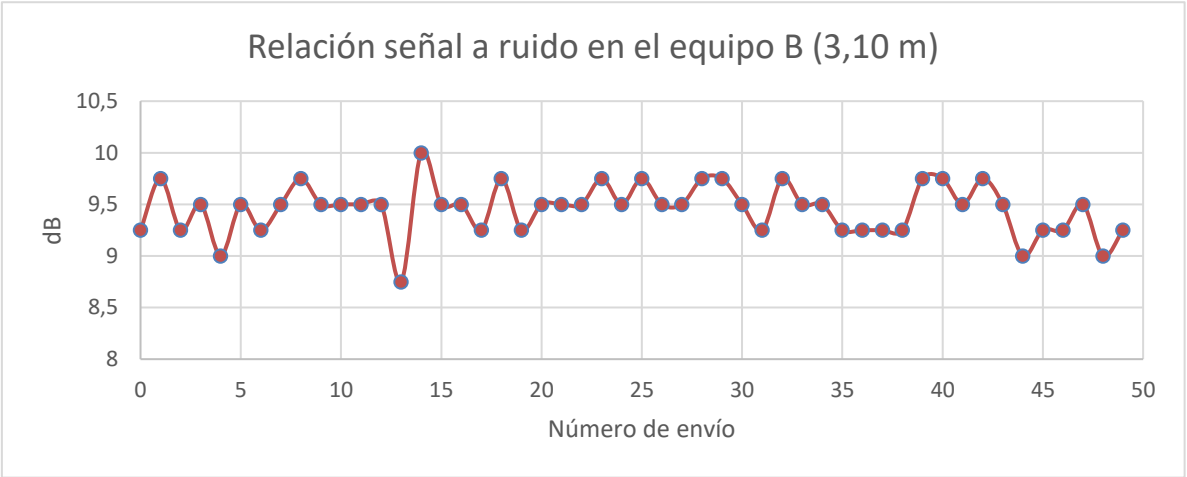
Para el equipo B, no se ha registrado tanta igualdad en la potencia recibida, oscilando entre -31 y -29 dBm, con mayor tendencia a recibir -31 dBm, encontrando -29 dBm como excepción entre los primeros 10 envíos. En cuanto a la relación señal a ruido, encontramos mayor constancia que en el equipo A, los valores oscilan entre 10 y 9,25 dB, con mayor tendencia a los 9,5 dB y encontrando un pico mínimo en 7,75 dB entorno al envío 85. En este caso no se ha perdido ningún envío.

En la siguiente prueba, se ha aumentado la distancia entre los equipos a 3,10 m. el objetivo es seguir analizando estos valores y ver como se degradan con la distancia a fin de encontrar la distancia máxima que se podrá cubrir. Además, se ha reducido la cantidad de envíos a 50 ya que es una muestra más que suficiente para los objetivos de la prueba.









Respecto al equipo A se ha vuelto a perder un envío, además ahora la potencia de recepción no es tan constante como en el caso anterior. Ahora oscila entre -51 y -45 dBm, siendo -47 dBm la potencia más repetida. Se puede apreciar como la recepción ha decaído aproximadamente 15 dBm. Respecto a la relación señal a ruido, prácticamente mantiene los valores del caso anterior, oscilando con mucha más constancia entre 9 y 10 dB, siendo ahora 9,25 dB el valor más repetido, con lo que hemos empeorado en 0,25 respecto al caso anterior.

En el caso del equipo B, obtenemos un mínimo de recepción en -53 dBm y hacia el final de los envíos vemos que se alcanza un máximo de -43 dBm, en este caso la potencia de recepción muestra más variaciones que en la distancia anterior, pero se sigue manteniendo un decaimiento de entre 15 y 20 dBm. Respecto a la relación señal a ruido, se sigue la misma tendencia que en el equipo A, dejando en este caso un mínimo de 8,75 dB, y ahora 9,5 dB es el valor más repetido. En líneas generales dentro de los dos primeros casos, la relación señal a ruido no parece alterar demasiado.

En la siguiente distancia se ha dado un salto importante. Ahora alcanzamos los 35 metros, además en este caso el emisor y el receptor no están en el mismo recinto, ya que mientras el emisor está dentro del laboratorio de Datakorum, el emisor se ha sacado a la calle:

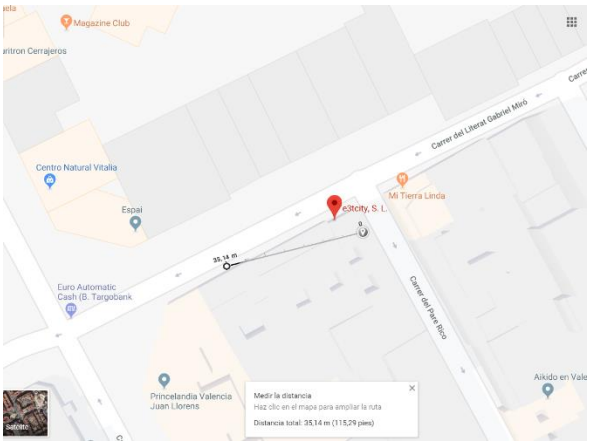
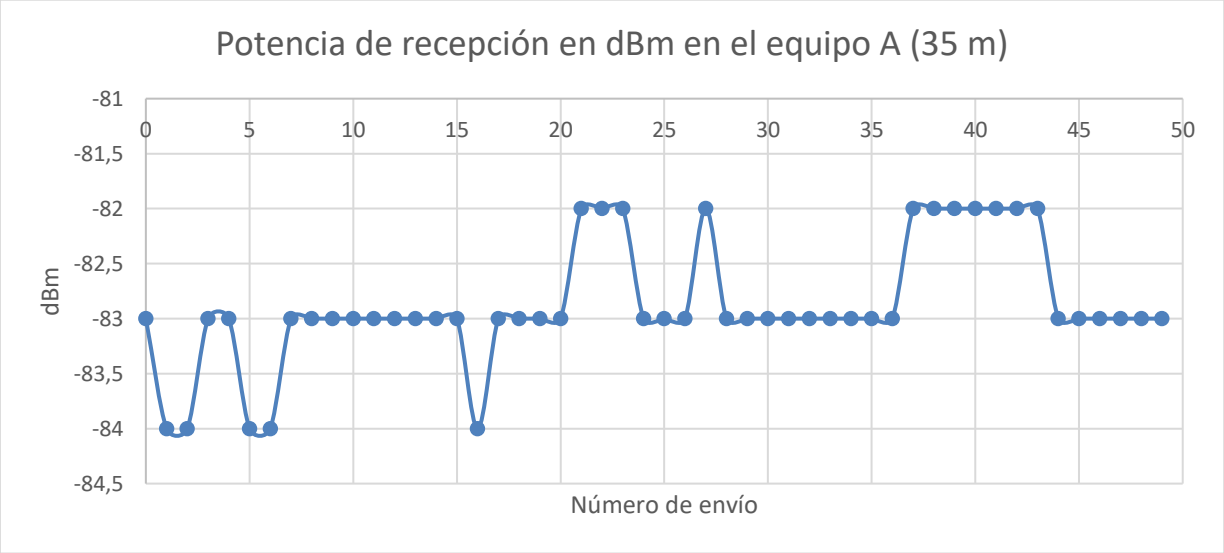
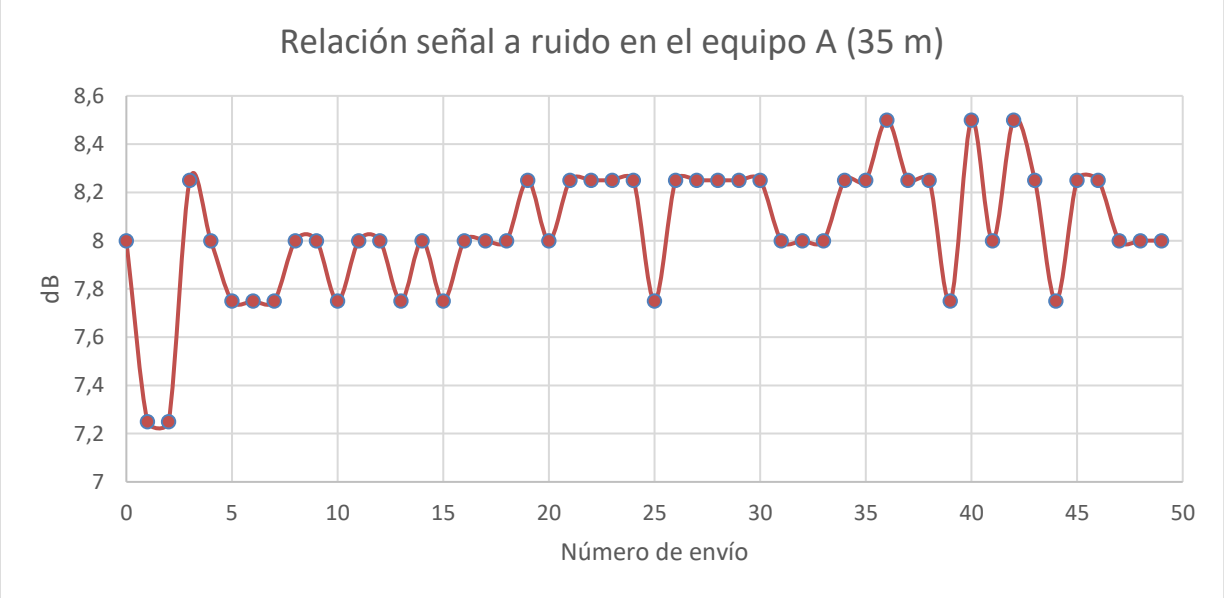


Figura 27. Localización de la prueba a 35 metros.

A fin de agilizar el estudio de la distancia, se ha simplificado, ahora ya no se medirá en el equipo A y B, ahora se ha limitado a analizar únicamente los datos recibidos por el equipo A. El resultado de las mediciones para 35 metros ha sido:





Se puede apreciar como la potencia de recepción ha decaído casi 40 dBm, llegando ahora a recibirse -83 dBm de forma más habitual, y la relación señal a ruido ha empeorado en general. Pese a que el mínimo que se ha medido es 7,25 dB, no se han superado los 8,5 dB.

El siguiente paso es más abrupto, ahora se han alcanzado los 75 metros:

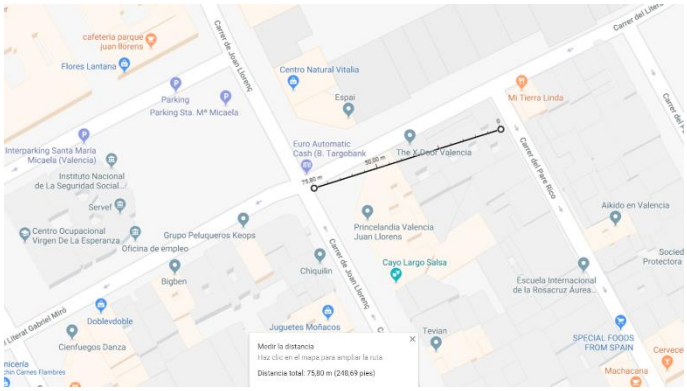
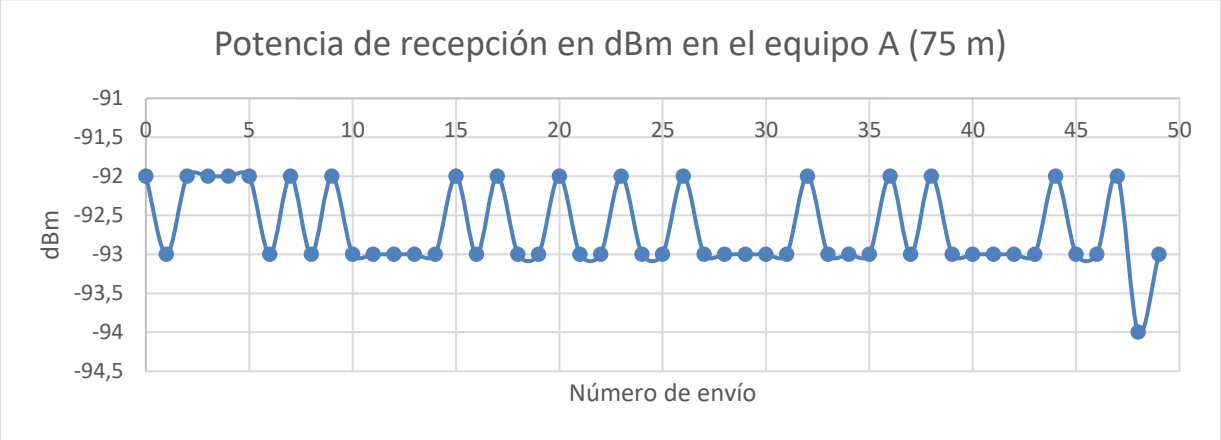
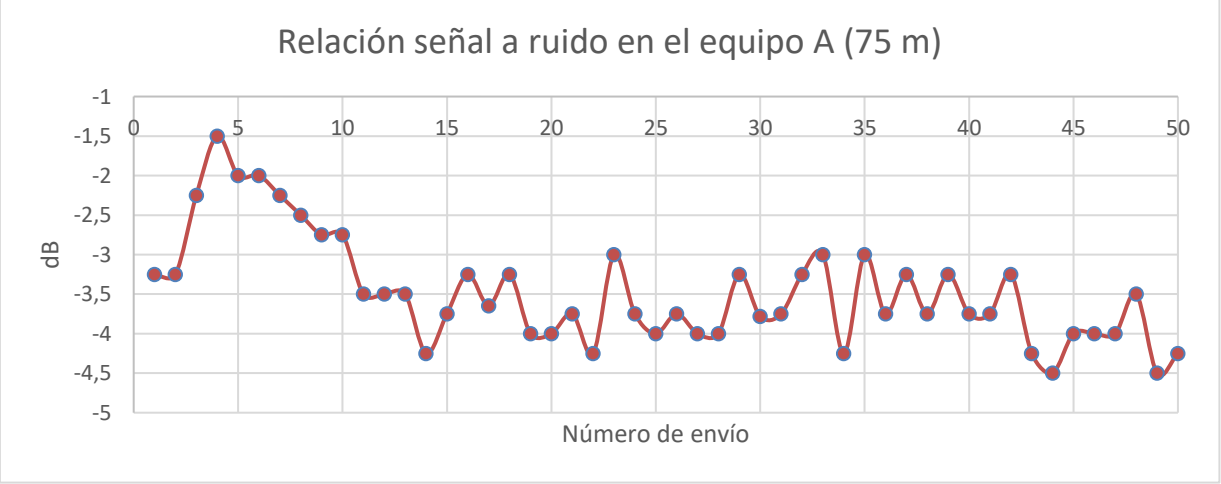


Figura 28Localización de la prueba a 75 metros.





En este caso, aunque la distancia ha aumentado de forma más considerable, la disminución de la potencia recibida sólo se ha reducido en 10 dB aproximadamente, esto puede ser debido a que en el caso anterior se ha puesto entre ambos equipos un bloque de edificio, pero ahora que ya se ha superado esa barrera, la señal no se pierde con tanta facilidad. Los valores oscilan entre -92 y -93 dBm, con un mínimo aislado en -94 dBm. En el caso de la relación señal a ruido, se ha impuesto el ruido sobre la señal, aunque aún no de forma en que perdamos la señal por completo, ya que se oscila entre -1,5 y -4,5 dB, sin embargo, cuanto mayor sea en valor absoluto, mayor dominio tendrá el ruido sobre la señal.

El siguiente paso es comprobar si podemos alcanzar la distancia entre equipos exigida para el proyecto, 100 metros:

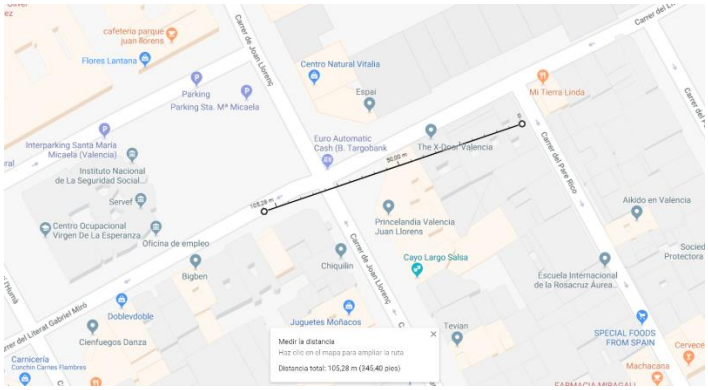
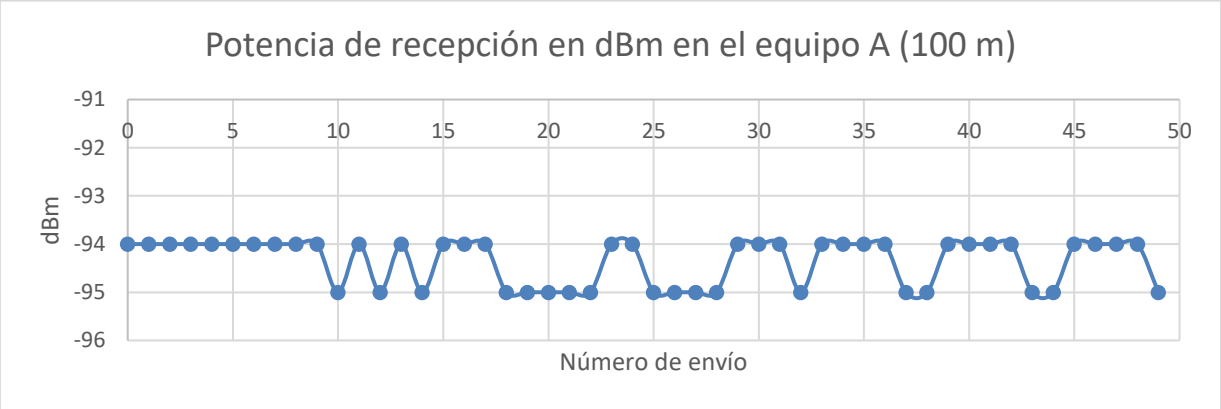
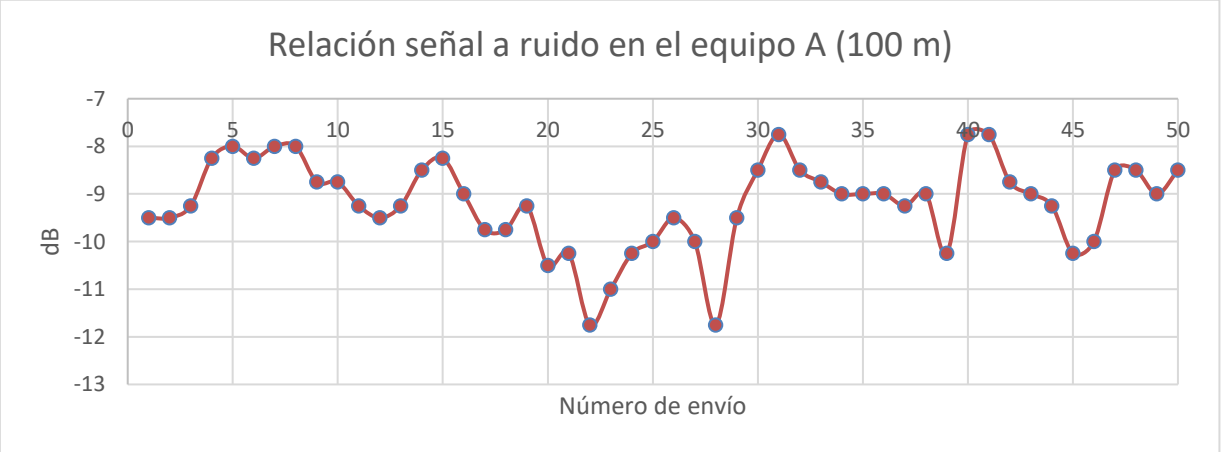


Figura 29. Localización de la prueba a 100 metros.





Se puede ver que la potencia recibida apenas varía respecto al caso anterior en comparación com los anteriores casos, apenas 2 dB en general. Ahora se reciben entre -94 y -95 dBm, siendo el primero el valor más obtenido. Como parte mala, se tiene que la relación señal a ruido si que ha empeorado de una manera algo más drástica, teniendo un valor mínimo de -11,75 dBm. Esto empieza a ser algo preocupante a la hora de recuperar nuestra señal. El valor máximo obtenido ha sido -7,75 dB y en este caso se aprecia una variación mucho más abrupta entre cada mensaje recibido.

Pese la mala relación señal a ruido, se puede afirmar que se cumple el requisito de distancia entre equipos, sin embargo, se realizará una última medición a 150 metros:

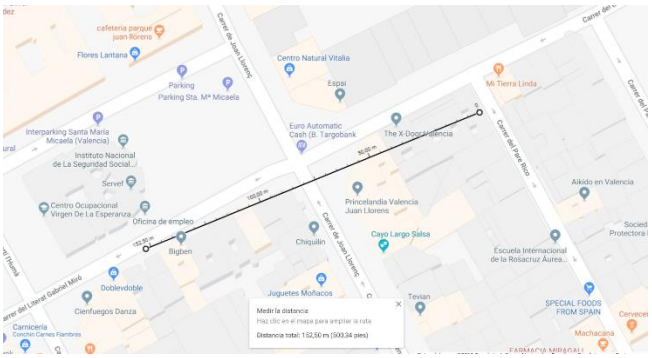
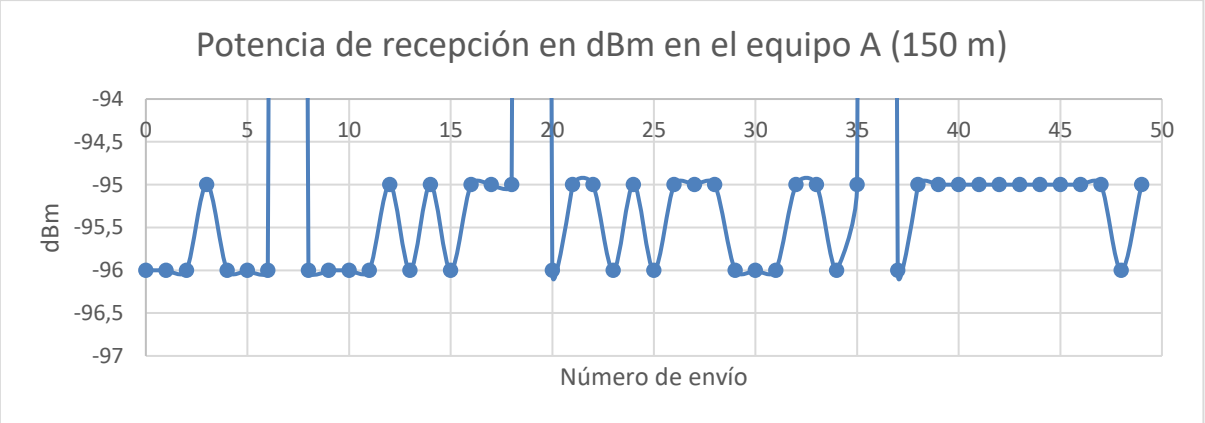
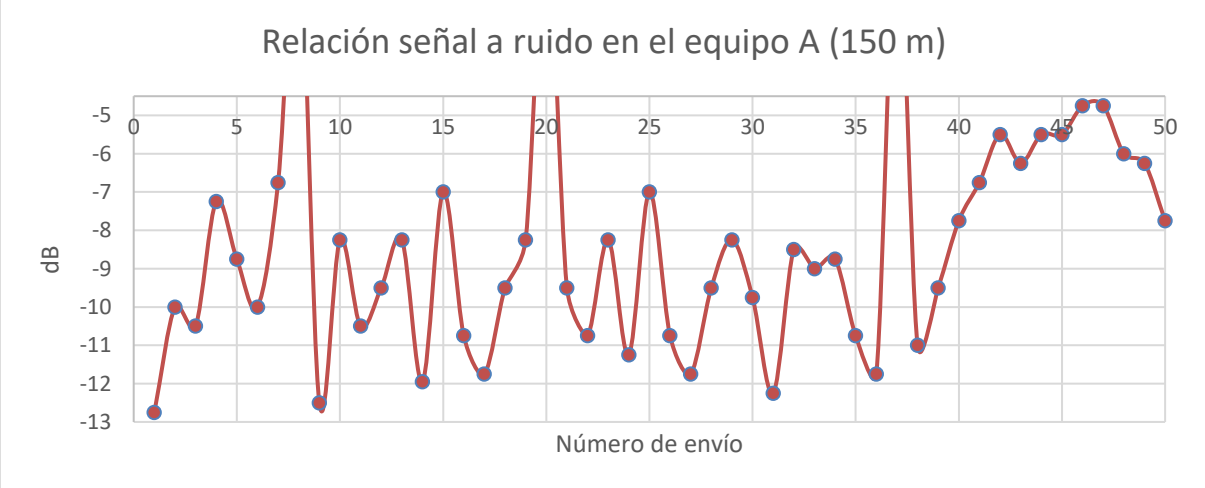


Figura 30. Localización de la prueba a 150 metros.





En este caso se han perdido 3 envíos, y se ha alcanzado un mínimo de potencia de recepción de -96 dBm. Al igual que antes, la distancia no empeora demasiado la potencia recibida, si en cambio la relación señal a ruido que ahora varía de manera más abrupta entre envíos, y pese que se ha obtenido un mínimo de -12,75 dB, hacia el tramo final de los envíos ha aumentado hasta rondar los -4,75 y -7 dB. Por lo que podemos garantizar que somos capaces de alcanzar los 100 metros y distancias mayores.

Para mejorar este aspecto de cara al producto final, debe estudiarse como se deberán configurar los parámetros de potencia emitida y factor de dispersión o ancho de banda, así como utilizar antenas que mejoren la adaptación de la señal tanto para emisión como para recepción. La correcta aplicación de estos parámetros mejorará tanto la potencia recibida como la relación señal a ruido.

4.5.6 Implementar redes de tres equipos o más basándonos en maestro-esclavo

El objetivo de esta prueba es meter un tercer equipo en la red. Una vez ya se sabe cómo funcionan todos los parámetros de envío y recepción, es sencillo adaptar la red para un tercer equipo o más,

bastará con definir bien la ID de cada uno de los equipos. Se ha asignado una dirección única a cada equipo de la red, siendo para tres equipos las direcciones 0xAA, 0xBB y 0xCC.

Este tercer equipo establece la comunicación LoRa gracias al módulo Ra-02, que difiere del módulo Ra-01 en que este nuevo módulo lleva integrado un conector SMA para poder elegir la antena que queremos conectar sin necesidad de adaptar el circuito.

Para ver que se puede manejar la red sin mayor complejidad, se han incorporado dos botones en cada uno de los equipos tal como se hizo en la prueba anterior, así el equipo A enviará a B y C, el equipo B a enviará a A y C, y finalmente el equipo C enviará a A y B. El mensaje para enviar sigue siendo el mensaje de 100 bytes que ya se ha empleado y para la visualización de esta prueba en concreto se ha utilizado la aplicación hercules.exe que nos permite visualizar los correspondientes puertos serie.

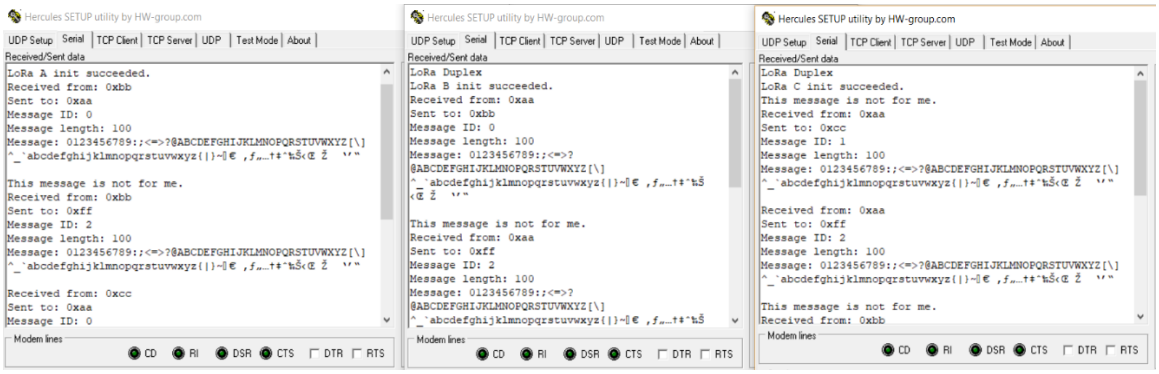


Figura 31. Lectura del puerto serie, Red de equipos.

Una vez se ha comprobado que el direccionamiento de cada equipo, así como la dirección de broadcast (0xFF) funciona correctamente, es decir, que nadie que no debe recibir un mensaje lo recibe y que todos los que deben recibirlo, lo hacen, se puede implementar una red basada en maestro-esclavo. En dicha red se pretende que el equipo A sea un maestro que controla a los esclavos B y C.

Para esta red, el equipo B tendrá asociados dos sensores, el sensor de temperatura MCP9700A-E/TO(-40ºC-125ºC) [16] y el sensor de humedad relativa HIH-5030-001 [17] asociados a las entradas analógicas A0 y A1. Este equipo se mantiene a la espera de que uno de estos dos valores, temperatura o humedad relativa, sean solicitados por el maestro de la red, el equipo A, al cual contestarán con el valor solicitado.

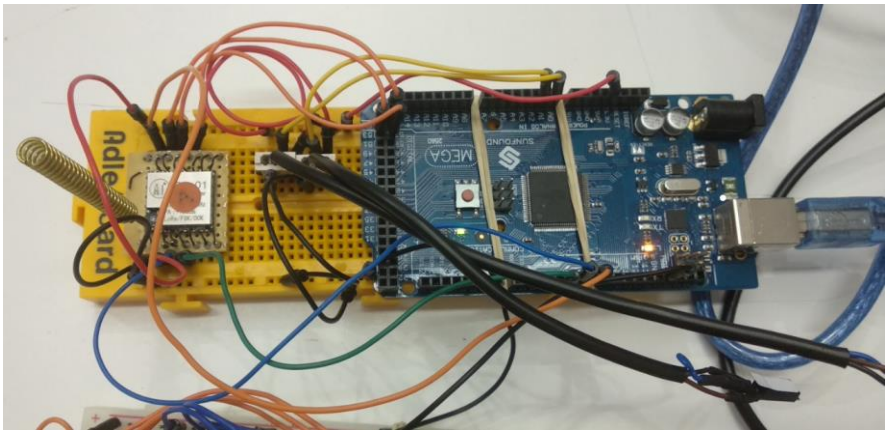


Figura 32. Montaje de los sensores.

En el equipo C se ha asociado una placa de relé adaptada para realizar pruebas con Arduino. La placa de relés conmuta dependiendo de si el estado de la salida digital asociada es alto o bajo, además, deberá alimentarse a 12 voltios para que el relé pueda conmutar y se asume que la conexión al relé será entre común y normalmente abierto, por lo que un estado alto cerrará el relé

y un estado bajo lo abrirá. Se han asociado los pines digitales 2 y 3 como salidas digitales para el control de relé.

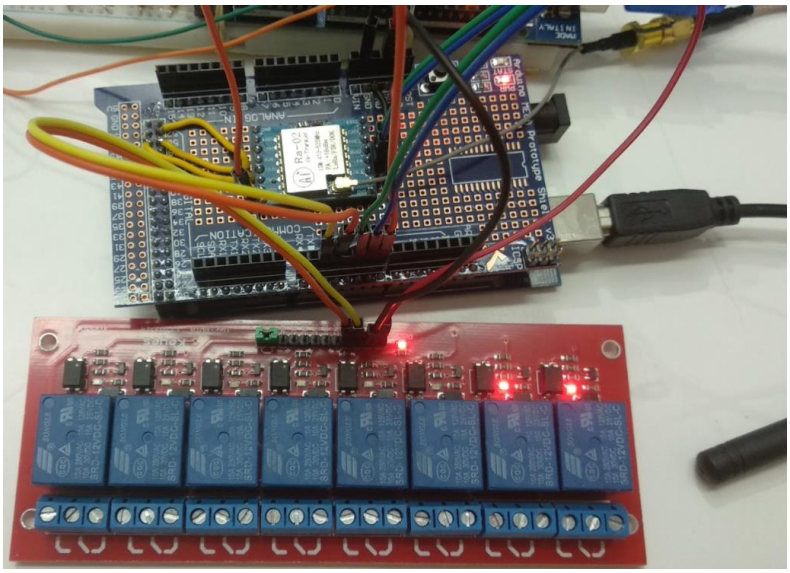


Figura 33. Montaje de los relés.

El Equipo A es el que solicita cambiar de estado los relés o leer los datos de sensores. Este envía un mensaje concreto a un equipo concreto, por ejemplo, si envía el mensaje "temperatura" al equipo B, este devolverá la temperatura que lee mediante su sensor, o si en cambio envía el mensaje "relay1" al equipo C, conmutará el relé 1 del equipo C. las peticiones están asociadas al mensaje, por lo que si se envía el mensaje "relay1" a la dirección de broadcast, el equipo C actuará pero el equipo B no hará nada. Se ha utilizado un total de cuatro botones en el equipo A para realizar las diferentes peticiones.

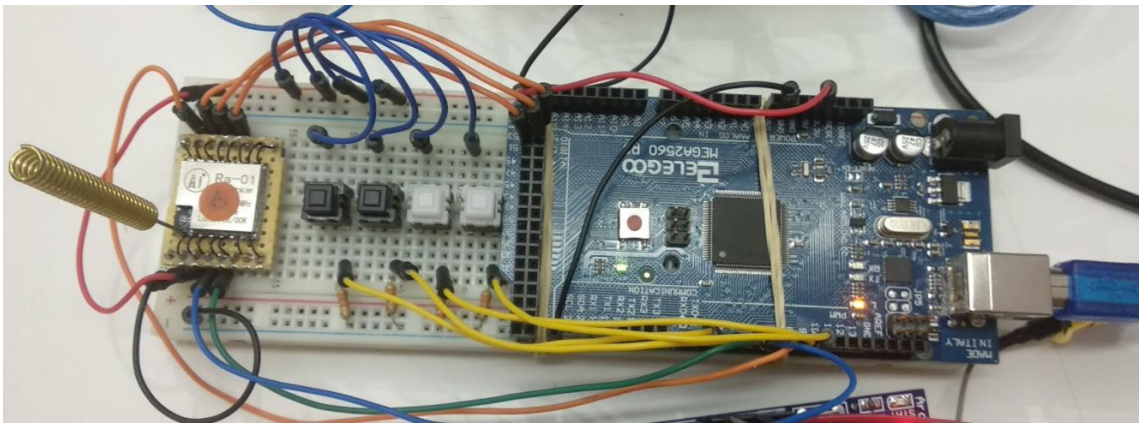


Figura 34. Montaje de los botones.

Los botones negros se han asociado a los mensajes "temperatura" y "humedad" que serán enviados al equipo B cuando sean pulsados, solicitando así que se lea la temperatura o la humedad según corresponda y se han asociado a los pines digitales 2 y 3 como entradas digitales. Los botones blancos, por su parte, manejan los mensajes "relay1" y "relay2" que se enviarán al equipo C y controlarán el cambio de estado de los relés 1 y 2, estos están asociados a los pines digitales 8 y 9 como entradas digitales.

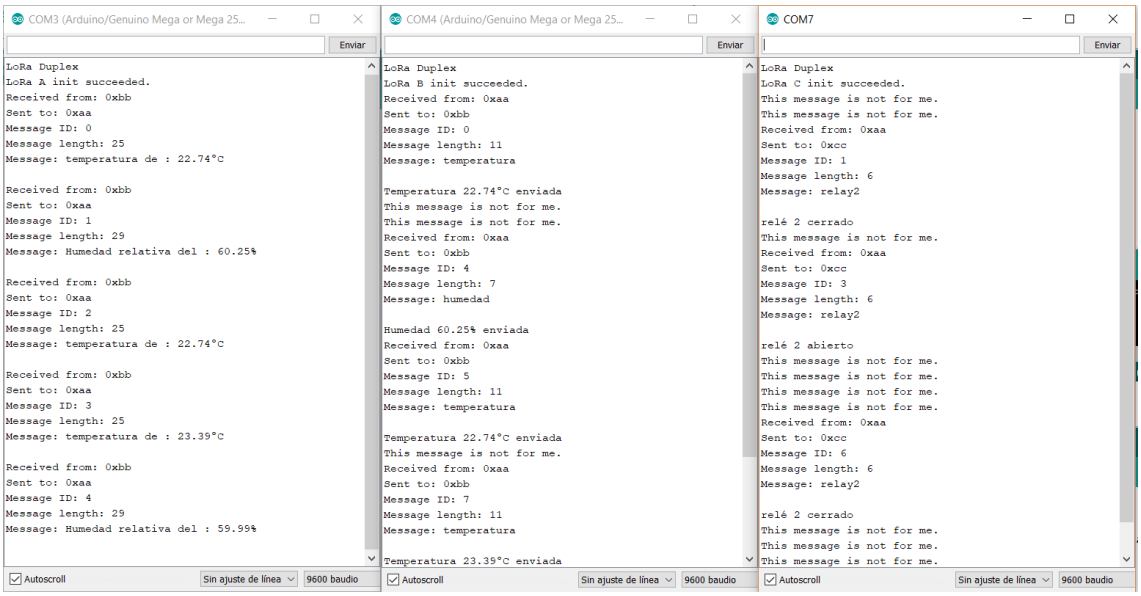


Figura 35. Lectura del puerto serie, lectura de los datos de los esclavos.

4.5.7 Integración de Modbus en los equipos que conforman la red

El objetivo de esta prueba es poder enviar un mensaje que se haya recibido vía LoRa mediante Modbus y viceversa. Para poder trabajar con Modbus se ha incluido la librería modbusRTU.h [18] y se ha empleado un conversor serie-Modbus externo propio de Datakorum. Este conversor recibe a través de un puerto serie y lo adapta para ser enviado mediante RS485.

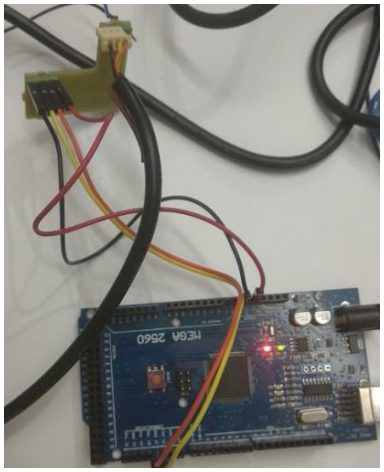


Figura 36. Montaje del conversor serie-Modbus.

Este pequeño circuito se conecta mediante el conector J1 al puerto serie de nuestro Arduino, concretamente al Serial2 y a la alimentación de 5V que este proporciona con su respectiva tierra. El conector J2 por su parte, se alimentará con ayuda de una fuente externa a 12V y a los cables A, B y tierra de Modbus. Se ha elegido para esta transmisión una velocidad de 9600 baudios en consonancia con el resto de las comunicaciones.

A diferencia de LoRa, la comunicación Modbus no es tan trivial, ya que funciona mediante registros de 16 bits sin signo (*unsigned int*), y su forma de operar consiste en enviar un mensaje o mensajes por un bus controlado únicamente por el maestro provocando el cambio de estado de los registros en los esclavos o pidiendo a determinados esclavos la actualización de algunos de los registros.

Los registros con los que se trabaja son los de retención (registro 40001 a 50000) y el objetivo será leer y escribir en ellos o enviar su valor mediante LoRa. Se van a configurar los veinte primeros registros en los módulos de Arduino, aunque solo se accederá a los cinco o seis primeros por sencillez de la prueba.

La red que se implementará consistirá en un ordenador que simulará ser un maestro Modbus gracias al programa CAS Modbus scanner. El esclavo de este maestro será un módulo Arduino que a su vez sea el maestro de la red LoRa. El maestro Modbus leerá y escribirá registros en el esclavo, este a su vez, trasladará la actualización de los registros vía LoRa al segundo Arduino donde también se han configurado los registros y solicitará la lectura de sensores o la activación de bobinas.

El segundo Arduino, será esclavo dentro de la red LoRa y transmitirá sus cambios en los registros. Además, leerá un sensor de temperatura cuya medida almacenará en un registro (40004, que en el maestro LoRa será 40005) y activará o apagará un LED azul en función del contenido de un registro (40003). El resto del desglose de los registros son registros de escritura y lectura para 40001 y 40002 con la peculiaridad de que el registro 40002 emulará un registro de solo lectura. Y finalmente el registro 40006 del maestro LoRa que será el 40005 en el esclavo y que tendrá valores de entre 0 y 100 para simular el estado de un *dimmer*. El echo de que en el maestro LoRa se utilicen dos registros para leer la temperatura se debe a que un registro sirve para solicitar la lectura (40004) y el otro para almacenar el valor leído (40005).

Los registros seleccionados sirven para emular el comportamiento de los equipos de Datakorum, ya que como funciones típicas se encuentran la lectura y escritura de datos, la actualización de estado de un registro, la activación de relé (simulada por el LED), la lectura de sensores y la regulación mediante un *dimmer*.

Las rutinas de control implementadas en CAS Modbus scanner son sencillas de lectura y escritura de registros, mientras que, para LoRa, se ha asignado una ID de mensaje a cada registro que se desea consultar o modificar, y que como mensaje se enviará el valor que se desea guardar o consultar en dicho registro. Por ejemplo, si se desea escribir el valor 10 en el registro 40001, seleccionaríamos esta rutina en el programa de ordenador, y el módulo de Arduino al observar este cambio en el registro, enviaría un mensaje con ID 1 y el mensaje “10” mediante LoRa. El segundo Arduino recibiría e identificaría el mensaje y actualizaría el valor de su registro 40001.

Los módulos de Arduino están en comunicación LoRa constante actualizando los valores de los registros, cada vez que uno de los registros cambia, se envía un mensaje para que su vecino realice la actualización del registro que corresponda, así, cada vez que el maestro realice una lectura de registros estos estarán actualizados.

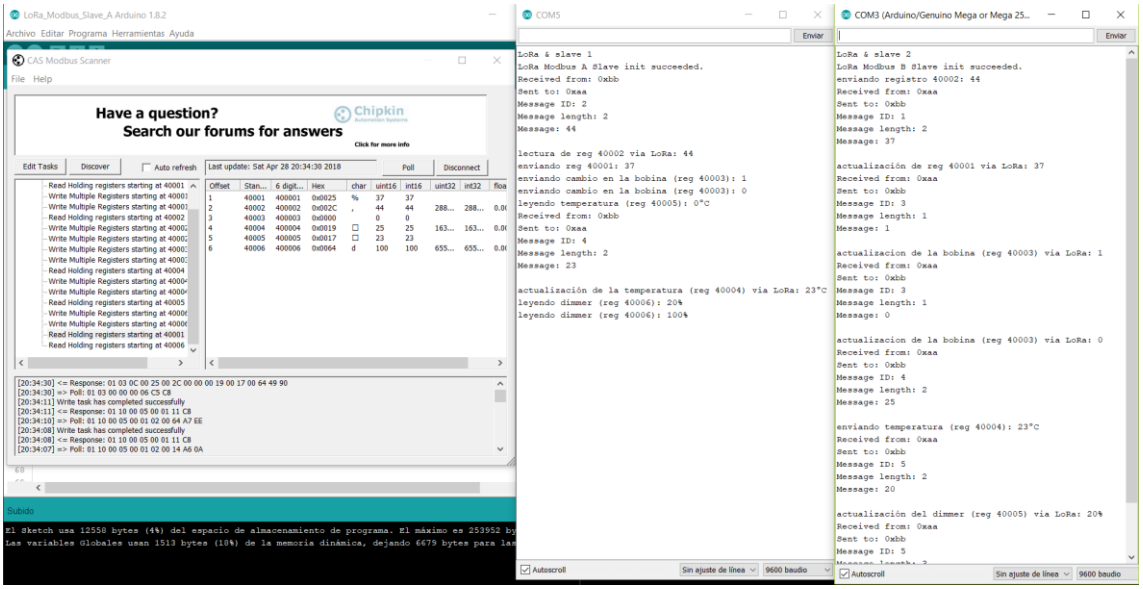


Figura 37. Lectura del puerto serie, mensajes modbus.

4.5.8 Implementación y compatibilidad con los equipos de Datakorum

Con esta última prueba, podrá confirmarse que es posible integrar LoRa con los equipos de Datakorum. Tras haber tenido éxito empaquetando Modbus vía LoRa y a la inversa, sólo queda darle una aplicación real. En el caso de prueba, se va a replicar la solución de parking que actualmente tiene Datakorum para controlar el aforo en parking públicos en exteriores, la cual se basa en calcular el número de vehículos que están ocupando plazas mediante la diferencia de entradas y salidas de vehículos, donde al existir diferentes accesos tanto de entrada como salida, los equipos que conforman la solución se comunican vía Modbus, siendo el Master de la red el encargado de subir el dato a la nube de Datakorum para que los usuarios y administradores del parking puedan saber cuántas plazas quedan libres.

El objetivo es sustituir el cable que conforma la red Modbus por la tecnología RF que proporciona LoRa. El funcionamiento consistirá en conectarse a los equipos de Datakorum por Modbus a nuestro prototipo LoRa, y este enviará las peticiones o lecturas de los registros hasta otro equipo LoRa que actualizará a su correspondiente equipo de Datakorum nuevamente mediante Modbus.

El caso práctico es el más sencillo: un maestro y un esclavo donde este último realiza la cuenta de entradas y salidas de vehículos y la acumula en registros que serán leídos por su maestro para evaluar el número total de plazas ocupadas y subir dicho dato a la nube. El maestro estará conectado a un equipo LoRa que simulará ser su esclavo respondiendo a las peticiones de actualización de estado cíclicas que realiza el maestro. Cada vez que el maestro solicite la actualización de los registros, el equipo LoRa pasará los datos y solicitará mediante un mensaje la actualización de los datos al equipo LoRa conectado al esclavo real que suplanta. En caso de este segundo equipo LoRa, su misión es actuar como el maestro Modbus consultando cíclicamente los registros, estos serán acumulados. Una vez se reciba el mensaje LoRa de actualizar los registros, este último equipo transmitirá la actualización mediante RF y reseteará sus acumulados.

El objetivo para el buen funcionamiento de la solución es lograr que los equipos LoRa sean invisibles a ojos de los equipos de Datakorum evitando así que deba desarrollarse un *firmware* específico para los equipos de las soluciones que ya existen en las que se pretende introducir LoRa.

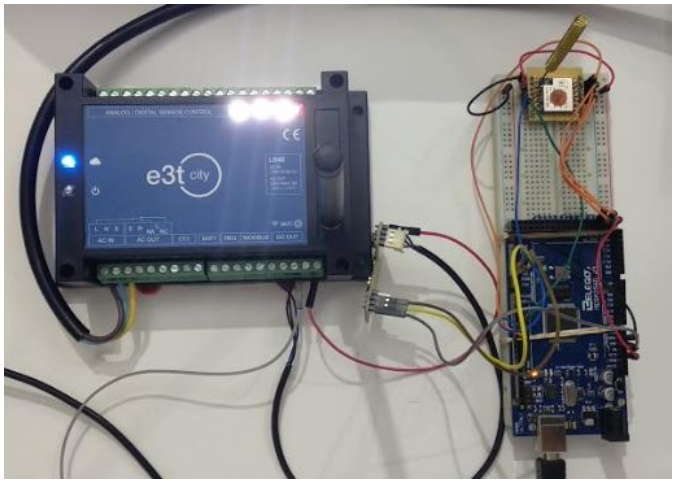


Figura 38. Montaje equipo esclavo de Datakorum.

El montaje para el equipo que gestiona la transmisión de la figura 38. Los 12 voltios necesarios para alimentar el circuito Modbus-serie son proporcionados directamente por el equipo de Datakorum, se puede ver como se conecta a la entrada Modbus del equipo y al puerto serie de Arduino. En el equipo que hace de esclavo el montaje queda como se muestra en la figura 39:

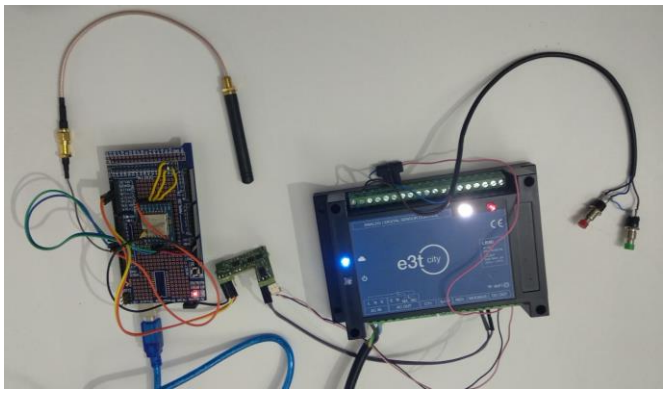


Figura 39. Montaje del equipo maestro de Datakorum.

Las conexiones son exactamente iguales que en el conexionado anterior, solo que, en esta ocasión, se han colocado unos botones que conmutan o no la salida de 3,3 voltios del equipo de Datakorum con las entradas de sensores para poder simular las entradas y salidas de vehículos.

El funcionamiento de esta red Modbus es sencilla, el maestro se limita a leer los 5 primeros registros mantenidos, en los cuales se contienen las salidas y entradas acumuladas, una vez se leen, se hace un *reset* de los registros por parte del esclavo, y el maestro se limitará a subir los datos a la nube. De una manera simplificada, el Arduino enlazado al equipo que sube los datos a la nube actúa exactamente igual que el equipo esclavo de Datakorum y de igual manera, el Arduino enlazado al equipo esclavo de Datakorum.

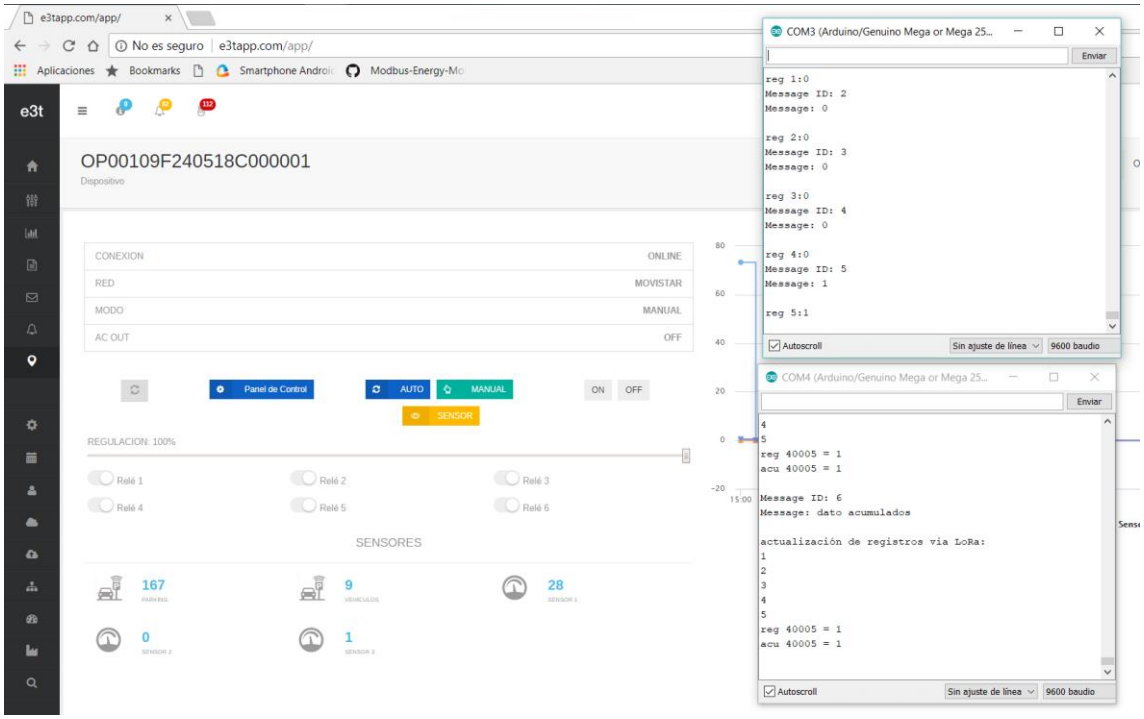


Figura 40. Panel del cloud de Datakorum junto a lectura del puerto serie.

Tal como se puede ver en la figura 40, se es capaz de enviar los datos para el *cloud* de Datakorum lo actualice. En la imagen se puede ver en la parte izquierda el flujo de mensajes lora entre los equipos, la ventana superior nos muestra el equipo Arduino conectado al equipo de Datakorum que actua de maestro y sube los datos a la nueve y la inferior el que enlazado al esclavo y se limita a transmitir los datos de entrada y salida de vehículos. El resto de la imagen corresponde a la aplicación web de Datakorum, en la que podemos ver el estado del dispositivo maestro, en el que vemos, de izquierda a derecha en la parte inferior el número de plazas libres del parking ficticio, el número ficticio de vehículos dentro del parking, el número de vehículos que han transitado el

parking y debajo se muestran los últimos datos registrados por el propio equipo maestro (que también es capaz de registrar entradas y salidas por si mismo) y los recibidos por su esclavo.

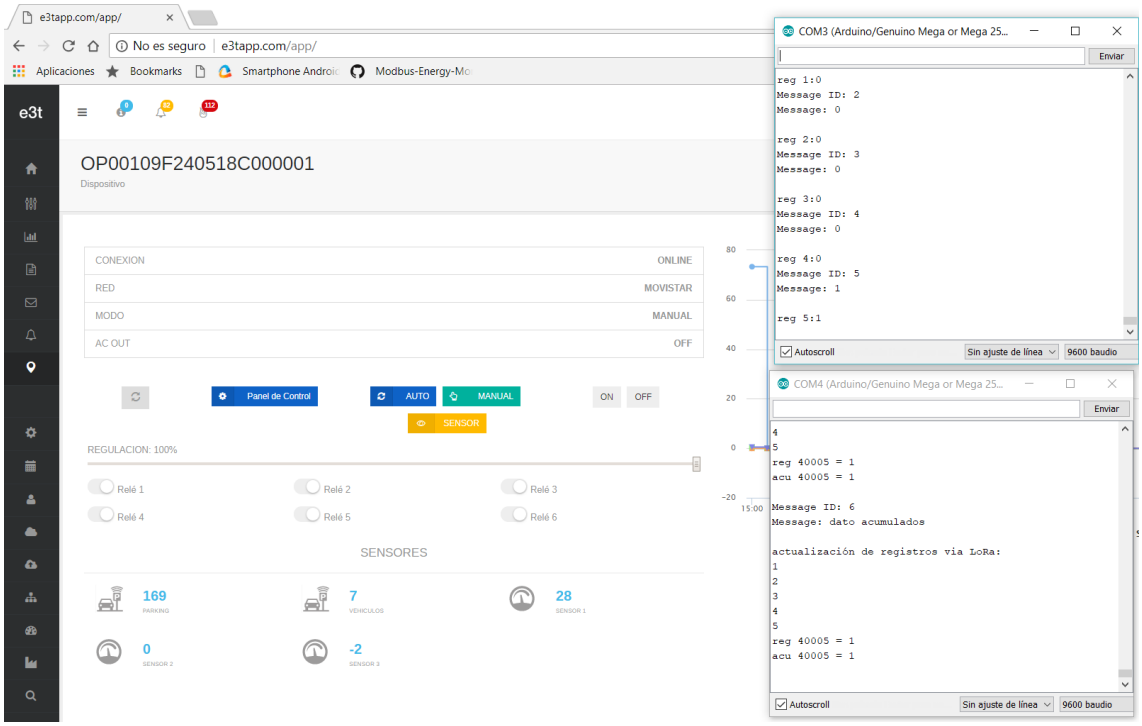


Figura 41. Salida de dos vehículos.

Ahora se simula la salida de dos vehículos mediante los botones, el dato es transmitido vía LoRa y se puede ver en el panel del equipo, se muestra en la figura 41. Se puede comprobar como se han registrado dos salidas en el esclavo y se han actualizado los datos en la nube. De igual manera pasa si simulamos una entrada.

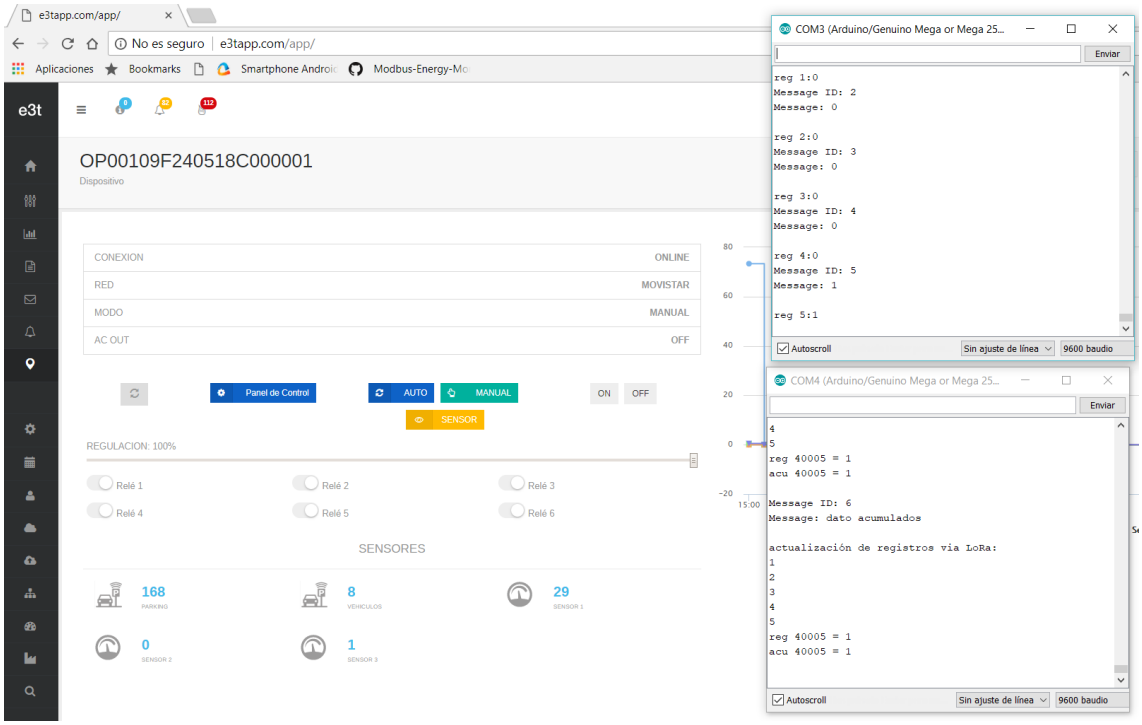


Figura 42. Entrada de un vehículo.

Tras haber tenido éxito en esta prueba, podemos dar por finalizado esta parte del proyecto en la que se pretende confirmar que somos capaces de obtener una solución valida con ayuda de LoRa y Modbus.

Capítulo 5. Conclusiones

En el desarrollo de tecnología RF dentro de la banda ISM, los factores más importantes a tener en cuenta son el alcance, la banda en la que se pretende operar y la capacidad de la red, siendo el consumo muy importante según qué casos, por ejemplo, si desea aislar en una zona de difícil acceso un equipo con batería. También es importante controlar el acceso a la comunicación, ya que en este tipo de bandas no suele ser difícil recibir los paquetes, por los que es preferible que se encripten los mensajes con un nivel de seguridad proporcional a la aplicación a ejecutar, ya que el acceso a la información que se transmite por parte de terceros puede ser crítico para que las soluciones desarrolladas por empresas puedan funcionar o simplemente no se desee que personas ajenas tengan acceso a ella.

Por otra parte, a la hora de combinar y traducir entre si distintos protocolos y vías de comunicación, es importante lograr que ambos puedan llegar a funcionar de manera semejante, ya que esto facilita y mucho el diseño y la implementación de la solución, pues el método para saltar de un protocolo a otro se ve gratamente facilitado.

Finalmente, para el caso de estudio, es importante que esta nueva manera de establecer comunicaciones sea lo más transparente posible para las tecnologías ya existentes a las que se desea incorporar esta nueva funcionalidad, de no ser así, no solo se tendría que desarrollar la nueva forma de comunicación, sino que haría falta readaptar la tecnología ya existente, lo cual lleva más carga de trabajo y más dificultades de cara a un funcionamiento genérico.

5.1 Cumplimiento de objetivos

Tal como se ha ido comprobando en las pruebas ejecutadas, se puede concluir que hasta este punto del proyecto se ha tenido éxito y puede ser una solución implementable.

El primer hito importante ha sido demostrar en el apartado 4.5.5 que se es capaz de comunicar en el alcance previsto en las especificaciones, el cual era 100 metros, e incluso superarlo, lo que ya hace posible su implementación en una instalación real.

El siguiente y más importante hito, ha sido con el que se han concluido las pruebas de funcionalidad en el apartado 4.5.8, en el cual no solo se ha visto como funciona el envío de datos Modbus vía LoRa y viceversa, sino que además es posible la comunicación con equipos de Datakorum y los datos son subidos a la nube, lo cual es la motivación y objetivo final de este proyecto.

Pese a que todas las pruebas e implementaciones han acabado resultando exitosas, son estos dos hitos los que dan lugar a decir que se han cumplido los objetivos del proyecto, y tal como se desarrollará en el apartado siguiente, se puede pasar ya a hablar de líneas futuras de actuación para el depurado, la mejora y profesionalización del desarrollo del proyecto y el producto final.

5.2 Líneas futuras de actuación

El desarrollo de este proyecto final de grado, es una primera etapa de un proyecto mayor para Datakorum. Como labores inmediatas tras lo llevado a cabo hasta este momento, queda desarrollar un prototipo más profesional con el que poder seguir realizando pruebas y mejoras, entre otras, una mejora del alcance eficaz y una depuración del funcionamiento a fin de realizar el mínimo de modificaciones conforme aumente la complejidad de las soluciones o se desarrollen nuevas tecnologías.

Se pretende desarrollar un hardware para el equipo final que permita tanto incorporarlo dentro de los equipos que ya existen como emplazarlo dentro de una carcasa independiente, de tal manera que pueda ser una funcionalidad ya incorporada o una expansión para algo ya existente.

El abanico de soluciones al que se pretende incorporar este nuevo dispositivo es mucho más amplio que el caso de los parkings puesto como ejemplo para la prueba. Entre las diferentes soluciones a las que es aplicable se encuentra el control de edificios, soluciones de alumbrado

pública, sistemas de control de consumo eléctrico, monitorización de entornos y parámetros ambientales e incluso el control y la actuación orientada a labores agrícolas, por lo que haciendo incidencia en el apartado de la profesionalización del proyecto, cuanto más genérico alcance a ser el dispositivo, mayor aplicabilidad, utilidad y ahorro podrá proporcionar.

Bibliografía.

[1] Mónica Tilves. «A fondo: IoT en España, mucho más que hogares conectados». [En línea]. Disponible en: https://www.silicon.es/a-fondo-iot-espana-mas-que-hogares-conectados-2314975?inf_&inf_by=5a7dbd44671db820288b4aca.

[2] «Home - WEMOS.CC». [En línea]. Disponible en: https://www.wemos.cc/.

[3] «Z-Wave», *Wikipedia*. 25-may-2018.

[4] «- The Internet of Things is powered by Z-Wave.», *Z-Wave Alliance*. [En línea]. Disponible en: https://z-wavealliance.org/.

[5] «Zigbee», *Wikipedia*. 09-may-2018.

[6] «About Us | Zigbee Alliance». Disponible en: http://www.zigbee.org/zigbee-for-developers/about-us/.

[7] «6LoWPAN», *Wikipedia*. 07-may-2018.

[8] «Sigfox», *Wikipedia*. 03-may-2018.

[9] «Descripción general de la plataforma LoRa | DigiKey». [En línea]. Disponible en: https://www.digikey.com/es/articles/techzone/2017/jun/develop-lora-for-low-rate-long-range-iot-applications.

[10] «About LoRa Alliance™ | LoRa Alliance™». [En línea]. Disponible en: https://lora-alliance.org/about-lora-alliance.

[11] «RN2483 - Wireless Modules - Microcontrollers and Processors». [En línea]. Disponible en: http://www.microchip.com/wwwproducts/en/rn2483.

[12] «Welcome to " Universal Scientific Industrial (Shanghai) Co., Ltd.» [En línea]. Disponible en: http://www.usish.com/english/pressroom_more.php?n_sn=23.

[13] «I-NUCLEO-LRWAN1 - USI® STM32™ Nucleo expansion board for LoRa™ - STMicroelectronics». [En línea]. Disponible en: http://www.st.com/en/evaluation-tools/i-nucleo-lrwan1.html.

[14] «Ra-01/Ra-02 LoRa 模块用户手册 [安信可科技]». [En línea]. Disponible en: http://wiki.ai-thinker.com/lora/man%60.

[15] S. Mistry, *arduino-LoRa: An Arduino library for sending and receiving data using LoRa radios*. 2018. Disponible en: https://github.com/sandeepmistry/arduino-LoRa.

[16] «MCP9700A-E/TO Microchip Technology | Sensors, Transducers | DigiKey». [En línea]. Disponible en: https://www.digikey.com/product-detail/en/microchip-technology/MCP9700A-E-TO/MCP9700A-E-TO-ND/1212508.

[17] «HIH-5030-001 Honeywell Sensing and Productivity Solutions | Sensors, Transducers | DigiKey». [En línea]. Disponible en: https://www.digikey.com/product-detail/en/honeywell-sensing-and-productivity-solutions/HIH-5030-001/480-3294-1-ND/2061078.

[18] samuel, *Modbus-Master-Slave-for-Arduino: Modbus Master-Slave library for Arduino*. 2018. Disponible en: https://github.com/smarmengol/Modbus-Master-Slave-for-Arduino/blob/master/ModbusRtu.h.