Diseño de una Arquitectura para la Comunicación entre Protocolos en IoT

Marco Córdoba Padilla, Frank Trejos Moya, Fernando Chinchilla Jiménez y Antonio González Torres*

Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
[mcordobap487,ftrejosm824,fchinchillaj980]@ulacit.ed.cr
agonzalez@ulacit.ac.cr*
http://www.ulacit.ac.cr

Resumen El uso de Internet y las tecnologías relacionadas se ha incrementado con el paso del tiempo. En ese contexto, Internet de las Cosas (IoT) ha entrado a jugar un papel de importancia con una gran cantidad de dispositivos y aplicaciones para ofrecer servicios y soluciones novedosas, que en muchos casos están atadas a protocolos y fabricantes particulares. De esta forma que la principal riqueza de IoT (la variedad de dispositivos, protocolos y fabricantes) se ha convertido en el mayor reto para garantizar la utilidad máxima de las posibilidades detrás de este concepto. La diversidad de IoT permite solucionar problemas de diferentes maneras, con costos y calidad variables, pero introduce dificultades relacionadas con la compatibilidad cuando se intenta realizar combinaciones específicas para resolver problemas particulares. El objetivo de este trabajo de investigación es proponer el diseño de una arquitectura de bajo costo basada en una puerta de enlace para facilitar la interconexión de dispositivos y protocolos diversos. Con ese fin se lleva a cabo la discusión sobre los diferentes elementos que componen la arquitectura de un sistema IoT, se estudian los principios de las puertas de enlace, se realiza la propuesta del diseño y se presenta un posible escenario de uso.

Palabras clave: Internet de las Cosas, Protocolos, Comunicaciones

1. Introducción

En años recientes ha surgido un gran número de dispositivos que se caracterizan por sus excelentes capacidades de comunicación, bajo costo y consumo energético, y sus capacidades reducidas tanto de procesamiento como de almacenamiento. Estos dispositivos han sido agrupados bajo el concepto de Internet de las Cosas[1] y se usan en áreas tan diversas como el transporte, la seguridad,

[1] Internet de las Cosas se deriva de Internet of Things en inglés y se asocia con las siglas IoT.

la salud, el seguimiento de los signos vitales de las personas, la inteligencia ambiental, la iluminación, el control de la temperatura de edificios y el acceso a áreas restringidas. En general, su uso está ligado con la búsqueda de mejoras a los procesos de las organizaciones y la calidad de vida de las personas.

Conforme el concepto de Internet de las Cosas (Ashton, 2009) ha tomado fuerza en años recientes, han surgido de forma masiva tanto fabricantes como nuevos dispositivos. A finales del 2015 el número de desarrolladores de aplicaciones y soluciones de IoT superó los $6,2$ millones (Rana, 2016), y mostró un crecimiento del $34\,\%$ con respecto al año anterior. Este crecimiento ha sido empujado por la caída en los costos de los dispositivos y el acceso a Internet.

Lo anterior, ha impulsado la rápida evolución de nuevas tecnologías, pero ha originado problemas de integración e interconexión entre los dispositivos producidos por diferentes fabricantes, debido a la ausencia de un protocolo o pila de protocolos dominante, como el caso de TCP/IP en las redes tradicionales[2]. A esto también ha contribuido la necesidad de desarrollar dispositivos especializados con características propias y diferenciadas, para resolver problemas particulares y complejos, que por lo general, requieren el uso de dispositivos de varios fabricantes.

Como parte de los esfuerzos que realizan los fabricantes para lograr mayor capacidad de interconexión, se han establecido varias alianzas para impulsar el desarrollo y crecimiento de IoT a través de la investigación y creación de nuevos productos. Tal es el caso de Z-Wave Alliance (T. Z.-W. Alliance, 2016), la cual impulsa el desarrollo del protocolo con el mismo nombre, y que desde su establecimiento en el 2005 ha incorporado a 375 compañías. Otro caso similar es la alianza (Z. Alliance, 2016) de fabricantes de dispositivos que utilizan el protocolo inalámbrico ZigBee, conformada por más de 400 compañías que utilizan dicho protocolo.

Sin embargo, la necesidad de realizar diseños en los cuales conviven e interactúan diferentes protocolos en un mismo sistema IoT sigue siendo una prioridad, porque la interoperabilidad entre estos (James Manyika y Dobbs, 2016) puede contribuir a generar ingresos adicionales a la industria en $40\,\%$.

Este trabajo propone un diseño para que los protocolos más utilizados en IoT puedan comunicarse usando una arquitectura basada en una puerta de enlace[3]. El principal aporte del trabajo realizado es la propuesta de una arquitectura de bajo costo para comunicar dispositivos y protocolos heterogéneos en el contexto de IoT.

Como consecuencia, la sección 2 analiza los principales elementos de una arquitectura de IoT, discute los conceptos relacionados con la interconexión entre dispositivos y estudia los fundamentos de las puertas de enlace. Con base en la información presentada en la sección 2, la sección 3 presenta el diseño de una

[2] Los dispositivos de Internet de las Cosas, en su mayoría, utilizan protocolos simples que requieren contar con menos capacidad de procesamiento y consumo de energía que los dispositivos que utilizan TCP/IP.

[3] Las puertas de enlace permiten la comunicación entre dispositivos en diferentes segmentos de una red, en los cuales utilizan protocolos diversos.

arquitectura de IoT basada en una puerta de enlace y analiza un escenario de uso para dicha propuesta. Finalmente, la sección 4 discute las principales conclusiones del trabajo.

2. Antecedentes

La arquitectura de alto nivel de un sistema de IoT es similar a la arquitectura genérica de cualquier otro sistema y se compone de elementos de entrada, procesamiento y salida. La diferencia básica es que la entrada de datos se puede realizar por medio de sensores y la salida se puede efectuar con actuadores. Así, los datos se adquieren del entorno por medio de sensores, se transmiten a los dispositivos de control (procesamiento) usando tecnologías y protocolos de comunicación, y una vez que son procesados, el resultado es enviado a los actuadores para modificar, si es el caso, las condiciones del entorno.

El procesamiento de datos en un sistema IoT requiere de protocolos de comunicación para el intercambio de datos y de algoritmos para su tratamiento y análisis. Los algoritmos se encargan de procesar los datos e integrarlos, de conformidad con las relaciones de comunicación que se pueden formar entre los dispositivos y la arquitectura del sistema.

Los sistemas de esta naturaleza también pueden recibir entradas de los usuarios; por lo general en la forma de parámetros de configuración o de actuación con base en los resultados. De forma similar, estos sistemas también pueden producir salidas tradicionales a un monitor o impresora. Por lo tanto la interfaz del usuario suele estar vinculada al dispositivo controlador, y es utilizada para configurar y gestionar el sistema (ver figura 1 y tabla 1).

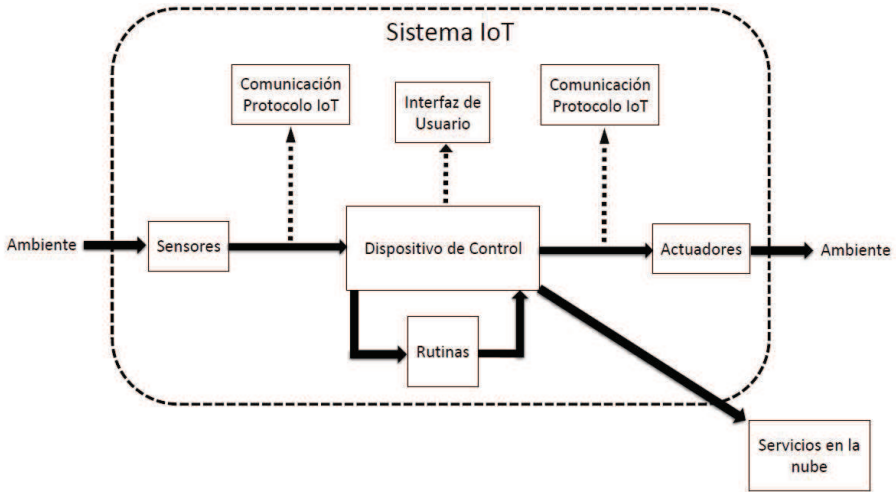

Figura 1. Elementos de la arquitectura de un sistema IoT

Conforme con lo anterior, la arquitectura de un sistemas de IoT, por lo general, se compone de los siguientes elementos o dispositivos:

Interfaz para la interacción con los usuarios (entrada y salida): la interfaz permite que el usuario configure el sistema, ingrese los parámetros de operación, revise resultados y ejecute operaciones. La función de la interfaz es facilitar el control y la administración de los dispositivos que conforman un sistema IoT. Cuando se adquiere un sistema de IoT, la interfaz de usuario puede venir incluida, pero cuando se desarrolla una solución personalizada es necesario hacerlo de acuerdo con los requerimientos del sistema.

Adquisición de datos del entorno (entrada): captura datos del entorno por medio de sensores y los envía al dispositivo de control para su procesamiento.

Protocolos de comunicación (procesamiento): se encargan del intercambio de información entre los dispositivos que conforman el sistema, y son un elemento crítico para su interconexión.

Equipo o software controlador (procesamiento): es el equipo que recibe los datos de los sensores, los procesa y de acuerdo con rutinas pre-establecidas, envía órdenes a los actuadores.

Procesamiento y análisis de los datos obtenidos (procesamiento): lo conforman los algoritmos y métodos que se encargan del tratamiento y análisis de los datos. Los sistemas IoT pueden utilizar servicios en la nube para almacenar y acceder recursos como bases de datos (e.g., SQL, NoSQL y NewSQL), servicios web y servidores.

Ejecución de tareas (salida): cuando la salida del sistema conlleva una actuación sobre el entorno, se ejecutan acciones por medio de actuadores para modificar determinadas condiciones. Pero cuando se busca modificar las condiciones del entorno, las tareas que se llevan a cabo pueden consistir en el análisis o ejecución de tareas adicionales de procesamiento.

Despliegue de resultados (salida): los resultados se pueden desplegar en un monitor para que el usuario tenga conocimiento de las actuaciones que realiza el sistema, o simplemente para que conozca el procesamiento, de forma similar a los sistemas tradicionales.

Una arquitectura más compleja es la propuesta por Intel (Intel, 2015), la cual contempla el uso de un gran número de protocolos de comunicación, conexión a sistemas de almacenamiento y análisis y, servidores locales y en la nube.

2.1. Interconexión de dispositivos

Las topologías de comunicación de los sistemas IoT se pueden clasificar como uno a uno (punto a punto), uno a muchos (estrella) y muchos a muchos (malla) (Pacelle, 2014). Según el tipo de topología que se utilice, los datos pueden ser recibidos, integrados y procesados por solo un dispositivo (el cual cumple la función de controlador general) o por cada dispositivo en el sistema.

En cualquiera de las topologías señaladas, los dispositivos receptores y transmisores conforman segmentos de comunicación (ver figura 1) que pueden utilizar diferentes protocolos. La clasificación genérica de estos segmentos es la siguiente:

- Sensor - Dispositivo de control
- Dispositivo de Control – Actuador

Los requerimientos de los sistemas de IoT con frecuencia requieren el uso de dispositivos con funciones especializadas y características específicas. Es común que se requiera dispositivos de diferentes fabricantes, los cuales pueden utilizar protocolos, medios de transmisión y distancias de cobertura distintas. Entre los protocolos de comunicación más utilizados en IoT se encuentran X10 (Cuevas, Martínez, y Merino, 2002), NFC, ZigBee, Bluetooth, RFID (Chavarría, s.f.), KNX (Jara Maldonado, 2015), Z-Wave (Buxeres Soler, 2014) y SigFox(Cárdenes Tacoronte, 2016) (ver tabla 1).

Protocolo	Uso	Frecuencia	Cobertura	Otras características
X1O	Red eléctrica doméstica	120 KHz	N/A	Utiliza la red eléctrica doméstica como medio de transmisión
NFC	Aplicaciones con poco volumen de datos	13,56 MHz	10 cm	Diseñado para aplicaciones de autenticación
KNX	Domótica	N/A	N/A	Paralelo a la red eléctrica
ZigBee	Datos inalámbricos	868 GHz 915 GHz 2,4 GHz	10 a 75 m	Diseñado para bajo consumo de energía
Z-Wave	Datos inalámbricos	Menos de 1 GHz (varía según el país)	30 a 200 m	Tranmisión de baja potencia
Bluetooth	Datos inalámbricos	2,4 GHz	10 m	Utiliza enlaces de frecuencia libre
RFID	Datos inalámbricos	9-135 KHz 13,56 MHz 433 MHz y 860-960MHz 2,45-5GHz	2 a 100 m	Tecnología con mayor rango de aplicaciones por las frecuencias en las que opera
SIGFOX	Smart Cities	868 o 902 MHz	3 a 5 Km	Se considera la mejor opción para Smart Cities por la distancia que logra abarcar

Cuadro 1. Comparación de los protocolos más utilizados por IoT

Algunos protocolos mencionados en la tabla 1 comparten ciertas características, como el tipo de aplicación o frecuencias de comunicaciones que utilizan, pero difieren en otras. Esto conlleva a problemas de compatibilidad que les impiden

interconectarse y requiere el uso de puertas de enlace para la interconexión de dispositivos que usan diferentes protocolos.

2.2. Puertas de enlace

Las puertas de enlace cumplen varias funciones; además de servir como intermediarias en la comunicación entre dispositivos. Esas funciones pueden incluir el procesamiento de información, gestión de la seguridad y controlador o administrador del sistema.

Las puertas de enlace puede ser implementadas por medio de software o hardware. En el caso de la implementación por software, por lo general se lleva a cabo usando bibliotecas internas. Estas bibliotecas se componen de interfaces programadas por los mismos desarrolladores de los protocolos, o por terceros. El código fuente y admite la posibilidad de agregarle funcionalidad a los protocolos. Estas interfaces son funciones que se pueden invocar desde diferentes lenguajes de programación. Por su parte, las puertas de enlace por hardware sirven como punto de interconexión de dispositivos por medio de interfaces físicas o procesadores de comunicaciones inalámbricas de distintos tipos.

El proceso de interconexión que realizan las puertas de enlace por software y hardware requiere la desencapsulación y encapsulación de datos, para decodificar y codificar la información en los formatos que utilizan tanto el origen como el destino de la comunicación. Esto implica que la puerta de enlace debe procesar las unidades de datos del protocolo (UDP) para cada capa del modelo o estándar de comunicaciones que utilizan los dispositivos en un segmento.

En el mercado se encuentran disponibles varias puertas de enlace, tanto de software como hardware. “Dell Edge Gateway”permite varias conexiones cableadas e inalámbricas (DELL, 2016b, 2016a) para interconectar protocolos como ZigBee, BACnet y ModBus, entre otros. Mientras que “Intel IoT Gatewayçonsiste en una familia de productos (Intel, 2016) que permiten comunicar dispositivos por medio de ZigBee, Bluetooth, USB, VPN y Wi-Fi. Por su parte, Texas Instruments (Texas Instruments Incorporated, 2016) y EuroTech (Eurotech, 2016a, 2016b) también cuentan con puertas de enlace que tienen características similares a las mencionadas.

3. Propuesta de diseño

Las arquitecturas comerciales de IoT pueden resultar costosas, lo cual pone de relieve la necesidad de contar con un diseño cuya implementación sea sencilla y económica. Con base en ello, este trabajo propone el diseño de una arquitectura basada en una puerta de enlace que se compone de un dispositivo de control, módulos de comunicación y bibliotecas para el intercambio de información entre el dispositivo de control y los módulos (ver figura 2).

El diseño propuesto toma ventaja de la arquitectura de Raspberry Pi (Raspberry Pi Foundation, 2016) y la utiliza como dispositivo de control, por ser una computadora de diseño reducido y propiedad registrada; pero de uso libre, lo cual

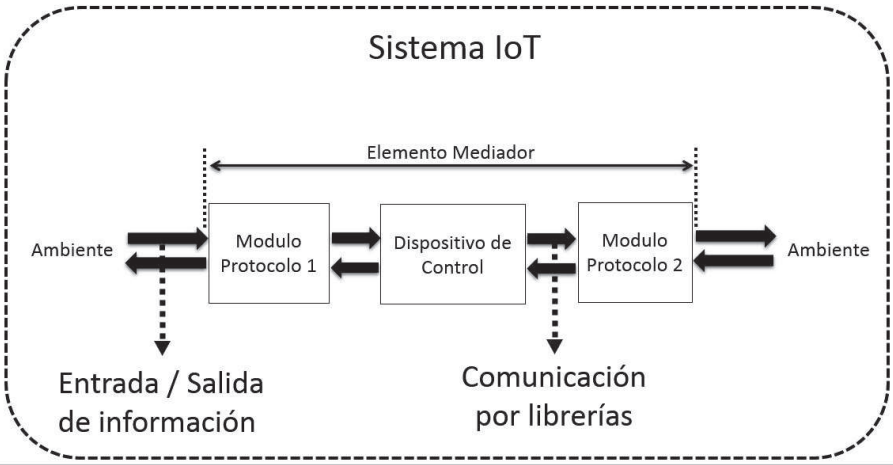

Figura 2. Arquitectura con dos módulos de comunicaciones

permite que los usuarios puedan modificar y agregar módulos de acuerdo con sus necesidades. Así, por ejemplo, es posible que agreguen módulos de memoria adicional u otros módulos para comunicarse con diferentes protocolos y tecnologías como ZigBee, Z-Wave, RFID, 3G y GSM. Además, es importante destacar que Raspberry Pi soporta el uso de Python, C, C++ y Ruby para programar diferentes algoritmos.

El sistema operativo oficial de Raspberry Pi es una versión adaptada de Debian, denominada como RaspBian, y el precio de los módulos de comunicación que se le pueden agregar es relativamente bajo. Esto hace que el costo de implementación de esta propuesta sea significativamente bajo, en comparación con las opciones de puertas de enlace propietarias que existen en el mercado.

El diseño propuesto contempla el uso de cualquiera de los protocolos de los módulos que soporta Raspberry Pi, pero cabe señalar que de acuerdo con la investigación realizada, los protocolos más utilizados por los sistemas IoT son Z-Wave y RFID.

3.1. Escenario de uso

Un edificio con un gran número de espacios cuenta con puertas de apertura y cierre automático, circuitos de iluminación, sistema de detección de incendios y cámaras de seguridad con sensores de movimiento.

Cada día por la mañana, se deben abrir las puertas, encender las luces de cada sitio de manera individual y revisar los videos de las cámaras. Este proceso, lo realiza solo una persona autorizada por razones de seguridad, pero presenta los siguientes inconvenientes:

- La apertura de puertas y encendido de luces toma 10 minutos en la mañana y 10 minutos por la tarde.

- El personal que trabaja en las instalaciones no puede ingresar antes de su hora de entrada oficial ni puede quedarse trabajando después de la hora de salida oficial. Esto afecta el desarrollo de algunos proyectos de alta prioridad debido al proceso burocrático para justificar las razones de una jornada diferente, y como consecuencia se activa un protocolo de seguridad especial.
- La revisión de los videos puede tomar varias horas, por lo que es frecuente que se realice cuando sucede un incidente.

En general, la administración no puede conocer detalles sobre los eventos que se generan en torno a la apertura de puertas, iluminación, alarmas de incendio y cámaras porque no cuenta con un sistema de alertas y estadísticas eficiente. Esto impide que los administradores puedan reaccionar a tiempo ante emergencias o variaciones en los patrones de comportamiento de los funcionarios y visitantes. Por lo tanto la organización y el escenario descrito requieren considerar el diseño e implementación de los siguientes sistemas:

Control: el fin de este sistema es controlar las luces, sensores de incendios, cámaras y la apertura de puertas utilizando los protocolos RFID y Z-Wave.

Gestión: el objetivo de este sistema es realizar el procesamiento de la información, enviar notificaciones de emergencia y realizar el análisis de patrones de identificación y comportamiento a partir de la información de los sensores y vídeos.

Conforme con lo anterior, el funcionamiento del subsistema de iluminación, apertura y cierre de puertas para este escenario se plantea de la siguiente forma:

- El personal autorizado cuenta con una tarjeta RFID como medio de identificación, cuya lectura es realizada por un módulo RFID.
- Una vez que la persona ha sido identificada, el sistema realiza la apertura de las puertas y el encendido de las luces mediante el envío de señales a los dispositivos Z-Wave.
  - Las luces se encienden por medio de un apagador Z-Wave.
  - La apertura de puertas se hace usando una cerradura de puerta Z-Wave.

Este subsistema requiere codificar cada tarjeta RFID con los datos personales del empleado correspondiente, realizar la configuración de la red de dispositivos Z-Wave de acuerdo con las instrucciones de los fabricantes y programar los scripts en un lenguaje de programación, como Python. Las rutinas que deben comprender los scripts cuando el lector RFID detecta una tarjeta son las siguientes:

- Encender los circuitos de luces y abrir la cerradura de las puertas, si la última condición de las luces es “apagado” y la condición de las cerraduras es “cerrado”.
- Apagar los circuitos de luces y cerrar las puertas si la última condición de las luces es “encendido” y la condición de las cerraduras es “abierto”.

En cuanto al sistema de gestión de eventos y análisis de patrones, este se encuentra conformado por el dispositivo de control y el sistema de análisis (localizado en la nube). La secuencia de funcionamiento y procesamiento de este sistema se realiza de acuerdo con los siguientes pasos:

Dispositivo de control: este dispositivo recibe datos de los diferentes dispositivos y envía notificaciones a las personas designadas por medio de un APP, de acuerdo con las reglas que tiene configuradas.

Procesamiento en la nube: el dispositivo de control además envía los datos de todos los eventos e imágenes que registran las cámaras a un sistema de análisis en la nube.

Sistema de análisis: este sistema se encuentra en la nube. Se encarga de procesar los datos conforme los recibe e integra los resultados del procesamiento con los resultados históricos. El análisis que realiza este sistema contempla desde los eventos relacionados con la apertura y cierre de puertas, encendido de luces y movimientos registrados por los sensores hasta el análisis de imágenes captadas por las cámaras con el fin de identificar personas y sus patrones de comportamiento.

Estadísticas y patrones: los resultados del análisis son representados de forma visual para hacerlos más comprensibles y útiles para los usuarios.

En cuanto a la implementación del sistema completo, se requieren los siguientes componentes de hardware:

Dispositivo de control - Raspberry Pi (PCB): este dispositivo se describe como una mini-computadora con todas las características necesarias para realizar las tareas de control y procesamiento de datos, pero además se conecta a la nube para enviar datos para su almacenamiento y procesamiento. El modelo utilizado debe contar con puerto Ethernet o conexión usando 802.11n.

Módulos Z-Wave: se recomienda utilizar Razberry (RaZberry, 2016) para permitir la comunicación de sensores y actuadores que usan Z-Wave. En concreto, los dispositivos que utilizaran Z-Wave son los apagadores de luces, los elementos de cierre y apertura de puertas, los sensores de incendios y las cámaras.

Razberry cuenta con una interfaz de usuario que permite su rápida implementación, pero también facilita el desarrollo de interfaces personalizadas por encontrarse disponible la documentación del fabricante para ese fin.

Módulo RFID: este módulo permite la lectura de las tarjetas RFID y mantiene activado en modo de lectura al dispositivo de control (Raspberry Pi) para que capte las señales transmitidas por los “tags” RFID.

4. Conclusiones

Este trabajo de investigación llevó a cabo una revisión bibliográfica sobre los principales protocolos y arquitecturas que se utilizan en IoT. Dicha revisión

permitió analizar y discutir sobre el estado actual de Internet de las Cosas y las implicaciones que tiene el uso de protocolos diferentes en los procesos de interconexión y comunicación.

Como resultado, fue posible conocer con mayor detalle y poner de manifiesto la relación que existe entre los protocolos, dispositivos, fabricantes y arquitecturas en el proceso de comunicación. Esto permitió proponer una arquitectura de bajo costo para la interconexión de protocolos y dispositivos heterogéneos en sistemas IoT.

Las ventajas del diseño presentado son su sencillez, posibilidades que ofrece para la interconexión, facilidad de implementación y bajo costo. Esto lo hace ideal para que sea utilizado para resolver problemas de poca y media complejidad, con personal poco especializado y sin necesidad de incurrir en altos costos.

La arquitectura, además incorpora elementos de análisis de información, tanto local como en la nube, para conocer con mayor detalle los eventos y procesos que han sido atendidos y procesados por el sistema.

Como trabajo futuro, se estará realizando la implementación de la arquitectura propuesta y se estarán desarrollando casos de uso de mayor complejidad para validar la arquitectura y agregar factores de la escalabilidad a la propuesta.

Referencias

Alliance, T. Z.-W. (2016). *The Internet of Things is powered by Z-Wave.* Descargado de `http://z-wavealliance.org/` pages 2

Alliance, Z. (2016, July). *The ZigBee Alliance creates IoT standards that help Control Your World.* Descargado de `http://www.zigbee.org/zigbeealliance/` pages 2

Ashton, K. (2009, June). *That 'Internet of Things' thing.* Descargado de `http://www.rfidjournal.com/articles/view?4986` pages 2

Buxeres Soler, A. (2014). Estudio y desarrollo de un sistema basado en una librería abierta para el uso del protocolo inalámbrico de domótica Z-Wave. pages 5

Cárdenes Tacoronte, D. (2016). Diseño e implementación de una herramienta para la verificación de cobertura de la red SIGFOX. Estudio de conectividad en una zona geográfica de orografía compleja. pages 5

Chavarría, D. A. C. (s.f.). Tecnología de comunicacionón de campo cercano (nfc) y sus aplicaciones. pages 5

Cuevas, J. C., Martínez, J., y Merino, P. (2002). El protocolo x10: una solución antigua a problemas actuales. En *Simposio de informática y telecomunicaciones (sit).* pages 5

DELL. (2016a). *Dell Edge Gateways for IoT.* Descargado de `http://www.dell.com/us/business/p/edge-gateway?s=bsd` pages 6

DELL. (2016b). *Edge Gateway 5000.* Descargado de `http://www.dell.com/us/business/p/dell-edge-gateway-5000/pd?ref=PD_OC` pages 6

Eurotech. (2016a). *IoT Gateways: Multi Service IoT Gateways.* Descargado de https://www.eurotech.com/en/products/devices/iot+gateways pages 6

Eurotech. (2016b). *ReliaGATE 10-11: Compact Multi-Service IoT Gateway, Industrial-grade, TI AM3352.* Descargado de https://www.eurotech.com/en/products/ReliaGATE%2010-11 pages 6

Intel. (2015). *Intel IoT Platform Reference Architecture.* Descargado de http://www.intel.com.au/content/dam/www/public/us/en/documents/white-papers/iot-platform-reference-architecture-paper.pdf pages 4

Intel. (2016). *Intel IoT Gateway Technology.* Descargado de https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html pages 6

James Manyika, J. W., y Dobbs, R. (2016). *Unlocking the potential of the Internet of Things.* Descargado de http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world pages 2

Jara Maldonado, P. A. (2015). Estudio y diseño de un sistema inmótico para seguridad, comunicación y confort, utilizando el protocolo KNX para el edificio Torre Piamonte ubicado en el sector de Totoracocha de la ciudad de Cuenca.
pages 5

Pacelle, M. (2014, April). *3 topologies driving IoT networking standards.* Descargado de http://radar.oreilly.com/2014/04/3-topologies-driving-iot-networking-standards.html pages 4

Rana, M. (2016, June). *Thirty-four Percent Rise in IoT Development.* Descargado de http://www.evansdata.com/press/viewRelease.php?pressID=237 pages 2

Raspberry Pi Foundation. (2016). *Raspberry Pi Foundation.* Descargado de https://www.raspberrypi.org/ pages 6

RaZberry. (2016). *RaZberry Project.* Descargado de https://razberry.z-wave.me/ pages 9

Texas Instruments Incorporated. (2016). *HVAC Gateway.* Descargado de http://www.ti.com/solution/iot_gateway pages 6