Internet de las Cosas (Internet of Things)

Ing. Alvaro Sanchez

Ing. José Restaino

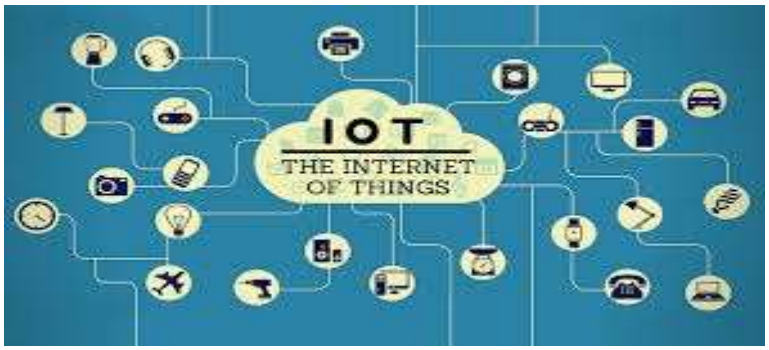
IoT

- El desarrollo de Internet en el siglo XXI, y el involucramiento de casi todas las actividades humanas con las prestaciones que brinda, han hecho aparecer nuevas tendencias tecnológicas, tales como Big Data, Cloud Computing e IoT. No solo se interconectan personas, sino también dispositivos y sensores. En ese contexto surge el término “Internet de las Cosas”, para designar a la interconexión de diversos dispositivos a Internet, para la recolección de datos en tiempo real.
- Entre los dispositivos se incluyen electrodomésticos, vehículos, edificaciones, etc., en los cuales se ubican medidores de temperatura, verificadores de ocupación, geolocalizadores, detectores de humo, y otros sensores de muy variados parámetros.
- El procesamiento de los datos permite prever acciones de seguridad, de administración logística, etc.
- Las redes de IoT suelen enfrentar desafíos relativos a la transmisión de datos de grandes cantidades de sensores hacia un local central, y al consumo de energía de cada sensor, lo que determina la duración de sus baterías.
- La implementación de este tipo de soluciones permite una sustancial mejora en la calidad de vida.

2

IoT

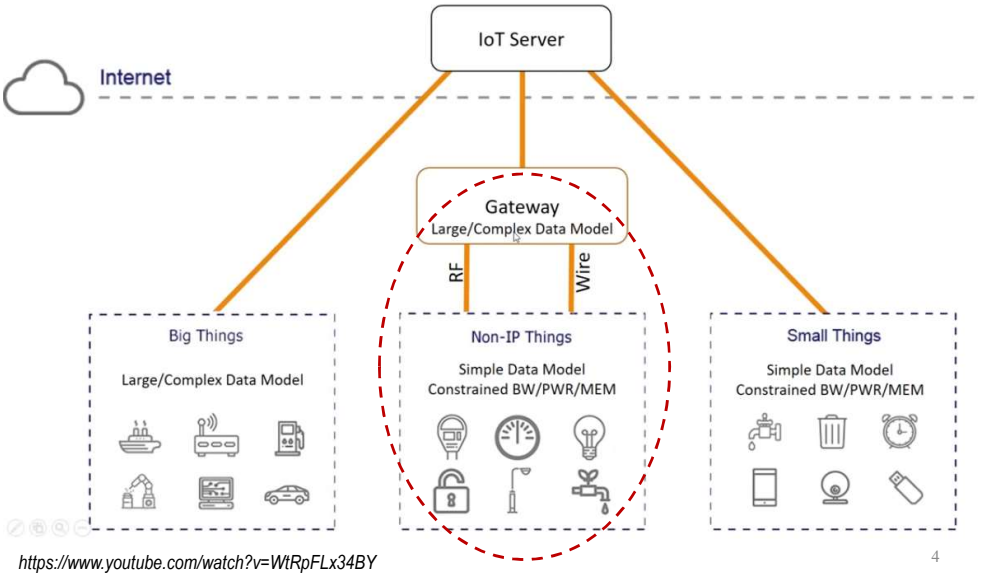
- Se estima que habrá 500 mil millones de dispositivos conectados a Internet para 2030 según un estudio de CISCO. Cada vez es mayor la cantidad y la variedad de dispositivos que pueden conectarse a internet. Contamos con teléfonos, electrodomésticos, automóviles, con acceso a las redes, ya no somos sólo las personas, sino también estos objetos o cosas cotidianas de nuestro entorno quienes se conectan a la red para aprovechar sus beneficios. Internet de las Cosas permitirá que podamos integrar objetos inteligentes de todo tipo y función, redes de sensores, y recursos de la Internet actual con las personas.



3

IoT

¿Internet de qué cosas?

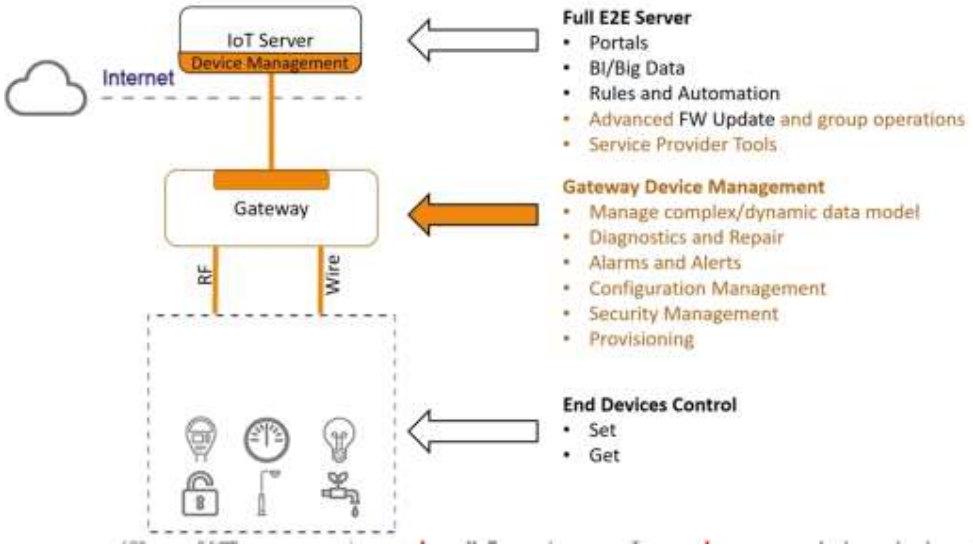


https://www.youtube.com/watch?v=WtRpFLx34BY

4

IoT

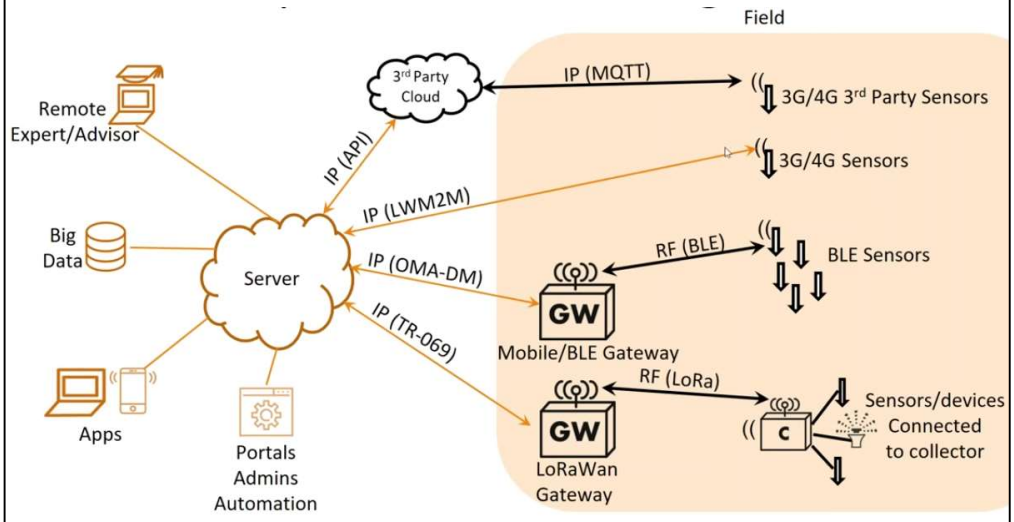
¿Internet de qué cosas?



IoT

¿Internet de qué cosas?

Posible arquitectura para agricultura



Cosas (Things)

Sensores

- Para recolectar información en un determinado sitio, para su posterior transmisión a través de Internet, se necesita disponer de **sensores**.
- Una vez obtenida la información, se necesita transmitirla por algún medio cableado o inalámbrico, al centro de procesamiento de la información, para lo cual puede recurrirse a concentradores de datos intermedios llamados “gateways”.
- La cantidad de sensores dispersos en diversos sitios puede plantear problemas tales como:
  - el grado de visibilidad entre el sensor y el objetivo a medir
  - la posible colisión de las transmisiones,
  - la lejanía entre cada sensor y el colector de datos al cual debe transmitir,
  - la posible necesidad de transmisión bidireccional,
  - la conveniencia de lograr la geolocalización, etc.

IoT

Tipos de sensores

- *Sensores de proximidad*: Estos sensores detectan movimiento y son frecuentemente usados en una configuración al detalle. Un revendedor puede usar la proximidad de un cliente con un producto para enviar ofertas y cupones directamente al smatphone. Sensores de proximidad también pueden ser usados para monitorear la disponibilidad de lugares de estacionamiento en grandes espacios como aeropuertos, centros comerciales y estadios.
- *Acelerómetro y giroscopio:* El acelerómetro es un instrumento utilizado para detectar vibraciones, inclinación y aceleración lineal. El giroscopio es usado para medir la velocidad angular y es utilizado principalmente en los mouses (ratones) 3D, en juegos y en entrenamientos de atletas profesionales.
- *Sensores de temperatura:* Se pueden usar esos dispositivos en casi todos los ambientes de IoT, desde el piso de la fábrica hasta los campos agrícolas. En las fábricas, estos sensores pueden medir continuamente la temperatura de una máquina para garantizar que permanezca dentro de un límite seguro. En las haciendas, pueden ser utilizados para rastrear la temperatura del suelo, agua y plantas para maximizar la producción.

IoT

Tipos de sensores

- *Sensor de humedad:* Semejante al sensor de temperatura, también se lo usa para controlar el desempeño de dispositivos. Se lo define como analógico o digital. Un sensor de humedad analógico marca la humedad relativa del aire utilizando un sistema capacitivo, que son los más utilizados. Este tipo de sensor es revestido generalmente de vidrio o cerámica. El material aislante que absorbe todo el agua, es hecho de un polímero que recibe y suelta el agua según la humedad relativa de una determinada área. Eso modifica el nivel de carga presente en el capacitor de placa de circuito eléctrico. El digital funciona a través de dos microsensores que son calibrados con la humedad relativa de un área. Ellos son convertidos en un formato digital por un proceso de conversión analógico a digital, realizado por un chip localizado en el mismo circuito. Una máquina con un sistema de electrodos hechos de polímeros es lo que produce la capacidad del sensor. Además, existen los sensores de humedad de suelo que son bastantes utilizados por productores agrícolas para medir las tasas de humedad antes, durante y después de la plantación y colecta.

IoT

Tipos de sensores

- *Sensor de presión:* La agricultura es la mayor usuaria y el área que más desperdicia agua en el mundo. Los agricultores usan el 70% del agua dulce del mundo, pero el 60% es desperdiciada debido al uso de sistemas de irrigación con fuga, métodos de aplicación ineficientes y el cultivo de culturas sedientas, de acuerdo con World Wildlife Fund. Los sensores de presión pueden ser utilizados para determinar el flujo de agua a través de tubos y para notificar a una persona o al equipo responsable cuando algo necesite ser corregido. Ellos también son usados en vehículos inteligentes y aeronaves para determinar la fuerza y la altitud, respectivamente.
- *Sensores de nivel:* Los sensores de nivel detectan el nivel de líquidos y otros fluidos, incluyendo suspensiones y materiales granulares, puesto que exhiben una superficie superior. Los sensores de nivel pueden ser usados para fines de gestión inteligente de residuos y reciclaje. Otras aplicaciones incluyen medir niveles de tanque, medición de combustible diesel, inventario de activos líquidos, alarmas de nivel alto o bajo, y control de irrigación.

IoT

Tipos de sensores

- *Conclusión:* Estas son algunas de las aplicaciones más comunes de sensores para IoT. Naturalmente, los vehículos autónomos poseen las tecnologías de los sensores, incluyendo sensores de fuerza, carga, tensión y torsión, así como sensores de movimiento, velocidad, desplazamiento, posición, vibración y choque. Incluso con estas adiciones, no existen decenas, sino centenas de otros datos que pueden ser analizados por los sensores.

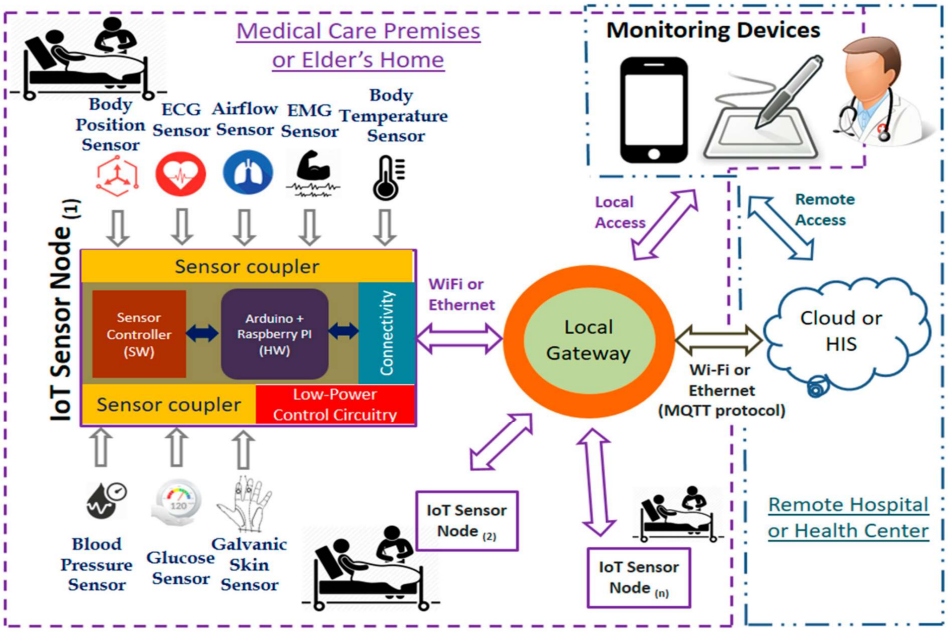
Tomado de: Canal Comstor, 'https://blogmexico.comstor.com/6-tipos-de-sensores-para-aplicacion-en-la-internet-de-las-cosas'.

Sensor de temperatura

Sensor de distancias

Sensor de humedad

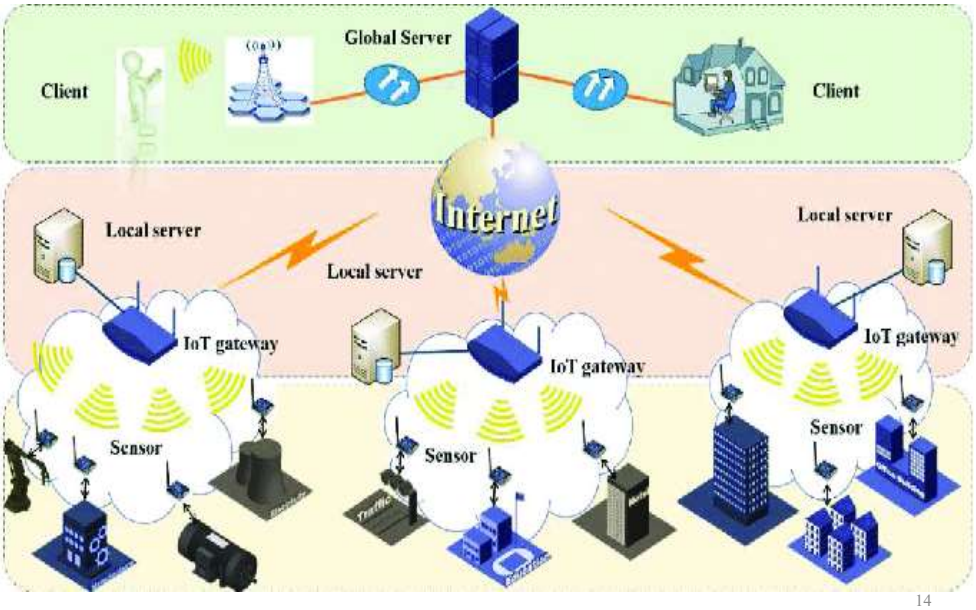
IoT


Medical Care Premises
or Elder's Home
Monitoring Devices
Body Position Sensor
ECG Sensor
Airflow Sensor
EMG Sensor
Body Temperature Sensor
IoT Sensor Node (1)
Sensor coupler
Sensor Controller (SW)
Arduino + Raspberry PI (HW)
Connectivity
Sensor coupler
Low-Power Control Circuitry
WiFi or Ethernet
Local Gateway
Local Access
Remote Access
Cloud or HIS
Wi-Fi or Ethernet (MQTT protocol)
Blood Pressure Sensor
Glucose Sensor
Galvanic Skin Sensor
IoT Sensor Node (2)
IoT Sensor Node (n)
Remote Hospital or Health Center

Información a transmitir

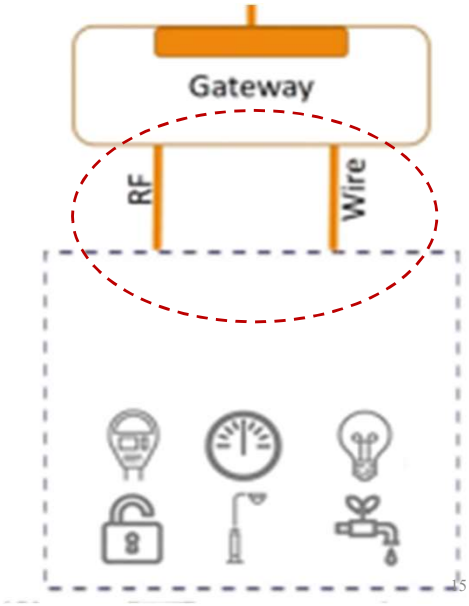
- Las características de la información a transmitir son determinantes para el diseño adecuado de la red IoT.
- Entre esas características se incluyen:
  - la cantidad de información de cada mensaje,
  - la frecuencia de envío de mensajes,
  - la viabilidad de interrogaciones cíclicas, o la necesidad de transmisión "espontánea" de avisos o alarmas,
  - la necesidad de confirmar la recepción de los mensajes y de retransmitirlos en caso de no confirmar su recepción.
- Las características anteriores determinan el tipo de tecnología de transmisión a emplear entre los sensores y la red, o bien entre los sensores y los gateways.

Tecnologías de transmisión para IoT



Tecnologías de transmisión para IoT

- Veremos algunas alternativas de redes de distintos alcances para la comunicación entre los sensores y el gateway



Tecnologías de transmisión para IoT

- **PAN: Personal Area Network**

  Una PAN (Personal Area Network - Red de Área Personal) es una red de espacio personal del tamaño de área que puede cubrir la voz humana. Estas redes permiten intercambiar información entre computadoras, teléfonos celulares, auriculares y otros dispositivos. Las tecnologías más utilizadas en estas redes son NFC (ISO/IEC 18000-3), ZigBee (IEEE 802.15.4), Bluetooth y Wi-Fi. Respecto de IoT, las redes WPAN se utilizan para la comunicación de las aplicaciones de control y monitorización (porque la mayoría de las tecnologías son inalámbricas). La tecnología ZigBee (IEEE 802.15.4) es un protocolo que ha sido diseñado especialmente para la automatización del hogar. Las velocidades de estas tecnologías típicamente son relativamente bajas (del orden de pocos kbps hasta algunos Mbps) ya que están diseñadas para atender tanto a la velocidad de transmisión, como al consumo de energía..

Tecnologías de transmisión para IoT

PAN - Bluetooth

Bluetooth es una especificación para redes inalámbricas de área personal (WPAN), que permite la transmisión de datos entre diferentes dispositivos mediante un enlace de radiofrecuencia en la banda ISM de 2.4 GHz. Existen múltiples versiones y evoluciones con distintas características de velocidad y consumo de energía, entre otros aspectos.

Los dispositivos que con mayor frecuencia utilizan esta tecnología son los teléfonos móviles, computadoras, y accesorios relacionados a éstos. El rango de alcance de esta tecnología está en el orden de pocos metros. El alcance y bitrate varían según la versión.

Clase	Alcance
1	100 m
2	5-10 m
3	1 m

Bluetooth - Potencia y alcance

Versión	Bitrate
1.2	1 Mbps
2.0 + EDR	3 Mbps
3.0 + HS	24 Mbps
4.0	32 Mbps

Bluetooth – Bitrate

17

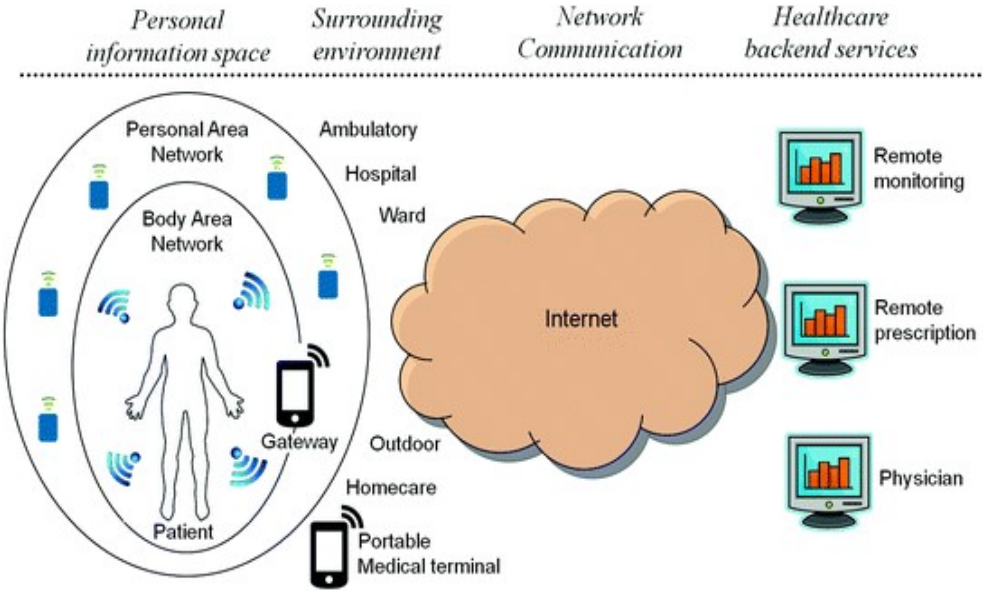
IoT

PAN - Bluetooth

- High speed communication over short distances
  - PAN (Personal Area Network)
- Connects our mobile devices
  - Smartphones
  - Tethering
  - Headsets and headphones
  - Health monitors
  - Automobile and phone integration
  - Smartwatches
  - External speakers

Tecnologías de transmisión para IoT

PAN - Bluetooth



IoT

PAN

Near field communication (NFC)

- Two-way wireless communication
  - Builds on RFID, which is mostly one-way
- Payment systems
  - Major credit cards
  - Online wallets
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

Tecnologías de transmisión para IoT

- **LAN: Local Area Network**

  Una LAN (Local Area Network - Red de Área Local) conecta varios dispositivos de red en un área de corta distancia, en el rango de cientos de metros según el medio de transmisión. Algunos formatos habituales son Ethernet sobre pares trenzados de cobre donde típicamente se alcanzan 90 metros según la versión, fibra óptica hasta algunos cientos de metros y Wi-Fi (IEEE 802.11 en sus múltiples versiones) algunas decenas de metros.

  Las velocidades de estas tecnologías son típicamente altas ya que en algunos casos son utilizadas por dispositivos que lo requieren y no tienen grandes restricciones de consumo de energía. Estas velocidades pueden variar desde unos pocos Mbps hasta algunos cientos de Gbps en las tecnologías actualmente disponibles.

Tecnologías de transmisión para IoT

LAN - Wi-Fi

Wi-Fi es una familia de tecnologías que permiten la interconexión inalámbrica de dispositivos electrónicos. Es una marca propiedad de la Wi-Fi Alliance, organización sin fines de lucro que adopta, prueba y certifica que los equipos cumplen los estándares IEEE 802.11 relacionados con redes inalámbricas de área local WLAN. Las distintas versiones de Wi-Fi (802.11 B/G/N/AC, entre otras) permiten distintas velocidades de transmisión (por ejemplo, 11 Mbps, 54 Mbps, 300 Mbps, 1.3 Gbps), entre otras características que las diferencian. Las distintas versiones utilizan bandas ISM de 2.4 GHz y 5 GHz.

Si bien los radios de cobertura teóricos son del orden de unos pocos cientos de metros según la versión, en la práctica (en ambientes urbanos, con interferencia, utilizando canales que están saturados debido a las bandas libres que utiliza, y con obstáculos como ser muros, vehículos u otros elementos de la vía pública) este radio de cobertura habitualmente no supera los 100 metros.

Existe abundante documentación, variedad de dispositivos y oferta de productos comerciales en el mercado ya que es considerada una tecnología robusta y madura.

Tecnologías de transmisión para IoT

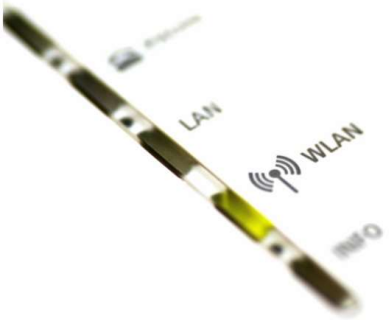
Wi-Fi

Característica / Versión	802.11a	802.11b	802.11g	802.11n	802.11ac
Frecuencia de Operación	5 GHZ	2.4 GHZ	2.4 GHZ	2.4 y 5 GHZ	5GHZ
Bitrate máximo	54 Mbps	11 Mbps	54 Mbps	150 Mbps	1300 Mbps
Alcance en exterior 120 m	140 m	140 m	250 m	250 m	
Ancho de Banda (MHz)	20	20/25	20	20/40	80/160
Año de liberación	1999	1999	2003	2009	2014

Tecnologías de transmisión para IoT

LAN - WiFi

- Wireless networking (802.11)
  - Managed by the IEEE LAN/MAN Standards Committee (IEEE 802)
- Many updates over time
  - Check with IEEE for the latest
- The Wi-Fi trademark
  - Wi-Fi Alliance handles interoperability testing



Tecnologías de transmisión para IoT

WAN: Wide Area Network

Una WAN (Wide Area Network - Red de Área Extensa) es una colección de múltiples redes LAN dispersas geográficamente (cientos de kilómetros una de otra).

Un ejemplo típico de una red WAN es Internet, en donde se resuelve la conectividad de redes ubicadas geográficamente en distintos países.

Las redes celulares (2G/3G/4G) permiten el acceso inalámbrico a las redes de datos.

Son desplegadas y administradas por empresas de telecomunicaciones (TELCOs, en Uruguay: ANTEL, Claro y Movistar). Estas empresas ofrecen la utilización de su infraestructura a cambio de una tarifa.

Estas tecnologías utilizan bandas que son licenciadas en Uruguay, por lo que si se desea implementar un proyecto que las utilice, se debe contratar el servicio. El área de cobertura depende del proveedor seleccionado, y el bitrate depende de la versión utilizada, variando desde pocos Kbps hasta pocos cientos de Mbps.

Existen redes WAN de baja velocidad tales como LPWAN (Low Power Wide Area Network - red de área extensa de baja potencia).

Tecnologías de transmisión para IoT

WAN - Redes celulares (2G/3G/4G)

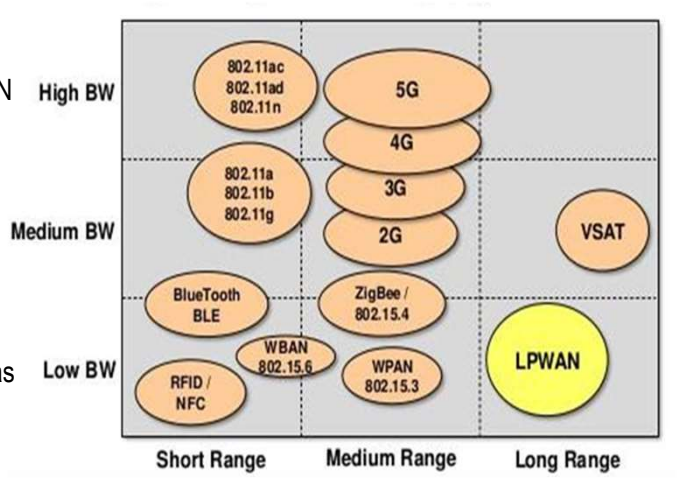
El dispositivo que se conecta a la red celular debe tener la capacidad de implementar el stack de protocolos IP. Todo esto se traduce en un aumento de capacidad de hardware, elevando el consumo de energía y el costo. Por este motivo, existen desarrollos de estándares [27] que optimizan el consumo de energía de los nodos a ser utilizados en aplicaciones de IoT.

Tecnologías de transmisión para IoT

WAN - LPWAN (Low Power Wide Area Networks)

Las redes LPWAN son redes inalámbricas diseñadas para permitir comunicaciones de largo alcance a un bitrate reducido entre objetos conectados, y alimentados por batería.

La energía consumida, el bajo bitrate y el uso previsto distinguen LPWAN de WAN, dado que esta última hace referencia a conectar usuarios y empresas, y transportar una mayor cantidad de datos, sin grandes restricciones de consumo de energía. El bitrate de las distintas tecnologías LPWAN habitualmente es del orden de unos pocos kbps.

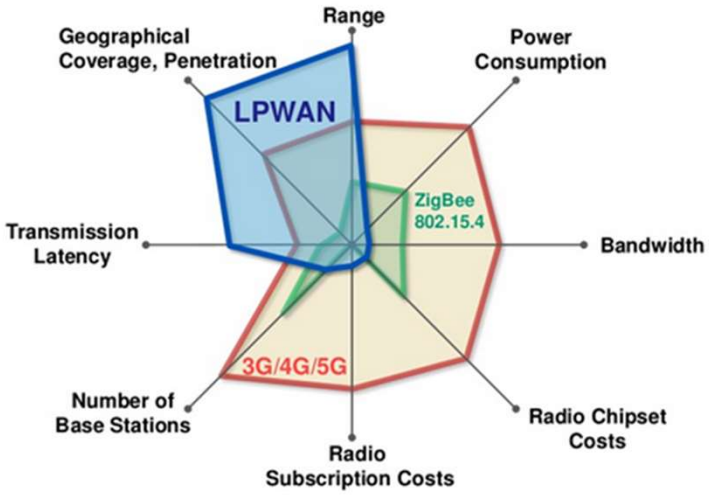


27

Tecnologías de transmisión para IoT

WAN - LPWAN

Una red LPWAN puede ser privada o pública. En este último caso permite a los propietarios de nodos implementar sistemas sin invertir en tecnología ni en infraestructura.



28

Tecnologías de transmisión para IoT

WAN - LPWAN

En la siguiente tabla se detallan algunos de los múltiples estándares y proveedores que compiten en tecnología LPWAN para IoT:

Tecnología	Sigfox	LoRa	NB LTE-M	LTE-M	EC-GSM	5G
Rango	<13 km	<11 km	< 15 km	< 11 km	< 15 km	< 15 km
Banda	No licenciada	No licenciada	Licenciada	Licenciada	Licenciada	Licenciada
Bitrate	<100 bps	<50 kbps	<150 kbps	< 1 Mbps	10 kbps	< 1 Mbps

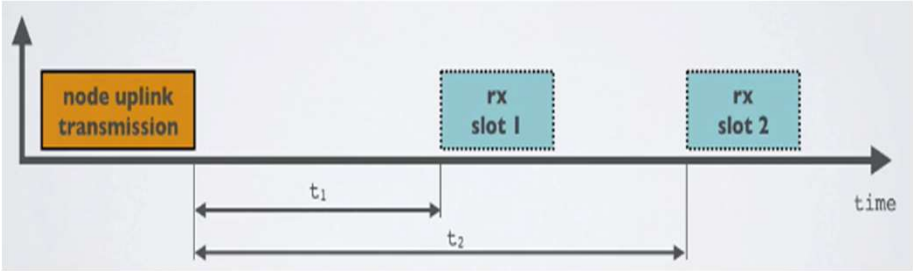
Tecnologías de transmisión para IoT

LORAWAN – Tipos de nodos finales

En LoRaWAN se prevén tres tipos de clases de nodo final.

Clase A

La más soportada en casi todos los dispositivos, este tipo ofrece el mayor ahorro de energía debido a que solo entra en modo escucha (llamado ventana RX) después de enviar datos hacia el gateway, por eso es ideal para dispositivos que usan una batería. Se pone en modo escucha en dos periodos de tiempo, 1s ± 20µs después de la transmisión y después de 1s ± 20µs de la primera vez que se pone en modo escucha.



Uplink y Downlink clase A.

30

Tecnologías de transmisión para IoT

LORAWAN – Tipos de nodos finales

Clase A

Bidireccional y asíncrona pura, la transmisión del uplink ocupa una ranura de tiempo, mientras que el downlink consta de dos ranuras. En cualquier momento el nodo final puede comenzar la transmisión, después de completada la Tx, el end node quedará en modo escucha dos veces.

Primero en una ventana de Rx llamada slot 1 que comienza en el tiempo t1 y posteriormente en otra llamada slot 2 que comienza en el tiempo t2. El gateway puede responder en la primer ventana o en la segunda pero no en ambas. Este paquete de respuesta del gateway contiene el ACK del paquete enviado así como datos de la aplicación si es necesario.

El uplink está programado por los dispositivos finales basados en sus propias necesidades y exigencias. Hay probabilidad de colisiones, si un nodo está transmitiendo y otro se despierta y decide transmitir en el mismo canal de frecuencia con configuraciones similares, se producirá una colisión. También presenta la mayor latencia de los tres tipos.

Tecnologías de transmisión para IoT

LORAWAN – Tipos de nodos finales

Clase B

En este tipo de dispositivos el inicio del protocolo de comunicación lo da el beacon que es un paquete de sincronismo. Comienza igual que la clase A, la diferencia es que después de completado esto, se abren más ventanas de Rx extras configurables por el usuario con un periodo llamado ranura ping, hasta la llegada del siguiente beacon llamado beacon period.

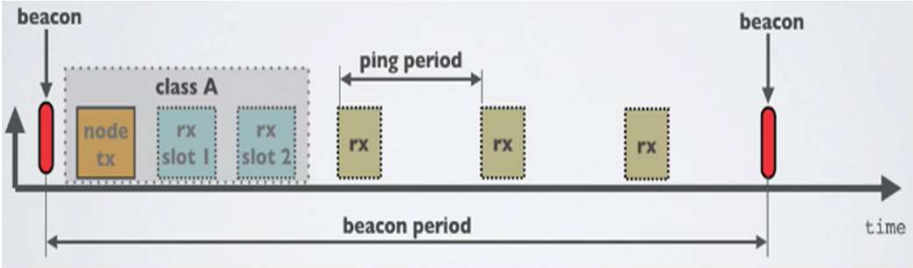


Figura - Uplink y Downlink clase B.

Tecnologías de transmisión para IoT

LORAWAN – Tipos de nodos finales

Clase B

Las ventanas de recepción extras son con base en tiempos predeterminados con el gateway, este tipo de nodos puede usar una batería o una fuente externa dependiendo de los tiempos asignados de escucha. Esto lo obtiene mediante el envío periódico de beacons por parte de la puerta de enlace.

Estos beacons permiten a los dispositivos estar sincronizados con el gateway, y de esta forma pueden negociar tiempos de recepción de paquetes desde la puerta de enlace al dispositivo en el downlink. Esta clase de dispositivos tienen un consumo mayor de energía que los de clase A debido a la recepción periódica de los beacons desde el gateway.

Tecnologías de transmisión para IoT

LORAWAN – Tipos de nodos finales

Clase C

Estos dispositivos después que realizan la Tx, tienen dos ventanas de Rx como en clase A pero a diferencia de los clase B, posteriormente al slot 2 permanecen en modo escucha hasta su siguiente Tx. Esta es la razón primordial por la cual estos nodos consumen más energía.

Figura - Uplink y Downlink clase C.

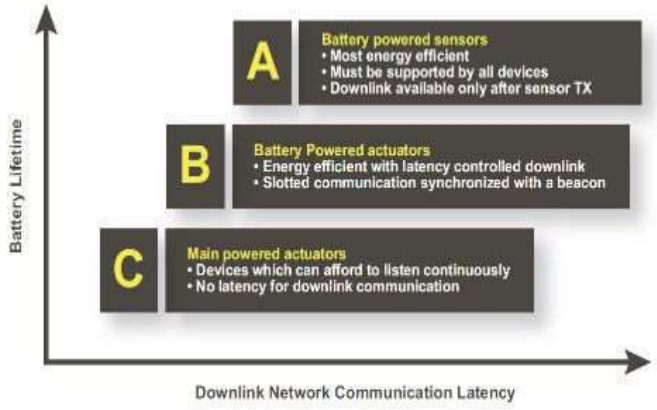
Tecnologías de transmisión para IoT

LORAWAN – Tipos de nodos finales

Clase C

Son dispositivos finales con ventana de recepción (Downlink) casi continuamente en modo escucha. Es decir, pueden recibir datos los dispositivos finales casi todo el tiempo excepto cuando éstos transmiten (Uplink)

Los tiempos de latencia son menores pero implica un mayor consumo de energía con respecto a las clases A y B. Por lo general estos dispositivos deben usar una fuente de alimentación externa.



Tecnologías de transmisión para IoT

LORAWAN – Resumen

- LoRaWAN es un protocolo de comunicación de baja velocidad, pero de gran alcance y baja potencia. Es una especificación abierta, por lo que cualquiera puede implementar el protocolo por sí mismo en su propio equipo.
- Banda ISM sin licencia.
- Alcance 5-10 km típico (muy dependiente de la línea de visión).
- Máxima potencia de salida 0.025 W.
- Seguridad basada en sesiones, donde cada sesión se inicia con claves estáticas, pero después de un intercambio de claves se utiliza un conjunto único de claves AES.
- LoRaWAN es ideal para sensores que envían valores poco frecuentemente.

Tecnologías de transmisión para IoT

LORAWAN – Resumen

- Las limitaciones en la banda de frecuencia utilizada pueden causar una alta latencia en los mensajes entregados. Por lo tanto, no es una opción para los productos de IoT que requieren un ciclo de retroalimentación inmediata. Debido a la cobertura limitada de una red privada, no es ideal para el seguimiento de vehículos que viajan largas distancias.
- Requiere invertir en la propia red con estaciones base, una estación base necesitará una conexión a Internet y energía.
- Los costos en invertir en la creación de la propia red se compensarán en el futuro al tener su propia red, lo que significa que puede crear cobertura donde sea necesario.

Tecnologías de transmisión para IoT

NB-IoT

- La cobertura es muy buena. Los dispositivos NB-IoT dependen de la cobertura celular, por lo que funcionan bien en interiores y en áreas urbanas densas.Tiene tiempos de respuesta más rápidos que LoRa y puede garantizar una mejor calidad de servicio.
- NB-IoT se ejecuta en el espectro de radio de la telefonía móvil y se complementa con canales GSM antiguos no utilizados o con espacio libre entre canales LTE.
- Necesita una frecuencia / canal regional dedicado costoso.
- Alcance 10-15 km.
- Máx potencia de salida 0.2 W..
- NB-IoT hereda la autenticación y el cifrado de LTE.

Tecnologías de transmisión para IoT

NB-IoT

- Actualización de sistemas basados en GSM. Principalmente para lecturas de sensores, seguimiento y gestión de flotas. En el futuro, la cobertura debería ser comparable a GSM.
- No es buena para conexión a internet de alta velocidad.
- Requiere una suscripción con un proveedor de telefonía móvil.
- Tiene costos en suscripción, tarjeta sim, costos de datos, hardware.

Tecnologías de transmisión para IoT

SIGFOX

- Sigfox es un operador de red LPWAN que ofrece una solución de conectividad IoT de extremo a extremo basada en sus tecnologías patentadas. Las estaciones base patentadas son equipadas con radios y las conecta a los servidores finales utilizando una red basada en IP.
- Los dispositivos finales se conectan a estas estaciones base mediante la modulación de desplazamiento de fase binaria (BPSK). Sigfox utiliza bandas ISM sin licencia, por ejemplo, 868 MHz en Europa, 915 MHz en América del Norte y 433 MHz en Asia.
- Al emplear la banda ultra estrecha, Sigfox usa el ancho de banda de frecuencia de manera eficiente y experimenta niveles de ruido muy bajos, lo que lleva a un consumo de energía muy bajo, una sensibilidad de receptor alta y un diseño de antena de bajo costo a expensas del rendimiento máximo de solo 100 bps.

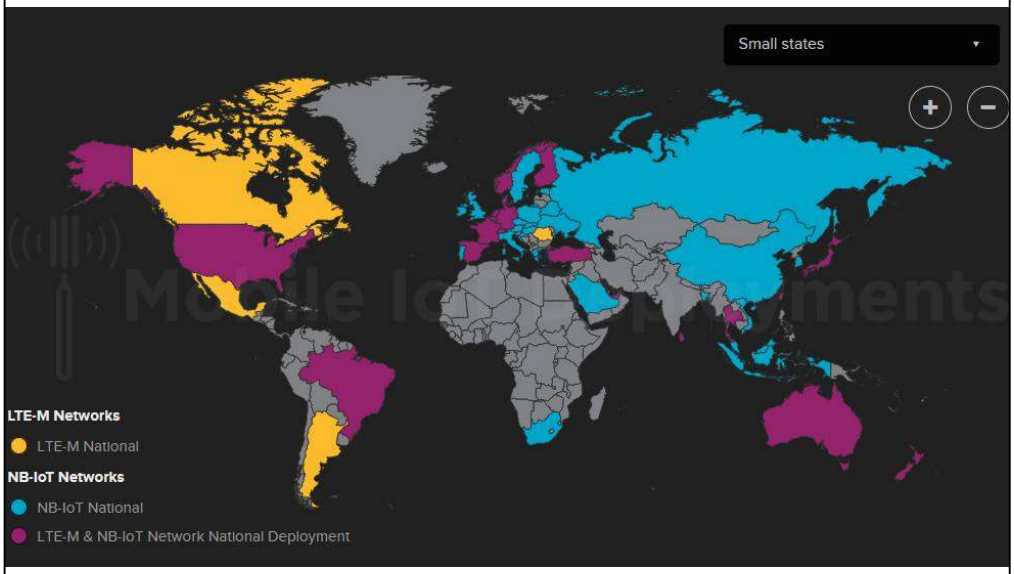
Tecnologías de transmisión para IoT

SIGFOX

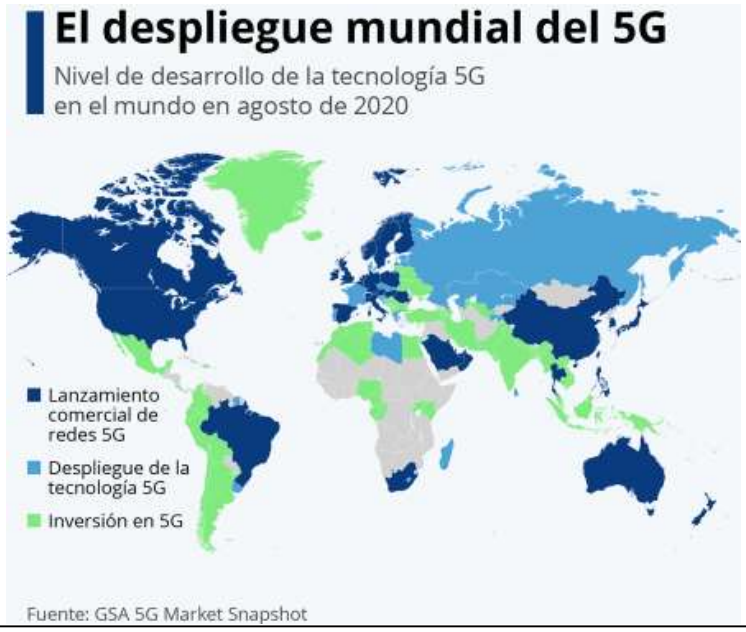
- El número de mensajes a través del enlace ascendente está limitado a 140 mensajes por día. La longitud máxima de carga útil para cada mensaje de enlace ascendente es de 12 bytes. Sin embargo, el número de mensajes a través del enlace descendente está limitado a cuatro mensajes por día.
- La longitud máxima de carga útil para cada mensaje de enlace descendente es de ocho bytes. Sin el soporte adecuado de acuses de recibo, la fiabilidad de la comunicación de enlace ascendente se garantiza utilizando la diversidad de tiempo y frecuencia. El mensaje de cada dispositivo se transmite varias veces (tres por defecto) a través de diferentes canales de frecuencia.
- Como las estaciones base pueden recibir mensajes simultáneamente en todos los canales, el dispositivo final puede elegir aleatoriamente un canal de frecuencia para transmitir sus mensajes. Esto simplifica el diseño del dispositivo final y reduce su costo.

Tecnologías de transmisión para IoT

Tecnologías de transmisión para IoT



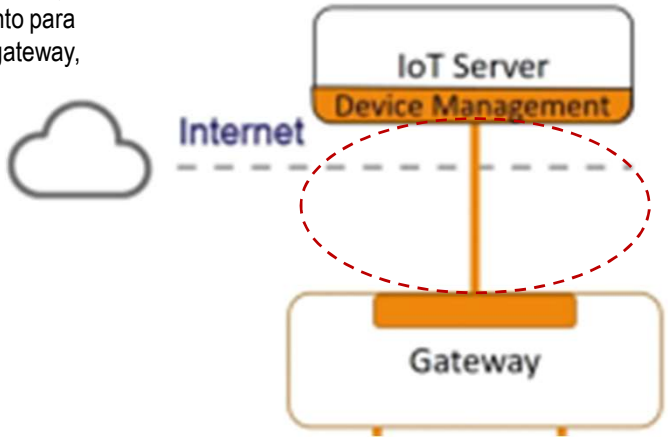
Tecnologías de transmisión para IoT



Protocolos para IoT

Protocolos de comunicación entre gateway y servidor

Veremos algunos protocolos y modos de funcionamiento para la comunicación entre gateway, servidores y usuarios.



45

Protocolos para IoT

Condicionantes de IoT para la elección de un protocolo

- En IoT puede llegar a haber gran cantidad de dispositivos, y posiblemente de gran variedad, tales como sensores de temperatura, de humo, de espacio; actuadores para encender o apagar artefactos, habilitar cerrojos; etc.
- Además, debe ser escalable, o sea, que puedan añadirse o retirarse dinámicamente dispositivos sin que el comportamiento global del sistema se modifique.
- Debe mantenerse débil interdependencia entre dispositivos.
- Algunos de los dispositivos serán dispositivos embebidos, de bajo costo y escasa capacidad de cálculo. Por tanto, el protocolo debe requerir poco procesamiento.
- Es deseable que el protocolo funcione la mayor variedad de dispositivos, sistemas operativos, y lenguajes de programación.
- Además, es posible que haya un gran número de comunicaciones simultáneas y, en general, se requiere una respuesta rápida. Esto requiere que los mensajes transmitidos sean pequeños y que no demanden mucho procesamiento.
- La seguridad es fundamental para dispositivos conectados a Internet.
- Finalmente, tenemos que poder acceder a los dispositivos fácilmente, por lo que tendremos que lidiar con direcciones dinámicas y DHCP, posibles conexiones con mala latencia o ancho de banda, dependencia con la infraestructura de la red, firewalls, etc.

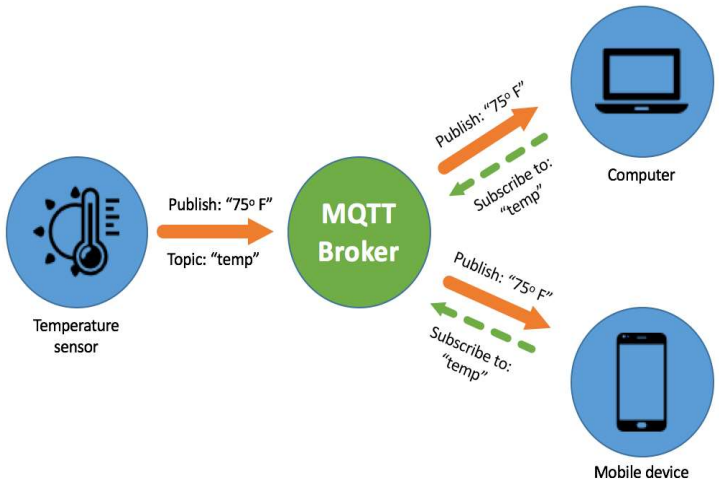
Protocolos para IoT

Metodologías en IoT

Vamos a repasar un par de términos en cuanto a metodologías que podemos encontrar en IoT. En realidad, los conceptos son parecidos, pero conviene entender las diferencias

Publish / Susbcribe (PubSub)

La metodología Pub/Sub es un patrón de mensajería donde un agente, el 'Subscriber', informa al **Broker** (Router) que quiere recibir un tipo de mensajes. Otro agente, el 'Publisher' puede publicar mensajes. El Broker distribuye los mensajes a los Subscribers.



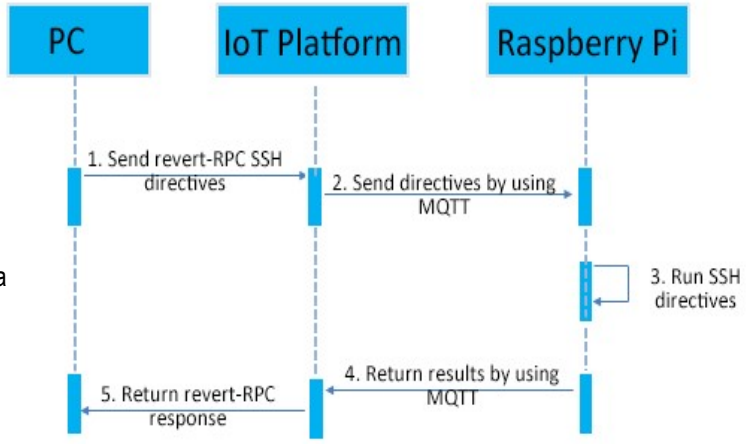
47

Protocolos para IoT

Metodologías en IoT

Revert Remote Procedure Calls (rRPC)

El rRPC es un patrón de ejecución remota de procedimientos donde un agente, llamado 'Callee', comunica al Router que proporciona un cierto procedimiento. Otro agente, llamado 'Caller', puede llamar a este procedimiento. El Router invoca el procedimiento en el Callee, recoge el resultado del proceso, y lo comunica al Caller que lo ha invocado.



48

Protocolos para IoT

Infraestructuras de servicios en IoT

Existen varias aproximaciones para realizar un patrón PubSub o rRPC. Vamos a ver dos de las principales. A efectos prácticos, podemos conseguir funcionalidades similares en ambos planteamientos, pero igual que en el caso anterior conviene ser consciente de la diferencia.

No obstante, también hay que destacar que existen soluciones que adoptan un comportamiento intermedio o híbrido entre ambos planteamientos.

Message queue

- En un servicio de mensajería de tipo Message Queue el Router genera una cola de mensajes única para cada uno de los clientes que inician la subscripción. El Router discrimina los mensajes empleando el identificador del cliente, aunque por supuesto existen mecanismos para distribuir a múltiples clientes.
- Estas colas de mensajes de cliente mantienen los mensajes recibidos hasta que son entregados al cliente. De forma que si se recibe un mensaje cuando el cliente no está conectado, se mantienen en el Router y son entregados cuando se conecta.
- Un ejemplo de Message Queue es una aplicación de mensajería tipo Whastapp o Telegram, donde el usuario recibe los mensajes que ha recibido mientras no estaba conectado. Otro ejemplo cotidiano es el buzón de correo de tu casa. Si estás fuera de vacaciones, cuando vuelves tienes todos tus mensajes esperándote.

Protocolos para IoT

Infraestructuras de servicios en IoT

Message Service

- Otro planteamiento es servicio de mensajería puro o Message Service. En este caso, el router distribuye inmediatamente los mensajes a los clientes conectados. Los mensajes se filtran por algún criterio, como el tema o el contenido del mensaje.
- A diferencia de un Message Queue, los mensajes entregados mientras el cliente está desconectado se pierden. No obstante, eso no significa que un servicio Message Service no pueda implementar algún tipo de persistencia de datos, por ejemplo, para analítica, históricos, o calidad del servicio.
- Un ejemplo de Message Services es un chat, donde no podemos recuperar los mensajes emitidos cuando no estábamos en la sala. Otro ejemplo cotidiano es una conversación a viva voz. Si alguien dice algo mientras estamos en otra habitación, aunque entremos nos hemos perdido lo que se dijo antes.

Protocolos para IoT

Entorno doméstico.

Cada día son más los hogares que disponen de uno o varios dispositivos IoT. Existen multitud de empresas que fabrican estos dispositivos. Cada uno tiene su propio protocolo de comunicación y aunque no es mucha la información que suelen facilitar, sobre todo si no son protocolos de código abierto, los más conocidos son:

OCF (Open Connectivity Foundation) es un protocolo impulsado por Samsung, Intel, Microsoft, Qualcomm, Electrolux entre otras. Es un proyecto de código abierto que ofrece interconectividad con la filosofía just-works. Este protocolo pretende garantizar la interoperabilidad de millones de dispositivos, gracias a una implementación de referencia (IoTivity) y un programa de certificación.

Protocolos para IoT

Entorno doméstico.

Thread (network protocol) fue creado por el conjunto de empresas denominado Thread Group. Es una tecnología basada en las comunicaciones por red mediante IPv6 que utiliza cifrado AES. Por ello y por la flexibilidad que ofrece, es un protocolo muy seguro y está preparado para el futuro.

AllJoyn fue lanzado por The AllSeen Alliance, compuesta por Haier, LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image, Technicolor y TP-Link. Es un estándar de código abierto, que facilita la comunicación entre dispositivos y aplicaciones, para todo tipo de protocolos de la capa de transporte.

HomePlug y **HomeGrid** son protocolos cuya comunicación se realiza a través de la red eléctrica. Esta tecnología de comunicación la implementan numerosas marcas. Dependiendo del producto adquirido, el tipo de cifrado es diferente, incluso algunos dispositivos transmiten la información sin cifrar.

MFi (Made For iPhone/iPod/iPad) es un protocolo de comunicaciones propio de Apple diseñado para interactuar con estos dispositivos. Los dispositivos y elementos de conexión de Apple incorporan un chip mediante el cual verifican que tanto los dispositivos, como los cables de conexión son originales.

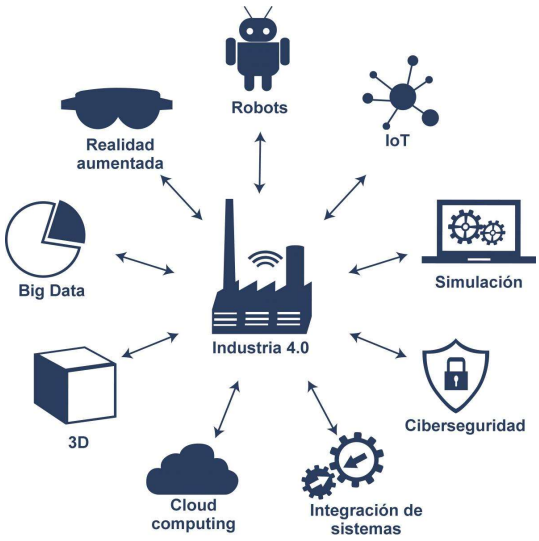
Protocolos para IoT

Entorno industrial

Ahora que hemos visto la necesidad y planteamiento de los protocolos destinados a aplicaciones de IoT, vamos a ver algunos de los muchos protocolos M2M disponibles.

MQTT (MQ Telemetry Transport) es un protocolo PubSub de Message Service que actúa sobre TCP. Destaca por ser ligero, sencillo de implementar. Resulta apropiado para dispositivos de baja potencia como los que frecuentemente tenemos en IoT. Está optimizado para el routing activo de un gran número de clientes conectados de forma simultánea.

WAMP (Web Application Messaging Protocol) es un protocolo abierto que se ejecuta sobre WebSockets, y provee tanto aplicaciones de PubSub como rRPC.



Protocolos para IoT

Entorno industrial

STOMP (Streaming Text Oriented Messaging Protocol, es un protocolo sencillo que emplea HTTP y mensajes de texto para buscar el máximo de interoperabilidad.

XMPP (Extensible Messaging and Presence Protocol) es un protocolo abierto basado en XML diseñado para aplicaciones de mensajería instantánea.

WMQ (WebSphere MQ) es un protocolo de Message Queue desarrolado por IMB.

DDS (Servicio de distribución de datos) este protocolo IoT para la comunicación de máquina a máquina en tiempo real fue desarrollado por el Object Management Group (OMG). Permite el intercambio de datos escalable. Este funciona en tiempo real, es confiable, de alto rendimiento e interoperable a través de la metodología de publicación-suscripción. En comparación con los protocolos MQTT y CoAP IoT, DDS utiliza una arquitectura sin intermediarios. Esto permite la multidifusión para brindar QoS de alta calidad a las aplicaciones.

AMQP (Advanced Message Queuing Protocol) es un protocolo PubSub de Message Queue. AMQP está diseñado para asegurar la confiabilidad e interoperabilidad. Está pensado para aplicaciones corporativas, con mayor rendimiento y redes de baja latencia. No resulta tan adecuado para aplicaciones de IoT con dispositivos de bajos recursos.

Protocolos para IoT

Entorno industrial

CoAP (Constrained Application Protocol) es un protocolo pensado para emplearse en dispositivos de IoT de baja capacidad. Emplea el modelo REST de HTTP con cabeceras reducidas, añadiendo soporte UDP, multicast, y mecanismos de seguridad adicionales.

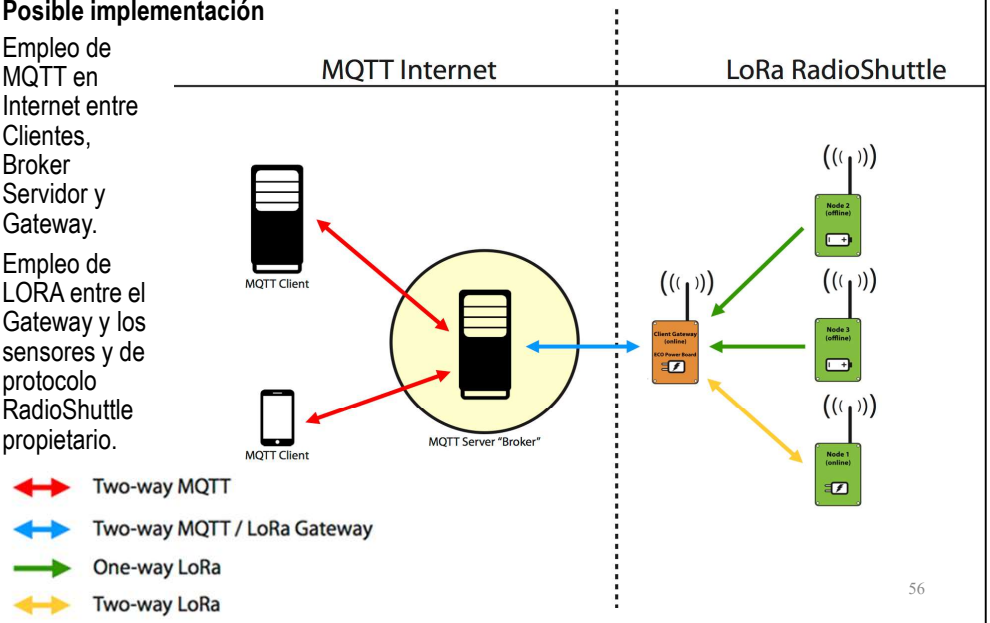
	Transporte	Modelo	Ámbito de aplicación	Conocimiento del contenido	Datos principales	Seguridad	Prioridad de los datos	Tolerancia a fallos
AMQP	TCP/IP	Intercambio de mensajes punto a punto	D2D D2C C2C	Ninguno	Codificados	TLS	Ninguno	Específica de la implementación
CoAP	UDP/IP	Petición/Respuesta (REST)	D2D	Ninguno	Codificados	DTLS	Ninguno	Descentralizado
DDS	UDP/IP (unicast + mcast) TCP/IP	Publicación/Suscripción Petición/Respuesta	D2D D2C C2C	Enrutamiento basado en el contenido, consultas	Declarados codificados	TLS, DTLS, DDS	Prioridades de transporte	Descentralizado
MQTT	TCP/IP	Publicación/Suscripción	D2C	Ninguno	No definidos	TLS	Ninguno	El nodo central (broker) es el punto único de fallo (SPoF)

Protocolos para IoT

Posible implementación

Empleo de MQTT en Internet entre Clientes, Broker Servidor y Gateway.

Empleo de LORA entre el Gateway y los sensores y de protocolo RadioShuttle propietario.



56

Protocolos para IoT

Seguridad

Ataques

El auge de los dispositivos IoT y su gran interconexión les convierte en el objetivo perfecto para los ciberdelincuentes. El número de amenazas de malware ha crecido en este ámbito, no sólo de forma cuantitativa sino también cualitativamente.

Algunos formas de ataques son:

- **Ataque por fuerza bruta** para «obtener» una clave, normalmente la utilizada por el protocolo Telnet. El cual es utilizado por algunos dispositivos de IoT para el acceso de forma remota.
- **Ataques por denegación de servicio** que producen indisponibilidad de los dispositivos por saturación.
- **Utilización como plataforma de ataque hacia otros dispositivos** del entorno, ya que por defecto suelen estar menos fortificados y son más accesibles desde el exterior de la red donde se encuentran.
- **Obtención de datos** de carácter personal de los usuarios como: hábitos de uso, contraseñas de acceso a servicios web e incluso datos de tarjetas de crédito.

.

Protocolos para IoT

Seguridad

Medidas de prevención

Para poder reducir el riesgo de la materialización de algunas de las amenazas que hemos descrito, debemos de implantar al menos las siguientes medidas:

- **Actualizaciones y parches.** Tener el dispositivo actualizado es importante para minimizar el riesgo de que éste sea vulnerable.
- **Autenticación, control de accesos y administración.** Evitar las contraseñas predeterminadas. Una contraseña robusta para acceder a la configuración del dispositivo es una buena medida contra accesos no deseados, así como administrarlos (en caso de que ser posible) solo de forma local.
- **Protección de los datos almacenados.** Se debe poder controlar qué datos almacenados dentro de nuestro dispositivo se envían a los fabricantes.
- **Uso de protocolos seguros.** Las comunicaciones con otros dispositivos y equipos deben hacerse a través de protocolos seguros.

Protocolos para IoT

Seguridad

Medidas de prevención

- **Bloquear puertos.** Siempre y cuando sea posible, es recomendable desactivar todos aquellos que no se vayan a utilizar, para evitar brechas de seguridad.
- **Plan de continuidad del servicio.** Tener un dispositivo que pueda trabajar de forma autónoma, es decir, sin supervisión remota por si se produce un fallo en la red, es muy importante, así como que el dispositivo cuente con un sistema de logs que almacene datos en caso de producirse un fallo para investigar las causas del mismo.

Cuestionario

1- Qué tipo de “cosas” interesa conectar mediante IoT?

2- Qué tipos de sensores son frecuentemente utilizados?

3- Cuál es la función de un Gateway en IoT?

4- Qué condiciones debe reunir un protocolo de comunicación en IoT?

5- Qué es un bróker en IoT?

6- Qué aspectos de seguridad deben tenerse en cuenta en IoT?