Ciberseguridad, Calidad de servicio y Localización

Alrededor de la implantación de las soluciones IoT, se plantea en este articulo la conveniencia de definir una correcta estrategia para la ciberseguridad, para el control de la calidad de los servicios radio y de la localización de personas/cosas en los edificios del futuro.

José Manuel Cámara Rodriguez
Director General Aplicaziones
jmc@aplicazion.es
www aplicazion.es
@Aplicaziones

Los que ya tenemos unos años a nuestra espalda hemos estado hablado de los edificios inteligentes y de la domótica desde hace mucho tiempo. Durante estas últimas décadas, los avances en electrónica, sistemas de control, comunicaciones e informática han permitido mejorar las prestaciones, reducir los costes de operaciones y aumentar el confort de nuestras viviendas / oficinas.

Así hemos conocido, por ejemplo, la revolución del cableado estructurado, de las ICT, de los sistemas de control, la aparición de las WiFi y ahora del IoT en los edificios. En cada época nuevas tecnologías han habilitado la aparición de nuevos servicios de comunicaciones y han permitido, en general, la reducción de los costes de las operaciones, la mejora de la explotación de los edificios y de la calidad de los servicios de los usuarios.

El IoT no será una excepción. La disponibilidad de dispositivos inteligentes de bajo costo y grandes capacidades de tráfico sin apenas coste, va a permitir un grado de automatización, control y calidad de vida que no hemos conocido hasta ahora.

Los procesos de ingeniería de estos proyectos IoT normalmente tienen sus propios desafíos y compromisos (prestaciones vs coste). Muchos de estos retos ya están en camino de resolverse (anchos de banda, miniaturización de sensores y radios, etc.). Sin embargo, hay otros que, según nuestra opinión, todavía no han sido tratados adecuadamente.

Por ello, en este escenario, desarrollamos aquí varias líneas de trabajo en las que nuestra empresa se está especializando y que consideramos de gran interés para el éxito futuro de los proyectos de despliegue de IoT en edificios:

1. Ciberseguridad
2. QoS en servicios inalámbricos
3. Localización de personas y cosas

Ilustración 1: Lineas de trabajo IoT en Aplicaziones

Ciberseguridad

Pensamos que el problema de las ciber-amenazas puede ser uno de los talones de Aquiles de las tecnologías que están detrás de las nuevas soluciones de IoT. Aunque ya llevamos un tiempo conviviendo con ellas en nuestras redes de banda ancha convencionales, no podemos decir que tengamos la situación controlada, pues cada día aparecen nuevas estrategias de ataque que intentan sacar partido de este mundo conectado.

Ahora, con la aparición del IoT, será muy fácil desplegar múltiples dispositivos (sensores, actuadores, lectores, etc.) inteligentes que se comunicarán entre ellos con gran facilidad. Estos nuevos ecosistemas se basan en la interoperabilidad y lo que por un lado es una ventaja, puede ser a la larga también una desventaja. Así, estos sistemas abiertos podrían ser explotados por los hackers para construir métodos de ataque a estas redes y por tanto comprometer su funcionamiento.

Nuestra visión es que la tecnología IoT se va a convertir en un producto de consumo y, por lo tanto, vamos hacia un escenario de tecnologías y productos heterogéneos, similar al que ahora vivimos con los smartphones o los PC.

Se nos ocurren múltiples ejemplos. Las cerraduras electrónicas se comprarán no tanto porque sean seguras (se dará por descontado), sino porque se puedan programar con múltiples funcionalidades o por compatibilidad con nuestro smartphone. Las luces pasarán a ser elementos de comunicaciones, decorativos y de entretenimiento. La temperatura de los despachos/habitaciones se regulará de modo automático y en función de las necesidades de cada persona. Se desarrollarán dispositivos en las viviendas que facilitarán la vida a las personas mayores y/o a las dependientes.

En fin, no vamos a extendernos en demasiados casos. Lo principal es que habrá múltiples dispositivos alrededor de nuestro entorno que se estarán comunicando con los sistemas de las viviendas, de los edificios, de las empresas y en último lugar con las propias personas.

Este escenario altamente conectado hace que sea muy necesario asegurar la inviolabilidad de las comunicaciones y la autentificación de los datos. Si no se construyen las soluciones IoT pensando en la ciberseguridad, las mismas (o parecidas) amenazas que nos encontramos en nuestras redes actuales redes IP se extenderán a este mundo y en este caso incluso pueden ser más peligrosas (p.e. pensemos en la regulación de dispositivos personales de salud).

Para enfrentarnos con este problema nuestra empresa está promoviendo en este momento en el uso de soluciones de Firewall Software UTM7 que puedan ser implantados en arquitecturas ARM, Intel y/o en la nube.

En la Figura 1 puede verse un diagrama sobre cómo se protegerían diferentes redes de sensores.

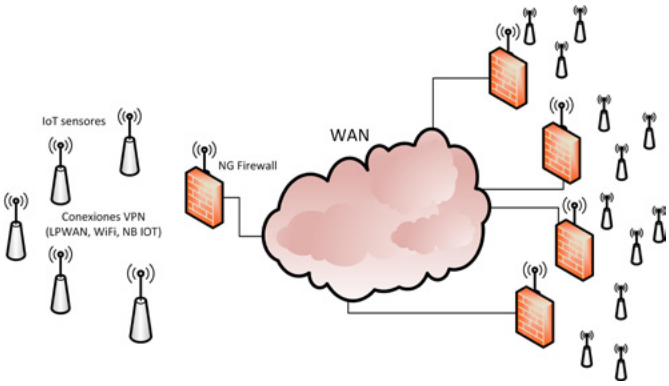

Figura 1

En este esquema algunos de los nodos se convierten también en Firewalls y el resto se conectan con ellos vía redes VPN con tráfico encriptado.

Implantando este tipo de soluciones en todo tipo de dispositivos o redes de dispositivos IoT se podrá aislar a los mismos de las amenazas que les lleguen desde internet, pudiendo definir además políticas en función de cada caso de uso o de dispositivo a controlar. Un caso típico de uso sería el de construir una sencilla red VPN para asegurar las comunicaciones de todos los dispositivos industriales (robots) en una fábrica o de los sensores de un edificio.

QoS en servicios móviles

En muchos casos los servicios IoT en los edificios estarán soportados por diferentes redes inalámbricas. Aquí va una colección de ellas: 4G, BLE, WiFi, LoRa, Sigfox, ZigBee, Dash7, RFID, NB IoT, etc. Cada una de estas tecnologías (y otras que aparecerán como el 5G) estarán peleando por su cachito de mercado. Los usuarios tendrán, muchas veces, varias alternativas para resolver sus necesidades y es muy probable que muchas de ellas coexistan en un mismo edificio, especializándose cada una en algunas funcionalidades y prestaciones.

En este escenario, entonces, dependeremos del buen funcionamiento de estas soluciones radio para el correcto funcionamiento de nuestras redes IoT. Para asegurar que las redes desplegadas funcionan adecuadamente, estamos proponiendo a los fabricantes de dispositivos de nuestros

proyectos que incluyan algún sistema de medición de la calidad de los servicios. Esto es algo crítico para poder disponer de comunicaciones fiables y seguras.

Sin embargo, ni siquiera para algo tan común como una red WiFi, se suele tener en cuenta la medición de la calidad de servicio. Así que normalmente acabamos con aquello de que la "red WiFi funciona mal".

Para empezar a concienciar a la industria hemos desarrollado unos sistemas de medida que permiten estresar estas redes y así analizar comportamientos ante diversas situaciones de tráfico. Hasta ahora se consideraba que simplemente con tener un buen nivel de señal (dBm) ya bastaba para tener unas buenas comunicaciones. Sin embargo, nosotros hemos demostrado que es además muy importante analizar las redes con carga real de conexiones y tráfico asociado. Así, en el gráfico de la Figura 2 puede verse el tráfico agregado de un Punto de Acceso (AP) WiFi en función de la carga de estaciones conectadas. La línea verde corresponde con un AP con un buen comportamiento. El rojo y el morado corresponde a AP que, aunque tienen buenas prestaciones con pocos clientes, rápidamente reducen sus prestaciones a medida que se le conectan más estaciones.

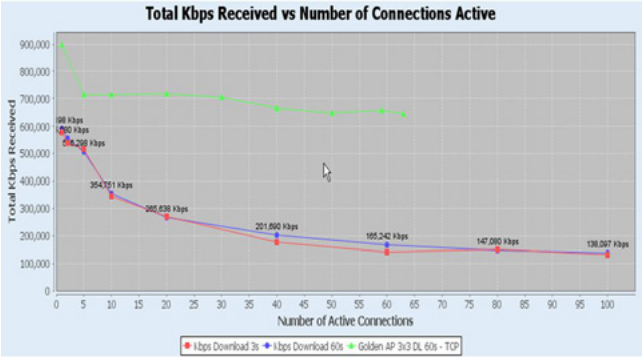

Figura 2

La conclusión es que no todos los dispositivos se comportan igual cuando se van cargando de conexiones.

Este mismo analisis deberíamos tenerlo en cuenta a la hora de elegir nuestras soluciones Wireless IoT. Una cosa es que se cumplan los estándares, otra que sean interoperables y una última es que, además, las prestaciones que están en los catálogos se cumplan. A veces, el problema se resuelve con un cambio en la configuración del sistema, pero otras veces, el producto (AP en este caso) es deficiente. Ya se sabe, nadie da duros a pesetas …

La realidad es que diseñar solo para tener cobertura se ha demostrado insuficiente para garantizar anchos de banda. En muchos casos es necesario realizar una verificación en campo para comprobar los SLA si se quiere estar seguro de que no nos están dando gato por liebre.

Para facilitar este tipo de medidas en nuestra empresa hemos desarrollado soluciones que permiten similar y probar escenarios de múltiples conexiones sobre redes Wireless. En la Figura 3 puede verse un equipo simulador de múltiples estaciones de radio, capaz de generar tráficos de 256 estaciones/dispositivos.


Figura 3

De esta manera se puede hacer una certificación de las redes inalámbricas una vez desplegadas y validar, de manera real, que los servicios IoT están funcionando de manera correcta y segura.

Para completar la perspectiva de este punto (Wireless QoS), queremos comentar que en este entorno de redes radio, hay que considerar que nuestros sistemas de medida deberían poder validar que las redes radio son capaces de asegurar las comunicaciones ante todo tipo de amenazas.

Figura 4

Como paradigma de los problemas con los que se enfrentan estos sistemas, tratamos a continuación el caso, no por conocido menos importante, de "man in the middle" (Fugura 4). Este ataque ha sido ampliamente utilizado desde el comienzo de las redes de comunicaciones de datos. Así un dispositivo, se pone en medio de las comunicaciones entre los equipos de las víctimas que no detectan nada

y se creen que están hablando entre ellos. Pero, para su desgracia, todo el tráfico está siendo redirigido a través del dispositivo del atacante, el cuál dispone de esta manera de acceso a toda la información que circula entre los dispositivos de las víctimas.

Al ser las redes radio más ubicuas, es más fácil para los atacantes acceder a los dispositivos de las víctimas (ya ni siquiera hay que conectar un cable a la red).

Afortunadamente existen soluciones conocidas para este problema y se basan en la utilización de redes Wireless seguras que llevan, entre otras cosas, sensores que detectan este tipo de ataques. Sin embargo, es increíble que a estas alturas la gran mayoría de las instalaciones WiFi de las Pymes en España no estén protegidas contra este problema. Así que, podemos imaginar que podrá pasar con las redes IoT si se generalizan y se despliegan sin tener este tipo de amenazas en cuenta.

Es por esto por lo que estamos proponiendo a nuestros clientes trasladar las buenas prácticas de las redes Wireless seguras al mundo IoT. Esto significa no solo unas inversiones adecuadas, sino también un diseño para conseguir unos SLA y/o QoS (prestaciones y ciberseguridad) determinados. Posteriormente se hace necesaria una certificación / verificación de estos compromisos. Con todo el marketing que se genera en nuestra industria, la única manera de asegurar que las redes se despliegan correctamente es midiéndolas.

Localización de personas y cosas

Como todo el mundo sabe en el interior de los edificios no es posible utilizar los servicios de localización basados en satélites. Sin embargo es precisamente en los edificios donde permanecemos la gran parte de del tiempo de nuestra vida y en los que se realizan la gran mayoría de las actividades económicas de nuestra sociedad. Esto ha conducido a una actividad frenética de nuestra industria para buscar soluciones de localización que funcionen en zonas sin cobertura GPS (centros comerciales, almacenes, metros, aeropuertos, etc.).

Así, en la actualidad, existen múltiples tecnologías y soluciones para la localización de personas y cosas. La gran mayoría se apoyan en el concepto de uso de balizas (RFID, WiFi, BLE y UWB son las más conocidas) como referencia.

Existe otra línea de investigación (en la que ha trabajado Aplicaziones) que consiste en el uso de la navegación inercial mediante el uso de sensores aplicados al movimiento de las personas. Esta solución minimiza la necesidad de balizas como referencia y, mediante unos algoritmos de fusión de múltiples fuentes de información, se consigue ubicar a las personas en interiores con un coste mínimo (Figura 5). Estos trabajos se han desarrollado en nuestra empresa desde hace más de 5 años. Incluso con alguno de nuestros proyectos hemos conseguido éxito en algunos programas europeos de investigación.

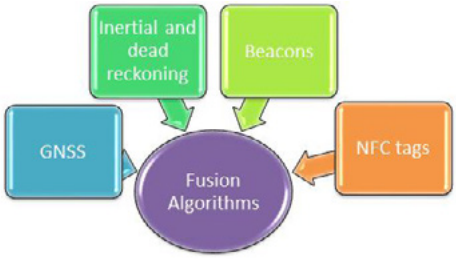

Figura 5

Pero además, con los despliegues de redes IoT actuales, estas estrategias deberán evolucionar, pues en breve tendremos múltiples dispositivos de bajo coste en los edificios que podremos utilizar para facilitar los servicios de localización. De esta manera los motores de posicionamiento basados en balizas, normalmente con algoritmos TDOA (Time Difference of Arrival) o AOA (Angle-of-Arrival), dispondrán de múltiples alternativas de redes para la determinación de la ubicación.

Esto es sólo un avance de la revolución que se avecina en los servicios de localización en edificios. Toca, por tanto, ponerse manos a la obra para que las empresas y las personas puedan sacar partido a toda esta innovación. La implementación de este tipo de soluciones de posicionamiento permitirá la aparición de nuevos sistemas de gestión de los recursos humanos (por ejemplo, facilitando los procesos de prevención de riesgos laborales) y de las cosas (controlando la ubicación de los activos valiosos).

Finalmente, y para dar una pequeña perspectiva del mercado de localización en interiores, solo queremos indicar unos datos de un último estudio realizado durante el mes de Noviembre del 2018 por una compañía de estudio de mercado americana (Marketinsights):

El mercado de localización y navegación en interiores alcanzará los USD 28,2 Billones, con una tasa agregada de crecimiento del 38,2% durante los próximos años.

Es por todo lo anterior por lo que creemos que tenemos una buena razón para ser optimistas de cara al futuro de las redes de IoT en los edificios.