Globalstar™

LIBRO ELECTRÓNICO

Más Allá de las Limitaciones Energéticas

Asegurando Dispositivos IoT Satelitales de Bajo Consumo

La oportunidad de mercado para los dispositivos IoT de bajo consumo se está expandiendo rápidamente a medida que las industrias buscan soluciones eficientes, escalables y duraderas que soporten despliegues de IoT masivo. Con el auge de las ciudades inteligentes, la agricultura de precisión, el seguimiento de activos y la gestión de flotas, la demanda de dispositivos de bajo consumo y ancho de banda reducido está en su nivel más alto.

Las empresas necesitan sensores IoT y soluciones de seguimiento que puedan funcionar durante años con un consumo mínimo de energía, reduciendo los costos de mantenimiento y permitiendo una conectividad remota y permanente. A medida que las industrias avanzan hacia el procesamiento en el borde y adoptan tecnologías inalámbricas más eficientes, los dispositivos IoT de bajo consumo serán esenciales para acceder a información de datos en tiempo real, minimizando los costos operativos y extendiendo la vida útil del dispositivo.

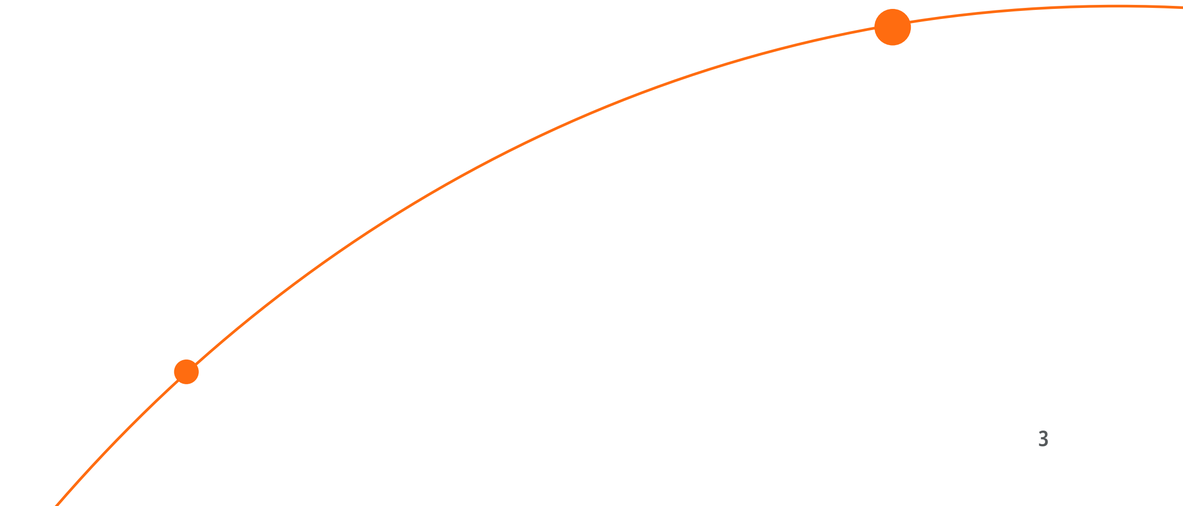
Los desafíos de seguridad asociados con los dispositivos IoT de bajo consumo se derivan de su despliegue masivo, su amplia accesibilidad y su capacidad limitada para soportar medidas de seguridad avanzadas. A diferencia de los sistemas de TI centralizados, que operan en entornos controlados, los dispositivos IoT de bajo consumo suelen instalarse en redes extensas y abiertas (en ciudades, zonas agrícolas o instalaciones de servicios públicos), lo que los hace vulnerables a amenazas cibernéticas.

La gran cantidad de dispositivos amplía la superficie de ataque, donde comprometer incluso una pequeña fracción puede desencadenar un efecto dominó en todo el sistema. Además, los ecosistemas IoT dependen de la interoperabilidad de varios proveedores, lo que significa que una debilidad en un solo dispositivo o capa de red puede introducir vulnerabilidades en todo el ecosistema, y así exponer datos confidenciales, interrumpir operaciones o incluso permitir ataques masivos de denegación de servicio (DDoS).

Para agravar aún más estos riesgos, los dispositivos IoT de bajo consumo tienen recursos muy limitados de procesamiento, memoria y almacenamiento, lo que dificulta la implementación de sistemas sólidos de encriptación, autenticación o detección de intrusiones. A diferencia de los dispositivos informáticos de alto rendimiento, que sí pueden soportar protocolos de seguridad robustos, muchos dispositivos IoT de bajo consumo carecen de capacidad para monitoreo en tiempo real, actualizaciones de software frecuentes o funciones criptográficas complejas.

Esto los convierte en objetivos para atacantes, que pueden aprovechar mecanismos de autenticación débiles, secuestrar las comunicaciones de los dispositivos o inyectar firmware malicioso. Y como estos dispositivos suelen estar diseñados para funcionar durante años con un mantenimiento mínimo, sus medidas de seguridad pueden quedar obsoletas con el tiempo, aumentando su vulnerabilidad a medida que evolucionan las amenazas.

Para abordar estos desafíos se requiere un equilibrio entre eficiencia y seguridad, de modo que se mitiguen los riesgos sin sobrecargar las capacidades limitadas de los dispositivos de bajo consumo. Los enfoques de seguridad están evolucionando para garantizar que incluso los dispositivos más livianos puedan funcionar de forma segura sin comprometer la eficiencia ni el rendimiento. Al aprovechar marcos de seguridad optimizados, métodos de autenticación adaptativos y protecciones basadas en la red, las organizaciones pueden mitigar los riesgos y, al mismo tiempo, mantener la escalabilidad y la durabilidad de sus despliegues IoT.



La Señal de Latido en la IoT

La seguridad, la optimización de energía y la eficiencia son consideraciones clave para la IoT impulsada por satélite. Un factor crítico que influye en las tres es si el dispositivo IoT requiere o no una señal de latido.

Un latido es una señal que envía un dispositivo para confirmar que está funcionando, incluso cuando no transmite datos nuevos. Si bien este enfoque tiene sus usos, los dispositivos IoT alimentados por satélite que solo envían datos cuando es necesario (lo que elimina la necesidad de un latido constante) ofrecen beneficios significativos, en particular en materia de seguridad y ahorro de energía.

Cómo la Comunicación Sin Latido Mejora la Seguridad de IoT

Cuando los dispositivos IoT no envían señales de latido regulares, reducen efectivamente su huella digital, lo que los hace menos susceptibles a interceptaciones, rastreos y ciberataques. Una señal de latido puede actuar como un faro que revela la ubicación y la presencia de un dispositivo dentro de una red. En aplicaciones donde la discreción y la seguridad son primordiales (como defensa, monitoreo de infraestructura crítica y rastreo de activos industriales), minimizar las transmisiones innecesarias puede prevenir posibles vulnerabilidades.

Los dispositivos IoT permanecen indetectables, excepto en los momentos críticos en que se requiere información en tiempo real. Al transmitir datos solo cuando es necesario, este enfoque de baja probabilidad de intercepción (LPI) y baja probabilidad de detección (LPD) dificulta considerablemente que actores malintencionados exploten transmisiones predecibles.

¿Qué Sucede Cuando Hay un Latido?

En los modelos tradicionales de IoT, muchos dispositivos envían un latido a intervalos predeterminados (cada pocos minutos, cada hora o diariamente), incluso si no hay datos significativos que informar. Esto permite a los operadores de red confirmar que el dispositivo está activo, garantizar una conectividad estable y detectar posibles fallas de forma temprana.

Sin embargo, esta transmisión regular genera varios desafíos:

- **Mayor consumo de energía:** Cada transmisión de latido consume energía, algo especialmente problemático en dispositivos IoT alimentados por batería o energía solar desplegados a largo plazo en el campo.
- **Costos más altos de transmisión de datos:** Las señales de latido frecuentes pueden incrementar notablemente los gastos en despliegues IoT vía satélite, donde la transmisión de datos es costosa.
- **Riesgos de seguridad y privacidad:** Los patrones de transmisión constantes crean una señal predecible, lo que facilita que los atacantes detecten y exploten la red.

Cuándo y Por Qué Algunos Dispositivos IoT Requieren un Latido

A pesar de sus desventajas, un latido puede ser esencial en algunas aplicaciones, particularmente aquellas que requieren monitoreo del dispositivo en tiempo real, detección inmediata de fallas o participación activa en la red.

Algunos escenarios clave en los que se requiere un latido incluyen:

- **Dispositivos médicos de IoT: L**os sistemas de monitoreo remoto de pacientes a menudo requieren conectividad constante para garantizar que los datos críticos de salud estén disponibles de forma continua.
- **Sistemas de alta seguridad:** Algunos sistemas bancarios o financieros dependen de latidos regulares para detectar posibles cortes o intentos de manipulación.
- **Mantenimiento de red y comprobaciones de estado del sistema:** En situaciones donde la latencia o el tiempo de inactividad podrían provocar fallas catastróficas, los latidos frecuentes ayudan a mantener la visibilidad operativa.

Desventajas: Cuando el Latido Resulta Contraproducente

Si bien los latidos permiten el monitoreo del dispositivo en tiempo real, sus desventajas son notables, sobre todo en los despliegues de IoT remotos y de bajo consumo.

- **Drenaje frecuente de energía:** Los dispositivos que se conectan continuamente a una red consumen energía más rápidamente, lo que requiere mantenimiento o reemplazo de baterías con más frecuencia.
- **Mayor costo de propiedad:** Las organizaciones incurren en tarifas de datos satelitales más altas cuando se producen transmisiones innecesarias con el tiempo.
- **Mayor riesgo de detección:** Los dispositivos que emiten señales regulares se convierten en objetivos fáciles de interceptar o atacar.

A medida que la IoT se expande a numerosas industrias a través de cientos de aplicaciones, la necesidad de una comunicación eficiente, segura y de bajo consumo es más crítica que nunca. La eliminación de la necesidad de un latido constante proporciona ventajas en ahorro de energía, seguridad y costos operativos. Si bien existen casos de uso válidos para el latido, el uso estratégico de transmisiones por eventos y según necesidad definirá la próxima generación de despliegues de IoT impulsados por satélite, garantizando que los dispositivos permanezcan funcionales en el campo durante períodos prolongados mientras se mantiene la integridad operativa.

Al adoptar un diseño sin latido, los dispositivos IoT pueden funcionar durante más tiempo, de forma más segura y más eficiente, lo que los convierte en la opción preferida para aplicaciones de misión crítica donde la energía, el costo y la discreción son prioridades.

Una Red con Seguridad de Extremo a Extremo

Una red tiene varios puntos de contacto donde pueden aparecer vulnerabilidades de seguridad, lo que genera varias superficies de ataque. Disponer de una red segura de extremo a extremo permite adoptar un enfoque holístico de seguridad.

Cómo Funciona una Red Satelital

1 El Dispositivo Inicia la Comunicación

- El dispositivo del usuario envía datos mediante señalesde radiofrecuencia.
- Los datos se cifran antes de la transmisión para garantizar su seguridad.
- El dispositivo está equipado con un módem satelital y una antena para comunicarse con el satélite.

2 Enlace Ascendente al Satélite

- El dispositivo transmite la señal cifrada a un satélite.
- El satélite recibe y retransmite la señal.

3 El Satélite retransmite la Señal

- El satélite envía directamente la señal al punto final a través de una conexión satélite-tierra.

4 Enlace Descendente a la Estación Terrestre

- El satélite envía la señal a una estación terrestre o puerta de enlace segura.
- La estación terrestre descifra, procesa y reenvía los datos al punto final designado.

5 El Punto Final Recibe los Datos

- El punto final (centro de comando militar, servidor en la nube u otro dispositivo) recibe los datos de forma segura.
- El cifrado garantiza que solo el destinatario previsto pueda descifrar y acceder al mensaje.

El Valor de la Seguridad de Red

En los sistemas IoT satelitales, la seguridad de red de extremo a extremo abarca las estrategias, tecnologías y protocolos que protegen la integridad, confidencialidad y disponibilidad de los datos mientras se desplazan por una red. Es esencial para impedir accesos no autorizados, ciberataques, violaciones de datos e interrupciones en los sistemas de comunicación.

Componentes clave de la seguridad de red

Confidencialidad

- Garantiza que solo los usuarios y dispositivos autorizados puedan acceder a datos confidenciales.
- Utiliza protocolos de cifrado para proteger la comunicación.

Integridad

- Evita la manipulación de datos al garantizar que los mensajes sean auténticos y permanezcan inalterados durante la transmisión.

Disponibilidad

- Garantiza que los usuarios legítimos puedan acceder a los recursos de la red cuando los necesiten, sin interrupciones causadas por ataques (p. ej., DDoS).

Debido a que las redes IoT satelitales transmiten datos confidenciales – como el estado de equipos remotos, monitoreo ambiental e información de seguimiento de activos –, sin medidas de seguridad sólidas, los hackers o actores maliciosos podrían interceptar, manipular o interrumpir las comunicaciones, lo que provocaría pérdidas financieras, tiempos de inactividad operativa o amenazas a la seguridad nacional.

A diferencia de las redes celulares, la comunicación satelital involucra múltiples puntos de relevo (estaciones terrestres, satélites, dispositivos receptores), lo que aumenta el riesgo de corrupción o interceptación de datos. Las VPN, el cifrado y otros métodos pueden ayudar a garantizar que los datos transmitidos permanezcan sin cambios y a prueba de manipulaciones desde el origen hasta el destino.

Cómo la Seguridad de Red Protege a los Dispositivos IoT de Bajo Consumo

Los dispositivos de bajo consumo funcionan con recursos computacionales limitados y un consumo de energía mínimo, y a menudo carecen de mecanismos de seguridad integrados. Los marcos de seguridad de red brindan una protección crítica para los dispositivos IoT de bajo consumo, garantizando la transmisión segura de datos, la autenticación del dispositivo y la protección contra el acceso no autorizado sin sobrecargar el consumo de energía del dispositivo.

Los mecanismos de seguridad tradicionales suelen agotar la energía demasiado rápido, lo que los hace poco prácticos para estos dispositivos. Al aprovechar la seguridad a nivel de red, los dispositivos IoT siguen siendo seguros, energéticamente eficientes y resistentes las amenazas cibernéticas, al tiempo que mantienen una conectividad confiable.

Una Nota sobre la Conectividad Satelital para Dispositivos de Bajo Consumo

Las soluciones integrales de hardware, software y de red pueden proporcionar una seguridad sólida para los dispositivos de bajo consumo. Sin embargo, es importante señalar que la conectividad celular no es la única vía para los dispositivos de bajo consumo.

La conectividad de bajo consumo también puede ofrecerse a través de satélites y resulta muy beneficiosa para aplicaciones de IoT masiva en las que la infraestructura celular es mínima o inexistente, como en el sector marítimo, la agricultura, el petróleo y gas, la minería y muchos otros.

El tipo de órbita satelital es crucial a la hora de considerar este método de conectividad para dispositivos de bajo consumo, y cuanto más cerca de la Tierra, mejor.

Cómo Ayudan los Satélites LEO a los Dispositivos de Bajo Consumo

Existen tres distancias orbitales diferentes para los satélites: órbita terrestre baja (LEO), órbita terrestre media (MEO) y órbita geoestacionaria (GEO). Como su nombre lo indica, los satélites LEO están mucho más cerca de la Tierra, y esta proximidad ofrece varias ventajas, en especial para dispositivos con capacidad de batería limitada.

A diferencia de los satélites GEO – que permanecen fijos sobre un mismo punto de la Tierra –, los satélites LEO se mueven más rápido y completan una órbita en 90-120 minutos. Las constelaciones de satélites LEO brindan una cobertura continua al transmitir las señales a medida que se desplazan por el cielo.

Principales maneras en que los satélites LEO respaldan a los dispositivos de bajo consumo:

- **Requisitos de energía reducidos:** Una de las ventajas más significativas de los satélites LEO es que su menor distancia a la Tierra significa que los dispositivos no necesitan transmitir señales con niveles de potencia tan altos. La diferencia de pérdida de trayectoria (o diferencia de presupuesto de enlace) entre LEO y GEO es de aproximadamente 28 dB. Dado que las señales de radio recorren un trayecto mucho más corto que los satélites GEO, la potencia de transmisión necesaria para la comunicación es ligeramente menor. Esto permite que los dispositivos conserven la vida útil de la batería, haciéndolos más eficientes para operaciones a largo plazo.

- **Menor latencia para mayor eficiencia energética:** Debido a su proximidad a la Tierra, los satélites LEO ofrecen una reducción en la latencia, lo que acorta el tiempo que un dispositivo debe permanecer activo para comunicarse, ahorrando energía. Esto resulta especialmente útil para los dispositivos IoT que dependen de la transmisión de datos intermitente y necesitan optimizar el uso de la batería.

- **Antenas más pequeñas y eficientes:** Gracias a su cercanía, los satélites LEO proporcionan una señal más fuerte, lo que permite que los dispositivos utilicen antenas más pequeñas y de bajo consumo en lugar de las grandes y voraces en energía requeridas para satélites GEO. Esto es fundamental en aplicaciones que necesitan hardware compacto y eficiente energéticamente, como rastreadores GPS portátiles, sensores meteorológicos remotos y dispositivos de monitoreo ambiental.

- **Más satélites para un acceso más sencillo:** Las redes de satélites LEO funcionan como constelaciones, lo que significa que hay varios satélites en órbita en todo momento. Los dispositivos no necesitan aumentar su potencia de transmisión para alcanzar a un solo satélite remoto. En cambio, se conectan al satélite más cercano, lo que prolonga la vida útil de la batería.

- **Formación de haces inteligente para optimizar el consumo de energía:** Los satélites LEO utilizan formación de haces, una técnica que concentra las señales de radio en áreas específicas en lugar de transmitirlas en todas las direcciones. Esto aumenta la intensidad de la señal y reduce la potencia que necesitan los dispositivos para comunicarse de manera eficaz. Los dispositivos pueden transmitir con niveles de potencia más bajos sin perder la calidad del enlace, lo que extiende la vida útil de la batería.

Los satélites LEO representan una solución transformadora para empresas e industrias que despliegan redes de comunicación de bajo consumo en entornos remotos o desafiantes. Al reducir los requisitos de energía, optimizar la eficiencia y brindar cobertura global, estos satélites están revolucionando la forma en que los dispositivos se mantienen conectados en un mundo que exige comunicaciones continuas y sostenibles.

El Valor de los Dispositivos de Bajo Consumo en el Ecosistema IoT

Los dispositivos IoT de bajo consumo están revolucionando las industrias al posibilitar la recopilación y el monitoreo de datos a largo plazo y con eficiencia energética en áreas remotas y con infraestructura limitada. Estos dispositivos impulsan la agricultura de precisión, el seguimiento de flotas, el monitoreo ambiental y la seguridad de activos críticos mientras funcionan con un mínimo de energía.

Póngase en contacto con nuestro equipo dedicado de expertos para descubrir cómo las soluciones satelitales de Globalstar pueden brindar seguridad, eficiencia y durabilidad a sus aplicaciones de IoT. Le mostraremos cómo la conectividad satelital global de Globalstar puede impulsar la innovación en cualquier lugar del mundo.

Globalstar™