



EBOOK

Beyond Power Constraints: Securing Low-Power Satellite IoT Devices





The market opportunity for low-power IoT devices is rapidly expanding as industries seek efficient, scalable, and long-lasting solutions to support Massive IoT deployments. With the rise of smart cities, precision agriculture, asset tracking, and fleet management, the demand for battery-efficient, low-bandwidth devices is at an all-time high.

Businesses need IoT sensors and tracking solutions that can operate for years on minimal power, reducing maintenance costs and enabling remote, always-on connectivity. As industries move toward edge computing and energy-efficient wireless technologies, low-power IoT devices will be essential in accessing real-time data insights while minimizing operations costs and extending device lifespan.

The security challenges associated with low-power IoT devices stem from their mass deployment, widespread accessibility, and limited ability to support advanced security measures. Unlike centralized IT systems, which operate in controlled environments, low-power IoT devices are often deployed in vast, open networks – across cities, farmland, utilities sites – making them vulnerable to cyber threats.

The sheer number of these devices creates an expanded attack surface, where compromising even a small fraction of them can have a cascading impact on an entire system. Additionally, IoT ecosystems rely on multi-vendor interoperability, meaning security weaknesses in one device or network layer can introduce vulnerabilities through the entire ecosystem, exposing sensitive data, disrupting operations, or even enabling large scale DDoS attacks.

Further compounding these risks, low-power IoT devices are inherently limited in processing power, memory, and storage, making it difficult to implement strong encryption, authentication, or intrusion detection systems. Unlike high-performance computing devices, which can support robust security protocols, many low-power IoT devices lack the resources for real-time monitoring, frequent software updates, or complex cryptographic functions.

This makes them targets for attackers seeking to exploit weak authentication mechanisms, hijack devices communications, or inject malicious firmware. And because these devices are often designed for long lifespans with minimal maintenance, their security measures may become outdated over time, leaving them increasingly vulnerable as threat landscapes evolve.

Addressing these challenges requires a balance between efficiency and security to mitigate risks without overwhelming the limited capabilities of low-power devices. Security approaches are evolving to ensure that even the most lightweight devices can operate safely without compromising efficiency or performance. By leveraging optimized security frameworks, adaptive authentication methods, and network-based safeguards, organizations can mitigate risks while maintaining the scalability and longevity of their IoT deployments.

The IoT Heartbeat Signal

Security, power optimization, and efficiency are key considerations for satellite-powered IoT. One critical factor influencing all three is whether an IoT device requires a heartbeat signal.

A heartbeat is a signal a device sends to confirm its operation, even when no new data is transmitted. While this approach has its uses, satellite-powered IoT devices that only send data when necessary – eliminating the need for a constant heartbeat – offer significant benefits, particularly for security and power conservation.

How No-Heartbeat Communication Enhances IoT Security

When IoT devices do not send regular heartbeat signals, they effectively reduce their digital footprint, making them less susceptible to interception, tracking, and cyberattacks. A heartbeat signal can act as a beacon that reveals a device's location and existence within a network. In applications where discretion and security are paramount – such as defense, critical infrastructure monitoring, and industrial asset tracking – minimizing unnecessary transmissions can prevent potential vulnerabilities.

IoT devices remain undetectable except during critical moments when real-time information is required. By only transmitting data when necessary, this low probability of interception (LPI) and low probability of detection (LPD) approach makes it significantly harder for bad actors to exploit predictable transmissions.



What Happens When There Is a Heartbeat?

In traditional IoT models, many devices send a heartbeat at predetermined intervals – every few minutes, hourly, or daily – even if there is no meaningful data to report. This allows network operators to confirm that the device is active, ensure stable connectivity, and detect potential failures early.

However, this regular transmission creates several challenges:

- **Increased power consumption:** Each heartbeat transmission uses energy, particularly problematic for battery-powered or solar-powered IoT devices deployed in the field for long-term operation.
- **Higher data transmission costs:** Frequent heartbeat signals can add up in satellite-based IoT deployments, where data transmission is expensive.
- **Security and privacy risks:** Constant transmission patterns create a predictable signal, making it easier for attackers to detect and exploit the network.

When and Why Some IoT Devices Require a Heartbeat

Despite its disadvantages, a heartbeat can be essential in some applications, particularly those that require real-time device monitoring, immediate failure detection, or active network engagement.

Some key scenarios where a heartbeat is required include:

- **Medical IoT devices:** Remote patient monitoring systems often require constant connectivity to ensure critical health data is continuously available.
- **High-security systems:** Some banking or financial systems rely on regular heartbeats to detect potential outages or tampering attempts.
- **Network maintenance and system health checks:** In situations where latency or downtime could cause catastrophic failures, frequent heartbeats help maintain operational visibility.



The Tradeoffs: When a Heartbeat is Disadvantageous

While heartbeats provide real-time device monitoring, their disadvantages are notable, particularly for low-power, remote IoT deployments.

- **Frequent power drain:** Devices that continuously check in with a network consume energy more quickly, requiring frequent maintenance or battery replacements.
- **Higher cost of ownership:** Organizations incur higher satellite data fees when unnecessary transmissions occur over time.
- **Greater risk of detection:** Devices emitting regular signals become easy targets for interception or network attacks.

As IoT expands into numerous industries through hundreds of applications, the need for efficient, low-power, and secure communication is more critical than ever. Eliminating the need for a constant heartbeat provides power conservation, security, and operational cost-efficiency advantages. While there are valid use cases for heartbeat, the strategic use of event-driven, needs-based transmission will define the next generation of satellite-powered IoT deployments, ensuring devices remain functional in the field for extended periods while maintaining operational integrity.

By leveraging a no-heartbeat design, IoT devices can function longer, more securely, and more efficiently – making them a preferred choice for mission-critical applications where power, cost, and stealth are priorities.

A Network with End-to-End Security

A network has several touchpoints where security vulnerabilities can appear, creating several attack surfaces. Having a secure network from end to end makes a holistic approach to security

How a Satellite Network Operates

1 The Device Initiates Communication

- The user device sends data using radio frequency signals
- The data is encrypted before transmission to ensure security
- The device is equipped with a satellite modem and an antenna to communicate with the satellite

2 Uplink to the Satellite

- The device transmits the encrypted signal to a satellite
- The satellite receives and retransmits the signal

3 Satellite Relays the Signal

- The satellite directly transmits the signal to the endpoint through a satellite-to-ground connection

4 Downlink to Ground Station

- The satellite sends the signal to a secure ground station or gateway
- The ground station decrypts, processes, and forwards the data to the designated endpoint

5 Endpoint Receives the Data

- The final endpoint (military command center, cloud server, another device) receives the data securely
- The encryption ensures only the intended recipient can decrypt and access the message

The Value of Network Security

End-to-end network security in satellite IoT systems consists of strategies, technologies, and protocols that protect data's integrity, confidentiality, and availability as it moves across a network. It's essential for preventing unauthorized access, cyberattacks, data breaches, and disruptions in communication systems.

Key Components of Network Security

✓ Confidentiality

- Ensures that only authorized users and devices can access sensitive data
- Uses encryption protocols to secure communication

✓ Integrity

- Prevents data tampering by ensuring messages are authentic and unaltered during transmission

✓ Availability

- Ensures that legitimate users can access network resources when needed, without disruption from attacks like DDoS

Because satellite IoT networks transmit sensitive data, such as remote equipment status, environmental monitoring, and asset tracking information. Without strong security measures, hackers or malicious actors could intercept, manipulate, or disrupt communications, leading to financial losses, operational downtime, or national security threats.

Unlike cellular networks, satellite communication involves multiple relay points (ground stations, satellites, receiving devices), which increases the risk of data corruption or interception. VPNs, encryption, and other methods can help ensure that transmitted data remains unchanged and tamper-proof from origin to destination.





How Network Security Supports Low-Power Devices in IoT Security

Low-power devices operate with limited computational resources and minimal power consumption and often lack built-in security mechanisms. Network security frameworks provide critical protection for low-power IoT devices, ensuring secure data transmission, device authentication, and protection from unauthorized access without overloading the device's power consumption.

Traditional security mechanisms often drain power too quickly, making them impractical for these devices. By leveraging network security at the network level, IoT devices remain secure, energy-efficient, and resistant to cyber threats while maintaining reliable connectivity.

A Note on Satellite Connectivity for Low-Power Devices

Critical hardware, software, and network approaches can offer robust security for low-power devices. However, it is important to note that cellular connectivity isn't the only path for low-power devices.

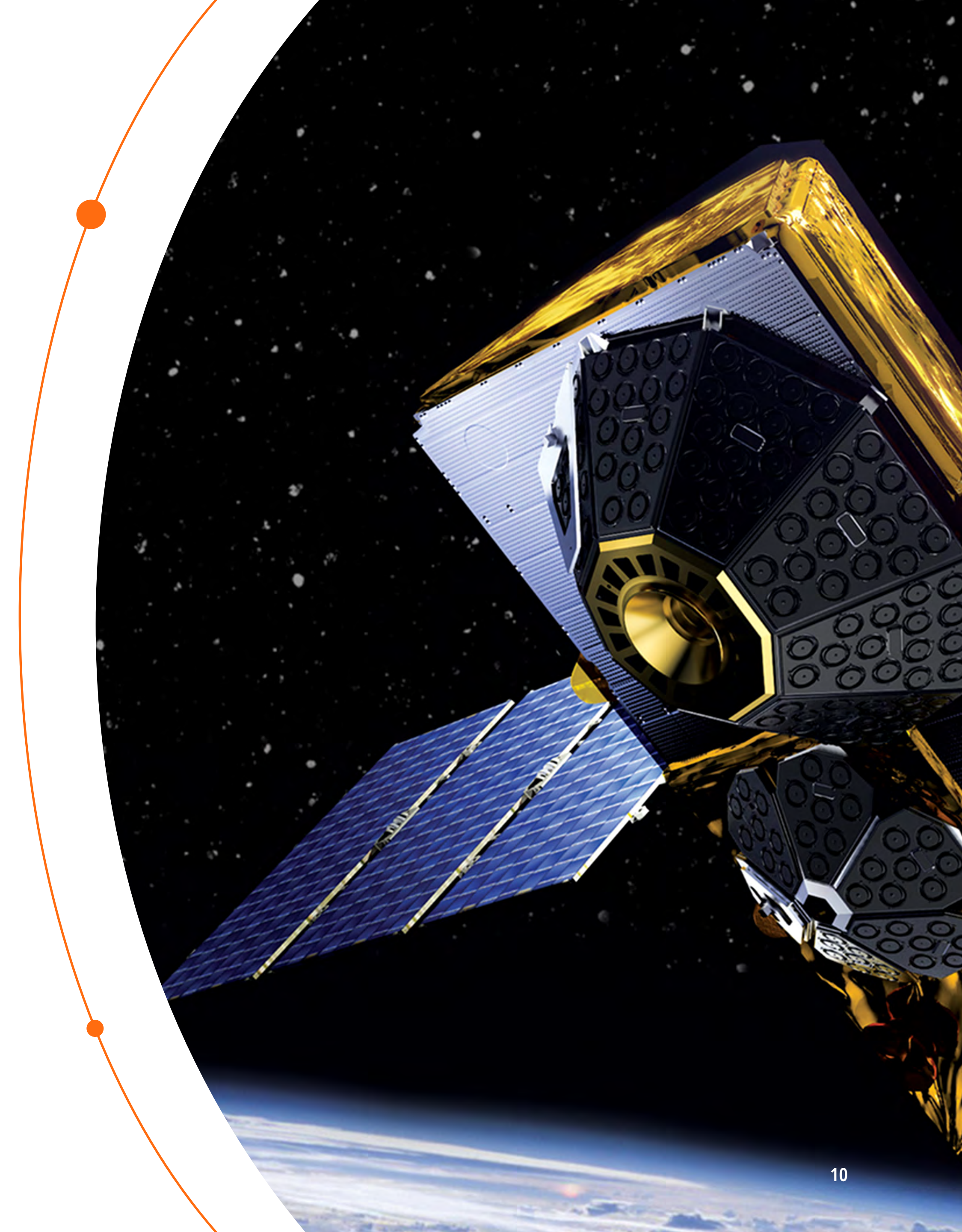
Low-power connectivity can be offered through satellites and is highly beneficial for Massive IoT applications where cellular infrastructure is minimal or unavailable, such as maritime, agriculture, oil and gas, mining, and many more.

The satellite orbit is crucial when considering this connectivity method for low-power devices, and the closer to Earth, the better.

How LEO Satellites Help with Low-Power Devices

There are three different orbital distances for satellites: low-earth Orbit (LEO), Medium-Earth Orbit (MEO), and Geostationary Orbit (GEO). As the name implies, LEO satellites are much closer to the earth, and this proximity provides several advantages, particularly for devices with limited battery capacity.


Unlike GEO satellites, which remain fixed over one point on Earth, LEO satellites move faster, completing an orbit in 90-120 minutes. Constellations of LEO satellites provide seamless coverage by handing off signals as they move across the sky.



There are several key ways that LEO satellites support low-power devices:

- **Reduced power requirements:** One of the most significant advantages of LEO satellites is that their shorter distance to Earth means devices don't need to transmit signals at high power levels. The LEO to GEO path loss difference (or link budget difference) is roughly 28dB. Since radio signals travel a much shorter path than GEO satellites, the transmission power required for communication is slightly lower. This allows devices to conserve battery life, making them more efficient for long-term operations.
- **Lower latency for energy efficiency:** Because of their proximity to Earth, LEO satellites offer a reduction in latency, which reduces a device's time spent staying active for communication, saving energy. This is especially useful for IoT devices that rely on intermittent data transmission and need to optimize battery usage.
- **Smaller and more efficient antennas:** Due to their proximity, LEO satellites provide a stronger signal, allowing devices to use smaller, low-power antennas instead of the large-power-hungry dishes required for GEO satellites. This is critical for applications where compact, energy-efficient hardware is necessary, such as wearable GPS trackers, remote weather sensors, and environmental monitoring devices.
- **More satellites for easier access:** LEO satellite networks operate as constellations, meaning multiple satellites are in orbit at any given time. Devices don't need to boost their power output to reach a single distant satellite. Instead, they connect to the nearest satellite, extending battery life.
- **Smart beamforming for power optimization:** LEO satellites use beamforming, which focuses radio signals toward specific areas instead of broadcasting in all directions. This increases signal strength and reduces the power devices need to communicate effectively. Devices can transmit at lower power levels while maintaining strong connections, extending battery life.

LEO satellites offer a game-changing solution for businesses and industries deploying low-power communication networks in remote or challenging environments. By reducing power requirements, optimizing efficiency, and providing global coverage, these satellites are revolutionizing how devices stay connected in a world that demands seamless and sustainable communication.



The Value of Low-Power Devices in the IoT Ecosystem

Low-power IoT devices are revolutionizing industries by enabling long-term, energy-efficient data collection and monitoring in remote and infrastructure-limited areas. These devices power precision agriculture, fleet tracking, environmental monitoring, and critical asset security while operating on minimal energy.

Contact our dedicated team of experts to discover how Globalstar's satellite solutions can deliver security, efficiency, and longevity for your IoT applications. We'll show you how Globalstar's global satellite connectivity can drive innovation anywhere in the world.

Globalstar ™