Globalstar™

EBOOK

# Além das Limitações de Energia

## Proteção a Dispositivos de IoT via Satélite de Baixo Consumo

A oportunidade de mercado para dispositivos de IoT de baixo consumo expande-se rapidamente à medida que os setores buscam soluções eficientes, expansíveis e  duradouras para permitir implantações de IoT massiva. Com o surgimento de cidades inteligentes, agricultura de precisão, rastreio de ativos e gerenciamento de frotas, a demanda por dispositivos eficientes em termos de bateria e de baixa largura de banda está sempre em alta.

As empresas precisam de sensores de IoT e soluções de rastreio que possam operar por anos com o consumo mínimo de energia, reduzindo custos de manutenção e permitindo conectividade remota e sempre ativa. À medida que os setores avançam em direção a tecnologias sem fio com eficiência energética e de computação de borda, os dispositivos de IoT de baixo consumo serão essenciais para acessar insights de dados em tempo real, minimizando os custos operacionais e estendendo a vida útil do dispositivo.

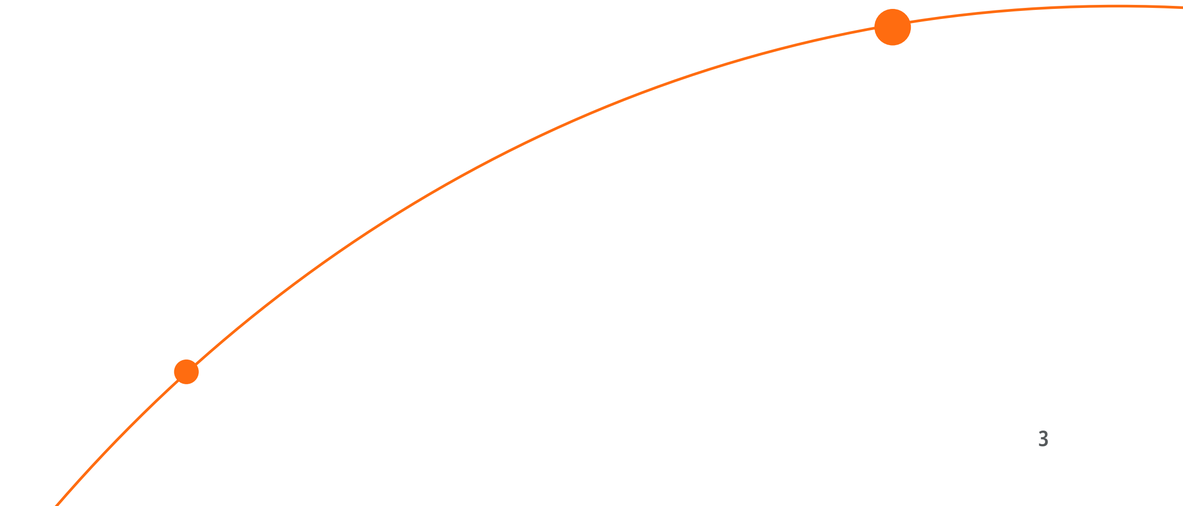
Os desafios em termos de segurança associados a dispositivos de IoT de baixo consumo decorrem de sua implantação em massa, ampla acessibilidade e capacidade limitada de suportar medidas de segurança avançadas. Diferentemente dos sistemas de TI centralizados, que operam em ambientes controlados, os dispositivos de IoT de baixo consumo geralmente são implantados em redes amplas e abertas (em cidades, áreas cultivadas, locais de serviços de utilidade pública), o que os torna vulneráveis a ameaças cibernéticas.

A grande quantidade desses dispositivos cria uma superfície de ataque expandida, em que comprometer mesmo uma pequena fração deles pode ter um impacto em cascata em todo o sistema. Além disso, os ecossistemas de IoT dependem da interoperabilidade de vários fornecedores; ou seja, falhas de segurança em um dispositivo ou camada de rede podem introduzir vulnerabilidades em todo o ecossistema, expondo dados sensíveis, interrompendo operações ou até mesmo permitindo ataques DDoS em larga escala.

Para agravar ainda mais esses riscos, os dispositivos de IoT de baixo consumo são inerentemente limitados em termos de poder de processamento, memória e armazenamento, dificultando a implementação de sistemas fortes de criptografia, autenticação ou detecção de invasões. Ao contrário dos dispositivos de computação de alto desempenho, que podem aceitar protocolos de segurança robustos, muitos dispositivos de IoT de baixo consumo não têm recursos para monitoramento em tempo real, atualizações frequentes de software ou funções criptográficas complexas.

Isso os torna alvos de invasores que buscam explorar mecanismos de autenticação frágeis, sequestrar comunicações de dispositivos ou injetar firmware malicioso. E como esses dispositivos geralmente são projetados para uma vida útil longa com manutenção mínima, suas medidas de segurança podem ficar desatualizadas com o tempo, deixando-os cada vez mais vulneráveis à medida que os cenários de ameaças evoluem.

Enfrentar esses desafios exige um equilíbrio entre eficiência e segurança para mitigar riscos sem sobrecarregar as capacidades limitadas dos dispositivos de baixo consumo. As abordagens de segurança estão evoluindo para garantir que mesmo os dispositivos mais leves possam operar com segurança sem comprometer a eficiência ou o desempenho. Ao usar estruturas de segurança otimizadas, métodos de autenticação adaptáveis e proteções baseadas em rede, as organizações podem mitigar riscos enquanto mantêm a expansibilidade e a durabilidade de suas implantações de IoT.



# O Sinal de Pulso da IoT

Segurança, otimização de energia e eficiência são considerações essenciais para a IoT alimentada por satélite. Um fator crucial que influencia os três é se um dispositivo de IoT requer um sinal de frequência.

Um pulso é um sinal que um dispositivo envia para confirmar seu funcionamento, mesmo quando nenhum dado novo é transmitido. Embora essa abordagem tenha suas utilidades, os dispositivos de IoT alimentados por satélite que só enviam dados quando necessário, eliminando a necessidade de um pulso constante, oferecem benefícios significativos, especialmente em termos de segurança e conservação de energia.

## Como a Comunicação Sem Pulso Melhora a Segurança da IoT

Quando os dispositivos de IoT não enviam sinais de pulso regulares, eles reduzem efetivamente sua pegada digital, tornando-os menos suscetíveis à interceptação, rastreio e ataques cibernéticos. Um sinal de pulso pode atuar como um farol que revela a localização e a existência de um dispositivo dentro de uma rede. Em aplicações em que a discrição e a segurança são fundamentais, como defesa, monitoramento de infraestrutura crítica e rastreio de ativos industriais, minimizar transmissões desnecessárias pode evitar possíveis vulnerabilidades.

Os dispositivos de IoT permanecem indetectáveis, exceto durante momentos críticos, quando são necessárias informações em tempo real. Ao transmitir dados somente quando necessário, essa abordagem de baixa probabilidade de interceptação (LPI) e baixa probabilidade de detecção (LPD) torna significativamente mais difícil para agentes mal-intencionados explorar transmissões previsíveis.

## O Que Acontece Quando Há um Pulso?

Em modelos de IoT tradicionais, muitos dispositivos enviam um pulso em intervalos predeterminados (a cada poucos minutos, a cada hora ou diariamente), mesmo que não haja dados significativos para relatar. Isso permite que os operadores de rede confirmem se o dispositivo está ativo, garantam conectividade estável e detectem possíveis falhas com antecedência.

**No entanto, essa transmissão regular cria vários desafios:**

- **Maior consumo de energia:** cada transmissão de pulso consome energia, o que é especialmente problemático para dispositivos de IoT alimentados por bateria ou energia solar implantados em campo para operação de longo prazo.
- **Maiores custos de transmissão de dados:** sinais de pulso constantes podem se somar em implantações de IoT baseadas em satélite, em que a transmissão de dados é cara.
- **Riscos à segurança e privacidade:** padrões de transmissão constantes geram um sinal previsível, facilitando a detecção e a exploração da rede por invasores.

## Quando e Por Que Alguns Dispositivos de IoT Exigem um Pulso

Apesar de suas desvantagens, um pulso pode ser essencial em algumas aplicações, especialmente aquelas que exigem monitoramento de dispositivos em tempo real, detecção imediata de falhas ou engajamento ativo na rede.

**Alguns cenários importantes em que um pulso é necessária incluem:**

- **Dispositivos médicos de IoT:** os sistemas de monitoramento remoto de pacientes geralmente exigem conectividade constante para garantir que dados críticos de saúde estejam continuamente disponíveis.
- **Sistemas de alta segurança:** alguns sistemas bancários ou financeiros dependem de pulsos regulares para detectar possíveis interrupções ou tentativas de alteração.
- **Verificações de integridade do sistema e manutenção da rede:** em situações quando a latência ou paralisações podem causar falhas catastróficas, os pulsos constantes ajudam a manter a visibilidade operacional.

## As Desvantagens: Quando um Pulso é Desvantajoso

Embora os pulsos forneçam monitoramento de dispositivos em tempo real, suas desvantagens são notáveis, especialmente em implantações de IoT remotas e de baixo consumo.

- **Consumo de energia frequente:** dispositivos que se conectam continuamente à rede consomem energia com mais rapidez, exigindo manutenção ou substituições de baterias frequentes.
- **Maior custo de propriedade:** quando ocorrem transmissões desnecessárias ao longo do tempo, isso implica em custos mais altos da transmissão de dados via satélite para as organizações.
- **Maior risco de detecção:** dispositivos que emitem sinais regularmente são alvos fáceis para interceptação ou ataques de rede.

À medida que a IoT se expande para vários setores por meio de centenas de aplicações, a necessidade de comunicação eficiente, de baixo consumo e segura é mais essencial do que nunca. Eliminar a necessidade de um pulso constante proporciona vantagens em termos de conservação de energia, segurança e economia operacional. Embora haja casos de uso válidos para pulso, o uso estratégico da transmissão baseada em eventos e necessidades definirá a próxima geração de implantações de IoT alimentadas por satélite, garantindo que os dispositivos permaneçam funcionais em campo por longos períodos e ainda mantenham a integridade operacional.

Ao usar um modelo sem pulso, os dispositivos de IoT podem funcionar por mais tempo, com mais segurança e eficiência, o que os torna a escolha preferível para aplicações indispensáveis, nas quais energia, custo e discrição são prioridades.

# Uma Rede com Segurança de Ponta a Ponta

Uma rede tem vários pontos de contato em que vulnerabilidades de segurança podem surgir, criando diversas superfícies de ataque. Ter uma rede segura de ponta a ponta proporciona uma abordagem holística em prol da segurança.

## Como Funciona uma Rede de Satélites

### 1 O Dispositivo Inicia a Comunicação

- O dispositivo do usuário envia dados por meio de sinaisde radiofrequência
- Os dados são criptografados antes da transmissão para garantir a segurança
- O dispositivo é equipado com um modem via satélite e uma antena para comunicação com o satélite

### 2 Uplink para o Satélite

- O dispositivo transmite o sinal criptografado para um satélite
- O satélite recebe e retransmite o sinal

### 3 O Satélite Retransmite o Sinal

- O satélite transmite o sinal diretamente para o endpoint por meio de uma conexão satélite–solo

### 4 Downlink para a Estação em Solo

- O satélite envia o sinal para uma estação em solo segura ouum gateway
- A estação em solo descriptografa, processa e encaminha os dados para o endpoint designado

### 5 O Endpoint Recebe os Dados

- O endpoint final (centro de comando militar, servidor em nuvem, outro dispositivo) recebe os dados com segurança
- A criptografia garante que somente o destinatário pretendido possa descriptografar e acessar a mensagem

## O Valor da Segurança de Rede

A segurança de rede de ponta a ponta em sistemas de IoT via satélite consiste em estratégias, tecnologias e protocolos que protegem a integridade, a confidencialidade e a disponibilidade dos dados à medida que eles se movem pela rede. É essencial para evitar acesso não autorizado, ataques cibernéticos, violações de dados e interrupções nos sistemas de comunicação.

**Componentes importantes da segurança de rede**

### Confidencialidade

- Garante que apenas dispositivos e usuários autorizados possam acessar dados sensíveis
- Usa protocolos de criptografia para proteger a comunicação

### Integridade

- Evita alteração de dados, garantindo que as mensagens sejam autênticas e permaneçam inalteráveis durante a transmissão

### Disponibilidade

- Garante que usuários legítimos possam acessar recursos de rede quando necessário, sem interrupção causada por ataques, como DDoS

Porque as redes de IoT via satélite transmitem dados sensíveis, como status de equipamentos remotos, monitoramento ambiental e informações de rastreio de ativos. Sem medidas de segurança fortes, hackers ou agentes mal-intencionados podem interceptar, manipular ou interromper as comunicações, levando a perdas financeiras, paralisação operacional ou ameaças à segurança nacional.

Ao contrário das redes celulares, a comunicação via satélite envolve vários pontos de retransmissão (estações em solo, satélites, dispositivos receptores), o que aumenta o risco de corrupção ou interceptação de dados. VPNs, criptografia e outros métodos podem ajudar a garantir que os dados transmitidos permaneçam inalterados e à prova de alteração desde a origem até o destino.

## Como a Segurança de Rede Auxilia Dispositivos de Baixo Consumo na Segurança da IoT

Dispositivos de baixo consumo operam com recursos computacionais limitados e consumo mínimo de energia e, muitas vezes, não possuem mecanismos de segurança integrados. Frameworks de segurança de rede fornecem proteção essencial para dispositivos de IoT de baixo consumo de energia, garantindo transmissão segura de dados, autenticação de dispositivos e proteção contra acesso não autorizado sem sobrecarregar o consumo de energia do dispositivo.

Os mecanismos de segurança tradicionais geralmente consomem energia com muita rapidez, o que os torna inviáveis para esses dispositivos. Ao usar a segurança de rede no nível da rede, os dispositivos de IoT permanecem seguros, eficientes em termos de consumo e resistentes a ameaças cibernéticas, mantendo uma conectividade confiável.

# Uma Observação sobre a Conectividade via Satélite para Dispositivos de Baixo Consumo

Avanços cruciais em hardware, software e rede podem oferecer segurança robusta para dispositivos de baixo consumo. No entanto, é importante observar que a conectividade celular não é o único caminho para dispositivos de baixo consumo.

A conectividade de baixo consumo pode ser oferecida via satélite e é altamente benéfica para aplicações numerosas de IoT em setores com infraestrutura celular mínima ou indisponível, como marítima, agrícola, de petróleo e gás, mineração e muito mais.

A órbita do satélite é crucial ao considerar esse método de conectividade para dispositivos de baixo consumo, e quanto mais próximo da Terra, melhor.

## Como os Satélites LEO Ajudam com Dispositivos de Baixo Consumo

Há três distâncias orbitais diferentes para satélites: órbita terrestre baixa (LEO), órbita terrestre média (MEO) e órbita geoestacionária (GEO). Como o nome indica, os satélites LEO estão muito mais próximos da Terra, e essa proximidade traz várias vantagens, especialmente para dispositivos com capacidade limitada de bateria.

Ao contrário dos satélites GEO, que permanecem fixos em um ponto da Terra, os satélites LEO se movem mais rápido, completando uma órbita em cerca de 90 a 120 minutos. Constelações de satélites LEO oferecem uma cobertura consistente ao transmitir sinais enquanto se movem pelo céu.

## Há vários meios importantes pelos quais os satélites LEO auxiliam dispositivos de baixo consumo:

- **Menos requisitos de energia:** uma das vantagens mais significativas dos satélites LEO é que sua menor distância da Terra permite que os dispositivos não precisem transmitir sinais de alta potência. A diferença de perda no percurso entre LEO e GEO (ou diferença de orçamento de link) é de aproximadamente 28 dB. Como os sinais de rádio percorrem um caminho muito mais curto do que os satélites GEO, a energiade transmissão necessária para a comunicação é um pouco menor. Isso permite que os dispositivos conservem a vida útil da bateria, tornando-os mais eficientes para operações de longo prazo.

- **Menor latência para eficiência energética:** devido à sua proximidade com a Terra, os satélites LEO oferecem uma redução na latência, o que reduz o tempo gasto pelo dispositivo para permanecer ativo para comunicação, economizando energia. Isso é especialmente útil para dispositivos de IoT que dependem de transmissão intermitente de dados e precisam otimizar o uso da bateria.

- **Antenas menores e mais eficientes:** devido à sua proximidade, os satélites LEO fornecem um sinal mais forte, permitindo que os dispositivos usem antenas menores e de baixo consumo no lugar de antenas parabólicas grandes que consomem muita energia, necessárias para os satélites GEO. Isso é crucial para aplicações que exigem hardware compacto e economizam energia, como rastreadores GPS vestíveis, sensores climáticos remotos e dispositivos de monitoramento ambiental.

- **Mais satélites para facilitar o acesso:** as redes de satélites LEO funcionam como constelações; ou seja, vários satélites estão em órbita a todo momento. Os dispositivos não precisam aumentar sua saída energética para alcançar um único satélite distante. Em vez disso, eles se conectam ao satélite mais próximo, aumentando a vida útil da bateria.

- **Formação de feixe inteligente para otimização de energia:** os satélites LEO usam formação de feixe, que concentra sinais de rádio em áreas específicas em vez de transmitir em todas as direções. Isso aumenta a intensidade do sinal e reduz a energia necessária para que os dispositivos se comuniquem de forma eficaz. Os dispositivos podem transmitir com níveis energéticos mais baixos, mantendo conexões fortes, prolongando a vida útil da bateria.

Os satélites LEO oferecem uma solução revolucionária para empresas e setores que implantam redes de comunicação de baixo consumo em ambientes remotos ou desafiadores. Ao reduzir os requisitos de energia, otimizar a eficiência e fornecer cobertura global, esses satélites estão revolucionando a maneira como os dispositivos permanecem conectados em um mundo que exige comunicação consistente e sustentável.

# O Valor dos Dispositivos de Baixo Consumo no Ecossistema da IoT

Dispositivos de IoT de baixo consumo estão revolucionando setores ao permitir a coleta e o monitoramento de dados de longo prazo e com eficiência energética em áreas remotas e com infraestrutura limitada. Esses dispositivos alimentam agricultura de precisão, rastreio de frotas, monitoramento ambiental e segurança de ativos essenciais, operando com o mínimo de energia.

Entre em contato com nossa equipe dedicada de especialistas para descobrir como as soluções de satélite da Globalstar podem oferecer segurança, eficiência e longevidade para suas aplicações de IoT. Mostraremos como a conectividade global via satélite da Globalstar pode impulsionar a inovação em qualquer lugar do mundo.

Globalstar™