kerlink
communication is everything

Whitepaper – January 2018

Optimizing Device Lifecycle Management Of Remote, IoT Connected, LPWA Devices

Introduction

Low-Power Wide Area (LPWA) Internet of Things technologies allow service providers and enterprises to offer long-range connectivity for battery-powered objects that consume little energy. Some popular use cases for LPWA devices include temperature and environmental sensors; smart meters for gas, electricity and water; asset and inventory tracking; agribusiness support; and industrial monitoring. One of the common attributes of LPWA devices is device longevity: generally, an LPWA-equipped sensor or a meter is expected to operate for more than 10 years.

Challenges of LPWAN DM

- Low power device
- Device longevity
- Device proliferation

But low-power and longevity requirements of Internet of Things (IoT) endpoints make LPWA device management (DM) an essential and challenging component of an end-to-end IoT solution. Managing a device that minimizes its consumption of power and has a 10 or more year expected lifetime is difficult. But managing millions of these types of devices cost effectively is even more challenging. Service providers and enterprises must select a leading LPWA IoT DM vendor in order to streamline their operations, adapt to changing regulatory, industry and market expectations and generate new revenue streams.

Device Management, a Critical Tool for Scalable Deployment and Management of IoT Devices

With billions of sensors, meters, actuators and other devices expected to be connected to the IoT, remote device management allows service providers and enterprises to:

- Directly manage network provisioning including device subscription
- Launch and support **new functionalities** and **applications**
- Ensure **compliance** with **telecommunication standards**
- Ensure **compliance** with r**egional radio regulations**
- Provide **security management** including key management for authentication
- Manage **radio performance** with dynamic LPWA network behavior monitoring
- Optimize **radio footprint** to manage device power consumption

> **“Kerlink’s Wanesy™ Device Management Platform offers mobile network operators, smart cities and enterprise customers a complete, secure and standard solution.”**
>
> *Yannick Delibie*
> *Kerlink, Chief Technology Officer*

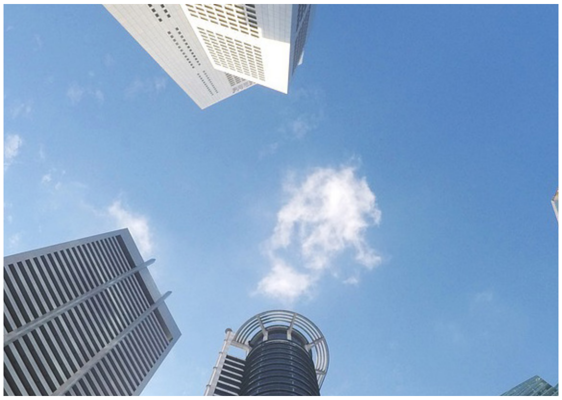
Kerlink's Wanesy™ Device Management Platform offers mobile network operators, smart cities and enterprise customers a complete, secure and standard solution to manage and optimize all connected devices over their lifetime.

Device Management for LPWA Networks Using ISM Bands

LPWA networks are based on the same star network topology as 3GPP networks including the presence of a core network, base stations, sensors, devices, radio communications and commissioning management systems. This type of network topology allows network operators to focus on high-quality security, the use of rating, billing and other operations systems and the use of various application-server interfaces.

But there are some key differences between LPWA and other 3GPP technologies. On the radio side, LPWA networks often use unlicensed, free spectrum for transmission and reception in the industrial, scientific and medical bands. These so-called **ISM bands** are defined by geographical regions as follows:

- Europe: 863-873Mhz
- North and South America: 902-928Mhz
- Asia: 915-928Mhz.



These unlicensed ISM bands must meet certain parameters that increase LPWA quality, but they also impose some constraints on the network, especially duty-cycle limitations of typically 1 percent on-air and transmission power of less than 14dBm-25mW to share radio resources. In addition, to maximize sensitivity up to -141dBm to facilitate long-range communications, the radio modulation (Ultra Narrow Band or LoRa®) uses low data rates, typically below 1kbit/s.

Because of the unique attributes of LPWA networks, service providers and enterprises must select IoT DM solutions that are uniquely designed to address and respond to the characteristics of LPWA networks and devices. IoT DM is powered by a set of technological tools and features for **managing the lifecycle of IoT-connected equipment** including LPWA end devices. These tools allow users of **Kerlink's Wanesy™ Device Management Platform** to:

- **Configure applicative parameters** including logical name, application destination and wake-up behavior
- **Configure protocol parameters** such as net address or radio parameters including channel and modulation
- **Ensure device security**, **key management** and **network subscription** including commissioning
- **Monitor device behavior**, power consumption and radio footprint
- **Manage network performance** with over-the-air adaptive channel configuration while managing radio footprint and cell scalability related to regional radio constraints
- **Conduct** complete or partial **over-the-air firmware** updates including in batches or pre-set campaigns

IoT DM is commonly used in mobile communications based on the Open Mobile Alliance DM (**OMA DM**) standard. This standard creates a protocol for LightweightM2M (**LwM2M**) over Constraint Application Protocol (**CoAP**) which is generally well suited to 3GPP topology networks. The Internet Engineering Task Force (**IETF**) is also defining a suite of protocol for LPWAN using CoAP Management Interface (**CoMI**).

Interestingly, the characteristics of LPWA networks impact some features of IoT DM. By adapting their solutions for the unique requirements of LPWA,

Word of the Expert 1:

CRUDEN - the six basic functions of device management

There are six basic operations that describe typical interactions between end devices and an IoT device management (DM) system. The acronym CRUDEN - a modified version of the acronym CRUD that is associated with computing and persistent storage - represents these six operations: **C**reate, **R**ead, **U**pdate, **D**elete, **E**xecute, **N**otify.

Create: A remote system can create a resource on an end device. For instance, a new firmware update session can be instantiated using the create operation.

Read: An IoT DM system is able to read end device resources. A common example of a read operation is the aggregation of radio interface statistics from a set of devices.

Update: Service providers and enterprises can use an update operation to change a configuration parameter including application behaviors on an end device.

Delete: Once created, resources including configuration resources can be erased by the delete operation.

Execute: What is pertinent and innovative for IoT device management platform is the ability not only to read and write, but also execute commands on end devices. These command could be simple such as reboot commands, but could also be more complex such as applying firmware updates, performing factory resets or activating an actuator.

Notify: Finally, a notify operation allows end devices to autonomously send data to remote systems without the need of polling. For example, an IoT device management system can subscribe to the battery level of the end device and request to be notified when the level reaches a prescribed threshold. No polling is required to complete this notification operation.

CoAP – a data transfer protocol for IoT

Constrained Application Protocol (**CoAP**), an IETF proposed standard as described in RFC 7252, is the standard and widely used data transfer protocol designed for LPWA end devices. CoAP is designed for constrained devices such as LoRaWAN™ end devices and provides a request/response interaction model very similar to the RESTful model. It easily maps with HTTP, but exhibits much lower overhead on the system.

Interestingly, CoAP provides a seventh operational function - the observe operation - to the CRUDEN capabilities. CoAP observe notifications, as described in RFC 7641, are directly mapped to IoT device management systems' notify operations.

CoAP for LoRaWAN™: some unique stakes and solutions

There are some unique features of LoRaWAN™ end devices that make implementation of the current CoAP standard challenging. In particular, CoAP assumes a virtually always-on connection to an end device, fairly immediate device-to-system response time and a payload that is much larger than the typical LoRaWAN™ end device delivers.

Therefore, to operate an IoT DM service for LoRaWAN™ end devices while providing the necessary CRUDEN operations, several solutions are being created to modify CoAP for LoRaWAN™. The Internet Engineering Task Force (**IETF**) LPWAN working group is defining CoAP Static Context Header Compression (**SCHC**) to fit CoAP to LoRaWAN™ and other LPWAN technologies. This work-in-progress defines an off-band allowance between end devices and remote servers to reduce the amount of in-band to transport to CoAP headers. In addition, the Open Mobile Alliance (**OMA**) is working on a definition to allow smaller CoAP payloads to accommodate LightweightM2M over LoRaWAN™.

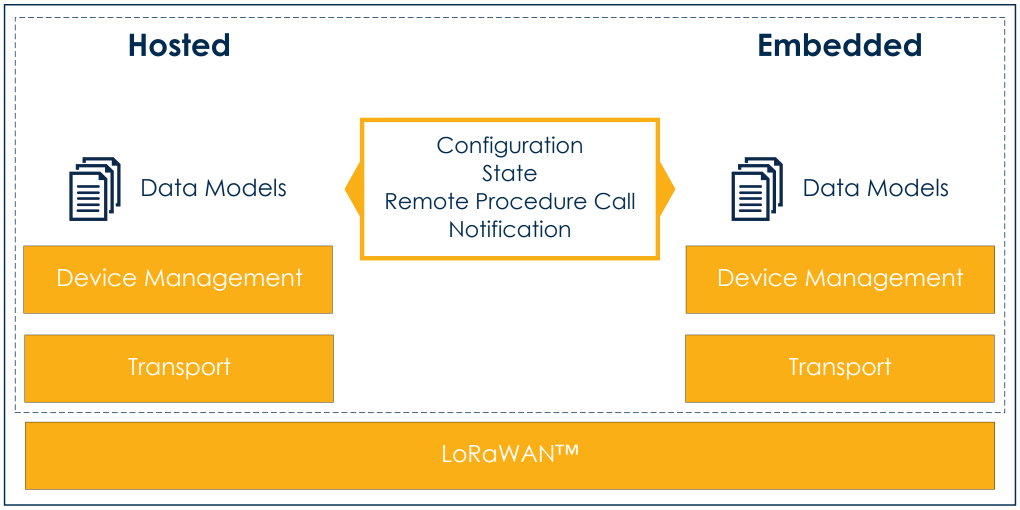


Figure 1: Device Management in a LoRaWAN™ Model

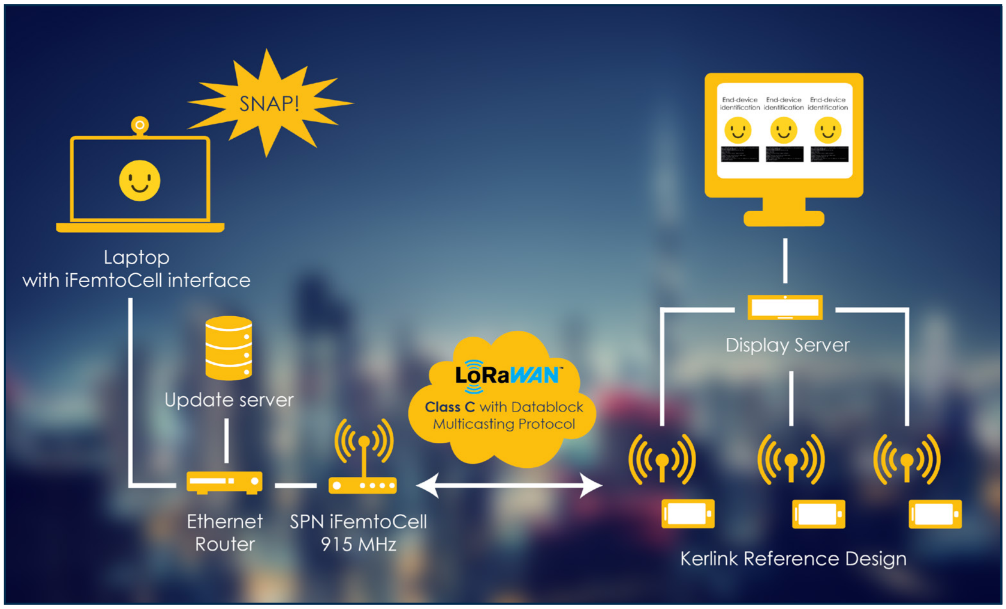


Figure 2: Kerlink IoT device management illustrating the LoRaWAN™ firmware updating process

Word of the Expert 2:

Which device management protocols and data models?

Accessing resources on an end-device using CoAP is done using a device management (DM) protocol that relies on an associated data model.

Standard DM protocols and data models can be used over LoRaWAN™ once the relevant CoAP protocol is available. We will focus on two different data models, LwM2M and CoMI .

LwM2M

LightweightM2M (**LwM2M**) is an Open Mobile Alliance (**OMA**) standard built on top of Internet Engineering Task Force (**IETF**) standards for transport protocols such as CoAP, CoAP Observe and Constrained RESTful Environments (**CoRE**) Link Format.

The LwM2M data model is specific to the standard. The LwM2M Technical Specification defines a series of objects and provides a template to define new objects. Available objects in the 1.0 specification include security, server, access control, device, connectivity monitoring, firmware update, location and connectivity statistics. Each object has resources. And each IoT device can have multiple instances of an object and multiple instances of an object's resource.

LwM2M objects are transported encoded. Several encoding schemes are defined in the specification including JSON, plain text and the more compact type-length-value (TLV) scheme. TLV is only usable over LoRaWAN™. LwM2M objects are accessed using standard CoAP requests (e.g., GET, PUT, POST and DELETE). Each object has a number identifier to reduce the URI length.

CoMI

CoAP Management Interface (**CoMI**) is an IETF Internet Draft, a preliminary technical specification. It is built on top of CoAP and is meant to complement IETF RFC 8040 RESTCON the same way that CoAP is mapped to HTTP. CoMI defines a network management interface for constrained devices including LoRaWAN™ end devices. The protocol is used to access end device resources using the YANG data modeling language. The protocol also has several optimizations to reduce payload size.

YANG 1.1 (RFC 7950) is a data modeling language used to describe end devices' configuration, state, remote procedure call and notifications. YANG data models are versioned, hierarchical and structured in modules and submodules with built-in types and several extensions including augmented hierarchies and derived types. YANG modules are text files that can be independent or part of a standard. Data models defined in YANG modules are encoded in XML in the proposed standard.

CoMI proposes a concise and efficient encoding based on the Concise Binary Object Representation (CBOR), another IETF Proposed Standard (RFC7049) using YANG-to-CBOR mapping. CoMI uses numeric identifiers for YANG called YANG Schema Item iDentifiers (SID). SIDs are registered when made public. And when multiple SIDs are used consecutively, delta encoding is used to reduce overhead.

This **combination of technologies and standards** allows enterprises and service providers to use a **fully featured Internet DM protocol on very constrained LPWA end devices**.

vendors like Kerlink can provide important LPWA-specific features of IoT DM including the ability to offer offline and maintenance status without updating; multicast capabilities with large volumes of data sent to targeted devices; and low-latency protocol adaptation such as LwM2M that is supported by a large number of service providers.

IoT device management: essential for LPWA installations

IoT remote device management is a critically important component of any IoT solution. The ability to cost-effectively and securely manage IoT devices is relevant to all IoT deployments. Based on 12 years of broad experience with worldwide customers, Kerlink has identified three reasons why IoT DM is essential in LPWA installations .

Why DM is essential for LPWA

Scale of LPWA devices

Longevity of LPWA devices

Inaccessibility of LPWA devices

1. LPWA installations at scale touch hundreds of thousands or millions of devices requiring a highly cost-efficient, scalable and global management tool.

- Communicating with extremely high numbers of IoT LPWA devices requires automated, bulk-device lifecycle management (e.g., provisioning, updating and deprovisioning). LPWA devices are generally part of large-scale deployments and benefit from bulk provisioning processes. In addition, a quality LPWA DM platform vendor supporting large-scale deployments should (1) provide **continuous quality assurance and patches** to the platform as needed, (2) **adapt the platform to the customer's evolving operational environment** with firmware, hardware and software updates and (3) **offer value-rich new features** to increase platform functionality.
- Bandwidth constraints require smarter, automated deployment of software and firmware to LPWA devices. Due to bandwidth constraints, operations departments must take into account **usage patterns** to prevent interference with usual operational or commercial communications.
- Revenue per device may be low which requires **automation to keep operational costs down** and ensure operations can financially scale in the long run.
- Third-party systems and platforms often interact with device installations and API end devices for efficient bulk operations and batch processes, therefore, **interoperability and open solutions** remain key for efficient deployment.

2. Longevity of LPWA devices requires unique features to support long-term operation and security.

- Connected devices have an expected lifetime of 10 years or more in many cases. This requires that they be **monitored and updated** by configuration or firmware switching to prevent overconsumption of power and bandwidth on the radio network.
- Intelligent DM maximizes the **efficiency of power** used for transmission so that a device's battery life is not unnecessarily diminished.
- DM must allow the **rollout of inevitable security updates** due to LPWA devices' longevity.
- Devices require endpoint radio configuration and firmware updates to stay up to date with the latest **developments in regulations**.
- Devices must be monitored to **proactively identify faults** and **prevent major problems upstream**.

3. Lack of LPWA IoT device accessibility requires a zero-touch, remote DM solution.

- **Devices must be easy to install, manage and diagnose remotely**. Installation and maintenance crews will frequently lack deep technical knowledge or adequate tools to

Word of the Expert 3:
Successfully execute over-the-air firmware updates

The LoRa Alliance™ produces recommendations for the firmware update over-the-air (FUOTA) process. Several steps are required to achieve FUOTA on a group of LoRaWAN™ end devices.

The process starts with a **multicast rendezvous** and **fragmentation session** setup. Once established, the firmware or any other binary large object is transmitted using LoRaWAN™ multicast capabilities. The LoRa Alliance™ recommendations also suggest that enterprises and service providers use the forward error correction technique to recover lost packets without the need for the network to be informed of the lost packets. Once the entire file is received, firmware authenticity and integrity are verified.

To start a **multicast session** on a group of LoRaWAN™ end devices, each device must be provisioned with session information. This can be achieved, as described earlier, using CRUDEN operations using a firmware update data model such as the one provided by LightweightM2M (LwM2M). The session information transports LoRaWAN™ specific data including multicast radio parameters (e.g., address and channel), security parameters (e.g., key derivation and counters) and session timing parameters (e.g., start point and duration).

Fragmentation information is also required for the end device to be able to reconstruct received data. Such pieces of information are not LoRaWAN™ specific and could be described using a more generic data model. Relevant information includes the number and size of each fragment sent from the update server and the encoding scheme to eventually recover missing packets.

Once setup, **multicast diffusion** of the data is handled solely by the LoRaWAN™ network layer. The multicast-capable network server selects the cluster of LoRaWAN™ gateways emitting the FUOTA request based on the relevant end devices. The timing, duty cycle and radio coverage

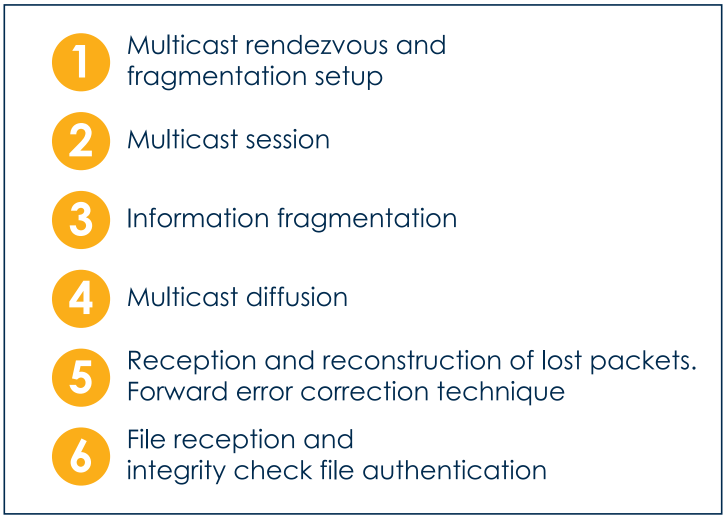

1. Multicast rendezvous and fragmentation setup
2. Multicast session
3. Information fragmentation
4. Multicast diffusion
5. Reception and reconstruction of lost packets. Forward error correction technique
6. File reception and integrity check file authentication

Figure 3: Over-the-air firmware updating process

criteria are also used to select the correct cluster of gateways.

Each end device is setup to receive data on the provided multicast address. The process handles the **reception and reconstruction of lost packets** using a **forward error correction code**. If a device becomes aware of the absence of a packet due to errors in the numbering sequence, the fragmentation session will keep sending the missing data containing redundant packets. A receiver can regenerate a missing fragment with the help of one or several backup packets and already received packets.

Finally, the system will validate the received data in two ways. First, the network will ensure that the **entire file** has been **received and reconstructed correctly**. This network integrity is done using a file integrity check, verifying a file against the network. Second, the system needs to **authenticate the file**. Authenticity must use cryptography to securely validate the origin of the file before applying it. Manufacturers can cryptographically sign the firmware file using asymmetric keys deployed during the manufacturing process of their devices.

triage the connectivity elements of these LPWA devices.

- Many IoT devices are deployed in areas that are physically difficult or costly to access. DM must provide capabilities to **configure and maintain a device remotely** once installed to allow easy troubleshooting and operation.
- Fast, simple provisioning allows solutions to be deployed quickly to **ensure the solution is replicable in a cost-effective way**.

Operator and Enterprise Benefits of LPWA Device Management

LPWA DM has several financial and operating benefits for a service provider or enterprise. These include:

- **Optimizing the total cost of ownership (TCO) and return on investment (ROI)** of deployment of LPWA networks. By using remote, automated device lifecycle management, a service provider or enterprise can **minimize manual DM procedures and lower ongoing operations costs** while **guaranteeing a constant high level of quality**.
- Adapting the embedded application during the lifetime of the device. Using over-the-air updates, a service provider or enterprise can update embedded applications to **keep up with market or connected services evolution to meet evolving end-customer expectations**.
- Increasing the ability to **leverage predictive and preventative maintenance** to **orchestrate multicast updates or configuration campaigns**.
- Bundling additional services with other pieces of the IoT offering to **provide new recurring revenues for service providers and enterprises**. A leading LPWA DM solution provides integrations to a service provider's and enterprise's other IoT systems.
- Addressing maintenance operations and trouble resolution with high efficiency. Using the real-time monitoring and alerting features of an IoT DM platform, a service provider or enterprise can provide **enhanced maintenance** to **quickly find and repair troubles** with devices or an underlying LPWA network.
- Managing the device fleet in a consistent way. LPWA DM allows a service provider or enterprise

to **manage its IoT devices with the same tools it would use to manage a fleet of mobile phones**. And some of these tools might be based on OMA DM standards for LwM2M to provide a standards-based solution.

- Reconfiguring devices to optimize network use. IoT DM allows a service provider or vendor to reconfigure devices on an LPWA network to **maximize network efficiencies and ensure global quality of service (QoS) across the network**.

Kerlink’s Device Management Solution

By providing its **Wanesy™ Device Management Platform** on top of its existing core network **Wanesy™ Management Center** (Operational Support System – OSS), Kerlink now offers a full offering for public or private service providers and enterprises to remotely and securely operate their connected devices. Combining state-of-the-art **LPWA network stations, core network management solutions** and end-device remote monitoring and configuration tools, Kerlink enables existing players and new entrants to **quickly roll-out and operate highly reliable connectivity networks** to **simplify their operations** and **generate new revenue streams**. Focused on leveraging industry-proven open solutions and promoting interoperability, Kerlink is dedicated to building a vibrant ecosystem around its solutions to boost IoT growth in verticals where use cases can be efficiently supported by LPWA connectivity. These include smart city, industry, agriculture, transport and asset management applications.

The company is a founder and board member of the LoRa Alliance™ and a world leading LoRaWAN™ IoT equipment and solutions provider. It has installed more than 70,000 Kerlink stations and other equipment in Europe, South Asia and South America for more than 260 clients.

About Kerlink

Kerlink, a co-founder and board member of the LoRa Alliance™, specializes in network solutions for the Internet of Things (IoT). Its mission is to provide its clients – telecom operators, businesses and public authorities – with equipment, software and services to design, launch and operate IoT networks. Over the past three years, Kerlink has invested more than €8 million in R&D. In just over 10 years, more than 70,000 Kerlink installations have been rolled out for more than 260 customers, including major telecom operators such as Tata Communications, and utilities such as GrDF and Suez. The company's solutions are enabling IoT networks worldwide with major deployments in Europe, South Asia and South America. In 2016, Kerlink generated revenues of €14.1 million, 25 percent internationally. Since 2013, it has posted average annual growth above 50 percent. Kerlink has been listed on Euronext Growth Paris since May 2016 and was added to the EnterNext PEA-PME 150, an index of 150 fast-growing French SMEs in 2017.

kerlink
communication is everything

WWW.KERLINK.COM

@KERLINK_NEWS

KERLINK

CONTACT@KERLINK.COM