**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **<IEEE Std 802.15.4 - low power wide area network>** |
| Date Submitted | 11 April, 2017 |
| Source | [][][address] | Voice: [ ]Fax: [ ]E-mail: [ ] |
| Re: | In response to the Call for Contributions from IEEE 802.15 IG lpwa |
| Abstract | [Summary of IEEE Std 802.15.4 LECIM |
| Purpose | [To allow IG lpwa to compare this LP-WAN against the use cases and other LP-WANs |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

IEEE Std 802.15.4:
Low Power-Wide Area Network (LP-WAN)

# Purpose

The purpose of this white paper is to inform the IETF lp-wan WG and the IEEE 802.15 IG LPWA about the characteristics and features of an IEEE 802.15.4 LP-WAN device. This LP-WAN standard is included in the IEEE Std 802.15.4-2015 and also the IEEE Std 802.15.4k-2013 where LP-WAN is referred to as LECIM (low energy critical infrastructure monitoring).

# IEEE Std 802.15.4 background

IEEE Std 802.15.4 is a very extensible and scalable standard for machine to machine communications needing low amounts of data transfer over long periods of time. The growth of IEEE Std 802.15.4 has been application driven in areas such as smart utility networks (SUN) i.e. Smart Grid, rail communications and control (RCC), medical body area network (MBAN), active radio frequency identification (RFID), industrial automation, and critical infrastructure monitoring (now known as LP-WAN).

IEEE Std 802.15.4 network topologies range from a simple star, extended star, clusters, hybrid star-mesh, to full mesh. This wide range of topologies allow applications to use the topology to which they are best suited. For example, critical infrastructure monitoring applications typically use a star topology to achieve long device ranges with minimal infrastructure compared to Smart Grid applications that require mesh topologies for large areas of device coverage and increased communications reliability.

The architecture of IEEE Std 802.15.4-2015 (the latest revision), is thoroughly extensible. The MAC has nine modes of operation with 13 optional behaviors. The PHY has nine modulation types with four distinct behaviors, 20 frequency bands with over 36,000 frequency channels, and 100 data rates ranging from 3 bits/s to 27,240 Mb/s.

# LP-WANs

## LP-WAN characteristics

LP-WAN devices must provide the MAC (layer 2) and PHY (layer 1) behaviors that allow a minimal network infrastructure to be implemented; and enables the collection of scheduled and event data from a large number of non-mains powered end points that are widely dispersed, or are in challenging propagation environments. To facilitate low energy operation necessary for multi-year battery life, MAC protocols minimize network maintenance traffic and device wake durations. In addition, LP-WAN devices must address the changing propagation and interference environments encountered over many years.

The following is a list of LP-WAN characteristics and the underlying behaviors that form them:

* Minimal infrastructure
* Star topology, i.e., coordinator communicates directly with devices.
* Commissioned network (not ad hoc)
* coordinators and end point devices are configured specifically for the deployed network.
* coordinators and end point devices are stateful, i.e., they are preconfigured with parameters that eliminate the need for numerous wireless messages sending configuration information.
* Long range
* High receiver sensitivity resulting from methods such as narrow bandwidth and/or high processing gain.
* Interference robustness resulting from mechanisms such as FEC, interleaved symbols, high processing gain.
* Very limited energy end point devices, such as:
* Ten to twenty year battery life with no maintenance, i.e., original battery supplies all energy for the life of the device.
* Energy harvesting with limited power supplies, i.e., short and infrequent transmission and reception durations.
* Significant difference between network coordinator and end point devices
* Network coordinator device may have significantly higher performance such as increased sensitivity and higher transmit power, and a larger energy supply, such as mains, than end point devices.
* Asymmetrical data flows
* Sensor end point: up-link dominates data flow with limited down-link data needs.
* Actuator end point: down-link dominates data flow with limited up-link data needs.

## LP-WAN desirable behaviors

The following concepts are intended to address the needs of LP-WAN applications: commissioning, low energy, range extension, and device sensitivity and robustness.

### Commissioning

Commissioning is a method of configuring important parameters such as application specific information, cryptographic information, and network constant parameters into a device prior to its joining the network. Commissioning by an installer allows the network to reduce the amount of data to be sent over-the-air (OTA) by creating statefulness. The commissioning parameters are not expected to change over the duration of the network.

The following is one, simple example of commissioning to enable communication among three LP-WAN devices (devices *A*, *B*, and *C*), where device *A* is a powered network coordinator and devices *B* and *C* are end point devices.

PHY settable attributes that would be commissioned:

* Modulation-related attributes: modulation type, and modulation rate
* Preamble-related attributes: preamble length, coding, spreading factor, and start frame delimiter
* Packet-related attributes: packet size, and coding

The PHY attributes such as channel-to-be-used, the Gold code seed value, and the spreading factor value need to be shared among communicating parties but do not necessarily need to be the same for each direction in a link. For example, if the aforementioned devices make up a star network, device A (network coordinator) may use one set of code/spreading for its beacon transmission and use two additional, unique codes/spreading or channels for reception from end point devices B and C. This ability to use different codes, or different channels, provides a mechanism to address hidden node problems and interference from other co-located networks. For example, two nodes hidden from each other may have overlapping transmissions that can successfully be decoded by a receiver, provided the receiver has the ability to simultaneously demodulate two or more different PHYs at the same time (e.g., additional processing resources, code division multiple access (CDMA), multichannel receiver). This ability eliminates the need for the end point devices to re-transmit hidden node collisions, thus saving energy and improving system capacity.

### Low energy

LP-WAN applications require very low energy operation in order to be able to either last 20 years on the original battery supply or on low power energy harvesting mechanisms. Achieving low energy operation is very difficult given the low data rates necessary for long range operation. Accordingly, LP-WAN networks should be capable of eliding any overhead octets not absolutely necessary in order to minimize transmit and receive durations, schedule link times to minimize device “on” durations, and maximize link reliability to minimize retransmissions.

The maximum frame size that an LP-WAN device is able to process, e.g. 2047 octets, can be larger than the LP-WAN device’s OTA packet size. To facilitate the multi-year battery life operation expected for many LP-WAN applications, and given the low OTA data rate provisioned by the PHY, it is recommended that small OTA packet sizes be used. In this manner, the frame could be fragmented into multiple smaller packets appropriate for transmission and reception.

As an example, the on-air time for a 2047 octet packet at a data rate of 12.5 kb/s will require a minimum of 1.3 seconds total air time to be transmitted or received. If that same frame has a spreading factor of eight applied to each bit, the OTA broadcast time will exceed 10 seconds. This increase in transmission and reception time will significantly reduce the battery life of a LP-WAN device, even allowing for low duty cycle operation. It should also be noted that the increased transmission time may also lead to regulatory duty cycle limitations, especially in the case of the network coordinator.

### Range extension

To keep infrastructure costs to a minimum, LP-WAN devices have large link margins to achieve long ranges without requiring router or repeater devices. Requiring a mesh topology would increase the number of devices needed to sustain the network and, in most cases, require mains power for these devices. To extend the coverage for supporting sparse dispersed devices beyond the link margin or to maintain connections in dramatically changing environments, Layer 2 repeaters located between the network coordinator and end point devices may be used to sustain the connections without reconfiguring the whole LP-WAN network.

### Device sensitivity and interference robustness

To support long range operations, the LP-WAN device is intended to have high receiver sensitivity and interference robustness. The required high receiver sensitivity (capable of supporting >120 dB path losses) is achieved via low data rates, forward error correction (FEC), high processing gains, and other such mechanisms. The interference rejection specification for the LP-WAN device needs to support the required reliability with respect to parameters such as co-channel rejection, improved receiver interference rejection, and blocking immunity. Attention is drawn to the class two receiver requirements of European standard ETSI EN 300 220-1 as an example of typical receiver immunity requirements for a LP-WAN device.

# IEEE 802.15.4 functionality necessary for LP-WAN

The following PHYs and behaviors have been added to IEEE Std 802.15.4 in order to implement LP-WAN applications: LP-WAN DSSS, LP-WAN FSK, MPDU fragmentation, frame priority, and time-slot relaying based link extension (TRLE).

## DSSS (direct sequence spread spectrum)

The DSSS used by LP-WAN devices differ from the other device’s DSSS in that they have significantly more processing gain to allow devices to receive messages with very low or negative carrier-to-noise ratios. High processing gain also allows for CDMA operation to reduce the possibility of collisions. The DSSS modulator reference diagram Figure 4.1 illustrates the various components (some optional) that make up a DSSS LP-WAN device.



Figure 4.1 DSSS reference modulator diagram

With high spreading factors and CDMA, transmitted signals from other devices within radio range of the receiver that are operating on different codes are likely to be undetectable, because they may fall below the effective noise floor. This should be taken into account when configuring the clear channel assessment (CCA) mode to be used; however, in many applications, sensing of the medium is not practical or useful, so selecting the CCA mode for use with the carrier sense multiple access (CSMA) algorithm that equates to CCA Mode 4 (ALOHA) is recommended.

An orthogonal variable spreading factor (OVSF) code is an additional option that may be used to identify the co-located orthogonal networks and clusters in order to provide double protection from outside interference. The OVSF code is the same as the Walsh code, except that each sequence has a different index number in the code set, which results from their different generator algorithms. A Gold code is used inside a co-located orthogonal network as the primary code.

There are a many options available in LP-WAN DSSS PHY that provide the ability to best address the applications throughout a diverse and changing set of regulatory environments. However, some of these options may not be possible in some regulatory environments, and it is up to the OEM and/or higher layers to specify options which comply with local regulations.

To illustrate how regulations affect option selections, under the current FCC regulations it would be legal to use a modulation rate of 400,000 symbols/s with certain restrictions. Specifically, in the 2.45 GHz ISM band the device would be required to use frequency hopping and would need to limit transmission duration to less than 400 ms. A packet size of 32 octets including FEC yields 512 modulation symbols per fragment. Using BPSK modulation, at a spreading factor of 256, the fragment duration would be 328 ms. Higher spreading factors would not be allowed under FCC rules. Other regulatory domains may deem frequency hopping is not required and the spreading factor (and maximum duration) may be allowed to extend above 256 (≥ 400 ms).

The calculation for the DSSS data rate, in kb/s, is ½ of modulation rate x chip/symbol divided by the spreading factor, where the chip/symbol is 1 for binary phase shift keying (BPSK) and 2 for offset quadrature phase shift keying (O-QPSK) and the ½ is due to the FEC. For example, the lowest possible DSSS O-QPSK data rate, i.e. 200,000 symbols/s with the largest spreading factor of 32,768, would be 3 b/s; while the highest data rate would be 31.25 kb/s using 1,000,000 symbols/s with the lowest spreading factor of 16. The specified sensitivity for the IEEE 802.15.4 DSSS LP-WAN is related to the data rate (hence also the modulation rate, modulation type, and spreading factor) with the minimum specification of -148 dBm for the lowest data rate of 3 b/s and -108 dBm for the highest data rate of 31.25 kb/s.

## FSK (frequency shift keying)

The LP-WAN FSK PHY uses a transmit signal characterized by a constant envelope, which allows for low implementation cost and good transmit power efficiency.

LP-WAN FSK devices are typically narrow bandwidth (hence low data rate) to permit higher sensitivity and an increased number of channels in each band, which can reduce the probability of packet collision. The data rates are 12.5 kb/s, 25 kb/s, and 37.5 kb/s using a bandwidth of either 100 kHz or 200 kHz.

The FSK reference modulation diagram Figure 4.2 illustrates the components of the IEEE 802.15.4 FSK LP-WAN device. Features, such as forward error correction, with a relatively high constraint length and robust interleaving, as well as spreading capability, are included to allow for further sensitivity gains. When used, the FEC uses a rate 1/2 convolutional coding with a constraint length of *K* = 7 either with or without interleaving. The spreading factor (SF) can be 1, 2, 4, 8, or 16. Finally, data whitening is included in IEEE Std 802.15.4 as an option.



Figure 4.2 FSK reference modulator diagram

## Fragmentation

### Overview

With the addition of very low data rate PHY operating modes, the resulting increase in the over-the-air duration of a MAC frame can lead to increased interference potential, susceptibility to channel conditions changing during the duration of a MAC frame transmission, and other effects that may reduce reliable transfer in some environments typical of LP-WAN applications. The long packet duration also brings a large cost for retransmission, both in terms of energy consumed and interference footprint.

Layer 1 fragmentation, where the MAC frame is fragmented, as opposed to layer 2 fragmentation where the datagram is fragmented, can improve the probability of successful transmission and reduce the cost of retransmission with less overhead per fragment since the MAC header is not included in each layer 1 fragment. With layer 1 fragmentation, the complete MAC frame is split into fragments at the transmitter for reassembly at the receiver. Each fragment is packaged into a PHY packet for transmission, and this smaller packet has a reduced interference footprint. Also, retransmissions can be performed on a per fragment basis without needing to retransmit the entire original frame. All IEEE 802.15.4 DSSS LP-WAN devices support layer 1 fragmentation.

### Layer 1 fragmentation

Layer 1 fragmentation operates on the MAC header (MHR) and MAC payload portions of the MAC frame, transparent to other MAC frame processing. Layer 1 fragmentation is specified so that it may be used with the PHYs defined in IEEE Std 802.15.4. Optimum use of fragmentation depends on many variables, including channel performance, the interference environment, and characteristics of the PHY selected (e.g., data rate and maximum frame size supported). An overview of the fragmentation process is shown in Figure 4.3.2.



Figure 4.3.2—Fragmentation process overview

When the LP-WAN DSSS PHY is being used, the packet size may be 16, 24, or 32 octets. Fragmentation enables all the MAC frame formats defined by IEEE Std 802.15.4 to be carried in the constrained packet size. Fragmentation operates on the complete MAC frame and adapts it to the characteristics of the specific PHY and PHY operating mode. The following example illustrates how layer 1 fragmentation may be applied to the LP-WAN DSSS PHY.

### Fragment context frame

The LP-WAN PHY allows for a unique code, a transaction identifier (TID) to be assigned to all links between the end-points and the PAN coordinator. The fragment context frame associates the TID with the description of the configuration for the following fragmentation sequence. For this example, consider a TID that is assigned for the down-link between the PAN coordinator and an end-point device. For the LP-WAN DSSS PHY, down-link addressing information is implied since in a star topology all down-links are from the coordinator and the spreading code for each end-point is unique. A context setup frame in this example, shown in Table 4.3.3, would be sent as a multipurpose frame with no sequence number, no addressing, no auxiliary security header, and the configuration parameters as the payload.

Table 4.3.3—Context setup frame when using LP-WAN DSSS PHY

| **Octets: 2** | **6** | **2/4** |
| --- | --- | --- |
| MAC header | Fragment Sequence Context Description | Frame check sequence |

### Fragment acknowledgment (Frak)

Since LP-WANs may spread the fragments out over a long time period, the fragment acknowledgments (Fraks) are handled differently than Imm-Ack frames or Enh-Ack frames. Fraks are sent as per the Frak policy stated in the context setup frame which are described in Table 4.3.4.

Table 4.3.4 Frak policy field values

|  |  |
| --- | --- |
| **Field value** | **Frak policy description** |
| 0 | A Frak frame shall be sent upon reception of each fragment. |
| 1 | Acknowledgment is based on time: A Frak frame shall be generated if Frak Progress Timeout value has elapsed since the reception of the fragment context frame or the last received fragment, whichever is later. In this mode, the originator will never stop waiting to get a Frak, even if the target does not want to Frak. |
| 2 | Acknowledge the last outstanding fragment: A Frak frame shall be generated only when the last expected fragment is received, or if Frak Progress Timeout value has elapsed since the last received fragment. |
| 3 | Reserved |

Frak policies 1 and 2 enable multiple fragments to be acknowledged in a single frame in a bitmap with bits set to “1” indicating those fragments that were received correctly and bits set to “0” indicating which fragments were not received. Fragments not received would be retransmitted by the sender until the Frak indicates the fragment was received correctly or the number of retries has surpassed the maximum retry number. Setting all bit positions of the bitmap to zero indicates an aborted transaction.

## Priority Channel Access (PCA)/Frame priority

Frame priority allows LP-WAN networks to exhibit low latencies for truly critical event messages versus those latencies for link maintenance or other lower priority messages.

Frame priority is established by two means: PCA allocations and the PCA backoff algorithm, described for CSMA-CA and for CCA Mode 4 (ALOHA). Both algorithms are used during contention access, but the PCA allocations can only be used when operating in beacon-enabled mode or TSCH. The PCA is only usable for critical event messages, but the critical event messages do have to compete with each other for access to the channel.

The PCA backoff algorithm is used whenever contention access is applied. It operates slightly differently based on whether CCA Mode 4 (ALOHA) is used or not. When CCA Mode 4 (ALOHA) is not used, the transmitting device remains in persistent mode.

## TRLE

For extending the range of a link in a star network composed of beacon-enabled devices or DSME-enabled devices, the TRLE PAN relays residing between the PAN coordinator and devices support transparent link connectivity without additional networking overhead to an end device.

The TRLE PAN relay operates with the frame filtering in relaying mode and relays MAC frames either in the direction of the PAN coordinator or in the direction of a device. The TRLE PAN relay provides a one-hop relaying link extension for the beacon-enabled PAN. The TRLE-enabled PAN coordinator and the TRLE PAN relays provide multi-hop relaying link extension for the DSME-enabled PAN.

Beacon frames from the TRLE-enabled PAN coordinator received by the PAN relays within the transmission range of the PAN coordinator from tier 1 of the TRLE-enabled PAN. The PAN relays that are within a transmission range of the tier 1 PAN relays, but not within PAN coordinator range, form tier 2 of the TRLE-enabled PAN, and so on, as illustrated in Figure 4.5. For any given PAN relay, a neighboring PAN relay closer to the PAN coordinator is called an inner PAN relay and a PAN relay closer to the end device is called an outer PAN relay. The relaying of a TRLE-enabled PAN is limited to seven tiers.



Figure 4.5 Hierarchy of relaying in the TRLE-enabled PAN

1. Use Cases
	1. Use case examples

The following use cases exemplify LP-WAN applications.

* 1. Oil and gas pipeline monitoring

## The key drivers of pipeline monitoring are as follows:

* Environmental protection
* Reliability (critical resources)
* Cost savings (increasing cost)
* Compliance (regulators)
	1. Water leak detection

## The key drivers of water leak detection are as follows:

* Permanent installation of large number of sensors underground
* Long range and ability to penetrate underground vaults
* Battery operated and long lifetime

Small data messages once per day and in case of alarm event (e.g., leak detected)

* Low installation cost (easy deployment) and low cost of maintenance
	1. Soil monitoring

The key drivers of soil monitoring are as follows:

* Power consumption

Low-cost batteries that last over many years

* Networking

Long range links to cover large fields

Ability to use mesh or tree networking for complicated environment

Ability to connecting WPAN with mobile networks

* Reliability and cost

Very low maintenance requirements

* 1. Inventory control - event driven with query

The application is for a warehouse floor with thousands of parts bins. Each bin has a battery operated RF link for communicating current quantity and changes in quantity to the central inventory control system. In this use case battery life is important.

Each bin contains only one part number. The RF link has an LCD display showing the quantity in the bin. It also has an “Increase Button” and a “Decrease Button.” When an operator adds units to the bin, he presses the Increase Button, and when parts are removed, he presses the Decrease Button. Each time a button is pressed, it generates an event to the RF module, which then transmits the change to the central inventory control. This would most likely use a contention access method for transmission, since events occur in an unscheduled manner.

The central inventory control receives events from all of the bins, as changes are made to the quantity contained in each bin. Both the local RF module and the central inventory control maintain the quantity in the bin.

For inventory auditing, it is necessary for the central inventory control to query each bin to check the quantity. This requires the central inventory control to initiate a transaction with each bin, either individually or as a broadcast/multicast message. The desire is to have all bins report within a reasonable time (minutes).

Also, since changes in quantity are event driven, the central inventory control needs a means to query each bin to make sure that it is still operational and that no “change in quantity” events were missed.

To minimize battery drain, the LP-WAN device is only activated when necessary:

* A change in quantity as indicated by a button event
* Some type of synchronous sniff/query operation for receiving queries from the central inventory control
* A response to query messages
	1. Building monitoring - time and event driven data with query

A building (or any structure) is being monitored by sensors that report measurement or state information over long periods, e.g., several minutes to several hours. There may also be sensors that report events or changes in state that are event driven and not time driven. Battery life is important.

Each measurement sensor is set to report its information at a certain interval, using either a guaranteed time slot or the contention access period. This gives very low duty cycle for normal operation, which is 99% of the usage. There may also be sensors that are event driven and report change in state, such as door open/closed, door locked/unlocked, switch on/ off, etc. This is also low duty cycle.

Occasionally there is an event, such as an emergency, where the central monitoring system requires readings from all sensors as soon as possible. The central controller sends a request to all sensors to report their current measurement or state. This requires a low latency response mechanism capable of maintaining long battery life.