LPWAN Overview
draft-farrell-lpwan-overview-03

Abstract

   Low Power Wide Area Networks (LPWAN) are wireless technologies with
   characteristics such as large coverage areas, low bandwidth, possibly
   very small packet and application layer data sizes and long battery
   life operation. This memo is an informational overview of the set of
   LPWAN technologies being considered in the IETF and of the gaps that
   exist between the needs of those technologies and the goal of running
   IP in LPWANs.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on May 4, 2017.

Table of Contents

1. **Introduction**

   [[Editor comments/queries are in double square brackets like this.]]

   This document provides background material and an overview of the
   technologies being considered in the IETF's Low Power Wide-Area
   Networking (LPWAN) working group. We also provide a gap analysis
   between the needs of these technologies and currently available IETF
   specifications.

   This document is largely the work of the people listed in Section 8.
   Discussion of this document should take place on the lp-wan@ietf.org
   list.

   [[Editor's note: the eventual fate of this draft is a topic for the
   WG to consider - it might end up as a useful RFC, or it might be best
   maintained as a draft only until its utility has dissapated. FWIW,
   the editor doesn't mind what outcome the WG choose.]]

2. **Common Concerns**

   [[Editors note: We may want a section like this that describes some
   cross-cutting issues, e.g. duty-cycles, some of the ISM band
   restrictions. This isn't intended to be a problem statement nor a
   set of requirements but just to describe some issues that affect more
   than one of the LPWAN technologies. Such a section might be better
   before or after Section 3, will see when text's added there. There
   is some text for this in the current "gaps" draft.]]

   Most technologies in this space aim for similar goals of supporting
   large numbers of low-cost, low-throughput devices at very low-cost
   and with very-low power consumption, so that even battery-powered
   devices can be deployed for years. And as the name implies, coverage
   of large areas is also a common goal. There are some differences
   however, e.g., the Narrowband IoT specifications Section 3.2 also aim
   for increased indoor coverage. However, by and large, the different
   technologies aim for deployment in very similar circumstances.

   Existing pilot deployments have shown huge potential and created much
   industrial interest in these technolgies. As of today, essentially
   no LPWAN devices have IP capabilities. Connecting LPWANs to the
   Internet would provide significant benefits to these networks in
   terms of interoperability, application deployment, and management,
   among others. The goal of the LPWAN WG is to adapt IETF defined
   protocols, addressing schemes and naming to this particular
   constrained environment.

3. LPWAN Technologies

This section provides an overview of the set of LPWAN technologies
that are being considered in the LPWAN working group. The text for
each was mainly contributed by proponents of each technology.

Note that this text is not intended to be normative in any sesne, but
simply to help the reader in finding the relevant layer 2
specifications and in understanding how those integrate with IETF-
defined technologies. Similarly, there is no attempt here to set out
the pros and cons of the relevant technologies. [[Editor: I assume
that's the right target here. Please comment if you disagree.]]

[[Editor's note: the goal here is 2-3 pages per technology. If
there's much more needed then we could add appendices I guess
depending on what text the WG find useful to include.]]

3.1. LoRaWAN

[[Text here is from [I-D.farrell-lpwan-lora-overview] And yes, this
section is too long right now. Will shorten.]]

3.1.1. Provenance and Documents

LoRaWAN is a wireless technology for long-range low-power low-data-
rate applications developed by the LoRa Alliance, a membership
consortium. <https://www.lora-alliance.org/> This draft is based on
version 1.0.2 [LoRaSpec] of the LoRa specification. (Note that
version 1.0.2 is expected to be published in a few weeks. We will
update this draft when that has happened. For now, version 1.0 is
available at [LoRaSpec1.0])

3.1.2. Characteristics

In LoRaWAN networks, end-device transmissions may be received at
multiple gateways, so during nominal operation a network server may
see multiple instances of the same uplink message from an end-device.

The LoRaWAN network infrastructure manages the data rate and RF
output power for each end-device individually by means of an adaptive
data rate (ADR) scheme. End-devices may transmit on any channel
allowed by local regulation at any time, using any of the currently
available data rates.

LoRaWAN networks are typically organized in a star-of-stars topology
in which gateways relay messages between end-devices and a central
"network server" in the backend. Gateways are connected to the
network server via IP links while end-devices use single-hop LoRaWAN

communication that can be received at one or more gateways. All
communication is generally bi-directional, although uplink
communication from end-devices to the network server are favoured in
terms of overall bandwidth availability.

This section introduces some LoRaWAN terms. Figure 1 shows the
entities involved in a LoRaWAN network.

```
+----------+
|End-device| * * *
+----------+        *   +---------+
                     * | Gateway +---+
+----------+        *   +---------+   |   +---------+
|End-device| * * *                  +---+ Network +--- Application
+----------+        *                 |   | Server  |
                     * +---------+    |   +---------+
+----------+        *   | Gateway +---+
|End-device| * * *   * +---------+
+----------+
    Key: *       LoRaWAN Radio
         +---+  IP connectivity
```
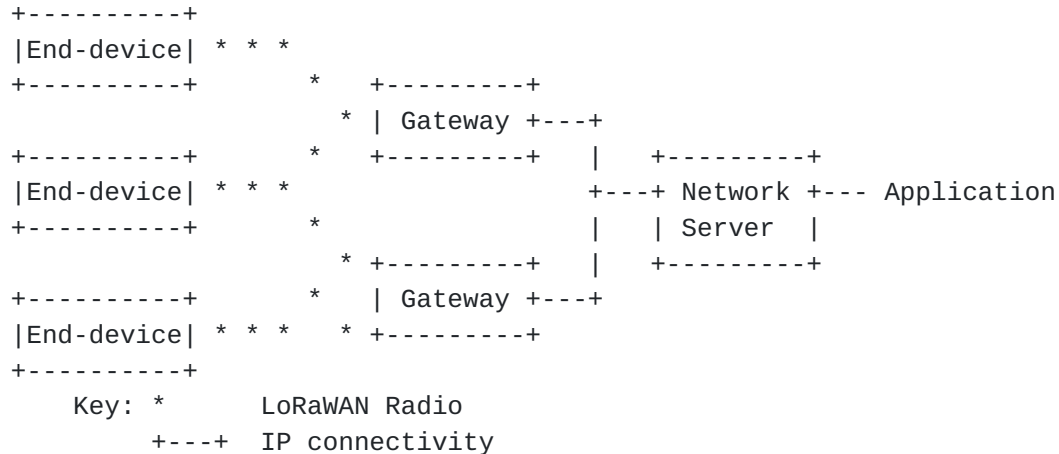
                    Figure 1: LoRaWAN architecture

o End-device: a LoRa client device, sometimes called a mote.
   Communicates with gateways.

o Gateway: a radio on the infrastructure-side, sometimes called a
   concentrator or base-station. Communicates with end-devices and,
   via IP, with a network server.

o Network Server: The Network Server (NS) terminates the LoRaWAN MAC
   layer for the end-devices connected to the network. It is the
   center of the star topology.

o Uplink message: refers to communications from end-device to
   network server or appliction via one or more gateways.

o Downlink message: refers to communications from network server or
   application via one gateway to a single end-device or a group of
   end-devices (considering multicasting).

o Application: refers to application layer code both on the end-
   device and running "behind" the network server. For LoRaWAN,
   there will generally only be one application running on most end-
   devices. Interfaces between the network server and application
   are not further described here.

o Classes A, B and C define different device capabilities and modes
   of operation for end-devices. End-devices can transmit uplink
   messages at any time in any mode of operation (so long as e.g.,
   ISM band restrictions are honoured). An end-device in Class A can
   only receive downlink messages at predetermined timeslots after
   each uplink message transmission. Class B allows the end-device
   to receive downlink messages at periodically scheduled timeslots.
   Class C allows receipt of downlink messages at anytime. Class
   selection is based on the end-devices' application use case and
   its power supply. (While Classes B and C are not further
   described here, readers may have seen those terms elsewhere so we
   include them for clarity.)

LoRaWAN radios make use of ISM bands, for example, 433MHz and 868MHz
within the European Union and 915MHz in the Americas.

The end-device changes channel in a pseudo-random fashion for every
transmission to help make the system more robust to interference and/
or to conform to local regulations.

As with other LPWAN radio technologies, LoRaWAN end-devices respect
the frequency, power and maximum transmit duty cycle requirements for
the sub-band imposed by local regulators. In most cases, this means
an end-device is only transmitting for 1% of the time, as specified
by ISM band regulations. And in some cases the LoRaWAN specification
calls for end-devices to transmit less often than is called for by
the ISM band regulations in order to avoid congestion.

Figure 2 below shows that after a transmission slot a Class A device
turns on its receiver for two short receive windows that are offset
from the end of the transmission window. The frequencies and data
rate chosen for the first of these receive windows depends on those
used for the transmit window. The frequency and data-rate for the
second receive window are configurable. If a downlink message
preamble is detected during a receive window, then the end-device
keeps the radio on in order to receive the frame.

End-devices can only transmit a subsequent uplink frame after the end
of the associated receive windows. When a device joins a LoRaWAN
network, there are similar timeouts on parts of that process.

```
|---------------------------|         |--------|      |--------|
|             Tx            |         |  Rx    |      |  Rx    |
|---------------------------|         |--------|      |--------|
                          |---------|
                          Rx delay 1
                          |------------------------|
                          Rx delay 2
```
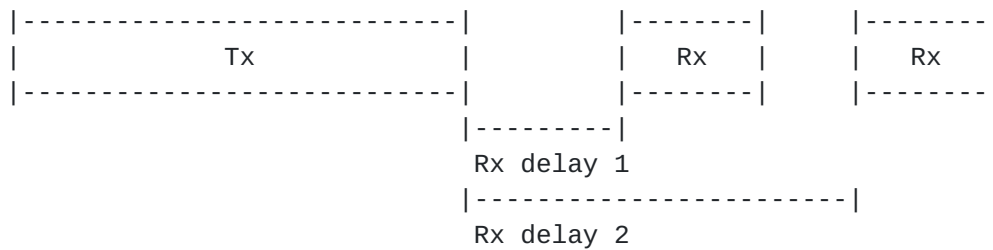
Figure 2: LoRaWAN Class A transmission and reception window

Given the different regional requirements the detailed specification
for the LoRaWAN physical layer (taking up more than 30 pages of the
specification) is not reproduced here. Instead and mainly to
illustrate the kinds of issue encountered, in Table 1 we present some
of the default settings for one ISM band (without fully explaining
those here) and in Table 2 we describe maxima and minima for some
parameters of interest to those defining ways to use IETF protocols
over the LoRaWAN MAC layer.

Parameters	Default Value
Rx delay 1	1 s
Rx delay 2	2 s (must be RECEIVE_DELAY1 + 1s)
join delay 1	5 s
join delay 2	6 s
868MHz Default channels	3 (868.1,868.2,868.3), date rate: 0.3-5 kbps

Table 1: Default settings for EU868MHz band

Parameter/Notes	Min	Max
Duty Cycle: some but not all ISM bands impose a limit in terms of how often an end-device can transmit. In some cases LoRaWAN is more stringent in an attempt to avoid congestion.	1%	no-limit
EU 868MHz band data rate/frame-size	250 bits/s : 59 octets	50000 bits/s : 250 octets
US 915MHz band data rate/frame-size	980 bits/s : 19 octets	21900 bits/s : 250 octets

Table 2: Minima and Maxima for various LoRaWAN Parameters

Note that in the case of the smallest frame size (19 octets), 8 octets are required for LoRa MAC layer headers leaving only 11 octets for payload (including MAC layer options). However, those settings do not apply for the join procedure - end-devices are required to use a channel that can send the 23 byte Join-request message for the join procedure.

Uplink and downlink higher layer data is carried in a MACPayload. There is a concept of "ports" (an optional 8 bit value) to handle different applications on an end-device. Port zero is reserved for LoRaWAN specific messaging, such as the join procedure.

The header also distinguishes the uplink/downlink directions and whether or not an acknowledgement ("confirmation") is required from the peer.

All payloads are encrypted and ciphertexts are protected with a cryptographic Message Integrity Check (MIC) - see Section 6 for details.

In addition to carrying higher layer PDUs there are Join-Request and Join-Response (aka Join-Accept) messages for handling network access. And so-called "MAC commands" (see below) up to 15 bytes long can be piggybacked in an options field ("FOpts").

LoRaWAN end-devices can choose various different data rates from a menu of available rates (dependent on the frequencies in use). It is

however, recommended that end-devices set the Adaptive Data Rate
("ADR") bit in the MAC layer which is a signal that the network
should control the data rate (via MAC commands to the end-device).
The network can also assert the ADR bit and control data rates at
it's discretion. The goal is to ensure minimal on-time for radios
whilst increasing throughput and reliability when possible. Other
things being equal, the effect should be that end-devices closer to a
gateway can successfully use higher data rates, whereas end-devices
further from all gateways still receive connectivity though at a
lower data rate.

Data rate changes can be validated via a scheme of acks from the
network with a fall-back to lower rates in the event that downlink
acks go missing.

There are 16 (or 32) bit frame counters maintained in each direction
that are incremented on each transmission (but not re-transmissions)
that are not re-used for a given key. When the device supports a 32
bit counter, then only the least significant 16 bits are sent in the
MAC header, but all 32 bits are used in cryptographic operations.
(If an end-device only supports a 16 bit counter internally, then the
topmost 16 bits are set to zero.)

There are a number of MAC commands for: Link and device status
checking, ADR and duty-cycle negotiation, managing the RX windows and
radio channel settings. For example, the link check response message
allows the network server (in response to a request from an end-
device) to inform an end-device about the signal attenuation seen
most recently at a gateway, and to also tell the end-device how many
gateways received the corresponding link request MAC command.

Some MAC commands are initiated by the network server. For example,
one command allows the network server to ask an end-device to reduce
it's duty-cycle to only use a proportion of the maximum allowed in a
region. Another allows the network server to query the end-device's
power status with the response from the end-device specifying whether
it has an external power source or is battery powered (in which case
a relative battery level is also sent to the network server).

The network server can also inform an end-device about channel
assignments (mid-point frequencies and data rates). Of course, these
must also remain within the bands assigned by local regulation.

A LoRaWAN network has a short network identifier ("NwkID") which is a
seven bit value. A private network (common for LoRaWAN) can use the
value zero. If a network wishes to support "foreign" end-devices
then the NwkID needs to be registered with the LoRA Alliance, in
which case the NwkID is the seven least significant bits of a

registered 24-bit NetID. (Note however, that the methods for
"roaming" are currently being enhanced within the LoRA Alliance, so
the situation here is somewhat fluid.)

In order to operate nominally on a LoRaWAN network, a device needs a
32-bit device address, which is the catentation of the NwkID and a
25-bit device-specific network address that is assigned when the
device "joins" the network (see below for the join procedure) or that
is pre-provisioned into the device.

End-devices are assumed to work with one or a quite limited number of
applications, which matches most LoRaWAN use-cases. The applications
are identified by a 64-bit AppEUI, which is assumed to be a
registered IEEE EUI64 value.

In addition, a device needs to have two symmetric session keys, one
for protecting network artefacts (port=0), the NwkSKey, and another
for protecting appliction layer traffic, the AppSKey. Both keys are
used for 128 bit AES cryptpgraphic operations. (See Section 6 for
details.)

So, one option is for an end-device to have all of the above, plus
channel information, somehow (pre-)provisioned, in which case the
end-device can simply start transmitting. This is achievable in many
cases via out-of-band means given the nature of LoRaWAN networks.
Table 3 summarises these values.

```
+---------+------------------------------------------------------------+
| Value   | Description                                                |
+---------+------------------------------------------------------------+
| DevAddr | DevAddr (32-bits) =  NwkId (7-bits) + device-specific      |
|         | network address (25 bits)                                  |
|         |                                                            |
| AppEUI  | IEEE EUI64 naming the application                          |
|         |                                                            |
| NwkSKey | 128 bit network session key for use with AES               |
|         |                                                            |
| AppSKey | 128 bit application session key for use with AES           |
+---------+------------------------------------------------------------+
```

Table 3: Values required for nominal operation

As an alternative, end-devices can use the LoRaWAN join procedure in
order to setup some of these values and dynamically gain access to
the network.

To use the join procedure, an end-device must still know the AppEUI.
In addition to the AppEUI, end-devices using the join procedure need

to also know a different (long-term) symmetric key that is bound to
the AppEUI - this is the application key (AppKey), and is distinct
from the application session key (AppSKey). The AppKey is required
to be specific to the device, that is, each end-device should have a
different AppKey value. And finally the end-device also needs a
long-term identifier for itself, syntactically also an EUI-64, and
known as the device EUI or DevEUI. Table 4 summarises these values.

```
+---------+----------------------------------------------------+
| Value   | Description                                        |
+---------+----------------------------------------------------+
| DevEUI  | IEEE EUI64 naming the device                       |
|         |                                                    |
| AppEUI  | IEEE EUI64 naming the application                  |
|         |                                                    |
| AppKey  | 128 bit long term application key for use with AES |
+---------+----------------------------------------------------+
```

Table 4: Values required for join procedure

The join procedure involves a special exchange where the end-device
asserts the AppEUI and DevEUI (integrity protected with the long-term
AppKey, but not encrypted) in a Join-request uplink message. This is
then routed to the network server which interacts with an entity that
knows that AppKey to verify the Join-request. All going well, a
Join-accept downlink message is returned from the network server to
the end-device that specifies the 24-bit NetID, 32-bit DevAddr and
channel information and from which the AppSKey and NwkSKey can be
derived based on knowledge of the AppKey. This provides the end-
device with all the values listed in Table 3.

There is some special handling related to which channels to use and
for multiple transmissions for the join-request which is intended to
ensure a successful join in as many cases as possible. Join-request
and Join-accept messages also include some random values (nonces) to
both provide some replay protection and to help ensure the session
keys are unique per run of the join procedure. If a Join-request
fails validation, then no Join-accept message (indeed no message at
all) is returned to the end-device. For example, if an end-device is
factory-reset then it should end up in a state in which it can re-do
the join procedure.

In this section we describe the use of cryptography in LoRaWAN. This
section is not intended as a full specification but to be sufficient
so that future IETF specifications can encompass the required
security considerations. The emphasis is on describing the
externally visible characteristics of LoRaWAN.

All payloads are encrypted and have data integrity. Frame options
(used for MAC commands) when sent as a payload (port zero) are
therefore protected. MAC commands piggy-backed as frame options
("FOpts") are however sent in clear. Since MAC commands may be sent
as options and not only as payload, any values sent in that manner
are visible to a passive attacker but are not malleable for an active
attacker due to the use of the MIC.

For LoRaWAN version 1.0.x, the NWkSkey session key is used to provide
data integrity between the end-device and the network server. The
AppSKey is used to provide data confidentiality between the end-
device and network server, or to the application "behind" the network
server, depending on the implementation of the network.

All MAC layer messages have an outer 32-bit Message Integrity Code
(MIC) calculated using AES-CMAC calculated over the ciphertext
payload and other headers and using the NwkSkey.

Payloads are encrypted using AES-128, with a counter-mode derived
from IEEE 802.15.4 using the AppSKey.

Gateways are not expected to be provided with the AppSKey or NwkSKey,
all of the infrastructure-side cryptography happens in (or "behind")
the network server.

When session keys are derived from the AppKey as a result of the join
procedure the Join-accept message payload is specially handled.

The long-term AppKey is directly used to protect the Join-accept
message content, but the function used is not an aes-encrypt
operation, but rather an aes-decrypt operation. The justification is
that this means that the end-device only needs to implement the aes-
encrypt operation. (The counter mode variant used for payload
decryption means the end-device doesn't need an aes-decrypt
primitive.)

The Join-accept plaintext is always less than 16 bytes long, so
electronic code book (ECB) mode is used for protecting Join-accept
messages.

The Join-accept contains an AppNonce (a 24 bit value) that is
recovered on the end-device along with the other Join-accept content
(e.g. DevAddr) using the aes-encrypt operation.

Once the Join-accept payload is available to the end-device the
session keys are derived from the AppKey, AppNonce and other values,
again using an ECB mode aes-encrypt operation, with the plaintext
input being a maximum of 16 octets.

3.2. Narrowband IoT (NB-IoT)

[[Text here is from [I-D.ratilainen-lpwan-nb-iot].]]

3.2.1. Provenance and Documents

Narrowband Internet of Things (NB-IoT) is developed and standardized
by 3GPP. The standardization of NB-IoT was finalized with 3GPP
Release-13 in June 2016, but further enhancements for NB-IoT are
worked on in the following releases, for example in the form of
multicast support. For more information of what has been specified
for NB-IoT, 3GPP specification 36.300 [TGPP36300] provides an
overview and overall description of the E-UTRAN radio interface
protocol architecture, while specifications 36.321 [TGPP36321],
36.322 [TGPP36322], 36.323 [TGPP36323] and 36.331 [TGPP36331] give
more detailed description of MAC, RLC, PDCP and RRC protocol layers
respectively.

3.2.2. Characteristics

[[Editor notes: Not clear if all the radio info here is needed. Not
clear what minimum MTU might be. Many 3GPP acronyms/terms to
eliminate or explain.]]

Specific targets for NB-IoT include: Less than 5$ module cost,
extended coverage of 164 dB maximum coupling loss, battery life of
over 10 years, ~55000 devices per cell and uplink reporting latency
of less than 10 seconds.

NB-IoT supports Half Duplex FDD operation mode with 60 kbps peak rate
in uplink and 30 kbps peak rate in downlink, and a maximum size MTU
of 1600 bytes. As the name suggests, NB-IoT uses narrowbands with
the bandwidth of 180 kHz in both, downlink and uplink. The multiple
access scheme used in the downlink is OFDMA with 15 kHz sub-carrier
spacing. On uplink multi-tone SC-FDMA is used with 15 kHz tone
spacing or as a special case of SC-FDMA single tone with either 15kHz
or 3.75 kHz tone spacing may be used.

NB-IoT can be deployed in three ways. In-band deployment means that
the narrowband is multiplexed within normal LTE carrier. In Guard-
band deployment the narrowband uses the unused resource blocks
between two adjacent LTE carriers. Also standalone deployment is
supported, where the narrowband can be located alone in dedicated
spectrum, which makes it possible for example to refarm the GSM
carrier at 850/900 MHz for NB-IoT. All three deployment modes are
meant to be used in licensed bands. The maximum transmission power
is either 20 or 23 dBm for uplink transmissions, while for downlink

transmission the eNodeB may use higher transmission power, up to 46 dBm depending on the deployment.

For signaling optimization, two options are introduced in addition to legacy RRC connection setup, mandatory Data-over-NAS (Control Plane optimization, solution 2 in [TGPP23720]) and optional RRC Suspend/ Resume (User Plane optimization, solution 18 in [TGPP23720]). In the control plane optimization the data is sent over Non Access Stratum, directly from Mobility Management Entity (MME) in core network to the UE without interaction from base station. This means there are no Access Stratum security or header compression, as the Access Stratum is bypassed, and only limited RRC procedures.

The RRC Suspend/Resume procedures reduce the signaling overhead required for UE state transition from Idle to Connected mode in order to have a user plane transaction with the network and back to Idle state by reducing the signaling messages required compared to legacy operation

With extended DRX the RRC Connected mode DRX cycle is up to 10.24 seconds and in RRC Idle the DRX cycle can be up to 3 hours.

NB-IoT has no channel access restrictions allowing up to a 100% duty-cycle.

3GPP access security is specified in [TGPP33203].

```
+--+
|UE| \                +------+      +------+
+--+  \               | MME  |------| HSS  |
       \           / +------+      +------+
+--+    \+-----+ /       |
|UE| ----| eNB |-        |
+--+    /+-----+ \       |
      /           \ +--------+
     /             \|        |    +------+      Service PDN
+--+ /              |  S-GW  |----| P-GW |---- e.g. Internet
|UE|                |        |    +------+
+--+                +--------+
```
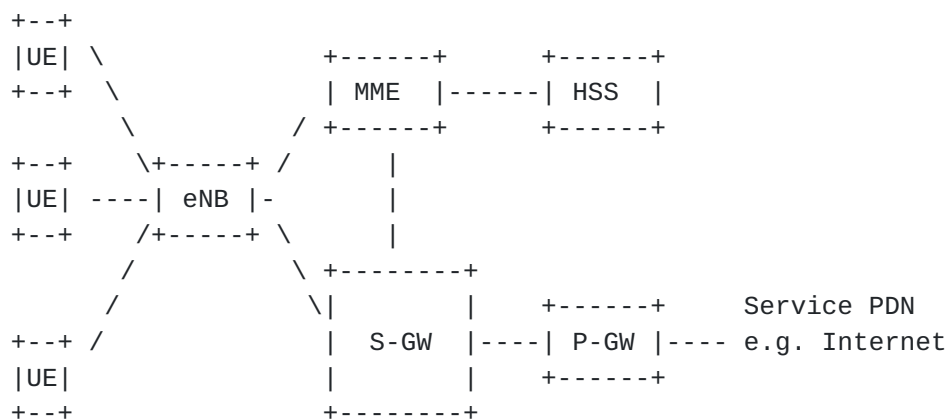
Figure 3: 3GPP network architecture

Mobility Management Entity (MME) is responsible for handling the mobility of the UE. MME tasks include tracking and paging UEs, session management, choosing the Serving gateway for the UE during initial attachment and authenticating the user. At MME, the Non Access Stratum (NAS) signaling from the UE is terminated.

Serving Gateway (S-GW) routes and forwards the user data packets
through the access network and acts as a mobility anchor for UEs
during handover between base stations known as eNodeBs and also
during handovers between other 3GPP technologies.

Packet Data Node Gateway (P-GW) works as an interface between 3GPP
network and external networks.

Home Subscriber Server (HSS) contains user-related and subscription-
related information. It is a database, which performs mobility
management, session establishment support, user authentication and
access authorization.

E-UTRAN consists of components of a single type, eNodeB. eNodeB is a
base station, which controls the UEs in one or several cells.

The illustration of 3GPP radio protocol architecture can be seen from
Figure 4.

```
+---------+                                             +---------+
| NAS     |----|-------------------------------|----| NAS     |
+---------+    |      +---------+---------+     |    +---------+
| RRC     |----|----| RRC     | S1-AP   |----|----| S1-AP   |
+---------+    |      +---------+---------+     |    +---------+
| PDCP    |----|----| PDCP    | SCTP    |----|----| SCTP    |
+---------+    |      +---------+---------+     |    +---------+
| RLC     |----|----| RLC     | IP      |----|----| IP      |
+---------+    |      +---------+---------+     |    +---------+
| MAC     |----|----| MAC     | L2      |----|----| L2      |
+---------+    |      +---------+---------+     |    +---------+
| PHY     |----|----| PHY     | PHY     |----|----| PHY     |
+---------+          +---------+---------+          +---------+
          LTE-Uu                        S1-MME
    UE                     eNodeB                     MME
```
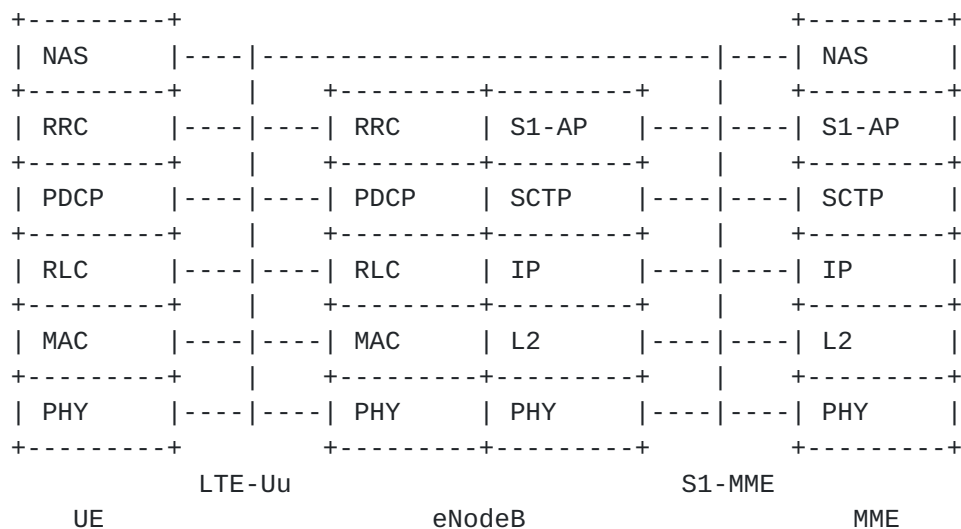
                 Figure 4: 3GPP radio protocol architecture

The radio protocol architecture of NB-IoT (and LTE) is separated into
control plane and user plane. Control plane consists of protocols
which control the radio access bearers and the connection between the
UE and the network. The highest layer of control plane is called
Non-Access Stratum (NAS), which conveys the radio signaling between
the UE and the EPC, passing transparently through radio network. It
is responsible for authentication, security control, mobility
management and bearer management.

Access Stratum (AS) is the functional layer below NAS, and in control
plane it consists of Radio Resource Control protocol (RRC)

[TGPP36331], which handles connection establishment and release
functions, broadcast of system information, radio bearer
establishment, reconfiguration and release. RRC configures the user
and control planes according to the network status. There exists two
RRC states, RRC_Idle or RRC_Connected, and RRC entity controls the
switching between these states. In RRC_Idle, the network knows that
the UE is present in the network and the UE can be reached in case of
incoming call. In this state the UE monitors paging, performs cell
measurements and cell selection and acquires system information.
Also the UE can receive broadcast and multicast data, but it is not
expected to transmit or receive singlecast data. In RRC_Connected
the UE has a connection to the eNodeB, the network knows the UE
location on cell level and the UE may receive and transmit singlecast
data. RRC_Connected mode is established, when the UE is expected to
be active in the network, to transmit or receive data. Connection is
released, switching to RRC_Idle, when there is no traffic to save the
UE battery and radio resources. However, a new feature was
introduced for NB-IoT, as mentioned earlier, which allows data to be
transmitted from the MME directly to the UE, while the UE is in
RRC_Idle transparently to the eNodeB.

Packet Data Convergence Protocol's (PDCP) [TGPP36323] main services
in control plane are transfer of control plane data, ciphering and
integrity protection.

Radio Link Control protocol (RLC) [TGPP36322] performs transfer of
upper layer PDUs and optionally error correction with Automatic
Repeat reQuest (ARQ), concatenation, segmentation and reassembly of
RLC SDUs, in-sequence delivery of upper layer PDUs, duplicate
detection, RLC SDU discard, RLC-re-establishment and protocol error
detection and recovery.

Medium Access Control protocol (MAC) [TGPP36321] provides mapping
between logical channels and transport channels, multiplexing of MAC
SDUs, scheduling information reporting, error correction with HARQ,
priority handling and transport format selection.

Physical layer [TGPP36201] provides data transport services to higher
layers. These include error detection and indication to higher
layers, FEC encoding, HARQ soft-combining. Rate matching and mapping
of the transport channels onto physical channels, power weighting and
modulation of physical channels, frequency and time synchronization
and radio characteristics measurements.

User plane is responsible for transferring the user data through the
Access Stratum. It interfaces with IP and consists of PDCP, which in
user plane performs header compression using Robust Header
Compression (RoHC), transfer of user plane data between eNodeB and

UE, ciphering and integrity protection. Lower layers in user plane
are similarly RLC, MAC and physical layer performing tasks mentioned
above.

Under worst-case conditions, NB-IoT may achieve data rate of roughly
200 bps. For downlink with 164 dB coupling loss, NB-IoT may achieve
higher data rates, depending on the deployment mode. Stand-alone
operation may achieve the highest data rates, up to few kbps, while
in-band and guard-band operations may reach several hundreds of bps.
NB-IoT may even operate with higher maximum coupling loss than 170 dB
with very low bit rates.

3.3. SIGFOX

[[Text here is from [I-D.zuniga-lpwan-sigfox-system-description].]]

3.3.1. Provenance and Documents

The SIGFOX LPWAN is in line with the terminology and specifications
being defined by the ETSI ERM TG28 Low Throughput Networks (LTN)
group [etsi_ltn]. As of today, SIGFOX's network has been fully
deployed in 6 countries, with ongoing deployments on 18 other
countries, which in total will reach 397M people.

3.3.2. Characteristics

SIGFOX LPWAN autonomous battery-operated devices send only a few
bytes per day, week or month, allowing them to remain on a single
battery for up to 10-15 years.

The radio interface is compliant with the following regulations:

   Spectrum allocation in the USA [fcc_ref]

   Spectrum allocation in Europe [etsi_ref]

   Spectrum allocation in Japan [arib_ref]

The SIGFOX LTN radio interface is also compliant with the local
regulations of the following countries: Australia, Brazil, Canada,
Kenya, Lebanon, Mauritius, Mexico, New Zealand, Oman, Peru,
Singapore, South Africa, South Korea, and Thailand.

The radio interface is based on Ultra Narrow Band (UNB)
communications, which allow an increased transmission range by
spending a limited amount of energy at the device. Moreover, UNB
allows a large number of devices to coexist in a given cell without
significantly increasing the spectrum interference.

Both uplink and downlink communications are possible with the UNB
solution. Due to spectrum optimizations, different uplink and
downlink frames and time synchronization methods are needed.

The main radio characteristics of the UNB uplink transmission are:

o Channelization mask: 100 Hz (600 Hz in the USA)

o Uplink baud rate: 100 baud (600 baud in the USA)

o Modulation scheme: DBPSK

o Uplink transmission power: compliant with local regulation

o Link budget: 155 dB (or better)

o Central frequency accuracy: not relevant, provided there is no
   significant frequency drift within an uplink packet

In Europe, the UNB uplink frequency band is limited to 868,00 to
868,60 MHz, with a maximum output power of 25 mW and a maximum mean
transmission time of 1%.

The format of the uplink frame is the following:

```
+--------+--------+--------+-----------------+-------------+-----+
|Preamble|  Frame | Dev ID |     Payload     |Msg Auth Code| FCS |
|        |  Sync  |        |                 |             |     |
+--------+--------+--------+-----------------+-------------+-----+
```

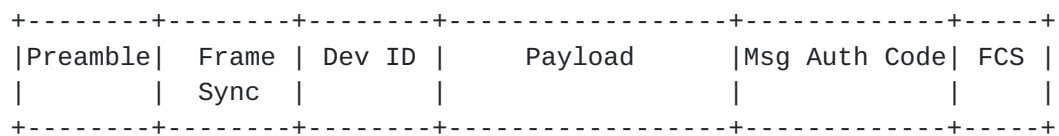   Figure 5: Uplink Frame Format

The uplink frame is composed of the following fields:

o Preamble: 19 bits

o Frame sync and header: 29 bits

o Device ID: 32 bits

o Payload: 0-96 bits

o Authentication: 16-40 bits

o Frame check sequence: 16 bits (CRC)

The main radio characteristics of the UNB downlink transmission are:

o Channelization mask: 1.5 kHz

o Downlink baud rate: 600 baud

o Modulation scheme: GFSK

o Downlink transmission power: 500 mW (4W in the USA)

o Link budget: 153 dB (or better)

o Central frequency accuracy: Centre frequency of downlink
   transmission are set by the network according to the corresponding
   uplink transmission.

In Europe, the UNB downlink frequency band is limited to 869,40 to
869,65 MHz, with a maximum output power of 500 mW with 10% duty
cycle.

The format of the downlink frame is the following:

```
+------------+-----+---------+-----------------+------------+-----+
|  Preamble  |Frame|   ECC   |     Payload     |Msg Auth Code| FCS |
|            |Sync |         |                 |            |     |
+------------+-----+---------+-----------------+------------+-----+
```
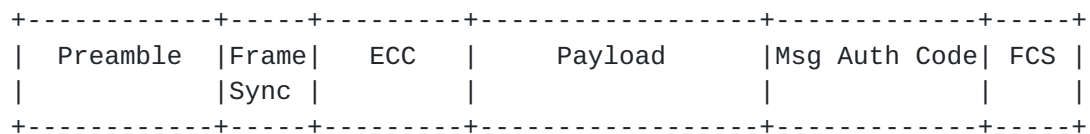
Figure 6: Downlink Frame Format

The downlink frame is composed of the following fields:

o Preamble: 91 bits

o Frame sync and header: 13 bits

o Error Correcting Code (ECC): 32 bits

o Payload: 0-64 bits

o Authentication: 16 bits

o Frame check sequence: 8 bits (CRC)

The radio interface is optimized for uplink transmissions, which are
asynchronous. Downlink communications are achieved by querying the
network for existing data from the device.

A device willing to receive downlink messages opens a fixed window
for reception after sending an uplink transmission. The delay and

duration of this window have fixed values. The LTN network transmits
the downlink message for a given device during the reception window.
The LTN network selects the BS for transmitting the corresponding
downlink message.

Uplink and downlink transmissions are unbalanced due to the
regulatory constraints on the ISM bands. Under the strictest
regulations, the system can allow a maximum of 140 uplink messages
and 4 downlink messages per device. These restrictions can be
slightly relaxed depending on system conditions and the specific
regulatory domain of operation.

```
        +--+
        |EP| *                      +------+
        +--+    *                   |  RA  |
              *                     +------+
        +--+        *                  |
        |EP| * * *    *                |
        +--+        *   +----+          |
                  * | BS | \  +--------+
        +--+        *   +----+ \ |        |
   DA -----|EP| * * *              |   SC   |----- NA
        +--+        *             / |        |
                  * +----+ /  +--------+
        +--+        *   | BS |/
        |EP| * * *    * +----+
        +--+          *
                  *
        +--+      *
        |EP| * *
        +--+
```
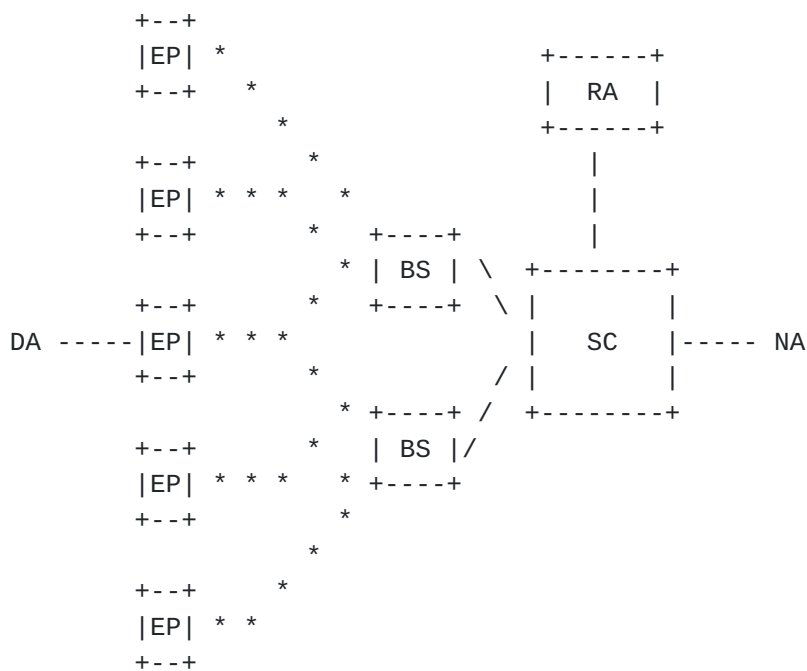
                 Figure 7: ETSI LTN architecture

Figure 7 depicts the different elements of the SIGFOX architecture.

SIGFOX has a "one-contract one-network" model allowing devices to
connect in any country, without any notion of roaming.

The architecture consists of a single core network, which allows
global connectivity with minimal impact on the end device and radio
access network. The core network elements are the Service Center
(SC) and the Registration Authority (RA). The SC is in charge of the
data connectivity between the Base Station (BS) and the Internet, as
well as the control and management of the BSs and End Points. The RA
is in charge of the End Point network access authorization.

The radio access network is comprised of several BSs connected
directly to the SC. Each BS performs complex L1/L2 functions,
leaving some L2 and L3 functionalities to the SC.

The devices or End Points (EPs) are the objects that communicate
application data between local device applications (DAs) and network
applications (NAs).

EPs (or devices) can be static or nomadic, as they associate with the
SC and they do not attach to a specific BS. Hence, they can
communicate with the SC through one or many BSs.

Due to constraints in the complexity of the EP, it is assumed that
EPs host only one or very few device applications, which communicate
to one single network application at a time.

The radio protocol provides mechanisms to authenticate and ensure
integrity of the message. This is achieved by using a unique device
ID and a message authentication code, which allow ensuring that the
message has been generated and sent by the device with the ID claimed
in the message.

Security keys are independent for each device. These keys are
associated with the device ID and they are pre-provisioned.
Application data can be encrypted by the application provider.

3.4. Wi-SUN Alliance Field Area Network (FAN)

[[Text here is via personal communication from Bob Heile
(bheile@ieee.org) and was authored by Bob and Sum Chin Sean. As
there is no I-D on which this is based, I've just cut'n'pasted the
text provided in here with no editing so far. Some editing will of
course be needed, as will references to specifications.]]

3.4.1. Provenance and Documents

The Wi-SUN Alliance is an industry alliance promoting global
interoperability and compliance to open-standards for smart city,
smart grid, smart utility, and a broad set of general IoT
applications. The Wi-SUN Alliance Field Area Network (FAN) profile
is open standards based (primarily on IETF and IEEE802 standards) and
was developed to address applications like smart municipality/city
infrastructure monitoring and management, electric vehicle (EV)
infrastructure, advanced metering infrastructure (AMI), distribution
automation (DA), supervisory control and data acquisition (SCADA)
protection/management, distributed generation monitoring and
management, and many more IoT applications. These applications,
although quite different in many respects, share a common set of

system requirements such as high network robustness, high scalability and superior security, which the Wi-SUN FAN addresses. Additionally, the Alliance has created a certification program to promote global multi-vendor interoperability.

The FAN profile is an IPv6 frequency hopping wireless mesh network with enterprise level security. The frequency hopping wireless mesh topology has multiple advantages such as superior network robustness, reliability due to high redundancy, good scalability due to the flexible mesh configuration and good resilience to interference. All these attributes address the industrial grade requirements set forth by various IoT application scenarios. Very low power modes are in development permitting long term battery operation of network nodes.

3.4.2. Characteristics

The FAN profile is an IPv6 frequency hopping wireless mesh network with enterprise level security. The frequency hopping wireless mesh topology has multiple advantages such as superior network robustness, reliability due to high redundancy, good scalability due to the flexible mesh configuration and good resilience to interference. All these attributes address the industrial grade requirements set forth by various IoT application scenarios. Very low power modes are in development permitting long term battery operation of network nodes.

As indicated above, the FAN profile is based on various open standards in IETF, IEEE802 and ANSI/TIA for low power and lossy networks. The FAN profile specification provides an application-independent IPv6-based transport service for both connectionless (i.e. UDP) and connection-oriented (i.e. TCP) services. There are two possible methods for establishing the IPv6 packet routing: mandatory Routing Protocol for Low-Power and Lossy Networks (RPL) at the Network layer or optional Multi-Hop Delivery Service (MHDS) at the Data Link layer. Refer to Figure 1 for a pictorial overview of the FAN protocol stack.

Layer	Description
IPv6 protocol suite	TCP/UDP
	6LoWPAN Adaptation + Header Compression
	DHCPv6 for IP address management.
	Routing using RPL.
	ICMPv6.
	Unicast and Multicast forwarding.
MAC based on IEEE 802.15.4e + IE extensions	Frequency hopping
	Discovery and Join
	Protocol Dispatch (IEEE 802.15.9)
	Several Frame Exchange patterns
	Optional Mesh Under routing (ANSI 4957.210).
PHY based on 802.15.4g	Various data rates and regions
Security	802.1X/EAP-TLS/PKI Authentication.
	802.11i Group Key Management
	Optional ETSI-TS-102-887-2 Node 2 Node Key Management

Table 5: Wi-SUN Stack Overivew

The Transport service is based on User Datagram Protocol (UDP) defined in RFC768 or Transmission Control Protocol (TCP) defined in RFC793.

The Network service is provided by IPv6 defined in RFC2460 with 6LoWPAN adaptation as defined in RC4944 and RFC6282. Additionally,

ICMPv6 as defined in RFC4443 is used for control plane in information exchange.

The Data Link service provides both control/management of the Physical layer and data transfer/management services to the Network layer. These services are divided into Media Access Control (MAC) and Logical Link Control (LLC) sub-layers. The LLC sub-layer provides a protocol dispatch service which supports 6LoWPAN and an optional MAC sub-layer mesh service. The MAC sub-layer is constructed using data structures defined in IEEE802.15.4-2015. Multiple modes of frequency hopping are defined. The entire MAC payload is encapsulated in an IEEE802.15.9 Information Element to enable LLC protocol dispatch between upper layer 6LoWPAN processing, MAC sublayer mesh processing, etc. These areas will be expanded once IEEE802.15.12 is completed

The PHY service is derived from a sub-set of the SUN FSK specification in IEEE802.15.4-2015. The 2-FSK modulation schemes, with channel spacing range from 200 to 600 kHz, are defined to provide data rates from 50 to 300 kbps, with Forward Error Coding (FEC) as an optional feature. Towards enabling ultra-low-power applications, the PHY layer design is also extendable to low energy and critical infrastructure monitoring networks, such as IEEE802.15.4k.

The FAN security supports Data Link layer network access control, mutual authentication, and establishment of a secure pairwise link between a FAN node and its Border Router, which is implemented with an adaptation of IEEE802.1X and EAP-TLS as described in RFC5216 using secure device identity as described in IEEE802.1AR. Certificate formats are based upon RFC5280. A secure group link between a Border Router and a set of FAN nodes is established using an adaptation of the IEEE802.11 Four-Way Handshake. A set of 4 group keys are maintained within the network, one of which is the current transmit key. Secure node to node links are supported between one-hop FAN neighbors using an adaptation of ETSI-TS-102-887-2. FAN nodes implement Frame Security as specified in IEEE802.15.4-2015.

The Wi-Sun Alliance FAN spec was developed to serve the LPWAN space among others. It already includes most needed networking elements as a result of the longstanding working relationships between the IETF and IEEE802. Nonetheless, the Alliance feels there is significant value to this LPWAN effort in IETF and strongly supports its objectives. Some of the things the Alliance hopes to accomplish through its participation are awareness (in the event changes are needed in the FAN spec), to help ensure consistency of approach, share relevant experience, and to address co-existence issues and potential interoperability since these solutions will be used in the

same markets in complementary ways. Because it is IP based, the Wi-
SUN FAN already readily interconnects to Ethernet and WiFi through
routers. It would be useful if the same could be accomplished with
other approaches.

4. Generic Terminology

[[Text here is from [I-D.minaburo-lpwan-gap-analysis].]]

LPWAN technologies, such as those discussed below, have similar
architectures but different terminology. We can identify different
types of entities in a typical LPWAN network:

o The Host, which are the devices or the things (e.g. sensors,
   actuators, etc.), they are named differently in each technology
   (End Device, User Equipment or End Point). There is a high
   density of hosts per radio gateway.

o The Radio Gateway, which is the end point of the constrained link.
   It is known as: Gateway, Evolved Node B or Base station.

o The Network Gateway or Router is the interconnection node between
   the Radio Gateway and the Internet. It is known as: Network
   Server, Serving GW or Service Center.

o AAA Server, which controls the user authentication, the
   applications. It is known as: Join-Server, Home Subscriber Server
   or Registration Authority. [[Ed: I'm not clear that AAA server is
   the right generic term here.]]

o At last we have the Application Server, known also as Packet Data
   Node Gateway or Network Application.

```
+----------------------------------------------------------------------+
| Function/     |           |            |            |                |
| Technology    | LORAWAN   |   NB-IOT   |   SIGFOX   |      IETF      |
+---------------+-----------+------------+------------+----------------+
|    Sensor,    |           |            |            |                |
|   Actuator,   |    End    |    User    |    End     |     Thing      |
|device, object |  Device   | Equipment  |   Point    |     (HOST)     |
+---------------+-----------+------------+------------+----------------+
| Transceiver   |           |  Evolved   |    Base    |     RADIO      |
|   Antenna     |  Gateway  |   Node B   |   Station  |    GATEWAY     |
+---------------+-----------+------------+------------+----------------+
|    Server     |  Network  |  Serving-  |   Service  |Network Gateway |
|               |  Server   |  Gateway   |   Center   |    (ROUTER)    |
+---------------+-----------+------------+------------+----------------+
|   Security    |   Join    |    Home    |Registration|                |
|    Server     |  Server   | Subscriber | Authority  |      AAA       |
|               |           |   Server   |            |     SERVER     |
+---------------+-----------+------------+------------+----------------+
| Application   |Application| Packet Data|   Network  |  APPLICATION   |
|               |  Server   |Node Gateway| Application|     SERVER     |
+----------------------------------------------------------------------+
```

Figure 8: LPWAN Architecture Terminology

```
  ()    ()   ()          |                       +------+
    ()  () () ()        / \            +--------+   | AAA  |
() () () () () ()      /   \=======|     /\     |====|Server|  +-----------+
  ()  ()    ()          |          | <--|--> |    +------+ |Application|
() ()  ()  ()         / \===========|     v     |=============| Server   |
   ()  ()  ()        /   \          +--------+               +-----------+
 HOSTS          Radio Gateways    Network Gateway
```
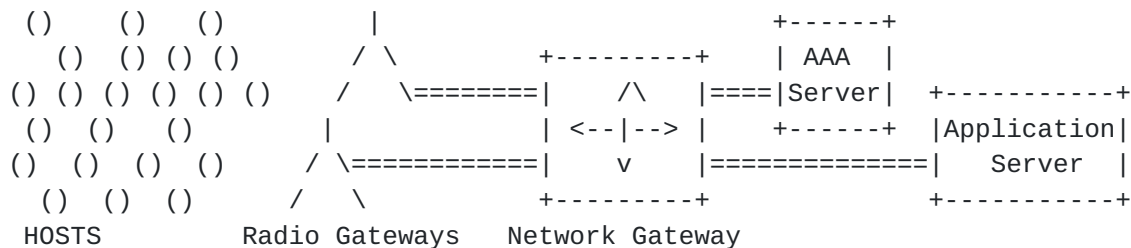
Figure 9: LPWAN Architecture

5. Gap Analysis

[[Text here is from [I-D.minaburo-lpwan-gap-analysis].]]

5.1. IPv6 and LPWAN

IPv6 [RFC2460] has been designed to allocate addresses to all the
nodes connected to the Internet. Nevertheless, the header overhead
of, at least, 40 bytes introduced by the protocol is incompatible
with the LPWAN constraints. If IPv6 (with no further optimization)
were used, several LPWAN frames would be needed just to carry the
header, discussion on this point is developed in the 6LoWPAN section
below. Another limitation comes from the IPv6 MTU requirement, by

which the layer below IP has to support packets of at least 1280 bytes [RFC2460].

IPv6 needs a configuration protocol (neighbor discovery protocol, NDP [RFC4861]) for a node to learn network parameters, and the node relation with its neighbours. This protocol generates a regular traffic with a large message size that does not fit LPWAN constraints.

5.1.1. Unicast and Multicast mapping

In some LPWAN technologies, layer two multicast is not supported. In that case, if the network topology is a star, the solution and considerations of section 3.2.5 of [RFC7668] may be applied.

5.2. 6LoWPAN and LPWAN

Several technologies that exhibit significant constraints in various dimensions have exploited the 6LoWPAN suite of specifications [RFC4944], [RFC6282], [RFC6775] to support IPv6 [I-D.hong-6lo-use-cases]. However, the constraints of LPWANs, often more extreme than those typical of technologies that have (re)used 6LoWPAN, constitute a challenge for the 6LoWPAN suite in order to enable IPv6 over LPWAN. LPWANs are characterised by device constraints (in terms of processing capacity, memory, and energy availability), and specially, link constraints, such as:

o very low layer two payload size (from ~10 to ~100 bytes),

o very low bit rate (from ~10 bit/s to ~100 kbit/s), and

o in some specific technologies, further message rate constraints (e.g. between ~0.1 message/minute and ~1 message/minute) due to regional regulations that limit the duty cycle.

5.2.1. 6LoWPAN Header Compression

6LoWPAN header compression reduces IPv6 (and UDP) header overhead by eliding header fields when they can be derived from the link layer, and by assuming that some of the header fields will frequently carry expected values. 6LoWPAN provides both stateless and stateful header compression. In the latter, all nodes of a 6LoWPAN are assumed to share compression context. In the best case, the IPv6 header for link-local communication can be reduced to only 2 bytes. For global communication, the IPv6 header may be compressed down to 3 bytes in the most extreme case. However, in more practical situations, the lowest IPv6 header size may be 11 bytes (one address prefix compressed) or 19 bytes (both source and destination prefixes

compressed). These headers are large considering the link layer
payload size of LPWAN technologies, and in some cases are even bigger
than the LPWAN PDUs. 6LoWPAN has been initially designed for IEEE
802.15.4 networks with a frame size up to 127 bytes and a throughput
of up to 250 kb/s, which may or may not be duty-cycled.

5.2.2. Address Autoconfiguration

In the ambit of 6LoWPAN, traditionally, Interface Identifiers (IIDs)
have been derived from link layer identifiers [RFC4944] . This allows
optimisations such as header compression. Nevertheless, recent
guidance has given advice on the fact that, due to privacy concerns,
6LoWPAN devices should not be configured to embed their link layer
addresses in the IID by default.

5.2.3. Fragmentation

As stated above, IPv6 requires the layer below to support an MTU of
1280 bytes [RFC2460]. Therefore, given the low maximum payload size
of LPWAN technologies, fragmentation is needed.

If a layer of an LPWAN technology supports fragmentation, proper
analysis has to be carried out to decide whether the fragmentation
functionality provided by the lower layer or fragmentation at the
adaptation layer should be used. Otherwise, fragmentation
functionality shall be used at the adaptation layer.

6LoWPAN defined a fragmentation mechanism and a fragmentation header
to support the transmission of IPv6 packets over IEEE 802.15.4
networks [RFC4944]. While the 6LoWPAN fragmentation header is
appropriate for IEEE 802.15.4-2003 (which has a frame payload size of
81-102 bytes), it is not suitable for several LPWAN technologies,
many of which have a maximum payload size that is one order of
magnitude below that of IEEE 802.15.4-2003. The overhead of the
6LoWPAN fragmentation header is high, considering the reduced payload
size of LPWAN technologies and the limited energy availability of the
devices using such technologies. Furthermore, its datagram offset
field is expressed in increments of eight octets. In some LPWAN
technologies, the 6LoWPAN fragmentation header plus eight octets from
the original datagram exceeds the available space in the layer two
payload. In addition, the MTU in the LPWAN networks could be
variable which implies a variable fragmentation solution.

5.2.4. Neighbor Discovery

6LoWPAN Neighbor Discovery [RFC6775] defined optimizations to IPv6
Neighbor Discovery [RFC4861], in order to adapt functionality of the
latter for networks of devices using IEEE 802.15.4 or similar

technologies. The optimizations comprise host-initiated interactions
to allow for sleeping hosts, replacement of multicast-based address
resolution for hosts by an address registration mechanism, multihop
extensions for prefix distribution and duplicate address detection
(note that these are not needed in a star topology network), and
support for 6LoWPAN header compression.

6LoWPAN Neighbor Discovery may be used in not so severely constrained
LPWAN networks. The relative overhead incurred will depend on the
LPWAN technology used (and on its configuration, if appropriate). In
certain LPWAN setups (with a maximum payload size above ~60 bytes,
and duty-cycle-free or equivalent operation), an RS/RA/NS/NA exchange
may be completed in a few seconds, without incurring packet
fragmentation. In other LPWANs (with a maximum payload size of ~10
bytes, and a message rate of ~0.1 message/minute), the same exchange
may take hours or even days, leading to severe fragmentation and
consuming a significant amount of the available network resources.
6LoWPAN Neighbor Discovery behavior may be tuned through the use of
appropriate values for the default Router Lifetime, the Valid
Lifetime in the PIOs, and the Valid Lifetime in the 6CO, as well as
the address Registration Lifetime. However, for the latter LPWANs
mentioned above, 6LoWPAN Neighbor Discovery is not suitable.

5.3. 6lo and LPWAN

The 6lo WG has been reusing and adapting 6LoWPAN to enable IPv6
support over a variety of constrained node link layer technologies
such as Bluetooth Low Energy (BLE), ITU-T G.9959, DECT-ULE, MS/TP-
RS485, NFC or IEEE 802.11ah.

These technologies are relatively similar in several aspects to IEEE
802.15.4, which was the original 6LoWPAN target technology. 6LoWPAN
has been the basis for the functionality defined by 6Lo, which has
mostly used the subset of 6LoWPAN techniques most suitable for each
lower layer technology, and has provided additional optimizations for
technologies where the star topology is used, such as BLE or DECT-
ULE.

The main constraint in these networks comes from the nature of the
devices (constrained devices), whereas in LPWANs it is the network
itself that imposes the most stringent constraints.

5.4. 6tisch and LPWAN

The 6tisch solution is dedicated to mesh networks that operate using
802.15.4e MAC with a deterministic slotted channel. The TSCH can
help to reduce collisions and to enable a better balance over the

   channels. It improves the battery life by avoiding the idle
   listening time for the return channel.

   A key element of 6tisch is the use of synchronization to enable
   determinism. TSCH and 6TiSCH may provide a standard scheduling
   function. The LPWAN networks probably will not support
   synchronization like the one used in 6tisch.

5.5. RoHC and LPWAN

   RoHC header compression mechanisms were defined for point to point
   multimedia channels, to reduce the header overhead of the RTP flows,
   it can also reduce the overhead of IPv4 or IPv6 or IPv4/v6/UDP
   headers. It is based on a shared context which does not require any
   state but packets are not routable. The context is initialised at
   the beginning of the communication or when it is lost. The
   compression is managed using a sequence number (SN) which is encoded
   using a window algorithm letting the reduction of the SN to 4 bits
   instead of 2 bytes. But this window needs to be updated each 15
   packets which implies larger headers. When RoHC compression is used
   we talk about an average header compression size to give the
   performance of compression. For example, the compression start
   sending bigger packets than the original (52 bytes) to reduce the
   header up to 4 bytes (it stays here only for 15 packets, which
   correspond to the window size). Each time the context is lost or
   needs to be synchronised, packets of about 15 to 43 bytes are sent.

   The RoHC header compression is not adapted to the constrained nodes
   of the LPWAN networks: it does not take into account the energy
   limitations and the transmission rate, and context is synchronised
   during the transmission, which does not allow a better compression.

5.6. ROLL and LPWAN

   The LPWAN technologies considered by the lpwan WG are based on a star
   topology, which eliminates the need for routing. Future works may
   address additional use-cases which may require the adaptation of
   existing routing protocols or the definition of new ones. As of the
   writing, the work done at the ROLL WG and other routing protocols are
   out of scope of the LPWAN WG.

5.7. CoRE and LPWAN

   CoRE provides a resource-oriented framework for applications intended
   to run on constrained IP networks. It may be necessary to adapt the
   protocols to take into account the duty cycling and the potentially
   extremely limited throughput of LPWANs.

For example, some of the timers in CoAP may need to be redefined.
Taking into account CoAP acknowledgements may allow the reduction of
L2 acknowledgements. On the other hand, the current work in progress
in the CoRE WG where the COMI/CoOL network management interface
which, uses Structured Identifiers (SID) to reduce payload size over
CoAP proves to be a good solution for the LPWAN technologies. The
overhead is reduced by adding a dictionary which matches a URI to a
small identifier and a compact mapping of the YANG model into the
CBOR binary representation.

5.8. Security and LPWAN

Most of the LPWAN technologies integrate some authentication or
encryption mechanisms that may not have been defined by the IETF.
The working group will work to integrate these mechanisms to unify
management. For the technologies which are not integrating natively
security protocols, it is necessary to adapt existing mechanisms to
the LPWAN constraints. The AAA infrastructure brings a scalable
solution. It offers a central management for the security processes,
draft-garcia- dime-diameter-lorawan-00 and draft-garcia-radext-
radius-lorawan-00 explain the possible security process for a LoRaWAN
network. The mechanisms basically are divided in: key management
protocols, encryption and integrity algorithms used. Most of the
solutions do not present a key management procedure to derive
specific keys for securing network and or data information. In most
cases, a pre-shared key between the smart object and the
communication endpoint is assumed.

5.9. Mobility and LPWAN

LPWANs nodes can be mobile. However, LPWAN mobility is different
from the one specified for Mobile IP. LPWAN implies sporadic traffic
and will rarely be used for high-frequency, real-time communications.
The applications do not generate a flow, they need to save energy and
most of the time the node will be down. The mobility will imply most
of the time a group of devices, which represent a network itself.
The mobility concerns more the gateway than the devices.

5.9.1. NEMO and LPWAN

NEMO Mobility solutions may be used in the case where some hosts
belonging to the same Network gateway will move from one point to
another and that they are not aware of this mobility.

5.10. DNS and LPWAN

   The purpose of the DNS is to enable applications to name things that
   have a global unique name. Lots of protocols are using DNS to
   identify the objects, especially REST and applications using CoAP.
   Therefore, things should be registered in DNS. DNS is probably a
   good topic of research for LPWAN technologies, while the matching of
   the name and the IP information can be used to configure the LPWAN
   devices.

6. Security Considerations

   [[Ed: Yep, these are tbd.]]

7. IANA Considerations

   There are no IANA considerations related to this memo.

8. Contributors

   As stated above this document is mainly a collection of content
   developed by the full set of contributors listed below. The main
   input documents and their authors were:

   o Text for Section 3.1 was provieded by Alper Yegin and Stephen
      Farrell in [I-D.farrell-lpwan-lora-overview].

   o Text for Section 3.2 was provided by Antti Ratilainen in
      [I-D.ratilainen-lpwan-nb-iot].

   o Text for Section 3.3 was provided by Juan Carlos Zuniga and Benoit
      Ponsard in [I-D.zuniga-lpwan-sigfox-system-description].

   o Text for Section 3.4 was provided via personal communication from
      Bob Heile (bheile@ieee.org) and was authored by Bob and Sum Chin
      Sean. There is no Internet draft for that at present.

   o Text for Section 5 was provided by Ana Minabiru, Carles Gomez,
      Laurent Toutain, Josep Paradells and Jon Crowcroft in
      [I-D.minaburo-lpwan-gap-analysis]. Additional text from that
      draft is also used elsewhere above.

   The full list of contributors are:

      Jon Crowcroft
      University of Cambridge
      JJ Thomson Avenue

        Cambridge, CB3 0FD
        United Kingdom

        Email: jon.crowcroft@cl.cam.ac.uk

        Carles Gomez
        UPC/i2CAT
        C/Esteve Terradas, 7
        Castelldefels 08860
        Spain

        Email: carlesgo@entel.upc.edu

        Bob Heile
        Wi-Sun Alliance
        11 Robert Toner Blvd, Suite 5-301
        North Attleboro, MA 02763
        USA

        Phone: +1-781-929-4832
        Email: bheile@ieee.org

        Ana Minaburo
        Acklio
        2bis rue de la Chataigneraie
        35510 Cesson-Sevigne Cedex
        France

        Email: ana@ackl.io

        Josep PAradells
        UPC/i2CAT
        C/Jordi Girona, 1-3
        Barcelona 08034
        Spain

        Email: josep.paradells@entel.upc.edu

        Benoit Ponsard
        SIGFOX
        425 rue Jean Rostand
        Labege 31670
        France

      Email: Benoit.Ponsard@sigfox.com
      URI: http://www.sigfox.com/

      Antti Ratilainen
      Ericsson
      Hirsalantie 11
      Jorvas 02420
      Finland

      Email: antti.ratilainen@ericsson.com

      Chin-Sean SUM
      Wi-Sun Alliance
      20, Science Park Rd
      Singapore 117674

      Phone: +65 6771 1011
      Email: sum@wi-sun.org

      Laurent Toutain
      Institut MINES TELECOM ; TELECOM Bretagne
      2 rue de la Chataigneraie
      CS 17607
      35576 Cesson-Sevigne Cedex
      France

      Email: Laurent.Toutain@telecom-bretagne.eu

      Alper Yegin
      Actility
      Paris, Paris
      FR

      Email: alper.yegin@actility.com

      Juan Carlos Zuniga
      SIGFOX
      425 rue Jean Rostand
      Labege 31670
      France

      Email: JuanCarlos.Zuniga@sigfox.com
      URI: http://www.sigfox.com/

9. Acknowledgements

   Thanks to all those listed in Section 8 for the excellent text.
   Errors in the handling of that are solely the editor's fault.

   Thanks to [your name here] for comments.

   Stephen Farrell's work on this memo was supported by the Science
   Foundation Ireland funded CONNECT centre <https://connectcentre.ie/>.

10. Informative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460,
              December 1998, <http://www.rfc-editor.org/info/rfc2460>.

   [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
              "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
              DOI 10.17487/RFC4861, September 2007,
              <http://www.rfc-editor.org/info/rfc4861>.

   [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,
              "Transmission of IPv6 Packets over IEEE 802.15.4
              Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007,
              <http://www.rfc-editor.org/info/rfc4944>.

   [RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6
              Datagrams over IEEE 802.15.4-Based Networks", RFC 6282,
              DOI 10.17487/RFC6282, September 2011,
              <http://www.rfc-editor.org/info/rfc6282>.

   [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C.
              Bormann, "Neighbor Discovery Optimization for IPv6 over
              Low-Power Wireless Personal Area Networks (6LoWPANs)",
              RFC 6775, DOI 10.17487/RFC6775, November 2012,
              <http://www.rfc-editor.org/info/rfc6775>.

   [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B.,
              Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low
              Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015,
              <http://www.rfc-editor.org/info/rfc7668>.

   [I-D.farrell-lpwan-lora-overview]
              Farrell, S. and A. Yegin, "LoRaWAN Overview", draft-
              farrell-lpwan-lora-overview-01 (work in progress), October
              2016.

   [I-D.minaburo-lpwan-gap-analysis]
              Minaburo, A., Gomez, C., Toutain, L., Paradells, J., and
              J. Crowcroft, "LPWAN Survey and GAP Analysis", draft-
              minaburo-lpwan-gap-analysis-02 (work in progress), October
              2016.

   [I-D.zuniga-lpwan-sigfox-system-description]
              Zuniga, J. and B. PONSARD, "SIGFOX System Description",
              draft-zuniga-lpwan-sigfox-system-description-00 (work in
              progress), July 2016.

   [I-D.ratilainen-lpwan-nb-iot]
              Ratilainen, A., "NB-IoT characteristics", draft-
              ratilainen-lpwan-nb-iot-00 (work in progress), July 2016.

   [TGPP36300]
              3GPP, "TS 36.300 v13.4.0 Evolved Universal Terrestrial
              Radio Access (E-UTRA) and Evolved Universal Terrestrial
              Radio Access Network (E-UTRAN); Overall description; Stage
              2", 2016,
              <http://www.3gpp.org/ftp/Specs/2016-09/Rel-14/36_series/>.

   [TGPP36321]
              3GPP, "TS 36.321 v13.2.0 Evolved Universal Terrestrial
              Radio Access (E-UTRA); Medium Access Control (MAC)
              protocol specification", 2016.

   [TGPP36322]
              3GPP, "TS 36.322 v13.2.0 Evolved Universal Terrestrial
              Radio Access (E-UTRA); Radio Link Control (RLC) protocol
              specification", 2016.

   [TGPP36323]
              3GPP, "TS 36.323 v13.2.0 Evolved Universal Terrestrial
              Radio Access (E-UTRA); Packet Data Convergence Protocol
              (PDCP) specification (Not yet available)", 2016.

   [TGPP36331]
              3GPP, "TS 36.331 v13.2.0 Evolved Universal Terrestrial
              Radio Access (E-UTRA); Radio Resource Control (RRC);
              Protocol specification", 2016.

[TGPP36201]
          3GPP, "TS 36.201 v13.2.0 - Evolved Universal Terrestrial
          Radio Access (E-UTRA); LTE physical layer; General
          description", 2016.

[TGPP23720]
          3GPP, "TR 23.720 v13.0.0 - Study on architecture
          enhancements for Cellular Internet of Things", 2016.

[TGPP33203]
          3GPP, "TS 33.203 v13.1.0 - 3G security; Access security
          for IP-based services", 2016.

[etsi_ltn]
          "ETSI Technical Committee on EMC and Radio Spectrum
          Matters (ERM) TG28 Low Throughput Networks (LTN)",
          February 2015.

[fcc_ref] "FCC CFR 47 Part 15.247 Telecommunication Radio Frequency
          Devices - Operation within the bands 902-928 MHz,
          2400-2483.5 MHz, and 5725-5850 MHz.", June 2016.

[etsi_ref]
          "ETSI EN 300-220 (Parts 1 and 2): Electromagnetic
          compatibility and Radio spectrum Matters (ERM); Short
          Range Devices (SRD); Radio equipment to be used in the 25
          MHz to 1 000 MHz frequency range with power levels ranging
          up to 500 mW", May 2016.

[arib_ref]
          "ARIB STD-T108 (Version 1.0): 920MHz-Band Telemeter,
          Telecontrol and data transmission radio equipment.",
          February 2012.

[LoRaSpec]
          LoRa Alliance, "LoRaWAN Specification Version V1.0.2", Nov
          2016, <URL TBD>.

[LoRaSpec1.0]
          LoRa Alliance, "LoRaWAN Specification Version V1.0", Jan
          2015, <https://www.lora-alliance.org/portals/0/specs/
          LoRaWAN%20Specification%201R0.pdf>.

Author's Address

Stephen Farrell (editor)
Trinity College Dublin
Dublin 2
Ireland

Phone: +353-1-896-2354
Email: stephen.farrell@cs.tcd.ie