Internet Engineering Task Force (IETF)
Request for Comments: 8376
Category: Informational
ISSN: 2070-1721

S. Farrell, Ed.
Trinity College Dublin

May 2018

Low-Power Wide Area Network (LPWAN) Overview

Abstract

Low-Power Wide Area Networks (LPWANs) 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 document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8376.

Table of Contents

1. Introduction

This document provides background material and an overview of the technologies being considered in the IETF’s IPv6 over Low Power Wide-Area Networks (LPWAN) Working Group (WG). It also provides a gap analysis between the needs of these technologies and currently available IETF specifications.

Most technologies in this space aim for a similar goal of supporting large numbers of very low-cost, low-throughput devices with very low power consumption, so that even battery-powered devices can be deployed for years. LPWAN devices also tend to be constrained in their use of bandwidth, for example, with limited frequencies being allowed to be used within limited duty cycles (usually expressed as a percentage of time per hour that the device is allowed to transmit). As the name implies, coverage of large areas is also a common goal. So, by and large, the different technologies aim for deployment in very similar circumstances.

While all constrained networks must balance power consumption / battery life, cost, and bandwidth, LPWANs prioritize power and cost benefits by accepting severe bandwidth and duty cycle constraints when making the required trade-offs. This prioritization is made in order to get the multiple-kilometer radio links implied by "Wide Area" in LPWAN's name.

Existing pilot deployments have shown huge potential and created much industrial interest in these technologies. At the time of writing, essentially no LPWAN end devices (other than for Wi-SUN) 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, where necessary, adapt IETF-defined protocols, addressing schemes, and naming conventions to this particular constrained environment.

This document is largely the work of the people listed in the Contributors section.

2. LPWAN Technologies

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

Note that this text is not intended to be normative in any sense; it simply exists to help the reader in finding the relevant Layer 2 (L2) 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.

2.1. LoRaWAN

2.1.1. Provenance and Documents

LoRaWAN is a wireless technology based on Industrial, Scientific, and Medical (ISM) that is used for long-range low-power low-data-rate applications developed by the LoRa Alliance, a membership consortium <https://www.lora-alliance.org/>. This document is based on Version 1.0.2 of the LoRa specification [LoRaSpec]. That specification is publicly available and has already seen several deployments across the globe.

2.1.2. Characteristics

LoRaWAN aims to support end devices operating on a single battery for an extended period of time (e.g., 10 years or more), extended coverage through 155 dB maximum coupling loss, and reliable and efficient file download (as needed for remote software/firmware upgrade).

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. Communication is generally bidirectional; uplink communication from end devices to the network server is favored in terms of overall bandwidth availability.

Figure 1 shows the entities involved in a LoRaWAN network.

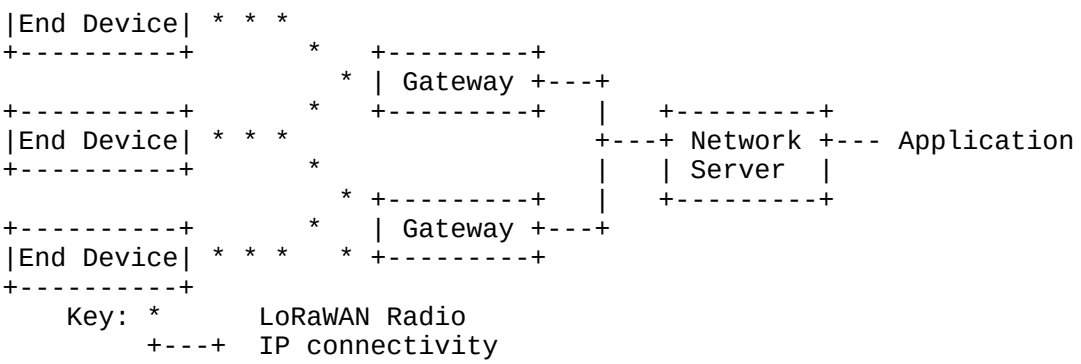

Figure 1: LoRaWAN Architecture

- End Device: a LoRa client device, sometimes called a "mote". Communicates with Gateways.

- 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.

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

- Join Server: The Join Server (JS) is a server on the Internet side of an NS that processes join requests from an end devices.

- Uplink message: refers to communications from an end device to a network server or application via one or more Gateways.

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

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

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 Radio Frequency (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.

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

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

Figure 2 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. 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.

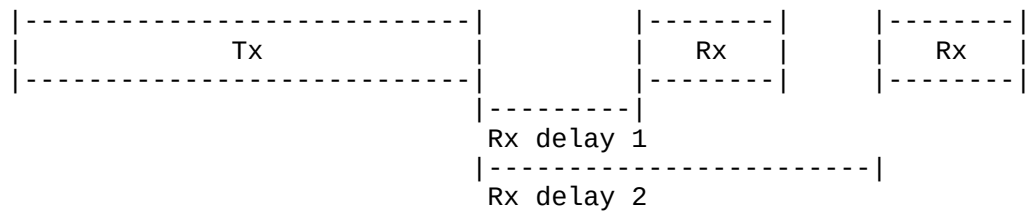

Figure 2: LoRaWAN Class A Transmission and Reception Window

Given the different regional requirements, the detailed specification for the LoRaWAN Physical layer (PHY) (taking up more than 30 pages of the specification) is not reproduced here. Instead, and mainly to illustrate the kinds of issue encountered, Table 1 presents some of the default settings for one ISM band (without fully explaining those here); Table 2 describes 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 + 1 s)
join delay 1	5 s
join delay 2	6 s
868MHz Default channels	3 (868.1,868.2,868.3), data rate: 0.3-50 kbit/s

Table 1: Default Settings for EU 868 MHz 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 restrictive in an attempt to avoid congestion.	1%	no limit
EU 868 MHz band data rate/frame size	250 bits/s : 59 octets	50000 bits/s : 250 octets
US 915 MHz 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 and data rate 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 configuration of the end device's network parameters (available channels, data rates, ADR parameters, Rx Delay 1 and 2, etc.).

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").

There are a number of MAC commands for link and device status checking, ADR and duty cycle negotiation, and managing the RX windows and radio channel settings. For example, the link check response message allows the NS (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 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 its 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).

In order to operate nominally on a LoRaWAN network, a device needs a 32-bit device address, which is assigned when the device "joins" the network (see below for the join procedure) or that is pre-provisioned into the device. In case of roaming devices, the device address is assigned based on the 24-bit network identifier (NetID) that is allocated to the network by the LoRa Alliance. Non-roaming devices can be assigned device addresses by the network without relying on a NetID assigned by the LoRa Alliance.

End devices are assumed to work with one or quite a limited number of applications, identified by a 64-bit AppEUI, which is assumed to be a registered IEEE EUI64 value [EUI64]. In addition, a device needs to have two symmetric session keys, one for protecting network artifacts (port=0), the NwkSKey, and another for protecting application-layer traffic, the AppSKey. Both keys are used for 128-bit AES cryptographic operations. So, one option is for an end device to have all of the above plus channel information, somehow (pre-)provisioned; in that 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 summarizes these values.

Value	Description
DevAddr	DevAddr (32 bits) = device-specific network address generated from the NetID
AppEUI	IEEE EUI64 value corresponding to the join server for an application
NwkSKey	128-bit network session key used with AES-CMAC
AppSKey	128-bit application session key used with AES-CTR
AppKey	128-bit application session key used with AES-ECB

Table 3: Values Required for Nominal Operation

As an alternative, end devices can use the LoRaWAN join procedure with a join server behind the NS in order to set up some of these values and dynamically gain access to the network. To use the join procedure, an end device must still know the AppEUI and a different (long-term) symmetric key that is bound to the AppEUI (this is the application key (AppKey), and it 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. Finally, the end device also needs a long-term identifier for itself, which is syntactically also an EUI-64 and is known as the device EUI or DevEUI. Table 4 summarizes 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. If all is going well, a Join-Accept downlink message is returned from the network server to the end device. That message 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.

All payloads are encrypted and have data integrity. MAC commands, when sent as a payload (port zero), are therefore protected. However, MAC commands piggybacked as frame options ("FOpts") are sent in clear. Any MAC commands sent as frame options and not only as payload, are visible to a passive attacker, but they are not malleable for an active attacker due to the use of the Message Integrity Check (MIC) described below.

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 MIC calculated using AES-CMAC with the input being 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 message 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.

2.2. Narrowband IoT (NB-IoT)

2.2.1. Provenance and Documents

Narrowband Internet of Things (NB-IoT) has been developed and standardized by 3GPP. The standardization of NB-IoT was finalized with 3GPP Release 13 in June 2016, and further enhancements for NB-IoT are specified in 3GPP Release 14 in 2017 (for example, in the form of multicast support). Further features and improvements will be developed in the following releases, but NB-IoT has been ready to be deployed since 2016; it is rather simple to deploy, especially in the existing LTE networks with a software upgrade in the operator’s base stations. For more information of what has been specified for NB-IoT, 3GPP specification 36.300 [TGPP36300] provides an overview and overall description of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) radio interface protocol architecture, while specifications 36.321 [TGPP36321], 36.322 [TGPP36322], 36.323 [TGPP36323], and 36.331 [TGPP36331] give more detailed descriptions

of MAC, Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), and Radio Resource Control (RRC) protocol layers, respectively. Note that the description below assumes familiarity with numerous 3GPP terms.

For a general overview of NB-IoT, see [nbiot-ov].

2.2.2. Characteristics

Specific targets for NB-IoT include: module cost that is Less than US $5, 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 Frequency Division Duplex (FDD) operation mode with 60 kbit/s peak rate in uplink and 30 kbit/s peak rate in downlink, and a Maximum Transmission Unit (MTU) size of 1600 bytes, limited by PDCP layer (see Figure 4 for the protocol structure), which is the highest layer in the user plane, as explained later. Any packet size up to the said MTU size can be passed to the NB-IoT stack from higher layers, segmentation of the packet is performed in the RLC layer, which can segment the data to transmission blocks with a size as small as 16 bits. As the name suggests, NB-IoT uses narrowbands with bandwidth of 180 kHz in both downlink and uplink. The multiple access scheme used in the downlink is Orthogonal Frequency-Division Multiplex (OFDMA) with 15 kHz sub-carrier spacing. In uplink, Sub-Carrier Frequency-Division Multiplex (SC-FDMA) single tone with either 15kHz or 3.75 kHz tone spacing is used, or optionally multi-tone SC-FDMA can be used with 15 kHz tone spacing.

NB-IoT can be deployed in three ways. In-band deployment means that the narrowband is deployed inside the LTE band and radio resources are flexibly shared between NB-IoT and normal LTE carrier. In Guard-band deployment, the narrowband uses the unused resource blocks between two adjacent LTE carriers. Standalone deployment is also supported, where the narrowband can be located alone in dedicated spectrum, which makes it possible, for example, to reframe a GSM carrier at 850/900 MHz for NB-IoT. All three deployment modes are used in licensed frequency 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.

A Maximum Coupling Loss (MCL) target for NB-IoT coverage enhancements defined by 3GPP is 164 dB. With this MCL, the performance of NB-IoT in downlink varies between 200 bps and 2-3 kbit/s, depending on the deployment mode. Stand-alone operation may achieve the highest data

rates, up to a few kbit/s, while in-band and guard-band operations may reach several hundreds of bps. NB-IoT may even operate with an MCL higher than 170 dB with very low bit rates.

For signaling optimization, two options are introduced in addition to the legacy LTE 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 (NAS), directly to/from the Mobile Management Entity (MME) (see Figure 3 for the network architecture) in the core network to the User Equipment (UE) without interaction from the base station. This means there is no Access Stratum security or header compression provided by the PDCP layer in the eNodeB, as the Access Stratum is bypassed, and only limited RRC procedures. Header compression based on Robust Header Compression (RoHC) may still optionally be provided and terminated in the MME.

The RRC Suspend/Resume procedures reduce the signaling overhead required for UE state transition from RRC Idle to RRC Connected mode compared to a legacy LTE operation in order to have quicker user-plane transaction with the network and return to RRC Idle mode faster.

In order to prolong device battery life, both Power-Saving Mode (PSM) and extended DRX (eDRX) are available to NB-IoT. With eDRX, the RRC Connected mode DRX cycle is up to 10.24 seconds; in RRC Idle, the eDRX cycle can be up to 3 hours. In PSM, the device is in a deep sleep state and only wakes up for uplink reporting. After the reporting, there is a window (configured by the network) during which the device receiver is open for downlink connectivity or for periodical "keep-alive" signaling (PSM uses periodic TAU signaling with additional reception windows for downlink reachability).

Since NB-IoT operates in a licensed spectrum, it has no channel access restrictions allowing up to a 100% duty cycle.

3GPP access security is specified in [TGPP33203].

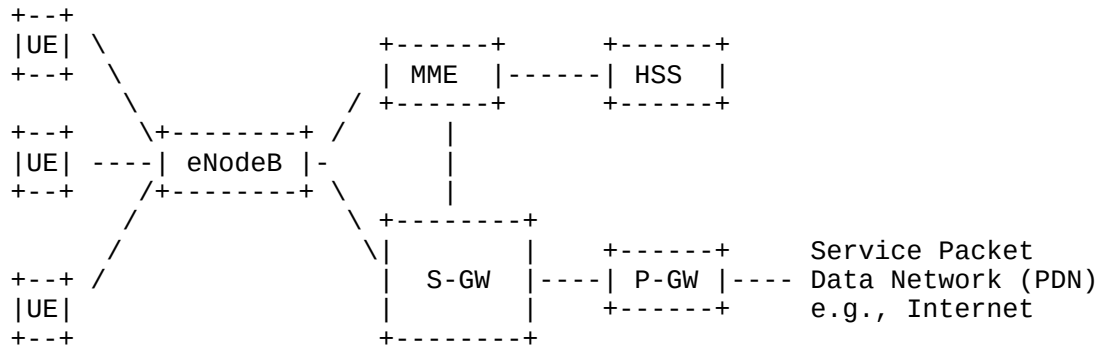

Figure 3: 3GPP Network Architecture

Figure 3 shows the 3GPP network architecture, which applies to NB-IoT. The MME is responsible for handling the mobility of the UE. The MME tasks include tracking and paging UEs, session management, choosing the Serving Gateway for the UE during initial attachment and authenticating the user. At the MME, the NAS signaling from the UE is terminated.

The 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 NB-IoT and other 3GPP technologies.

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

The Home Subscriber Server (HSS) contains user-related and subscription-related information. It is a database that 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 that controls the UEs in one or several cells.

The 3GPP radio protocol architecture is illustrated in Figure 4.

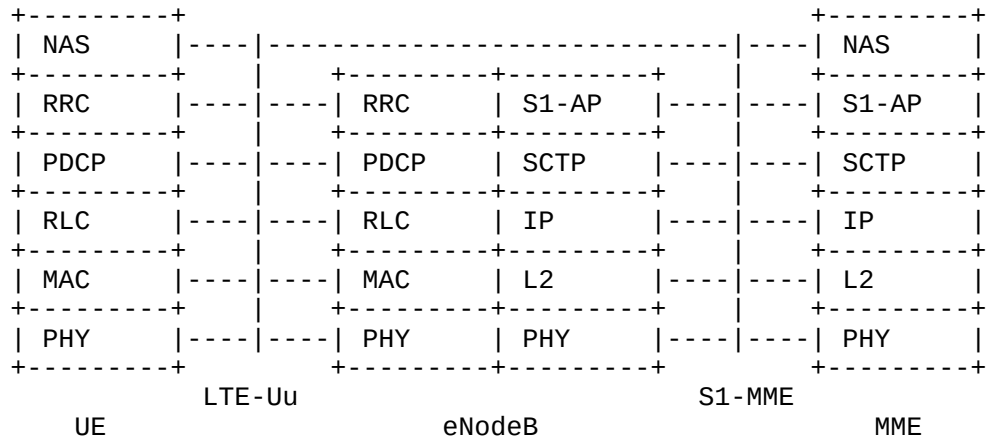

Figure 4: 3GPP Radio Protocol Architecture for the Control Plane

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

The Access Stratum (AS) is the functional layer below the NAS; in the control plane, it consists of the Radio Resource Control (RRC) protocol [TGPP36331], which handles connection establishment and release functions, broadcast of system information, radio-bearer establishment, reconfiguration, and release. The RRC configures the user and control planes according to the network status. There exist two RRC states, RRC_Idle or RRC_Connected, and the 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 an incoming call/downlink data. 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 unicast data. In RRC_Connected state, the UE has a connection to the eNodeB, the network knows the UE location on the cell level, and the UE may receive and transmit unicast data. An RRC connection is established when the UE is expected to be active in the network, to transmit or receive data. The RRC connection is released, switching back to RRC_Idle, when there is no more traffic; this is in order to preserve UE battery life and radio resources.

However, as mentioned earlier, a new feature was introduced for NB-IoT that allows data to be transmitted from the MME directly to the UE and then transparently to the eNodeB, thus bypassing AS functions.

The PDCP's [TGPP36323] main services in the control plane are transfer of control-plane data, ciphering, and integrity protection.

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

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

The PHY [TGPP36201] provides data-transport services to higher layers. These include error detection and indication to higher layers, Forward Error Correction (FEC) encoding, HARQ soft-combining, rate-matching, mapping of the transport channels onto physical channels, power-weighting and modulation of physical channels, frequency and time synchronization, and radio characteristics measurements.

The user plane is responsible for transferring the user data through the Access Stratum. It interfaces with IP and the highest layer of the user plane is the PDCP, which, in the user plane, performs header compression using RoHC, transfer of user-plane data between eNodeB and the UE, ciphering, and integrity protection. Similar to the control plane, lower layers in the user plane include RLC, MAC, and the PHY performing the same tasks as they do in the control plane.

2.3. Sigfox

2.3.1. Provenance and Documents

The Sigfox LPWAN is in line with the terminology and specifications being defined by ETSI [etsi_unb]. As of today, Sigfox's network has been fully deployed in 12 countries, with ongoing deployments in 26 other countries, giving in total a geography of 2 million square kilometers, containing 512 million people.

2.3.2. Characteristics

Sigfox LPWAN autonomous battery-operated devices send only a few bytes per day, week, or month, in principle, allowing them to remain on a single battery for up to 10-15 years. Hence, the system is designed as to allow devices to last several years, sometimes even buried underground.

Since the radio protocol is connectionless and optimized for uplink communications, the capacity of a Sigfox base station depends on the number of messages generated by devices, and not on the actual number of devices. Likewise, the battery life of devices depends on the number of messages generated by the device. Depending on the use case, devices can vary from sending less than one message per device per day to dozens of messages per device per day.

The coverage of the cell depends on the link budget and on the type of deployment (urban, rural, etc.). The radio interface is compliant with the following regulations:

Spectrum allocation in the USA [fcc_ref]

Spectrum allocation in Europe [etsi_ref1] [etsi_ref2]

Spectrum allocation in Japan [arib_ref]

The Sigfox 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 are supported, although the system is optimized for uplink communications. 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:

- Channelization mask: 100 Hz / 600 Hz (depending on the region)
- Uplink baud rate: 100 baud / 600 baud (depending on the region)

- Modulation scheme: DBPSK
- Uplink transmission power: compliant with local regulation
- Link budget: 155 dB (or better)
- Central frequency accuracy: not relevant, provided there is no significant frequency drift within an uplink packet transmission

For example, 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 duty cycle of 1%.

The format of the uplink frame is the following:

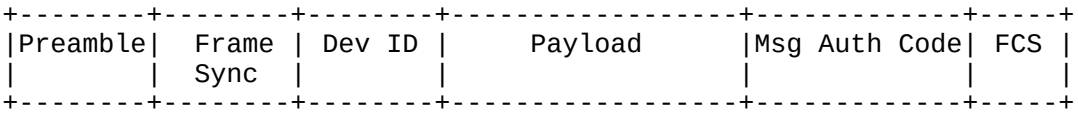

Figure 5: Uplink Frame Format

The uplink frame is composed of the following fields:

- Preamble: 19 bits
- Frame sync and header: 29 bits
- Device ID: 32 bits
- Payload: 0-96 bits
- Authentication: 16-40 bits
- Frame check sequence: 16 bits (Cyclic Redundancy Check (CRC))

The main radio characteristics of the UNB downlink transmission are:

- Channelization mask: 1.5 kHz
- Downlink baud rate: 600 baud
- Modulation scheme: GFSK
- Downlink transmission power: 500 mW / 4W (depending on the region)
- Link budget: 153 dB (or better)

- Central frequency accuracy: the center frequency of downlink transmission is set by the network according to the corresponding uplink transmission.

For example, 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:

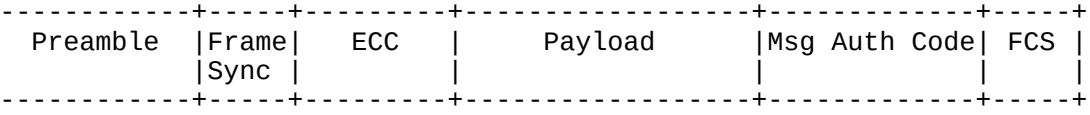

Figure 6: Downlink Frame Format

The downlink frame is composed of the following fields:

- Preamble: 91 bits
- Frame sync and header: 13 bits
- Error Correcting Code (ECC): 32 bits
- Payload: 0-64 bits
- Authentication: 16 bits
- Frame check sequence: 8 bits (CRC)

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

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 network transmits the downlink message for a given device during the reception window, and the network also selects the BS for transmitting the corresponding downlink message.

Uplink and downlink transmissions are unbalanced due to the regulatory constraints on ISM bands. Under the strictest regulations, the system can allow a maximum of 140 uplink messages

and 4 downlink messages per device per day. These restrictions can be slightly relaxed depending on system conditions and the specific regulatory domain of operation.

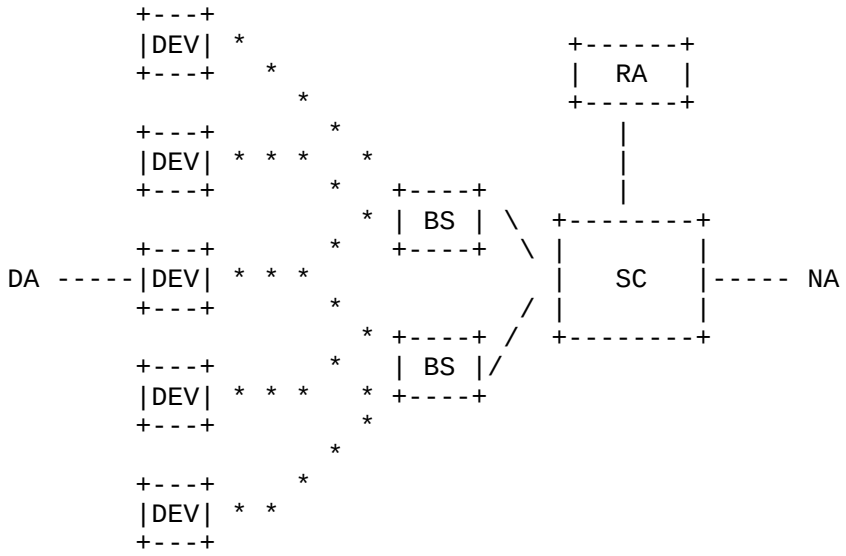

Figure 7: Sigfox Network Architecture

Figure 7 depicts the different elements of the Sigfox network architecture.

Sigfox has a "one-contract one-network" model allowing devices to connect in any country, without any need or notion of either roaming or handover.

The architecture consists of a single cloud-based 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 BS and the Internet, as well as the control and management of the BSs and End Points (EPs). The RA is in charge of the EP 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 (DEVs) or EPs are the objects that communicate application data between local Device Applications (DAs) and Network Applications (NAs).

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

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

The radio protocol authenticates and ensures the integrity of each message. This is achieved by using a unique device ID and an AES-128-based message authentication code, ensuring that the message has been generated and sent by the device with the ID claimed in the message. Application data can be encrypted at the application level or not, depending on the criticality of the use case, to provide a balance between cost and effort versus risk. AES-128 in counter mode is used for encryption. Cryptographic keys are independent for each device. These keys are associated with the device ID and separate integrity and confidentiality keys are pre-provisioned. A confidentiality key is only provisioned if confidentiality is to be used. At the time of writing, the algorithms and keying details for this are not published.

2.4. 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. Paul Duffy (paduffy@cisco.com) also provided additional comments/input on this section.

2.4.1. Provenance and Documents

The Wi-SUN Alliance <https://www.wi-sun.org/> is an industry alliance 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 IEEE 802 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. Additionally, the Alliance has created a certification program to promote global multi-vendor interoperability.

The FAN profile is specified within ANSI/TIA as an extension of work previously done on Smart Utility Networks [ANSI-4957-000]. Updates to those specifications intended to be published in 2017 will contain

details of the FAN profile. A current snapshot of the work to produce that profile is presented in [wisun-pressie1] and [wisun-pressie2].

2.4.2. Characteristics

The FAN profile is an IPv6 wireless mesh network with support for enterprise-level security. The frequency-hopping wireless mesh topology aims to offer superior network robustness, reliability due to high redundancy, good scalability due to the flexible mesh configuration, and good resilience to interference. Very low power modes are in development permitting long-term battery operation of network nodes.

The following list contains some overall characteristics of Wi-SUN that are relevant to LPWAN applications.

- Coverage: The range of Wi-SUN FAN is typically 2 - 3 km in line of sight, matching the needs of neighborhood area networks, campus area networks, or corporate area networks. The range can also be extended via multi-hop networking.

- High-bandwidth, low-link latency: Wi-SUN supports relatively high bandwidth, i.e., up to 300 kbit/s [FANOV], enables remote update and upgrade of devices so that they can handle new applications, extending their working life. Wi-SUN supports LPWAN IoT applications that require on-demand control by providing low link latency (0.02 s) and bidirectional communication.

- Low-power consumption: FAN devices draw less than 2 uA when resting and only 8 mA when listening. Such devices can maintain a long lifetime, even if they are frequently listening. For instance, suppose the device transmits data for 10 ms once every 10 s; theoretically, a battery of 1000 mAh can last more than 10 years.

- Scalability: Tens of millions of Wi-SUN FAN devices have been deployed in urban, suburban, and rural environments, including deployments with more than 1 million devices.

A FAN contains one or more networks. Within a network, nodes assume one of three operational roles. First, each network contains a Border Router providing WAN connectivity to the network. The Border Router maintains source-routing tables for all nodes within its network, provides node authentication and key management services, and disseminates network-wide information such as broadcast schedules. Second, Router nodes, which provide upward and downward packet forwarding (within a network). A Router also provides

services for relaying security and address management protocols. Finally, Leaf nodes provide minimum capabilities: discovering and joining a network, sending/receiving IPv6 packets, etc. A low-power network may contain a mesh topology with Routers at the edges that construct a star topology with Leaf nodes.

The FAN profile is based on various open standards developed by the IETF (including [RFC768], [RFC2460], [RFC4443], and [RFC6282]). Related IEEE 802 standards include [IEEE.802.15.4] and [IEEE.802.15.9]. For Low-Power and Lossy Networks (LLNs), see ANSI/TIA [ANSI-4957-210].

The FAN profile specification provides an application-independent IPv6-based transport service. There are two possible methods for establishing IPv6 packet routing: the Routing Protocol for Low-Power and Lossy Networks (RPL) at the Network layer is mandatory, and Multi-Hop Delivery Service (MHDS) is optional at the Data Link layer. Figure 8 provides an overview of the FAN network stack.

The Transport service is based on UDP (defined in [RFC768]) or TCP (defined in [RFC793].

The Network service is provided by IPv6 as defined in [RFC2460] with an IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) adaptation as defined in [RFC4944] and [RFC6282]. ICMPv6, as defined in [RFC4443], is used for the control plane during information exchange.

The Data Link service provides both control/management of the PHY and data transfer/management services to the Network layer. These services are divided into MAC and Logical Link Control (LLC) sub-layers. The LLC sub-layer provides a protocol dispatch service that supports 6LoWPAN and an optional MAC sub-layer mesh service. The MAC sub-layer is constructed using data structures defined in [IEEE.802.15.4]. Multiple modes of frequency hopping are defined. The entire MAC payload is encapsulated in an [IEEE.802.15.9] Information Element to enable LLC protocol dispatch between upper-layer 6LoWPAN processing and MAC sub-layer mesh processing, etc. These areas will be expanded once [IEEE.802.15.12] is completed.

The PHY service is derived from a subset of the SUN FSK specification in [IEEE.802.15.4]. The 2-FSK modulation schemes, with a channel-spacing range from 200 to 600 kHz, are defined to provide data rates from 50 to 300 kbit/s, with 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.

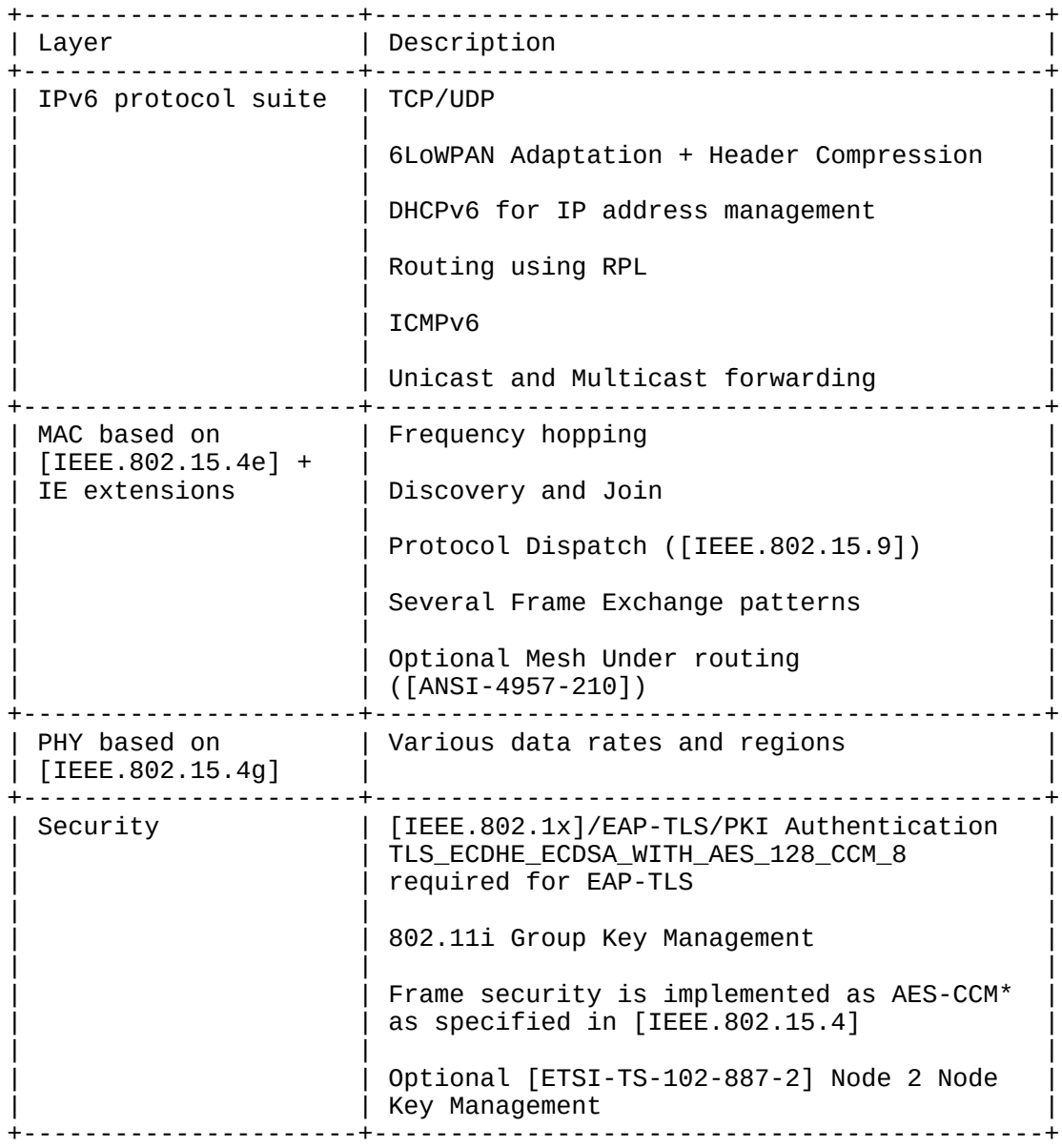

Figure 8: Wi-SUN Stack Overview

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 [IEEE.802.1x] and EAP-TLS as described in [RFC5216] using secure device identity as described in [IEEE.802.1AR]. 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 [IEEE.802.11] Four-Way Handshake. A set of four 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 [IEEE.802.15.4].

3. Generic Terminology

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

- End devices are the devices or the "things" (e.g., sensors, actuators, etc.); they are named differently in each technology (End Device, User Equipment, or EP). There can be a high density of end devices per Radio Gateway.

- The Radio Gateway, which is the EP of the constrained link. It is known as: Gateway, Evolved Node B or base station.

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

- LPWAN-AAA server, which controls user authentication. It is known as the Join-Server, Home Subscriber Server, or Registration Authority. (We use the term LPWAN-AAA server because we’re not assuming that this entity speaks RADIUS or Diameter as many/most AAA servers do; but, equally, we don’t want to rule that out, as the functionality will be similar.)

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

Function/ Technology	LoRaWAN	NB-IoT	Sigfox	Wi-SUN	IETF
Sensor, Actuator, device, object	End Device	User Equipment	End Point	Leaf Node	Device (DEV)
Transceiver Antenna	Gateway	Evolved Node B	Base Station	Router Node	Radio Gateway
Server	Network Server	PDN GW/ SCEF*	Service Center	Border Router	Network Gateway (NGW)
Security Server	Join Server	Home Subscriber Server	Registration Authority	Authent. Server	LPWAN-AAA Server
Application	Application Server	Application Server	Network Application	Appli-cation	Application (App)

* SCEF = Service Capability Exposure Function

Figure 9: LPWAN Architecture Terminology

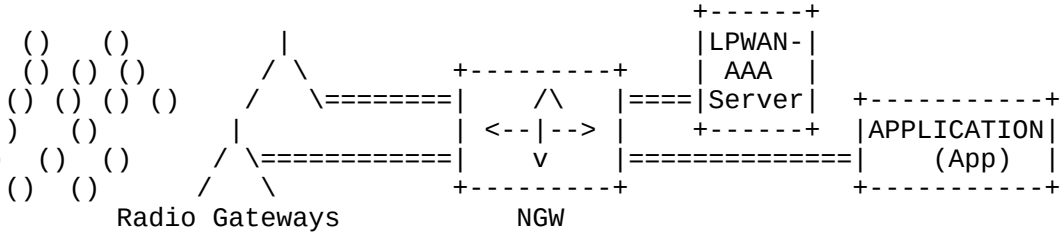

Figure 10: LPWAN Architecture

In addition to the names of entities, LPWANs are also subject to possibly regional frequency-band regulations. Those may include restrictions on the duty cycle, for example, requiring that hosts only transmit for a certain percentage of each hour.

4. Gap Analysis

This section considers some of the gaps between current LPWAN technologies and the goals of the LPWAN WG. Many of the generic considerations described in [RFC7452] will also apply in LPWANs, as end devices can also be considered to be a subclass of (so-called) "smart objects". In addition, LPWAN device implementers will also need to consider the issues relating to firmware updates described in [RFC8240].

4.1. Naive Application of IPv6

IPv6 [RFC8200] 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 LPWAN constraints. If IPv6 with no further optimization were used, several LPWAN frames could be needed just to carry the IP header. Another problem arises from IPv6 MTU requirements, which require the layer below to support at least 1280 byte packets [RFC2460].

IPv6 has a configuration protocol: Neighbor Discovery Protocol (NDP) [RFC4861]). For a node to learn network parameters, NDP generates regular traffic with a relatively large message size that does not fit LPWAN constraints.

In some LPWAN technologies, L2 multicast is not supported. In that case, if the network topology is a star, the solution and considerations from Section 3.2.5 of [RFC7668] may be applied.

Other key protocols (such as DHCPv6 [RFC3315], IPsec [RFC4301] and TLS [RFC5246]) have similarly problematic properties in this context. Each protocol requires relatively frequent round-trips between the host and some other host on the network. In the case of cryptographic protocols (such as IPsec and TLS), in addition to the round-trips required for secure session establishment, cryptographic operations can require padding and addition of authenticators that are problematic when considering LPWAN lower layers. Note that mains powered Wi-SUN mesh router nodes will typically be more resource capable than the other LPWAN technologies discussed. This can enable use of more "chatty" protocols for some aspects of Wi-SUN.

4.2. 6LoWPAN

Several technologies that exhibit significant constraints in various dimensions have exploited the 6LoWPAN suite of specifications ([RFC4944], [RFC6282], and [RFC6775]) to support IPv6 [USES-6LO]. 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 characterized by device constraints (in terms of processing capacity, memory, and energy availability), and especially, link constraints, such as:

- tiny L2 payload size (from ~10 to ~100 bytes),
- very low bit rate (from ~10 bit/s to ~100 kbit/s), and
- 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.

4.2.1. 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 smallest 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 was initially designed for [IEEE.802.15.4] networks with a frame size up to 127 bytes and a throughput of up to 250 kbit/s, which may or may not be duty cycled.

4.2.2. Address Autoconfiguration

Traditionally, Interface Identifiers (IIDs) have been derived from link-layer identifiers [RFC4944]. This allows optimizations 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. [RFC8065] provides guidance on better methods for generating IIDs.

4.2.3. Fragmentation

As stated above, IPv6 requires the layer below to support an MTU of 1280 bytes [RFC8200]. 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 the 2003 version of [IEEE.802.15.4] (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 the 2003 version of [IEEE.802.15.4]. 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.

4.2.4. Neighbor Discovery

6LoWPAN Neighbor Discovery [RFC6775] defines optimizations to IPv6 ND [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 ND 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 ND 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 6LoWPAN Context Option (6CO), as well as the address Registration Lifetime. However, for the latter LPWANs mentioned above, 6LoWPAN ND is not suitable.

4.3. 6lo

The 6lo WG has been reusing and adapting 6LoWPAN to enable IPv6 support over link-layer technologies such as Bluetooth Low Energy (BTLE), ITU-T G.9959 [G9959], Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE), MS/TP-RS485, Near Field Communication (NFC) IEEE 802.11ah. (See <https://datatracker.ietf.org/wg/6lo/> for details on the 6lo WG.) These technologies are similar in several aspects to [IEEE.802.15.4], which was the original 6LoWPAN target technology.

6lo has mostly used the subset of 6LoWPAN techniques best suited for each lower-layer technology and has provided additional optimizations for technologies where the star topology is used, such as BTLE 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.

4.4. 6tisch

The IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch) solution is dedicated to mesh networks that operate using [IEEE.802.15.4e] MAC with a deterministic slotted channel. Time-Slotted Channel Hopping (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.

4.5. RoHC

RoHC is a header compression mechanism [RFC3095] developed for multimedia flows in a point-to-point channel. RoHC uses three levels of compression, each level having its own header format. In the first level, RoHC sends 52 bytes of header; in the second level, the header could be from 34 to 15 bytes; and in the third level, header size could be from 7 to 2 bytes. The level of compression is managed by a Sequence Number (SN), which varies in size from 2 bytes to 4 bits in the minimal compression. SN compression is done with an

algorithm called Window-Least Significant Bits (W-LSB). This window has a 4-bit size representing 15 packets, so every 15 packets, RoHC needs to slide the window in order to receive the correct SN, and sliding the window implies a reduction of the level of compression. When packets are lost or errored, the decompressor loses context and drops packets until a bigger header is sent with more complete information. To estimate the performance of RoHC, an average header size is used. This average depends on the transmission conditions, but most of the time is between 3 and 4 bytes.

RoHC has not been adapted specifically to the constrained hosts and networks of LPWANs: it does not take into account energy limitations nor the transmission rate. Additionally, RoHC context is synchronized during transmission, which does not allow better compression.

4.6. ROLL

Most technologies considered by the LPWAN WG are based on a star topology, which eliminates the need for routing at that layer. Future work may address additional use cases that may require adaptation of existing routing protocols or the definition of new ones. As of the time of writing, work similar to that done in the Routing Over Low-Power and Lossy Network (ROLL) WG and other routing protocols are out of scope of the LPWAN WG.

4.7. CoAP

The Constrained Application Protocol (CoAP) [RFC7252] provides a RESTful framework for applications intended to run on constrained IP networks. It may be necessary to adapt CoAP or related protocols to take into account the extreme duty cycles 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 acknowledgments may allow the reduction of L2 acknowledgments. On the other hand, the current work in progress in the CoRE WG where the Constrained Management Interface (COMI) / Constrained Objects Language (CoOL) network management interface which, uses Structured Identifiers (SIDs) to reduce payload size over CoAP may prove to be a good solution for the LPWAN technologies. The overhead is reduced by adding a dictionary that matches a URI to a small identifier and a compact mapping of the YANG data model into the Concise Binary Object Representation (CBOR).

4.8. Mobility

LPWAN 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.

In addition, LPWAN mobility may mostly apply to groups of devices that represent a network; in which case, mobility is more a concern for the Gateway than the devices. Network Mobility (NEMO) [RFC3963] or other mobile Gateway solutions (such as a Gateway with an LTE uplink) may be used in the case where some end devices belonging to the same network Gateway move from one point to another such that they are not aware of being mobile.

4.9. DNS and LPWAN

The Domain Name System (DNS) [RFC1035], enables applications to name things with a globally resolvable name. Many protocols use the DNS to identify hosts, for example, applications using CoAP.

The DNS query/answer protocol as a precursor to other communication within the Time-To-Live (TTL) of a DNS answer is clearly problematic in an LPWAN, say where only one round-trip per hour can be used, and with a TTL that is less than 3600 seconds. It is currently unclear whether and how DNS-like functionality might be provided in LPWANs.

5. Security Considerations

Most LPWAN technologies integrate some authentication or encryption mechanisms that were defined outside the IETF. The LPWAN WG may need to do work to integrate these mechanisms to unify management. A standardized Authentication, Authorization, and Accounting (AAA) infrastructure [RFC2904] may offer a scalable solution for some of the security and management issues for LPWANs. AAA offers centralized management that may be of use in LPWANs, for example [LoRaWAN-AUTH] and [LoRaWAN-RADIUS] suggest possible security processes for a LoRaWAN network. Similar mechanisms may be useful to explore for other LPWAN technologies.

Some applications using LPWANs may raise few or no privacy considerations. For example, temperature sensors in a large office building may not raise privacy issues. However, the same sensors, if deployed in a home environment, and especially if triggered due to human presence, can raise significant privacy issues: if an end device emits a (encrypted) packet every time someone enters a room in a home, then that traffic is privacy sensitive. And the more that

the existence of that traffic is visible to network entities, the more privacy sensitivities arise. At this point, it is not clear whether there are workable mitigations for problems like this. In a more typical network, one would consider defining padding mechanisms and allowing for cover traffic. In some LPWANs, those mechanisms may not be feasible. Nonetheless, the privacy challenges do exist and can be real; therefore, some solutions will be needed. Note that many aspects of solutions in this space may not be visible in IETF specifications but can be, e.g., implementation or deployment specific.

Another challenge for LPWANs will be how to handle key management and associated protocols. In a more traditional network (e.g., the Web), servers can "staple" Online Certificate Status Protocol (OCSP) responses in order to allow browsers to check revocation status for presented certificates [RFC6961]. While the stapling approach is likely something that would help in an LPWAN, as it avoids an RTT, certificates and OCSP responses are bulky items and will prove challenging to handle in LPWANs with bounded bandwidth.

6. IANA Considerations

This document has no IANA actions.

7. Informative References

[ANSI-4957-000]
ANSI/TIA, "Architecture Overview for the Smart Utility Network", ANSI/TIA-4957.0000 , May 2013.

[ANSI-4957-210]
ANSI/TIA, "Multi-Hop Delivery Specification of a Data Link Sub-Layer", ANSI/TIA-4957.210 , May 2013.

[arib_ref] ARIB, "920MHz-Band Telemeter, Telecontrol and Data Transmission Radio Equipment", ARIB STD-T108 Version 1.0, February 2012.

[ETSI-TS-102-887-2]
ETSI, "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol; Part 2: Data Link Layer (MAC Sub-layer)", ETSI TS 102 887-2, Version V1.1.1, September 2013.

[etsi_ref1] ETSI, "Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 1: Technical characteristics and methods of measurement", Draft ETSI EN 300-220-1, Version V3.1.0, May 2016.

[etsi_ref2] ETSI, "Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU for non specific radio equipment", Final draft ETSI EN 300-220-2 P300-220-2, Version V3.1.1, November 2016.

[etsi_unb] ETSI ERM, "System Reference document (SRdoc); Short Range Devices (SRD); Technical characteristics for Ultra Narrow Band (UNB) SRDs operating in the UHF spectrum below 1 GHz", ETSI TR 103 435, Version V1.1.1, February 2017.

[EUI64] IEEE, "Guidelines for 64-bit Global Identifier (EUI),Organizationally Unique Identifier (OUI), and Company ID (CID)", August 2017, <http://standards.ieee.org/develop/regauth/tut/eui.pdf>.

[FANOV] IETF, "Wi-SUN Alliance Field Area Network (FAN) Overview", IETF 97, November 2016, <https://www.ietf.org/proceedings/97/slides/slides-97-lpwan-35-wi-sun-presentation-00.pdf>.

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

[G9959] ITU-T, "Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications", ITU-T Recommendation G.9959, January 2015, <http://www.itu.int/rec/T-REC-G.9959>.

[IEEE.802.11] IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE 802.11.

[IEEE.802.15.12]
IEEE, "Upper Layer Interface (ULI) for IEEE 802.15.4 Low-Rate Wireless Networks", IEEE 802.15.12.

[IEEE.802.15.4]
IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE 802.15.4, <https://standards.ieee.org/findstds/standard/802.15.4-2015.html>.

[IEEE.802.15.4e]
IEEE, "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer", IEEE 802.15.4e.

[IEEE.802.15.4g]
IEEE, "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks", IEEE 802.15.4g.

[IEEE.802.15.9]
IEEE, "IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams", IEEE Standard 802.15.9, 2016, <https://standards.ieee.org/findstds/standard/802.15.9-2016.html>.

[IEEE.802.1AR]
ANSI/IEEE, "IEEE Standard for Local and metropolitan area networks - Secure Device Identity", IEEE 802.1AR.

[IEEE.802.1x]
IEEE, "Port Based Network Access Control", IEEE 802.1x.

[LoRaSpec] LoRa Alliance, "LoRaWAN Specification Version V1.0.2", July 2016, <https://lora-alliance.org/sites/default/files/2018-05/lorawan1_0_2-20161012_1398_1.pdf>.

[LoRaWAN] Farrell, S. and A. Yegin, "LoRaWAN Overview", Work in Progress, draft-farrell-lpwan-lora-overview-01, October 2016.

[LoRaWAN-AUTH]
Garcia, D., Marin, R., Kandasamy, A., and A. Pelov, "LoRaWAN Authentication in Diameter", Work in Progress, draft-garcia-dime-diameter-lorawan-00, May 2016.

[LoRaWAN-RADIUS]
Garcia, D., Lopez, R., Kandasamy, A., and A. Pelov, "LoRaWAN Authentication in RADIUS", Work in Progress, draft-garcia-radext-radius-lorawan-03, May 2017.

[LPWAN-GAP]
Minaburo, A., Ed., Gomez, C., Ed., Toutain, L., Paradells, J., and J. Crowcroft, "LPWAN Survey and GAP Analysis", Work in Progress, draft-minaburo-lpwan-gap-analysis-02, October 2016.

[NB-IoT] Ratilainen, A., "NB-IoT characteristics", Work in Progress, draft-ratilainen-lpwan-nb-iot-00, July 2016.

[nbiot-ov] IEEE, "NB-IoT Technology Overview and Experience from Cloud-RAN Implementation", Volume 24, Issue 3 Pages 26-32, DOI 10.1109/MWC.2017.1600418, June 2017.

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <https://www.rfc-editor.org/info/rfc768>.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

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

[RFC2904] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, "AAA Authorization Framework", RFC 2904, DOI 10.17487/RFC2904, August 2000, <https://www.rfc-editor.org/info/rfc2904>.

[RFC3095] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, DOI 10.17487/RFC3095, July 2001, <https://www.rfc-editor.org/info/rfc3095>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <https://www.rfc-editor.org/info/rfc3963>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc4944>.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI 10.17487/RFC5216, March 2008, <https://www.rfc-editor.org/info/rfc5216>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc6775>.

[RFC6961] Pettersen, Y., "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", RFC 6961, DOI 10.17487/RFC6961, June 2013, <https://www.rfc-editor.org/info/rfc6961>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7452] Tschofenig, H., Arkko, J., Thaler, D., and D. McPherson, "Architectural Considerations in Smart Object Networking", RFC 7452, DOI 10.17487/RFC7452, March 2015, <https://www.rfc-editor.org/info/rfc7452>.

[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, <https://www.rfc-editor.org/info/rfc7668>.

[RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <https://www.rfc-editor.org/info/rfc8065>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8240] Tschofenig, H. and S. Farrell, "Report from the Internet of Things Software Update (IoTSU) Workshop 2016", RFC 8240, DOI 10.17487/RFC8240, September 2017, <https://www.rfc-editor.org/info/rfc8240>.

[Sigfox] Zuniga, J. and B. PONSARD, "Sigfox System Description", Work in Progress, draft-zuniga-lpwan-sigfox-system-description-04, December 2017.

[TGPP23720] 3GPP, "Study on architecture enhancements for Cellular Internet of Things", 3GPP TS 23.720 13.0.0, 2016.

[TGPP33203] 3GPP, "3G security; Access security for IP-based services", 3GPP TS 23.203 13.1.0, 2016.

[TGPP36201] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description", 3GPP TS 36.201 13.2.0, 2016.

[TGPP36300] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2", 3GPP TS 36.300 13.4.0, 2016, <http://www.3gpp.org/ftp/Specs/2016-09/Rel-14/36_series/>.

[TGPP36321] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification", 3GPP TS 36.321 13.2.0, 2016.

[TGPP36322] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification", 3GPP TS 36.322 13.2.0, 2016.

[TGPP36323] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification (Not yet available)", 3GPP TS 36.323 13.2.0, 2016.

[TGPP36331] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification", 3GPP TS 36.331 13.2.0, 2016.

[USES-6LO] Hong, Y., Gomez, C., Choi, Y-H., and D-Y. Ko, "IPv6 over Constrained Node Networks(6lo) Applicability & Use cases", Work in Progress, draft-hong-6lo-use-cases-03, October 2016.

[wisun-pressie1] Beecher, P., "Wi-SUN Alliance", March 2017, <http://indiasmartgrid.org/event2017/10-03-2017/4.%20Roundtable%20on%20Communication%20and%20Cyber%20Security/1.%20Phil%20Beecher.pdf>.

[wisun-pressie2] Heile, B., "Wi-SUN Alliance Field Area Network (FAN)Overview", As presented at IETF 97, November 2016, <https://www.ietf.org/proceedings/97/slides/slides-97-lpwan-35-wi-sun-presentation-00.pdf>.

Acknowledgments

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

In addition to those in the Contributors section, thanks are due to (in alphabetical order) the following for comments:

Abdussalam Baryun
Andy Malis
Arun (arun@acklio.com)
Behcet SariKaya
Dan Garcia Carrillo
Jiazi Yi
Mirja Kuhlewind
Paul Duffy
Russ Housley
Samita Chakrabarti
Thad Guidry
Warren Kumari

Alexander Pelov and Pascal Thubert were the LPWAN WG Chairs while this document was developed.

Stephen Farrell's work on this memo was supported by Pervasive Nation, the Science Foundation Ireland's CONNECT centre national IoT network <https://connectcentre.ie/pervasive-nation/>.

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:

- Text for Section 2.1 was provided by Alper Yegin and Stephen Farrell in [LoRaWAN].
- Text for Section 2.2 was provided by Antti Ratilainen in [NB-IoT].
- Text for Section 2.3 was provided by Juan Carlos Zuniga and Benoit Ponsard in [Sigfox].
- Text for Section 2.4 was provided via personal communication from Bob Heile and was authored by Bob and Sum Chin Sean. There is no Internet-Draft for that at the time of writing.
- Text for Section 4 was provided by Ana Minabiru, Carles Gomez, Laurent Toutain, Josep Paradells, and Jon Crowcroft in [LPWAN-GAP]. Additional text from that document is also used elsewhere above.

The full list of contributors is as follows:

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
United States of America

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

Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara, CA 95050
United States of America

Email: charliep@computer.org

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 117674
Singapore

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
France

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/

Author’s Address

Stephen Farrell (editor)
Trinity College Dublin
Dublin 2
Ireland

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