Network Working Group A. Minaburo
Internet-Draft Acklio
Intended status: Informational L. Toutain
Expires: December 25, 2016 Institut MINES TELECOM ; TELECOM Bretagne
June 23, 2016

LPWAN GAP Analysis
draft-minaburo-lpwan-gap-analysis-00

Abstract

Low Power Wide Area Networks (LPWAN) are different technologies covering different applications based on long range, low bandwidth and low power operation. The use of IETF protocols in the LPWAN technologies should contribute to the deployment of a wide number of applications in an open and standard environment where actual technologies will be able to communicate. This document makes a survey of the principal characteristics of these technologies and covers a cross layer analysis on how to adapt and use the actual IETF protocols, but also the gaps for the integration of the IETF protocol stack in the LPWAN technologies.

Status of This Memo

Copyright Notice

1. Introduction

LPWAN (Low-Power Wide Area Network) technologies are a kind of constrained and challenged networks [RFC7228]. They can operate in license or license-exempt bands to provide connectivity to a vast number of battery-powered devices requiring limited communications. If the existing pilot deployments have shown the huge potential and the industrial interest in their capabilities, the loose coupling with the Internet makes the device management and network operation complex. More importantly, LPWAN devices are, as of today, with no IP capabilities. The goal is to adapt IETF defined protocols, addressing schemes and naming spaces to this constrained environment.

2. Problem Statement

The LPWANs are large-scale constrained networks in the sense of [RFC7228] with the following characteristics:

- very small frame payload as low as 12 bytes. Typical traffic patterns are composed of a large majority of frames with payload size around 15 bytes and a small minority of up to 100 byte frames. Some nodes will exchange less than 10 frames per day.
- very low bandwidth, most LPWAN technologies offer a throughput between 50 bit/s to 250 kbit/s, with a duty cycle of 0.1% to 10% on some ISM bands.
- high packet loss, which can be the result of bad transmission conditions or collisions between nodes.
- variable MTU for a link depending on the used L2 modulation.
- highly asymmetric and in some cases unidirectional links.
- ultra dense networks with thousands to tens of thousands of nodes.
- different modulations and radio channels.
- sleepy nodes to preserve energy.

In the terminology of [RFC7228], these characteristics put LP-WANs into the "challenged network" category where the IP connectivity has to be redefined or modified. Therefore, LP-WANs need to be considered as a separate class of networks. The intrinsic characteristics, current usages and architectures will allow the group to make and justify the design choices. Some of the desired properties are:

- keep compatibility with current Internet:
  * preserve the end-to-end communication principle.
  * maintain independence from L2 technology.
  * use or adapt protocols defined by IETF to this new environment that could be less responsive.
  * use existing addressing spaces and naming schemes defined by IETF.
- ensure the correspondence with the stringent LPWAN requirements, such as:
  * limited number of messages per device.
  * small message size, with potentially no L2 fragmentation.
  * RTTs potentially orders of magnitude bigger than existing constrained networks.
- optimize the protocol stack in order to limit the number of duplicated functionalities; for instance acknowledgements should not be done at several layers.

3. Identified gaps in current IETF groups concerning LPWANs

3.1. IPv6 and LPWAN

IPv6 [RFC2460] has been designed to allocate addresses to all the nodes connected to the Internet. Nevertheless the 40 bytes of overhead introduced by the protocol are incompatible with the LPWAN constraints. If IPv6 were used, several LPWAN frames will be needed just to carry the header. Another limitation comes from the MTU limit, which is 1280 bytes required from the layer 2 to carry IPv6 packet [RFC1981]. This is a side effect of the PMTU discovery mechanism, which allows intermediary routers to send to the source an ICMP message (packet too big) to reduce the size. An attacker will be able to forge this message and reduce drastically the transmission

performances. This limit allows to mitigate the impact of this attack.

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

3.2. 6LoWPAN, 6lo and LPWAN

6LoWPAN only resolves the IPv6 constraints by drastically reducing IPv6 overhead to about 4 bytes for ND traffic, but the header compression is not better for an end-to-end communications using global addresses (up to 20 bytes). 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 with no duty cycle regarding the usage of the network.

IEEE 802.15.4 is a CSMA/CA protocol which means that every unicast frame is acknowledged. Because IEEE 802.15.4 has its own reliability mechanism by retransmission, 6LoWPAN does not have reliable delivery. Some LPWAN technologies do not provide such acknowledgements at L2 and would require other reliability mechanisms.

6lo extends the usage of 6LoWPAN to other technologies (BLE, DECT, ...), with similar characteristics to IEEE 802.15.4. 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 constraint.

6LoWPAN has optimized Neighbor Discovery by reducing the message size, the periodic exchanges and removing multicast message for point-to-point exchanges with border router.

3.3. 6tisch and LPWAN

6TiSCH is complementary to LPWA technologies.

A key element of 6tisch is the use of synchronization to enable determinism. TSCH and 6TiSCH may provide a standard scheduling function. An LPWA may or may not support synchronization like the one used in 6tisch. 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.

3.4. ROLL and LPWAN

The LPWANs considered by the 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. For the moment, the work done at the ROLL WG and other routing protocols are out of scope of the LPWAN WG.

3.5. CORE and LPWAN

CoRE provides a resource-oriented application 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. 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. The actual 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 LPWA technologies. The overhead is reduced by adding a dictionary which match a URI to a small identifier and a compact mapping of the YANG model into the CBOR binary representation.

3.6. Security and LPWAN

Most of the LPWA 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, the group will adapt existing mechanisms to the LPWA 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 explains the possible security process for a LORAWAN network. The mechanisms basically are divided by: 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 it is assumed a pre-shared key between the smart object and the communication endpoint.

3.7. Mobility and LPWAN

LPWA nodes can be mobile. However, LPWAN mobility is different than 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 the mobility concerns more the gateway than the devices.

3.8. 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 registred in DNS. DNS is probably a good point of research for the LPWA technologies, while the matching of the name and the IP information can be used to configured the LPWA devices.

4. Annex A -- survey of LPWAN technologies

Different technologies can be included under the LPWAN acronym. The following list is the result of a survey among the first participant to the mailing-list. It cannot be exhaustive but is representative of the current trends.

Technology	range	Throughput	MAC MTU
LoRa	2-5 km urban <15 km suburban	0.3 to 50 kbps	256 B
SIGFOX	10 km urban 50 km rural	100 bps	12 B
IEEE802.15.4k LECIM	< 20 km LoS < 5 km NoLoS	1.5 bps to 128 kbps	16/24/ 32 B
IEEE802.15.4g SUN	2-3 km LoS	4.8 kbps to 800 kbps	2047 B
RPMA	65 km LoS 20 km NoLoS	up: 624kbps down: 156kbps mob: 2kbps	64 B
DASH-7	2 km	9 kbps 55.55 kbps 166.66 kbps	256 B
Weightless-w	5 km urban	1 kbps to 10 Mbps	min 10 B
Weightless-n	<5 km urban <30 km suburban	30 kbps to 100kbps	max 20 B
Weightless-p	> 2 km urban	up to 100kbps	
NB-IoT *	<15 km	~ 200kbps	>1000B

* supports segmentation

Figure 1: Survey of LPWAN technologies

The table Figure 1 gives some key performance parameters for some candidate technologies. The maximum MTU size must be taken carefully, for instance in LoRa, it take up to 2 sec to send a 50 Byte frame using the most robust modulation. In that case the theoretical limit of 256 B will be impossible to reach.

Most of the technologies listed in the Annex A work in the ISM band and may be used for private a public networks. Weightless-W uses white spaces in the TV spectrum and NB-LTE will use licensed channels. Some technologies include encryption at layer 2.

5. Annex B -- Security in LPWAN technologies

LORAWAN

LoRaWAN provides a joining procedure called "Over the Air Activation" that enables a smart object to securely join the network, deriving the necessary keys to perform the communications securely. The messages are integrity protected and the application information is ciphered with the derived keys from the joining procedure.

The joining procedure consists of one exchange, that entails a join-request message and a join-accept message. Upon successful authentication, the smart- object and the network-server are able to derive two keys to secure the communications (AppSKey and NwkSKey)

SIGFOX

SIGFOX provides secure communications, providing integrity of the messages and ciphered application information. No information about how the keys are distributed to the end devices.

IEEE802.15.4k and IEEE802.15.4g

There is no mention of acquiring key material to secure the communications.

DASH-7

DASH-7 defines 2 keys for specific users (root, user) and a network key. Provides network security, integrity and encryption. The process of how these keys are distributed is not explained.

RPMA

They use security algorithms and provides for mutual device authentication, message authentication and message confidentiality. No mention of how the key material is distributed.

Weightless

They offer a joining procedure to network by authenticating the smart object. Integrity of the messages, encryption and key distribution

NB-IoT

ToDo. Not Access to the specification.

6. Acknowledgements

Thanks you very much for the discussion and feedback on the LPWAN mailing list, namely, Pascal Thubert, Carles Gomez, Samita Chakrabarti, Xavier Vilajosana, Misha Dohler, Florian Meier, Timothy J. Salo, Michael Richardson, Robert Cragie, Paul Duffy, Pat Kinney, Joaquin Cabezas and Bill Gage.

We would like also to thanks the input made for the security part to Dan Garcia Carrillo et Rafael Marin Lopez

7. Normative References

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, DOI 10.17487/RFC1981, August 1996, <http://www.rfc-editor.org/info/rfc1981>.

[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>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <http://www.rfc-editor.org/info/rfc7228>.

Authors' Addresses

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

Email: ana@ackl.io

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