

6LoWPAN Working Group	E. Kim
Internet-Draft	ETRI
Intended status: Informational	D. Kaspar
Expires: January 28, 2012	Simula Research Laboratory
	N.G. Chevrollier
	TNO
	JP. Vasseur
	Cisco Systems, Inc
	July 27, 2011

Design and Application Spaces for 6LoWPANs
draft-ietf-6lowpan-usecases-10

Abstract

This document investigates potential application scenarios and use cases for low-power wireless personal area networks (LOWPANs). This document provides dimensions of design space for LOWPAN applications. A list of use cases and market domains that may benefit and motivate the work currently done in the 6LoWPAN WG is provided with the characteristics of each dimension. A complete list of practical use cases is not the goal of this document.

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 January 28, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

[Table of Contents](#)

- *1. [Introduction](#)
- *1.1. [Terminology](#)
- *1.2. [Premise of network configuration](#)
- *2. [Design Space](#)
- *3. [Application Scenarios](#)
- *3.1. [Industrial Monitoring](#)
- *3.1.1. [A Use Case and its Requirements](#)
- *3.1.2. [6LoWPAN Applicability](#)
- *3.2. [Structural Monitoring](#)
- *3.2.1. [A Use Case and its Requirements](#)
- *3.2.2. [6LoWPAN Applicability](#)
- *3.3. [Connected Home](#)
- *3.3.1. [A Use Case and its Requirements](#)
- *3.3.2. [6LoWPAN Applicability](#)
- *3.4. [Healthcare](#)
- *3.4.1. [A Use Case and its Requirements](#)
- *3.4.2. [6LoWPAN Applicability](#)
- *3.5. [Vehicle Telematics](#)
- *3.5.1. [A Use Case and its Requirements](#)

- *3.5.2. [6LoWPAN Applicability](#)
- *3.6. [Agricultural Monitoring](#)
 - *3.6.1. [A Use Case and its Requirements](#)
 - *3.6.2. [6LoWPAN Applicability](#)
- *4. [Security Considerations](#)
- *5. [IANA Considerations](#)
- *6. [Acknowledgements](#)
- *7. [References](#)
 - *7.1. [Normative References](#)
 - *7.2. [Informative References](#)
- *[Authors' Addresses](#)

[1. Introduction](#)

Low-power and lossy networks (LLNs) is the term commonly used to refer to networks made of highly constrained nodes (limited CPU, memory, power) interconnected by a variety of “lossy” links (low-power radio links or powerline communication (PLC)). They are characterized by low speed, low performance, low cost, and unstable connectivity. A LoWPAN is a particular instance of an LLN, formed by devices complying with the IEEE 802.15.4 standard [[refs.ieee802.15.4](#)]. Their typical characteristics can be summarized as follows:

As any other LLN, a LoWPAN does not necessarily comprise of sensor nodes only, but may also consist of actuators. For instance, in an agricultural environment, sensor nodes might be used to detect low soil humidity and then send commands to activate the sprinkler system. After defining common terminology in [Section 1.1](#) and describing the characteristics of LoWPANs in [Section 2](#), this document provides a list of use cases and market domains that may benefit and motivate the work currently done in the 6LoWPAN WG.

[1.1. Terminology](#)

Readers are expected to be familiar with all the terms and concepts that are discussed in "[IPv6 over Low-Power Wireless Personal Area Networks \(6LoWPANs\): Overview, Assumptions, Problem Statement, and Goals](#)" [[RFC4919](#)], and "[Transmission of IPv6 Packets over IEEE 802.15.4 Networks](#)" [[RFC4944](#)].

Readers would benefit from reading 6LoWPAN ND [[I-D.ietf-6lowpan-nd](#)], 6LoWPAN header compression [[I-D.ietf-6lowpan-hc](#)], and 6LoWPAN Routing

Requirements [\[I-D.ietf-6lowpan-routing-requirements\]](#) for the details of the 6LoWPAN work.

This document defines the following terms:

LC (Local Controller) A logical functional entity that performs the special role of coordinating and controlling its child nodes for local data aggregation, status management of local nodes, etc. There may be multiple instances of local controller nodes in a LoWPAN.

LBR (LoWPAN Border Router) A border router is located at the junction of separate LoWPAN networks or between a LoWPAN network and another IP network. There may be one or more LBRs at the LoWPAN network boundary. A LBR is the responsible authority for IPv6 Prefix propagation for the LoWPAN network it is serving. An isolated LoWPAN also contains a LBR in the network, which provides the prefix(es) for the isolated network.

[1.2. Premise of network configuration](#)

The IEEE 802.15.4 standard distinguishes between two types of nodes, reduced-function devices (RFDs) and full-function devices (FFDs). As this distinction is based on some MAC features that are not always in use, we are not using this distinction in this document.

6LoWPAN networks can be deployed using either route-over or mesh-under architectures. As the choice of route-over or mesh-under does not affect the applicability of 6LoWPAN technologies to the use cases described in the document, we will use the term "6LoWPAN network" to mean either a route-over or mesh-under network.

Communication to corresponding nodes outside of the LoWPAN is becoming increasingly important for convenient data collection and remote control purposes. The intermediate LoWPAN nodes act as packet forwarders (LM) or LoWPAN routers (LR) and connect the entire LoWPAN in a multi-hop fashion. LoWPAN Border Routers (LBRs) are used to interconnect a LoWPAN to other networks, or to form an extended LoWPAN by connecting multiple LoWPANs. Before LoWPAN nodes obtain their IPv6 addresses and the network is configured, each LoWPAN executes a link-layer configuration either by the mechanisms specified in 6lowpan ND [\[I-D.ietf-6lowpan-nd\]](#) or by using a coordinator who is responsible for link-layer short address allocation. However, the link-layer coordinator functionality is out of the scope of this document. Details of address allocation of 6LoWPAN ND is in [\[I-D.ietf-6lowpan-nd\]](#).

A LoWPAN can be configured as Mesh Under or Route Over (see Terminology in [\[I-D.ietf-6lowpan-nd\]](#)). In a Route Over configuration, multihop transmission is carried out by LRs using IP routing. In a Mesh Under configuration, the link-local scope reaches to the boundaries of the LoWPAN, and multihop transmission is achieved by forwarding data at the link layer or in an 6LoWPAN adaptation layer. More information about Mesh Under and Route Over is in 6LoWPAN ND [\[I-D.ietf-6lowpan-nd\]](#) and 6LoWPAN Routing Requirements [\[I-D.ietf-6lowpan-routing-requirements\]](#).

2. Design Space

Inspired by [\[refs.roemer\]](#), this section lists the dimensions used to describe the design space of wireless sensor networks in the context of the 6LoWPAN Working Group. The design space is already limited by the unique characteristics of a LoWPAN (e.g., low-power, short range, low-bit rate) as described in [\[RFC4919\]](#). The possible dimensions for scenario categorization used in this document are described as follows:

*Deployment: LoWPAN nodes can be scattered randomly or they may be deployed in an organized manner in a LoWPAN. The deployment can occur at once, or as an iterative process. The selected type of deployment has an impact on node density and location. This feature affects how to organize (manually or automatically) the LoWPAN and how to allocate addresses in the network.

*Network Size: The network size takes into account nodes that provide the intended network capability. The number of nodes involved in a LoWPAN could be small (10 nodes), moderate (several 100s), or large (over a 1000).

*Power Source: The power source of nodes, whether the nodes are battery-powered or mains-powered, influences the network design. The power may also be harvested from solar cells or other sources of energy. Hybrid solutions are possible where only part of the network is mains-powered.

*Connectivity: Nodes within a LoWPAN are considered "always connected" when there is a network connection between any two given nodes. However, due to external factors (e.g., extreme environment, mobility) or programmed disconnections (e.g., sleeping mode), the network connectivity can be from "intermittent" (i.e., regular disconnections) to "sporadic" (i.e., almost always disconnected network). Differences in L2 duty-cycling settings may additionally impact the connectivity due to highly varying bit-rates.

*Multi-hop communication: The multi-hop communication factor highlights the number of hops that has to be traversed to reach the edge of the network or a destination node within it. A single hop may be sufficient for simple star-topologies, but a multi-hop communication scheme is required for more elaborate topologies, such as meshes or trees. In previous work by academia and industry on LoWPANs, various routing mechanisms were introduced, such as data-centric, event-driven, address-centric, localization-based, geographical routing, etc. This document does not make use of such a fine granularity but rather uses topologies and single/multi-hop communication.

*Traffic Pattern: several traffic patterns may be used in LoWPANs. To name a few, Point-to-Multi-Point (P2MP), Multi-Point-to-Point (MP2P) and Point-to-Point (P2P).

*Security Level: LoWPANs may carry sensitive information and require high-level security support where the availability, integrity, and confidentiality of the information are crucial.

*Mobility: Inherent to the wireless characteristics of LoWPANs, nodes could move or be moved around. Mobility can be an induced factor (e.g., sensors in an automobile), hence not predictable, or a controlled characteristic (e.g., pre-planned movement in a supply chain).

*Quality of Service (QoS): QoS issues in LoWPANs may be very different from the traditional end-to-end QoS as in LoWPAN applications, one end is not a single sensor node, but often a group of sensor nodes. Parameters for QoS should consider collective data for latency, packet loss, data throughput, etc. In addition, QoS requirements can be different based on the data delivery model such as event-driven, query-driven, continuous real-time, or continuous non-real-time delivery model, which usually coexist in LoWPAN applications. QoS issues in LoWPANs are more likely related to corresponding application specific data delivery requirements within resource-constrained LoWPANs.

3. Application Scenarios

This section lists a fundamental set of LoWPAN application scenarios in terms of system design. A complete list of practical use cases is not the objective of this document.

3.1. Industrial Monitoring

LoWPAN applications for industrial monitoring can be associated with a broad range of methods to increase productivity, energy efficiency, and safety of industrial operations in engineering facilities and manufacturing plants. Many companies currently use time-consuming and expensive manual monitoring to predict failures and to schedule maintenance or replacements in order to avoid costly manufacturing downtime. LoWPANs can be inexpensively installed to provide more frequent and more reliable data. The deployment of LoWPANs can reduce equipment downtime and eliminate manual equipment monitoring that is costly to be carried out. Additionally, data analysis functionality can be placed into the network, eliminating the need for manual data transfer and analysis.

Industrial monitoring can be largely split into the following application fields:

*Process Monitoring and Control: combining advanced energy metering and sub-metering technologies with wireless sensor networking in order to optimize factory operations, reduce peak demand, ultimately lower costs for energy, avoid machine downtimes, and increase operation safety.

A plant's monitoring boundary often does not cover the entire facility but only those areas considered critical to the process. Easy to install wireless connectivity extends this line to include peripheral areas and process measurements that were previously infeasible or impractical to reach with wired connections.

*Machine Surveillance: ensuring product quality and efficient and safe equipment operation. Critical equipment parameters such as vibration, temperature, and electrical signature are analyzed for abnormalities that are suggestive of impending equipment failure (see [Section 3.2](#)).

*Supply Chain Management and Asset Tracking: with the retail industry being legally responsible for the quality of sold goods, early detection of inadequate storage conditions with respect to temperature will reduce risk and cost to remove products from the sales channel. Examples include container shipping, product identification, cargo monitoring, distribution and logistics.

*Storage Monitoring: sensor systems designed to prevent releases of regulated substances to ground water, surface water and soil. This application field may also include theft/tampering prevention systems for storage facilities or other infrastructure, such as pipelines.

3.1.1. A Use Case and its Requirements

Example: Hospital Storage Rooms

In a hospital, maintenance of the right temperature in storage rooms is very critical. Red blood cells need to be stored at 2 to 6 degrees Celsius, blood platelets at 20 to 24 C, and blood plasma below -18 C. For anti-cancer medicine, maintaining a humidity of 45% to 55% is required. Storage rooms have temperature sensors and humidity sensors every 25m to 100m, based on the floor plan and the location of shelves, as indoor obstacles distort the radio signals. At each blood pack a sensor tag can be installed to track the temperature during delivery. A LoWPAN node is installed in each container of a set of blood packs. In this case, highly dense networks must be managed.

All nodes are statically deployed and manually configured with either a single- or multi-hop connection. Different types of LoWPAN nodes are configured based on the service and network requirements. Especially, LCs play a role in aggregation of the sensed data from blood packs. In the extended networks, more than one LoWPAN LCs can be installed in a storage room. In the case that the sensed data from an individual node is urgent event-driven data such as outrange of temperature or humidity, it will not be accumulated (and further delayed) by the LCs but immediately relayed.

All LoWPAN nodes do not move unless the blood packs or a container of blood packs is moved. Moving nodes get connected by logical attachment to a new LoWPAN. When containers of blood packs are transferred to another place of the hospital or by ambulance, the LoWPAN nodes on the containers associate to a new LoWPAN.

This type of application works based on both periodic and event-driven notifications. Periodic data is used for monitoring the temperature and humidity in the storage rooms. The data over or under a pre-defined threshold is meaningful to report. Blood cannot be used if it is exposed to the wrong environment for about 30 minutes. Thus, event-driven data sensed on abnormal occurrences is time-critical and requires secure and reliable transmission.

LoWPANs must be provided with low installation and management costs, and for the transportation of blood containers, precise location tracking of containers is important. The hospital network manager or staff can be provided with an early warning of possible chain ruptures, for example by conveniently accessing comprehensive online reports and data management systems.

Dominant parameters in industrial monitoring scenarios:

- *Deployment: pre-planned, manually attached

- *Mobility: no (except for asset tracking)

- *Network Size: medium to large size, high node density

- *Power Source: most of the time battery-operated

- *Security Level: business-critical. Secure transmission must be guaranteed.

- *Multi-hop communication: multi-hop networking

- *Connectivity: always on for crucial processes

- *QoS: important for time-critical event-driven data

- *Traffic Pattern: P2P (actuator control), MP2P (data collection)

- *Other Issues: Sensor network management, location tracking, real-time early warning

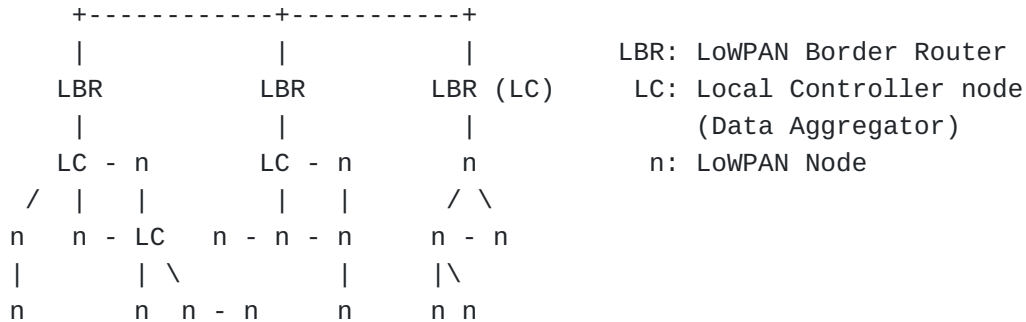
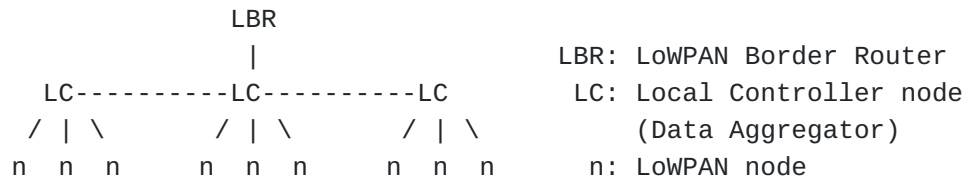
3.1.2. 6LoWPAN Applicability

The network configuration of the above use case can differ substantially by system design. As illustrated in [Figure 1](#), the simplest way is to build a star topology inside of each storage room. Based on the layout and size of the storage room, the LoWPAN can be configured in a different way of mesh topology as shown in [Figure 2](#). Each LoWPAN node may reach the LBR by a predefined routing/forwarding mechanism. Each LoWPAN node configures its link-local address and obtains a prefix from its LBR by an 6LoWPAN ND procedure [[I-D.ietf-6lowpan-nd](#)]. LoWPAN nodes need to build a multi-hop connection to reach the LCs and LBR.

Secure data transmission and authentication is crucial in a hospital scenario to prevent personal information to be retrieved by an adversary. Confidential data must be encrypted not only in transmission, but also when stored on nodes, because nodes can potentially be stolen.

The data volume is usually not so large in this case, but is sensitive to delay. Data aggregators can be installed for each storage room, or just one data aggregator can collect all data. To make a light transmission, UDP is likely to be chosen, but secure transmission and security mechanism must be added. To increase security, link-layer mechanisms and/or additional security mechanisms should be used. Because a failure of a LoWPAN node can critically affect the storage of the blood packs, network management is important in this use-case. A light-weight management mechanism must be provided for the management. The service quality of this case is highly related to effective handling of event-driven data which is delay intolerant and mission critical. The event of wrong humidity and temperature needs to be detected as quickly and reliable as possible. It is important to provide efficient resource usage for such data with consideration of minimal usage of energy. Energy aware QoS support in wireless sensor networks is a challenging issue [[refs.chen](#)]. It can be considered to provide appropriate data aggregation for minimizing the delay, maximizing the accuracy of the delivery by using power-affluent nodes, or aided by middleware or other types of network elements.

When a container is moved out from the storage room, and connected to the other hospital system (if the hospital buildings are fully or partly covered with LoWPANs), a mechanism to rebind to a new parent node and a new LoWPAN must be supported. In the case that it is moved by an ambulance, it will be connected to an LBR in the vehicle. This type of mobility is supported by 6LoWPAN ND and routing mechanism. LoWPANs must be provided with low installation and management costs, providing benefits such as reduced inventory, and precise location tracking of containers, and mobile equipment (moving beds at the hospital or ambulances).



3.2. Structural Monitoring

Intelligent monitoring in facility management can make safety checks and periodic monitoring of the architecture status highly efficient. Mains-powered nodes can be included in the design phase of a construction or battery-equipped nodes can be added afterwards. All nodes are static and manually deployed. Some data is not critical for security protection (such as periodic or query-driven notification of normal room temperature), but event-driven emergency data (such as a fire alarm) must be handled in a very critical manner.

3.2.1. A Use Case and its Requirements

Example: Bridge Safety Monitoring

A 1000m long concrete bridge with 10 pillars is described. Each pillar and the bridge body contain 5 sensors to measure the water level, and 5 vibration sensors are used to monitor its structural health. The LoWPAN nodes are deployed to have 100m line-of-sight distance from each other. All nodes are placed statically and manually configured with a single-hop connection to the local coordinator. All LoWPAN nodes are immobile while the service is provided. Except from the pillars, there are no special obstacles of attenuation to the node signals, but careful configuration is needed to prevent signal interference between LoWPAN nodes.

The physical network topology is changed in case of node failure. On the top part of each pillar, a sink node is placed to collect the sensed data. The sink nodes of each pillar become data gathering point of the LoWPAN hosts at the pillar and act as local coordinators. This use case can be extended to medium or large size sensor networks to monitor a building or for instance the safety status of highways and tunnels. Larger networks of the same kind still have similar

characteristics such as static node placement, manual deployment and dependent on the blue print of the structure, mesh topologies will be built with mains-powered relay points. Periodic, query-driven, and event-driven real-time data gathering is performed and the emergency event-driven data must be delivered without delay.

Dominant parameters in structural monitoring applications:

- *Deployment: static, organized, pre-planned
- *Mobility: none
- *Network Size: small (dozens of nodes) to large
- *Power Source: mains-powered nodes are mixed with battery powered (mains-power nodes will be used for local coordination or relays).
- *Security Level: safety-critical. Secure transmission must be guaranteed. Only authenticated users must be able to access and handle the data.
- *Multi-hop communication: multi-hop mesh networking is recommended to be supported.
- *Connectivity: always connected or intermittent by sleeping mode scheduling.
- *QoS: Emergency notification (fire, over-threshold vibrations, water level, etc.) is required to have priority of delivery and must be transmitted in a highly reliable manner.
- *Traffic Pattern: MP2P (data collection), P2P (localized querying)
- *Other Issues: accurate sensing and reliable transmission are important. In addition, sensor status reports should be maintained in a reliable monitoring system.

3.2.2. 6LoWPAN Applicability

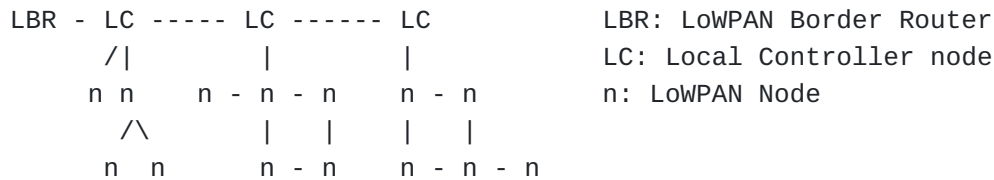
The network configuration of this use case can be done by simple topologies, however, there are many extended use cases for more complex structures. The example bridge monitoring case may be the simplest case (an example topology is illustrated in [Figure 3](#)).

The LoWPAN Nodes are installed on the place after manual optimization of their location. As the communication of the leaf LoWPAN nodes may be limited to the data gathering points, both 16-bit and 64-bit can be used for IPv6 link-local addresses [[RFC4944](#)].

Each pillar might have one LC for data collection from each pillar. Communication schedules should be set up between leaf nodes and their LC to efficiently gather the different types of sensed data. Each data

packet may include meta-information about its data, or the type of sensors could be encoded in its address during the address allocation. This type of application works based on periodic, query-driven and event-driven notifications. The data over or under a pre-defined threshold is meaningful to report. Event-driven data sensed on abnormal occurrences is time-critical and requires secure and reliable transmission. Conflictly, for energy conservation, all nodes may have periodic and long sleep modes but wake up on certain events. To ensure the reliability of such emergency event-driven data, such data is immediately relayed to a power-affluent or mains-power node which usually takes a LoWPAN router role, and does not go into a long sleep status. The data gathering entity can be programmed to trigger actuators installed in the infrastructure, when a certain threshold value has been reached.

Due to the safety-critical data of the structure, authentication and security are important issues here. Only authenticated users must be allowed to access the data. Additional security should be provided at the LBR for restricting the access from outside of the LoWPAN. The LBR may take charge of authentication of LoWPAN nodes. Reliable and secure data transmission must be guaranteed.



3.3. Connected Home

The "Connected" Home or "Smart" home is with no doubt an area where LoWPANs can be used to support an increasing number of services:

- *Home safety/security
- *Home Automation and Control
- *Healthcare (see above section)
- *Smart appliances and home entertainment systems

In home environments LoWPAN networks typically comprise a few dozen and probably in the near future a few hundreds of nodes of various nature: sensors, actuators and connected objects.

3.3.1. A Use Case and its Requirements

Example: Home Automation

The home automation and control system LoWPAN offers a wide range of services: local or remote access from the Internet (via a secured edge router) to monitor the home (temperature, humidity, activation of remote video surveillance, status of the doors (locked or open), etc.) but also for home control (activate the air conditioning/heating, door locks, sprinkler systems, etc.). Fairly sophisticated systems can also optimize the level of energy consumption thanks to a wide range of input from various sensors connected to the LoWPAN: light sensors, presence detection, temperature, etc. in order to control electric window shades, chillers, air flow control, air conditioning and heating with the objective to optimize energy consumption.

With the emergence of "Smart Grid" applications, the LoWPAN may also have direct interactions with the Grid itself via the Internet to report the amount of KWatts that could be load shed (Home to Grid) and to receive dynamic load shedding information if/when required (Grid to home): this application is also referred to as Demand-Response application. Another service known as Demand Side Management (DSM) could be provided by utilities to monitor and report to the user its energy consumption with a fine granularity (on a per device basis). Other inputs such as dynamic pricing can also be received by the user from the utility that can then turn on and off some appliances according to its local policy in order to reduce its energy bill. In terms of home safety and security, the LoWPAN is made of motion- and audio-sensors, sensors at doors and windows, and video cameras to which additional sensors can be added for safety (gas, water, CO, Radon, smoke detection). The LoWPAN typically comprises a few dozen nodes forming an ad-hoc network with multi-hop routing since the nodes may not be in direct range. It is worth mentioning that the number of devices tends to grow considering the number of new applications for the home. In its most simple form, all nodes are static and communicate with a central control module but more sophisticated scenarios may also involve inter-device communication. For example, a motion/presence sensor may send a multicast message to a group of lights to be switched on, or a video camera will be activated sending a video stream to a gateway that can be received on a cell phone.

Ergonomics in Connected Homes is a key and the LoWPAN must be self-managed and easy to install. Traffic patterns may greatly vary depending on the applicability and so does the level of reliability and QoS expected from the LoWPAN. Humidity sensing is typically not critical and requires no immediate action whereas tele-assistance or gas leak detection is critical and requires a high degree of reliability. Furthermore, although some actions may not involve critical data, still the response time and network delays must be on the order of a few hundreds of milliseconds to preserve the user experience (e.g. use a remote control to switch a light on). A minority of nodes are mobile (with slow motion). With the emergence of energy related applications it becomes crucial to preserve data confidentiality. Connected Home LoWPAN usually do not require multi-topology or QoS routing. Fairly simple QoS mechanisms are enough for

handling emergency data. It can be programmed to alarm by actuators or to operate sprinklers.

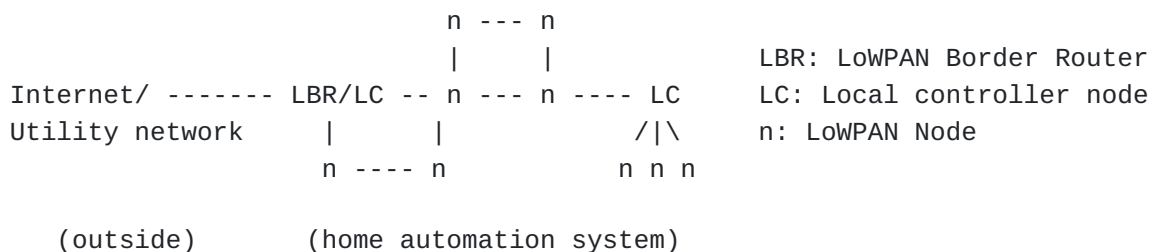
Dominant parameters for home automation applications:

- *Deployment: multi-hop topologies
- *Mobility: some degree of mobility
- *Network Size: medium number of nodes, potentially high density
- *Power Source: mix of battery and mains-powered devices
- *Security Level: authentication and encryption required
- *Multi-hop communication: no requirement for multi-topology or QoS routing
- *Connectivity: intermittent (usage-dependent sleep modes)
- *QoS: support of limited QoS for emergency data (alarm)
- *Traffic Pattern: P2P (inter-device), P2MP and MP2P (polling)

3.3.2. 6LoWPAN Applicability

In the home automation use case, the network topology is made of a mix of a battery operated and mains-powered nodes that both communicate with each other and a LBR provides connectivity to the outside of world for control management ([Figure 4](#)).

In home network, installation and management must be extremely simple for the user. Link local IPv6 addresses can be used by nodes with no external communication and the LBR allocates routable addresses to communicate with other LoWPAN nodes not reachable over a single radio transmission.



In some scenarios, the traffic will be sent to a LC for processing that may in turn decide of local actions (switch a light on, ...). In other scenarios, all devices will send their data to the LCs that may also act as the LBR for data processing and potential relay of data to outside of the LoWPAN. It does not mean that every device gets through

the LC and LBR for communicating each other. For the sake of illustration, some of the data may be processed to trigger local action (e.g. switch off an appliance), simply store and sent once enough data has been accumulated (e.g. energy consumption for the past 6 hours for a set of appliances) or could trigger an alarm immediately sent to a datacenter (e.g. gas leak detection).

Although in the majority of cases nodes within the LoWPAN will be in direct range, some nodes will reach the LBR/LC with a 2-3 hops path (with the emergence of several low-power media such as low-power PLC) in which case LoWPAN routers will be deployed in the home to interconnect the various IPv6 links.

The home LoWPAN must be able to provide extremely reliable communication in support of some specific application (e.g. fire, gas leak detection, health monitoring) whereas other application may not be critical (e.g humidity monitoring). Such emergency data has the same QoS issues with the event-driven data in the other applications, and can be delivered by pre-defined paths through mains-powered node without being stored in intermediate nodes such as LCs. Similarly some information may require the use of security mechanisms for authentication, confidentiality.

3.4. Healthcare

LoWPANs are envisioned to be heavily used in healthcare environments. They have a big potential to ease the deployment of new services by getting rid of cumbersome wires and simplify patient care in hospitals and for home care. In healthcare environments, delayed or lost information may be a matter of life or death.

Various systems, ranging from simple wearable remote controls for tele-assistance or intermediate systems with wearable sensor nodes monitoring various metrics to more complex systems for studying life dynamics, can be supported by LoWPANs. In the latter category, a large amount of data from various LoWPAN nodes can be collected: movement pattern observation, checks that medicaments have been taken, object tracking, and more. An example of such a deployment is described in [\[refs.hartog\]](#) using the concept of Personal Networks.

3.4.1. A Use Case and its Requirements

Example: healthcare at home by tele-assistance

A senior citizen who lives alone wears one to few wearable LoWPAN nodes to measure heartbeat, pulse rate, etc. Dozens of LoWPAN nodes are densely installed at home for movement detection. A LBR at home will send the sensed information to a connected healthcare center. Portable base stations with LCDs may be used to check the data at home, as well. The different roles of devices have different duty-cycles, which affect node management.

Multipath interference may often occur due to the mobility of the patients at home, where there are many walls and obstacles. Even during

sleeping, the change of the body position may affect the radio propagation.

Data is gathered both periodically and event-driven. In this application, event-driven data can be very time-critical. Thus, real-time and reliable transmission must be guaranteed.

Privacy also becomes a serious issue in this case, as the sensed data is very personal. A small set of secret keys can be shared within the sensor nodes during bootstrapping procedures in order to build a secure link without using much of memory and energy. In addition, different data will be provided to the hospital system from what is given to a patient's family members. Role-based access control is needed to support such services, thus support of authorization and authentication is important.

Dominant parameters in healthcare applications:

- *Deployment: pre-planned

- *Mobility: moderate (patient's mobility)

- *Network Size: small, high node density

- *Power Source: hybrid

- *Security Level: Data privacy and security must be provided. Encryption is required. Role based access control is required to be supported by light weight authentication mechanism

- *Multi-hop communication: multi-hop for homecare devices, star topology on patients body. Multipath interference due to walls and obstacles at home must be considered.

- *Connectivity: always on

- *QoS: high level of reliability support (life and death implication), role-based

- *Traffic Pattern: MP2P/P2MP (data collection), P2P (local diagnostic)

- *Other issues: Plug-and-play configuration is required for mainly non-technical end-users. Real-time data acquisition and analysis are important. Efficient data management is needed for various devices which have different duty-cycles, and for role-based data control. Reliability and robustness of the network are also essential.

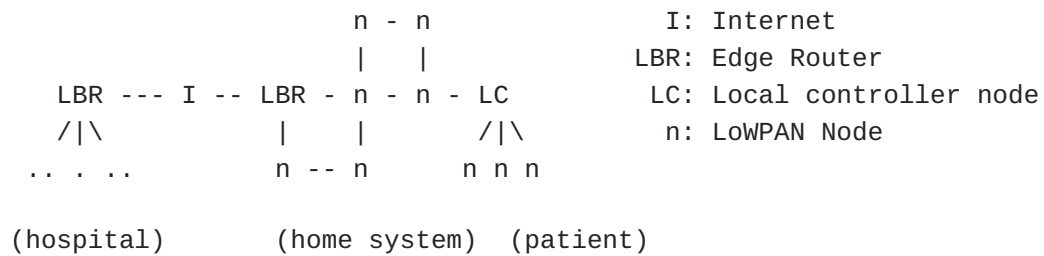
3.4.2. 6LoWPAN Applicability

In this use case, the local network size is rather small (less than 10s of nodes). The home care system is statically configured with multi-hop

paths and the patient's body network can be built as a star topology. The LBR at home is the sink node in the routing path from sources on the patient's body. A plug-and-play configuration is required. As the communication of the system is limited to a home environment, both 16-bit and 64-bit can be used for IPv6 link-local addresses [RFC4944]. An example topology is provided in Figure 5.

The patient's body network can be simply configured as a star topology with a LC dealing with data aggregation and dynamic network attachment when the patient moves around at home. As multipath interference may often occur due to the patients' mobility at home, the deployment of LoWPAN nodes and transmission paths should be well considered. At home, some nodes can be installed with power-affluence status, and those LoWPAN nodes can be used for relaying points or data aggregation points.

The sensed information must be maintained with the identification of the patient no matter if the patient visits the connected hospital or stays at home. If the patient's LoWPAN uses globally unique IPv6 address, the address can be used for the identification. However, it causes cost for privacy and security. The hospital LoWPAN where the patient's information is transferring needs to operate additional identification system together with strong authority and authentication mechanism. The connection between the LBR at home and the LBR at Hospital must be reliable and secure, as the data is privacy-critical. To achieve this, additional policy for security is recommended between the two LoWPAN.



3.5. Vehicle Telematics

LoWPANs play an important role in intelligent transportation systems. Incorporated in roads, vehicles, and traffic signals, they contribute to the improvement of safety of transporting systems. Through traffic or air-quality monitoring, they increase the possibilities in terms of traffic flow optimization and help reducing road congestion.

3.5.1. A Use Case and its Requirements

Example: Telematics

As shown in Figure 6, LoWPAN Nodes are included in roads during their construction for motion monitoring. When a car passes over these nodes,

the possibility is then given to track the trajectory and velocity of cars for safety purposes.

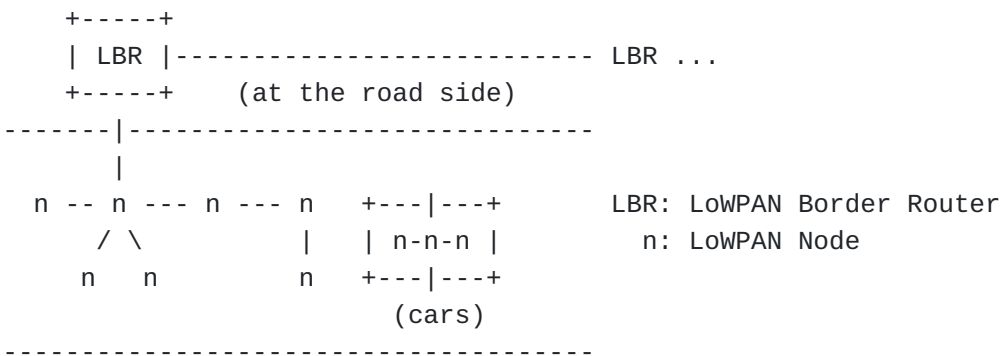
The lifetime of the LoWPAN Nodes incorporated into roads is expected to be as long as the life time of the roads (about 10 years). Multi-hop communication is possible between LoWPAN Nodes, and the network should be able to cope with the deterioration over time of the node density due to power fails. Sink nodes placed at the side of road are most likely mains-powered, LoWPAN Nodes in the roads run on battery. Power saving schemes might intermittently disconnect the nodes. A rough estimate of 4 nodes per square meter is needed. Other applications may involve car-to-car communication for increased road safety.

Dominant parameters in vehicle telematics applications:

- *Deployment: pre-planned (road, vehicle)
- *Mobility: none (road infrastructure), high (vehicle)
- *Network Size: large (road infrastructure), small (vehicle)
- *Power Source: hybrid
- *Security Level: handling physical damage and link failure
- *Multi-hop communication: multi-hop, especially ad-hoc
- *Connectivity: intermittent
- *Traffic Pattern: mostly Multi-Point-to-Point (MP2P), Point-to-Multi-Point (P2MP)

3.5.2. 6LoWPAN Applicability

For this use case, the network topology includes fixed LBRs that are mains-powered and have a connection to high speed networks (e.g., Internet) in order to reach the transportation control center ([Figure 6](#)). These LBRs may be logically combined with LC as a data sink to gather sensed data from a number of LoWPAN Nodes inserted in the tarmac of the road. In the road infrastructure, a LoWPAN with one LBR forms a fixed network and the LoWPAN nodes are installed by manual optimization of their location.



Given the fact that nodes are incorporated in the road, tampering with sensors is difficult for an adversary. However, the application must be robust against possible attacks and node failures. Sensed data should thus be used primarily for monitoring purposes, not to instruct (and potentially mislead) traffic participants.

3.6. Agricultural Monitoring

Accurate temporal and spatial monitoring can significantly increase agricultural productivity. Due to natural limitations, such as a farmers' inability to check the crop at all times of day or inadequate measurement tools, luck often plays a too large role in the success of harvests. Using a network of strategically placed sensors, indicators such as temperature, humidity, and soil condition can be automatically monitored without labor intensive field measurements. For example, sensor networks could provide precise information about crops in real time, enabling businesses to reduce water, energy, and pesticide usage and enhancing environment protection. The sensing data can be used to find optimal environments for the plants. In addition, the data on the planting condition can be saved by sensor tags, which can be used in supply chain management.

3.6.1. A Use Case and its Requirements

Example: Automated Vineyard

In a vineyard with medium to large geographical size, a number of 50 to 100 LC nodes are manually deployed in order to provide full signal coverage over the study area. An additional number of 100 to 1000 leaf nodes with (possibly heterogeneous) specialized sensors (i.e., humidity, temperature, soil condition, sunlight) are attached to the LCs in local wireless star topologies, periodically reporting measurements to the associated LCs. For example, in a 20-acre vineyard with 8 parcels of land, 10 LowPAN Nodes are placed within each parcel to provide readings on temperature and soil moisture. The LowPAN Nodes are able to support a multi-hop forwarding/routing scheme to enable data transmission to a sink node at the edge of the vineyard. Each of the 8 parcels contains one data aggregator to collect the sensed data.

Localization is important for this type of LoWPAN where installed in a geographically large area, for pinning down where an event occurred, and for combining gathered data with their actual position. Using manual deployment, device addresses can be used for identifying the position and localization. For randomly deployed nodes, a localization algorithm needs to be applied.

There might be various types of sensor devices deployed in a single LoWPAN, each providing raw data with different semantics. Thus, an additional method is required to correctly interpret sensor readings. Each data packet may include meta-information about its data, or a type of a sensor could be encoded in its address during address allocation. Dominant parameters in agricultural monitoring:

*Deployment: pre-planned

The nodes are installed outdoors or in a greenhouse with high exposure to water, soil, dust, in dynamic environments of moving people and machinery, with growing crop and foliage. LoWPAN nodes can be deployed in a pre-defined manner, considering the harsh environment.

*Mobility: all static

*Network Size: medium to large, low to medium density

*Power Source: all nodes are battery-powered except the sink, or energy harvesting

*Security Level: depending on business-purpose. Light-weight security or a simple shared key management can be used depending on the business purpose.

*Multi-hop communication: mesh topology with local star connections.

*Connectivity: intermittent (many sleeping nodes)

*Traffic Pattern: Mainly MP2P/P2MP. P2P actuator triggering.

*Other issues: Time synchronization among sensors are required, but the traffic interval may not be frequent (e.g. once in 30 minutes to 1 hour).

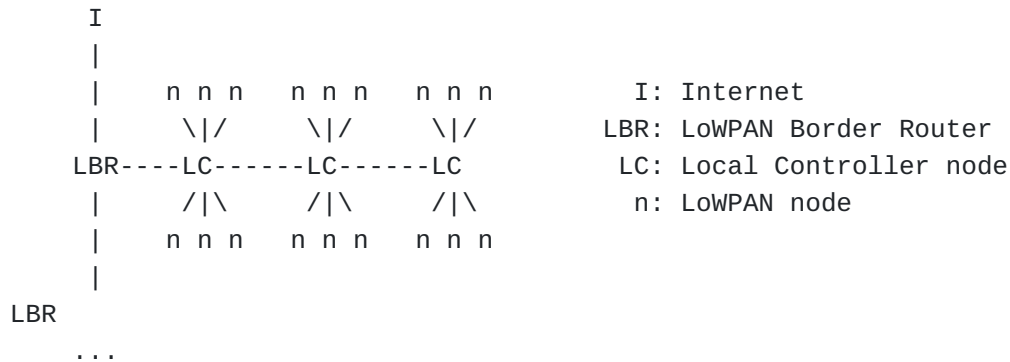
3.6.2. 6LoWPAN Applicability

The network configuration in this use case might, in the most simple case, look like illustrated in [Figure 7](#). This static scenario consists of one or more fixed LBR that are mains-powered and have a high-bandwidth connection to a backbone link, which might be placed in a control center, or connect to the Internet. The LBRs are strategically

located at the border of vineyard parcels, acting as data sinks. A number of LCs are placed along a row of plants with individual LoWPAN nodes spread around them.

While the LBRs implement the IPv6 Neighbor Discovery protocol (RFC 4861 [\[RFC4861\]](#)) to connect the outside of the LoWPAN, the LoWPAN Nodes operate a more energy-considering ND described in [\[I-D.ietf-6lowpan-nd\]](#), which includes basic bootstrapping and address assignment. Each LBR can have predefined forward management information to a central data aggregation point, if necessary.

LoWPAN nodes may send event-driven notifications when readings exceed certain thresholds, such as low soil humidity; which may automatically trigger a water sprinkler in the local environment. For increased energy efficiency, all LoWPAN Nodes are in periodic sleep state. However, the LCs need to be aware of sudden events from the leaf nodes. Their sleep periods should therefore be set to shorter intervals. Communication schedules must be set up between master and leaf nodes, and time synchronization is needed to account for clock drift. Also, the result of data collection may activate actuators. Context-awareness, node identification and data collection on the application level are necessary.



4. Security Considerations

Relevant security considerations are listed by application scenario in [Section 3](#) and the security considerations in RFC 4919 [\[RFC4919\]](#) and RFC 4944 [\[RFC4944\]](#) apply as well.

The physical exposure of LoWPAN nodes (especially in outdoor networks) allows an adversary to capture, clone, tamper with, or even destroy these devices. Given the safety issues involved in some use cases, these threats place high demands for resiliency and survivability upon the LoWPAN. The generally wireless channels of LoWPANs are susceptible to several security threats. Without proper security measures, confidential information might be snooped by a "man in the middle". An attacker might also modify or introduce data packets into the network, for example to manipulate sensor readings or to take control over sensors and actuators. This specification expects that the link layer is sufficiently protected, either by means of physical or IP security for the backbone link or with MAC sublayer cryptography. However, link-

layer encryption and authentication may not be sufficient to provide confidentiality, authentication, integrity, and freshness to both data and signaling packets.

Due to their low-power nature, LoWPANs are especially vulnerable to denial-of-service (DoS) type attacks. Example DoS attacks include attempts to drain a node's battery by excessive querying or to introduce a high-power jamming signal that makes LoWPAN nodes dysfunctional. Security solutions must therefore be lightweight and support node authentication, so that message integrity can be guaranteed and misbehaving nodes can be denied participation in the network. A node must authenticate itself to trusted nodes before taking part in the LoWPAN.

While IPsec is mandatory with IPv6 [\[RFC4944\]](#), considering the power constraints and limited processing capabilities of IEEE802.15.4 devices, IPsec is computationally expensive; Internet key exchange (IKEv2) messaging described in [\[RFC5996\]](#) is not suited for LoWPANs as the amount of signaling in these networks should be minimized. Thus, LoWPANs may need to define their own keying management method that requires minimum overhead in terms of packet size and message exchange [\[refs.dutertre\]](#). IPsec provides authentication and confidentiality between end nodes and across multiple LoWPAN links, and may be useful only when two nodes want to apply security to all exchanged messages. However, in many cases, the security may be requested at the application layer as needed, while other messages can flow in the network without security overhead.

Security requirements may differ by use case. For example, industrial and structural monitoring applications are safety-critical and secure transmission must be guaranteed, so that only authenticated users are able to access and handle the data. In health care systems, data privacy is an important issue. Encryption is required, and role-based access control is needed for proper authentication. In home automation scenarios, critical applications such as door locks, require a high security and robustness against intrusion. On the other hand, a remote controlled light switch has no critical security threats.

[5. IANA Considerations](#)

This document contains no actions for IANA.

[6. Acknowledgements](#)

Thanks for David Cypher for giving more insight on the IEEE 802.15.4 standard, and Irene Fernandez, Shoichi Sakane and Paul Chilton for review and valuable comments.

7. References

7.1. Normative References

[1]	Kent, S. and K. Seo, " Security Architecture for the Internet Protocol ", RFC 4301, December 2005.
[2]	Narten, T., Nordmark, E., Simpson, W. and H. Soliman, " Neighbor Discovery for IP version 6 (IPv6) ", RFC 4861, September 2007.
[3]	Kushalnagar, N., Montenegro, G. and C. Schumacher, " IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals ", RFC 4919, August 2007.
[4]	Montenegro, G., Kushalnagar, N., Hui, J. and D. Culler, " Transmission of IPv6 Packets over IEEE 802.15.4 Networks ", RFC 4944, September 2007.
[5]	Kaufman, C., Hoffman, P., Nir, Y. and P. Eronen, " Internet Key Exchange Protocol Version 2 (IKEv2) ", RFC 5996, September 2010.
[6]	IEEE Computer Society, "IEEE Std. 802.15.4-2006 (as amended)", 2007.

7.2. Informative References

[1]	Shelby, Z, Chakrabarti, S and E Nordmark, " Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN) ", Internet-Draft draft-ietf-6lowpan-nd-17, June 2011.
[2]	Hui, J and P Thubert, " Compression Format for IPv6 Datagrams in Low Power and Lossy Networks (6LoWPAN) ", Internet-Draft draft-ietf-6lowpan-hc-15, February 2011.
[3]	Kim, E, Kaspar, D, Gomez, C and C Bormann, " Problem Statement and Requirements for 6LoWPAN Routing ", Internet-Draft draft-ietf-6lowpan-routing-requirements-09, February 2011.
[4]	Roemer, K. and F. Mattern, "The Design Space of Wireless Sensor Networks", December 2004.
[5]	den Hartog, F., Schmidt, J. and A. de Vries, "On the Potential of Personal Networks for Hospitals", May 2006.
[6]	Dutertre, B., Cheung, S. and J. Levy, "Lightweight key management in wireless sensor networks by leveraging initial trust", April 2004.
[7]	Chen, D. and P. K. Varshney, "QoS Support in Wireless Sensor Networks: A survey", June 2004.

Authors' Addresses

Eunsook Kim Kim ETRI 161 Gajeong-dong Yuseong-gu Daejeon, 305-700
Korea Phone: +82-42-860-6124 EMail: eunah.ietf@gmail.com

Dominik Kaspar Kaspar Simula Research Laboratory Martin Linges v 17
Snaroya, 1367 Norway Phone: +47-4748-9307 EMail:
dokaspar.ietf@gmail.com

Nicolas G. Chevrollier Chevrollier TNO
Brassersplein 2 P.O. Box 5050 Delft, 2600 The Netherlands Phone:
+31-15-285-7354 EMail: nicolas.chevrollier@tno.nl

JP Vasseur Vasseur Cisco Systems, Inc 1414 Massachusetts Avenue
Boxborough, MA 01719 USA EMail: jpv@cisco.com