Internet Engineering Task Force (IETF)
Request for Comments: 6568
Category: Informational
ISSN: 2070-1721

E. Kim
ETRI
D. Kaspar
Simula Research Laboratory
JP. Vasseur
Cisco Systems, Inc.

April 2012

Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

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 Working Group 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 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 a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6568.

Table of Contents

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 Power-Line 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 [5]. Their typical characteristics can be summarized as follows:

- Limited Processing Capability: The smallest common LoWPAN nodes have 8-bit processors with clock rates around 10 MHz. Other models exist with 16-bit and 32-bit cores (typically ARM7), running at frequencies on the order of tens of MHz.

- Small Memory Capacity: The smallest common LoWPAN nodes have a few kilobytes of RAM with a few dozen kilobytes of ROM/flash memory. While memory sizes of nodes continue to grow (e.g., IMote has 64 KB SRAM, 512 KB Flash memory), the nature of small memory capacity for LoWPAN nodes remains a challenge.

- Low Power: Wireless radios for LoWPANs are normally battery-operated. Their radio frequency (RF) transceivers often have a current draw of about 10 to 30 mA, depending on the used transmission power level. In order to reach common indoor ranges of up to 30 meters and outdoor ranges of 100 meters, the used transmission power is set around 0 to 3 dBm. Depending on the processor type, there is an additional battery current consumption of the CPU itself, commonly on the order of tens of milliamperes. However, the CPU power consumption can often be reduced by a thousandfold when switching to sleep mode.

- Short Range: The Personal Operating Space (POS) defined by IEEE 802.15.4 implies a range of 10 meters. For real implementations, the range of LoWPAN radios is typically measured in tens of meters, but can reach over 100 meters in line-of-sight situations.

- Low Bit Rate: The IEEE 802.15.4 standard defines a maximum over-the-air rate of 250 kbit/s, which is most commonly used in current deployments. Alternatively, three lower data rates of 20, 40, and 100 kbit/s are defined.

As with any other LLN, a LoWPAN is not necessarily comprised 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 Working Group.

1.1. Terminology

Readers are expected to be familiar with all terms and concepts discussed in "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [2], and "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [3].

Readers would benefit from reading 6LoWPAN Neighbor Discovery (ND) [6], 6LoWPAN header compression [7], and 6LoWPAN routing requirements [8] for details of 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 located at the junction of separate LoWPANs or between a LoWPAN and another IP network. There may be one or more LBRs at the LoWPAN boundary. An LBR is the responsible authority for IPv6 Prefix propagation for the LoWPAN it serves. An isolated LoWPAN also contains an LBR in the network; the LBR 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 Medium Access Control (MAC) features that are not always in use, we are not using this distinction in this document.

6LoWPANs 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" 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 on the link layer or as LoWPAN routers, and connect the entire LoWPAN in a multi-hop fashion. 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 [6] or by using a coordinator that 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 in 6LoWPAN ND are in [6].

A LoWPAN can be configured as mesh-under or route-over (see Terminology in [6]). In a route-over configuration, multi-hop transmission is carried out by LoWPAN routers using IP routing. In a mesh-under configuration, the link-local scope reaches to the boundaries of the LoWPAN, and multi-hop transmission is achieved by forwarding data at the link layer or in a 6LoWPAN adaptation layer. More information about mesh-under and route-over is in [6] and [8].

2. Design Space

Inspired by [9], 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 [2]. 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 (ten), moderate (several hundred), or large (over a thousand).

- 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), network connectivity can be from "intermittent" (i.e., regular disconnections) to "sporadic" (i.e., almost always disconnected). Differences in L2 duty-cycling settings may additionally impact connectivity due to highly varying bit rates.

- Multi-Hop Communication: The multi-hop communication factor highlights the number of hops that have 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 on LoWPANs by academia and industry, 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 -- Point-to-Multipoint (P2MP), Multipoint-to-Point (MP2P), and Point-to-Point (P2P), to name a few.

- 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) -- and 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; these delivery models 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 perform. 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: This application field combines 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. Wireless connectivity that is easy to install extends this line to include peripheral areas and process measurements that were previously infeasible or impractical to reach with wired connections.

- Machine Surveillance: This application field ensures 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.

- 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 the risk and cost of removing products from the sales channel. Examples include container shipping, product identification, cargo monitoring, distribution, and logistics.

- Storage Monitoring: This application field includes sensor systems designed to prevent releases of regulated substances into 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 degrees C, and blood plasma below -18 degrees C. For anti-cancer medicine, maintaining a humidity of 45% to 55% is required. Storage rooms have temperature sensors and humidity sensors every 25 to 100 m, 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. In particular, LCs play a role in aggregation of the sensed data from blood packs. In the extended networks, more than one LoWPAN LC 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 in 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 temperature and humidity in the storage rooms. The data over or under a predefined 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.
- Network Size: Medium to large size, high node density.
- Power Source: Battery-operated most of the time.
- Connectivity: Always on for crucial processes.
- Multi-Hop Communication: Multi-hop networking.
- Traffic Pattern: P2P (actuator control), MP2P (data collection).
- Security Level: Business-critical. Secure transmission must be guaranteed.
- Mobility: None (except for asset tracking).
- QoS: Important for time-critical event-driven data.
- 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 -- 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 a 6LoWPAN ND procedure [6]. LoWPAN nodes need to build a multi-hop connection to reach the LCs and LBR.

Secure data transmission and authentication are crucial in a hospital scenario, to prevent personal information from being 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 a 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 lightweight management mechanism must be provided for this management.

The service quality of this case is highly related to effective handling of event-driven data that is delay intolerant and mission critical. Wrong humidity and wrong temperature are events that need to be detected as quickly and reliably 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 [12]. It can be considered to provide appropriate data aggregation for minimizing delay and maximizing accuracy of delivery by using power-affluent nodes, or can be aided by middleware or other types of network elements.

When a container is moved out of the storage room and connected to another 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 the 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 (e.g., beds moved in the hospital, ambulances).

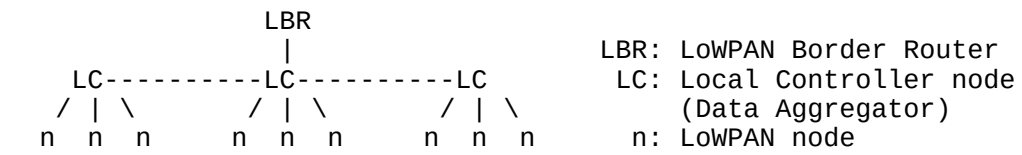

Figure 1: Storage Rooms with a Simple Star Topology

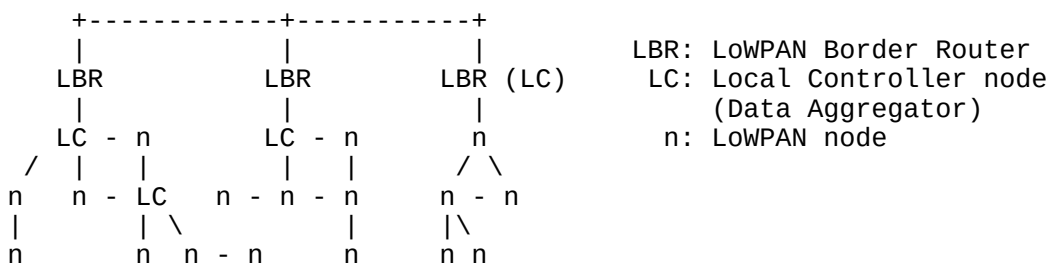

Figure 2: Storage Rooms with a Mesh Topology

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 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 1000-m-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 100-m 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 for the pillars, there are no special obstacles causing attenuation of 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 points of the LoWPAN hosts at the pillar and act as local coordinators.

This use case can be extended to medium or large 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 and manual deployment; depending on the blueprint 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.
- Network Size: Small (dozens of nodes) to large.
- Power Source: Mains-powered nodes are mixed with battery-powered nodes. (Mains-powered nodes will be used for local coordination or relays.)
- Connectivity: Always connected, or intermittent via sleeping mode scheduling.
- Multi-Hop Communication: It is recommended that multi-hop mesh networking be supported.
- Traffic Pattern: MP2P (data collection), P2P (localized querying).
- Security Level: Safety-critical. Secure transmission must be guaranteed. Only authenticated users must be able to access and handle the data.
- Mobility: None.
- 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.
- 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 via 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 in 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 addresses can be used for IPv6 link-local addresses [3].

Each pillar might have one LC for data collection. 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 address allocation.

This type of application works based on periodic, query-driven, and event-driven notifications. The data over or under a predefined threshold is meaningful to report. Event-driven data sensed on abnormal occurrences is time-critical and requires secure and reliable transmission. Alternatively, 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-powered node that 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 access from outside of the LoWPAN. The LBR may take charge of authentication of LoWPAN nodes. Reliable and secure data transmission must be guaranteed.

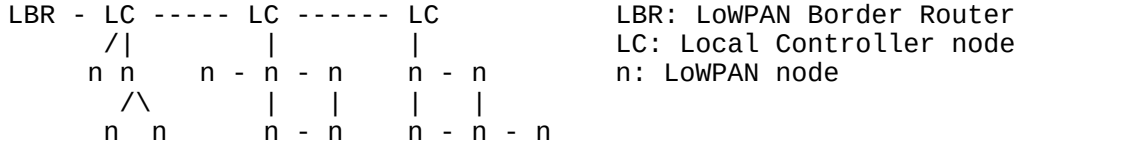

Figure 3: A Bridge Monitoring Scenario

3.3. Connected Home

The "Connected" Home or "Smart" home is without doubt an area where LoWPANs can be used to support an increasing number of services:

- Home safety/security
- Home automation and control
- Healthcare (see Section 3.4)
- Smart appliances and home entertainment systems

In home environments, LoWPANs typically comprise a few dozen and, probably in the near future, a few hundred nodes of various types: 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.), as well as home control (activate 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 emergence of "Smart Grid" applications, the LoWPAN may also have direct interactions with the Grid itself via the Internet to report the amount of kilowatts 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 a Demand-Response application. Another service, known as Demand-Side Management (DSM), could be provided by utilities to monitor and report to the user his energy consumption, with a fine granularity (on a per-device basis). A user can also receive other inputs from the utility, such as dynamic pricing; according to local policy, the utility may then turn some appliances on or off in order to reduce its energy bill.

In terms of home safety and security, the LoWPAN is made up of motion sensors and audio sensors, sensors at doors and windows, and video cameras; additional sensors can be added for safety (gas, water, CO, Radon, smoke detection). The LoWPAN is typically comprised of 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 simplest 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 may be activated to send a video stream to a cell phone via a gateway.

Ergonomics in connected homes is key, and the LoWPAN must be self-managed and easy to install. Traffic patterns may vary greatly, depending on applicability; 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, the response time and network delays must still be on the order of a few hundred milliseconds for optimal 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 LoWPANs usually do not require multi-topology or QoS routing. Fairly simple QoS mechanisms are enough for handling emergency data; they can be programmed to alarm via actuators or to operate sprinklers.

Dominant parameters for home automation applications:

- Deployment: Multi-hop topologies.
- Network Size: Medium number of nodes, potentially high density.
- Power Source: Mix of battery-powered and mains-powered devices.
- Connectivity: Intermittent (usage-dependent sleep modes).
- Multi-Hop Communication: No requirement for multi-topology or QoS routing.
- Traffic Pattern: P2P (inter-device), P2MP, and MP2P (polling).
- Security Level: Authentication and encryption required.

- o Mobility: Some degree of mobility.

- o QoS: Support of limited QoS for emergency data (alarm).

3.3.2. 6LoWPAN Applicability

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

In the 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.

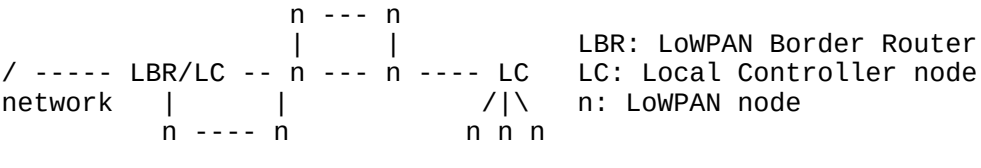

Figure 4: Home Automation Scenario

In some scenarios, traffic will be sent to a LC for processing; the LC may in turn decide on local actions (switch a light on, ...). In other scenarios, all devices will send their data to the LCs, which in turn may also act as the LBR for data processing and potential relay of data outside of the LoWPAN. It does not mean that all devices communicate with each other via the LC and LBR. 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 send data once enough data has been accumulated (e.g., energy consumption for the past 6 hours for a set of appliances), or trigger an alarm that is 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 path of 2-3 hops (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 applications (e.g., fire, gas-leak detection, health monitoring), whereas other applications may not be critical (e.g., humidity monitoring). Such emergency data has the same QoS issues as does event-driven data in other applications and can be delivered by pre-defined paths through mains-powered nodes without being stored in intermediate nodes such as LCs. Similarly, some information may require the use of security mechanisms for authentication and confidentiality.

3.4. Healthcare

LoWPANs are envisioned to be heavily used in healthcare environments. They have a high potential for easing the deployment of new services by getting rid of cumbersome wires and simplifying patient care in hospitals and at home (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 [10] 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 several wearable LoWPAN nodes to measure heartbeat, pulse rate, etc. Dozens of LoWPAN nodes are densely installed at home for movement detection. An 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 patients at home, where there are many walls and obstacles. Even during sleep, the change of body position may affect radio propagation.

Data is gathered in both periodic and event-driven fashion. 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 memory and energy. In addition, different data will be provided to the hospital system from that 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.
- Network Size: Small, high node density.
- Power Source: Hybrid.
- Connectivity: Always on.
- Multi-Hop Communication: Multi-hop for home-care devices; patient's body network is star topology. Multipath interference due to walls and obstacles at home must be considered.
- Traffic Pattern: MP2P/P2MP (data collection), P2P (local diagnostic).
- Security Level: Data privacy and security must be provided. Encryption is required. It is required that role-based access control be supported by a lightweight authentication mechanism.
- Mobility: Moderate (patient's mobility).
- QoS: High level of reliability support (life-or-death implication), role-based.
- 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 that 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 (say, 10 nodes or less). 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 addresses can be used for IPv6 link-local addresses [3]. 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 patient's 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 whether the patient visits the connected hospital or stays at home. If the patient's LoWPAN uses a globally unique IPv6 address, the address can be used for patient identification. However, this incurs a cost in terms of privacy and security. The hospital LoWPAN to which the patient's information is transferred needs to operate an additional identification system, together with a strong authority and authentication mechanism. The connection between the LBR at home and the LBR at the hospital must be reliable and secure, as the data is privacy-critical. To achieve this, an additional policy for security between the two LoWPANs is recommended.

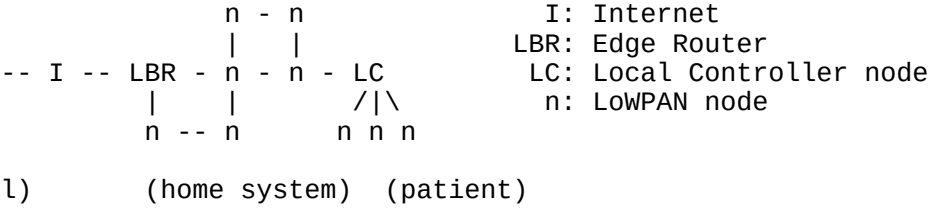

Figure 5: A Mobile Healthcare Scenario

3.5. Vehicle Telematics

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

3.5.1. A Use Case and Its Requirements

Example: Telematics

As shown in Figure 6, LoWPAN nodes for motion monitoring are incorporated into roads during road construction. When a car passes over these nodes, it is then possible to track, for safety purposes, the trajectory (path) and velocity of the car.

The lifetime of LoWPAN nodes incorporated into roads is expected to be as long as the lifetime 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 node density due to power failures. Sink nodes placed at the side of the road are most likely mains-powered; LoWPAN nodes in the roads run on batteries. 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).
- Network Size: Large (road infrastructure), small (vehicle).
- Power Source: Hybrid.
- Connectivity: Intermittent.
- Multi-Hop Communication: Multi-hop, especially ad hoc.
- Traffic Pattern: Mostly MP2P, P2MP.
- Security Level: Handling physical damage and link failure.
- Mobility: None (road infrastructure), high (vehicle).

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., the Internet) in order to reach the transportation control center (Figure 6). These LBRs may be logically combined with a LC as a data sink to gather sensed data from a number of LoWPAN nodes inserted in the road pavement. 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.

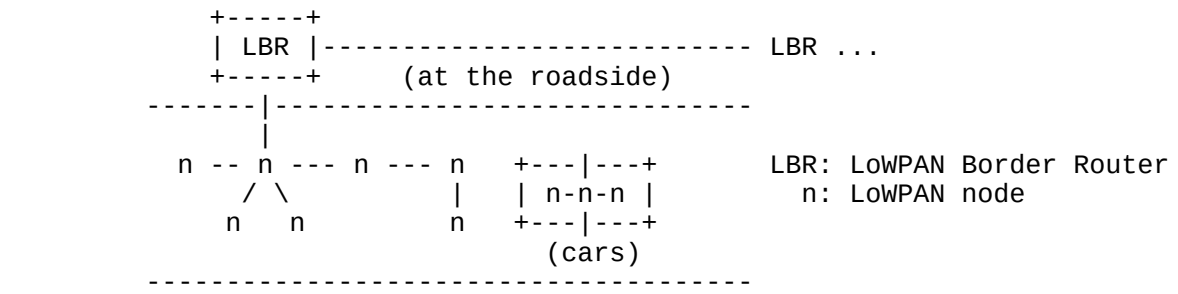

Figure 6: Telematics Scenario

Given the fact that nodes are incorporated into 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 farmer's inability to check crops at all times of the day, or inadequate measurement tools, luck often plays too large a 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 environmental protection. The sensing data can be used to find optimal environments for the plants. In addition, the data on planting conditions 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 of medium to large geographical size, between 50 and 100 LC nodes are manually deployed in order to provide full signal coverage over the study area. An additional 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 when installed in a geographically large area, in order to pin down where an event occurred, and to combine gathered data with the actual positions of the devices. Using manual deployment, device addresses can be used for identifying their 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 the type of 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, and dust, in dynamic environments of moving people and machinery, and with growing crops and foliage. LoWPAN nodes can be deployed in a predefined manner, with consideration given to harsh environments.

- Network Size: Medium to large, low to medium density.

- Power Source: All nodes are battery-powered except the sink, or energy harvesting.

- Connectivity: Intermittent (many sleeping nodes).

- Multi-Hop Communication: Mesh topology with local star connections.

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

- Security Level: Depends on purpose of the business. Lightweight security or simple shared-key management can be used, depending on the purpose of the business.

- Mobility: All static.

- Other Issues: Time synchronization among sensors is required, but the traffic interval may not be frequent (e.g., once every 30 to 60 minutes).

3.6.2. 6LoWPAN Applicability

The network configuration in this use case might, in the simplest case, look like the configuration illustrated in Figure 7. This static scenario consists of one or more fixed LBRs that are mains-powered and have a high-bandwidth connection to a backbone link, which might be placed in a control center or connected 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 [1]) to connect to the outside of the LoWPAN, the LoWPAN nodes operate a more energy-conserving ND described in [6], 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 at the application level are necessary.

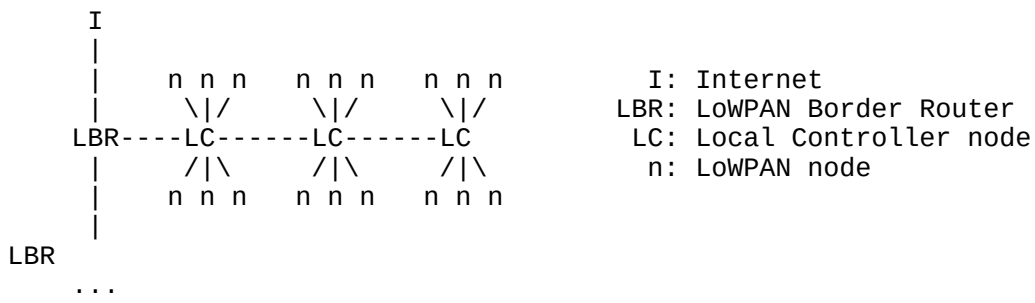

Figure 7: Automated Vineyard Scenario

4. Security Considerations

Relevant security considerations are listed by application scenario in Section 3. The security considerations in RFC 4919 [2] and RFC 4944 [3] 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 of 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) 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.

Considering the power constraints and limited processing capabilities of IEEE 802.15.4 devices, IPsec is computationally expensive; Internet key exchange (IKEv2) messaging as described in [4] is not suited for LoWPANs, as the amount of signaling in these networks should be minimized. Thus, LoWPANs may need to define their own key-management method that requires minimum overhead in terms of packet size and message exchange [11]. 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. Recent work [13] shows some promise for minimal IKEv2 implementations.

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 healthcare 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 high security and robustness against intrusion. On the other hand, a remote-controlled light switch has no critical security threats.

5. Acknowledgements

Special thanks to Nicolas Chevrollier for participating in the initial design of the document. Also, thanks to David Cypher for giving more insight on the IEEE 802.15.4 standard, and to Irene Fernandez, Shoichi Sakane, and Paul Chilton for their review and valuable comments.

6. References

6.1. Normative References

[1] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[2] 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.

[3] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[4] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[5] IEEE Computer Society, "IEEE Standard for Local and Metropolitan Area Networks -- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE Std. 802.15.4-2011, September 2011.

6.2. Informative References

[6] Shelby, Z., Ed., Chakrabarti, S., and E. Nordmark, "Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN)", Work in Progress, October 2011.

[7] Hui, J., Ed., and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

[8] Kim, E., Kaspar, D., Gomez, C., and C. Bormann, "Problem Statement and Requirements for 6LoWPAN Routing", Work in Progress, November 2011.

[9] Roemer, K. and F. Mattern, "The Design Space of Wireless Sensor Networks", IEEE Wireless Communications, Vol. 11, No. 6, pp. 54-61, December 2004.

[10] den Hartog, F., Schmidt, J., and A. de Vries, "On the potential of personal networks for hospitals", International Journal of Medical Informatics, 75, pp. 658-663, May 2006.

[11] Dutertre, B., Cheung, S., and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust", SDL Technical Report SRI-SDL-04-02, April 2004.

[12] Chen, D. and P.K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey", Proc. 2004 Int. Conf. Wireless Networks (ICWN 2004), June 2004.

[13] Kivinen, T., "Minimal IKEv2", Work in Progress, February 2011.

Authors' Addresses

Eunsook Kim
ETRI
161 Gajeong-dong
Yuseong-gu
Daejeon 305-700
Korea

Phone: +82-42-860-6124
EMail: eunah.ietf@gmail.com

Dominik Kaspar
Simula Research Laboratory
Martin Linges v 17
Snaroya 1367
Norway

Phone: +47-6782-8200
EMail: dokaspar.ietf@gmail.com

JP. Vasseur
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
USA

EMail: jpv@cisco.com