Internet Engineering Task Force (IETF)
Request for Comments: 6606
Category: Informational
ISSN: 2070-1721

E. Kim
ETRI
D. Kaspar
Simula Research Laboratory
C. Gomez
Universitat Politecnica de Catalunya/Fundacio i2CAT
C. Bormann
Universitaet Bremen TZI

May 2012

Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing

Abstract

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) are formed by devices that are compatible with the IEEE 802.15.4 standard. However, neither the IEEE 802.15.4 standard nor the 6LoWPAN format specification defines how mesh topologies could be obtained and maintained. Thus, it should be considered how 6LoWPAN formation and multi-hop routing could be supported.

This document provides the problem statement and design space for 6LoWPAN routing. It defines the routing requirements for 6LoWPANs, considering the low-power and other particular characteristics of the devices and links. The purpose of this document is not to recommend specific solutions but to provide general, layer-agnostic guidelines about the design of 6LoWPAN routing that can lead to further analysis and protocol design. This document is intended as input to groups working on routing protocols relevant to 6LoWPANs, such as the IETF ROLL WG.

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/rfc6606.

Copyright Notice

Copyright (c) 2012 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.

Table of Contents

1. Problem Statement

6LoWPANs are formed by devices that are compatible with the IEEE 802.15.4 standard [IEEE802.15.4]. Most of the LoWPAN devices are distinguished by their low bandwidth, short range, scarce memory capacity, limited processing capability, and other attributes of inexpensive hardware. The characteristics of nodes participating in LoWPANs are assumed to be those described in the 6LoWPAN problem statement [RFC4919], and in the IPv6 over IEEE 802.15.4 document [RFC4944], which has specified how to carry IPv6 packets over IEEE 802.15.4 and similar networks. Whereas IEEE 802.15.4 distinguishes two types of devices called full-function devices (FFDs) and reduced-function devices (RFDs), this distinction is based on some features of the Medium Access Control (MAC) layer that are not always in use. Hence, the distinction is not made in this document. Nevertheless, some 6LoWPAN nodes may limit themselves to the role of hosts only, whereas other 6LoWPAN nodes may take part in routing. This host/ router distinction can correlate with the processing and storage capabilities of the device and power available in a similar way to the idea of RFDs and FFDs.

IEEE 802.15.4 networks support star and mesh topologies. However, neither the IEEE 802.15.4 standard nor the 6LoWPAN format specification ([RFC4944]) define how mesh topologies could be obtained and maintained. Thus, 6LoWPAN formation and multi-hop routing can be supported either below the IP layer (the adaptation layer or Logical Link Control (LLC)) or the IP layer. (Note that in the IETF, the term "routing" usually, but not always [RFC5556], refers exclusively to the formation of paths and the forwarding at the IP layer. In this document, we distinguish the layer at which these services are performed by the terms "route-over" and "mesh-under". See Sections 2 and 3.) A number of IP routing protocols have been developed in various IETF working groups. However, these existing routing protocols may not satisfy the requirements of multi-hop routing in 6LoWPANs, for the following reasons:

o 6LoWPAN nodes have special types and roles, such as nodes drawing their power from primary batteries, power-affluent nodes, mains-powered and high-performance gateways, data aggregators, etc. 6LoWPAN routing protocols should support multiple device types and roles.

o More stringent requirements apply to LoWPANs, as opposed to higher-performance or non-battery-operated networks. 6LoWPAN nodes are characterized by small memory sizes and low processing power, and they run on very limited power supplied by primary non-rechargeable batteries (a few KB of RAM, a few dozen KB of ROM/ flash memory, and a few MHz of CPU is typical). A node's lifetime is usually defined by the lifetime of its battery.

o Handling sleeping nodes is very critical in LoWPANs, more so than in traditional ad hoc networks. LoWPAN nodes might stay in sleep mode most of the time. Taking advantage of appropriate times for transmissions is important for efficient packet forwarding.

o Routing in 6LoWPANs might possibly translate to a simpler problem than routing in higher-performance networks. LoWPANs might be either transit networks or stub networks. Under the assumption that LoWPANs are never transit networks (as implied by [RFC4944]), routing protocols may be drastically simplified. This document will focus on the requirements for stub networks. Additional requirements may apply to transit networks.

- Routing in LoWPANs might possibly translate to a harder problem than routing in higher-performance networks. Routing in LoWPANs requires power optimization, stable operation in lossy environments, etc. These requirements are not easily satisfiable all at once [ROLL-PROTOCOLS].

These properties create new challenges for the design of routing within LoWPANs.

The 6LoWPAN problem statement [RFC4919] briefly mentions four requirements for routing protocols:

(a) low overhead on data packets

(b) low routing overhead

(c) minimal memory and computation requirements

(d) support for sleeping nodes (consideration of battery savings)

These four high-level requirements describe the basic requirements for 6LoWPAN routing. Based on the fundamental features of 6LoWPANs, more detailed routing requirements, which can lead to further analysis and protocol design, are presented in this document.

Considering the problems above, detailed 6LoWPAN routing requirements must be defined. Application-specific features affect the design of 6LoWPAN routing requirements and corresponding solutions. However, various applications can be profiled by similar technical characteristics, although the related detailed requirements might differ (e.g., a few dozen nodes in a home lighting system need appropriate scalability for the system’s applications, while millions of nodes for a highway infrastructure system also need appropriate scalability).

This routing requirements document states the routing requirements of 6LoWPAN applications in general, providing examples for different cases of routing. It does not imply that a single routing solution will be favorable for all 6LoWPAN applications, and there is no requirement for different routing protocols to run simultaneously.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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].

This specification makes use of the terminology defined in [6LoWPAN-ND].

3. Design Space

Apart from a wide variety of conceivable routing algorithms for 6LoWPANs, it is possible to perform routing in the IP layer (using a route-over approach) or below IP, as defined by the 6LoWPAN format document [RFC4944] (using the mesh-under approach). See Figure 1.

The route-over approach relies on IP routing and therefore supports routing over possibly various types of interconnected links.
Note: The ROLL WG is now working on route-over approaches for Low-power and Lossy Networks (LLNs), not specifically for 6LoWPANs. This document focuses on 6LoWPAN-specific requirements; it may be used in conjunction with the more application-oriented requirements defined by the ROLL WG.

The mesh-under approach performs the multi-hop communication below the IP link. The most significant consequence of the mesh-under mechanism is that the characteristics of IEEE 802.15.4 directly affect the 6LoWPAN routing mechanisms, including the use of 64-bit (or 16-bit short) link-layer addresses instead of IP addresses. A 6LoWPAN would therefore be seen as a single IP link.

Most statements in this document consider both the route-over and mesh-under cases.

Figure 1 shows the place of 6LoWPAN routing in the entire network stack.

```
 +----------------------------+  +------------------------------+
 |      Application Layer     |  |      Application Layer       |
 +----------------------------+  +------------------------------+
 | Transport Layer (TCP/UDP) |  |  Transport Layer (TCP/UDP)  |
 +----------------------------+  +------------------------------+
 |     Network Layer (IPv6)   |  |  Network      +----------+  |
 +----------------------------+  |  Layer        | Routing |  |
 |  6LoWPAN                   |  |  (IPv6)       +----------+  |
 |  Adaptation                |  +------------------------------+
 |  Layer       +-----------+ |  |  6LoWPAN Adaptation Layer   |
 +--------------| Routing* |-+  +------------------------------+
 | 802.15.4 MAC +-----------+ |  |        802.15.4 MAC          |
 +----------------------------+  +------------------------------+
 |         802.15.4 PHY       |  |        802.15.4 PHY          |
 +----------------------------+  +------------------------------+
  * Here, "Routing" is not equivalent to IP routing,
    but includes the functionalities of path computation and
    forwarding under the IP layer.
    The term "Routing" is used in the figure in order to
    illustrate which layer handles path computation and
    packet forwarding in mesh-under as compared to route-over.
```

Figure 1: Mesh-Under Routing (Left) and Route-Over Routing (Right)

In order to avoid packet fragmentation and the overhead for reassembly, routing packets should fit into a single IEEE 802.15.4 physical frame, and application data should not be expanded to an extent that they no longer fit.

3.1. Reference Network Model

For multi-hop communication in 6LoWPANs, when a route-over mechanism is in use, all routers (i.e., 6LoWPAN Border Routers (6LBRs) and 6LoWPAN Routers (6LRs)) perform IP routing within the stub network (see Figure 2). In this case, the link-local scope covers the set of nodes within symmetric radio range of a node.

When a LoWPAN follows the mesh-under configuration, the 6LBR is the only IPv6 router in the LoWPAN (see Figure 3). This means that the IPv6 link-local scope includes all nodes in the LoWPAN. For this, a mesh-under mechanism MUST be provided to support multi-hop transmission.

```
     h    h
    /     |                       6LBR: 6LoWPAN Border Router
6LBR -- 6LR --- 6LR --- h          6LR: 6LoWPAN Router
        / \                          h: Host
       h  6LR --- h
           |
          / \
       6LR - 6LR -- h
```

Figure 2: An Example of a Route-Over LoWPAN

```
     h    h
    /     |                     6LBR: 6LoWPAN Border Router
6LBR --- m --- m --- h             m: mesh-under forwarder
        / \                        h: Host
       h   m --- h
           |
          / \
         m - m -- h
```

Figure 3: An Example of a Mesh-Under LoWPAN

Note than in both mesh-under and route-over networks, there is no expectation of topologically based address assignment in the 6LoWPAN. Instead, addresses are typically assigned based on the EUI-64 addresses assigned at manufacturing time to nodes, or based on a (from a topological point of view) more or less random process assigning 16-bit MAC addresses to individual nodes. Within a 6LoWPAN, there is therefore no opportunity for aggregation or summarization of IPv6 addresses beyond the sharing of (one or more) common prefixes.

Not all devices that are within radio range of each other need to be part of the same LoWPAN. When multiple LoWPANs are formed with globally unique IPv6 addresses in the 6LoWPANs, and device (a) of LoWPAN [A] wants to communicate with device (b) of LoWPAN [B], the normal IPv6 mechanisms will be employed. For route-over, the IPv6 address of (b) is set as the destination of the packets, and the devices perform IP routing to the 6LBR for these outgoing packets. For mesh-under, there is one IP hop from device (a) to the 6LBR of [A], no matter how many radio hops they are apart from each other. This, of course, assumes the existence of a mesh-under routing protocol in order to reach the 6LBR. Note that a default route to the 6LBR could be inserted into the 6LoWPAN routing system for both route-over and mesh-under.

4. Scenario Considerations and Parameters for 6LoWPAN Routing

IP-based LoWPAN technology is still in its early stage of development, but the range of conceivable usage scenarios is tremendous. The numerous possible applications of sensor networks make it obvious that mesh topologies will be prevalent in LoWPAN environments and robust routing will be a necessity for expedient communication. Research efforts in the area of sensor networking have put forth a large variety of multi-hop routing algorithms [Bulusu]. Most related work focuses on optimizing routing for specific application scenarios, which can be realized using several modes of communication, including the following [Watteyne]:

- o Flooding (in very small networks)
- o Hierarchical routing
- o Geographic routing
- o Self-organizing coordinate routing

Depending on the topology of a LoWPAN and the application(s) running over it, different types of routing may be used. However, this document abstracts from application-specific communication and describes general routing requirements valid for overall routing in LoWPANs.

The following parameters can be used to describe specific scenarios in which the candidate routing protocols could be evaluated.

a. Network Properties:

* Number of Devices, Density, and Network Diameter:
  These parameters usually affect the routing state directly (e.g., the number of entries in a routing table or neighbor list). Especially in large and dense networks, policies must be applied for discarding "low-quality" and stale routing entries in order to prevent memory overflow.

* Connectivity:
  Due to external factors or programmed disconnections, a LoWPAN can be in several states of connectivity -- anything in the range from "always connected" to "rarely connected". This poses great challenges to the dynamic discovery of routes across a LoWPAN.

* Dynamicity (including mobility):
  Location changes can be induced by unpredictable external factors or by controlled motion, which may in turn cause route changes. Also, nodes may dynamically be introduced into a LoWPAN and removed from it later. The routing state and the volume of control messages may heavily depend on the number of moving nodes in a LoWPAN and their speed, as well as how quickly and frequently environmental characteristics influencing radio propagation change.

* Deployment:
  In a LoWPAN, it is possible for nodes to be scattered randomly or to be deployed in an organized manner. The deployment can occur at once, or as an iterative process, which may also affect the routing state.

* Spatial Distribution of Nodes and Gateways:
  Network connectivity depends on the spatial distribution of the nodes and on other factors, such as device number, density, and transmission range. For instance, nodes can be placed on a grid, or randomly located in an area (as can be modeled by a two-dimensional Poisson distribution), etc. Assuming a random spatial distribution, an average of 7 neighbors per node are required for approximately 95% network connectivity (10 neighbors per node are needed for 99% connectivity) [Kuhn]. In addition, if the LoWPAN is connected to other networks through infrastructure nodes called gateways, the number and spatial distribution of these gateways affect network congestion and available data rate, among other things.

* Traffic Patterns, Topology, and Applications:
  The design of a LoWPAN and the requirements for its application have a big impact on the network topology and the most efficient routing type to be used. For different traffic patterns (point-to-point, multipoint-to-point, point-to-multipoint) and network architectures, various routing mechanisms have been developed, such as data-centric, event-driven, address-centric, and geographic routing.

* Classes of Service:
  For mixing applications of different criticality on one LoWPAN, support of multiple classes of service may be required in resource-constrained LoWPANs and may require a new routing protocol functionality.

* Security:
  LoWPANs may carry sensitive information and require a high level of security support where the availability, integrity, and confidentiality of data are of prime relevance. Secured messages cause overhead and affect the power consumption of LoWPAN routing protocols.

b. Node Parameters:

* Processing Speed and Memory Size:
  These basic parameters define the maximum size of the routing state and the maximum complexity of its processing. LoWPAN nodes may have different performance characteristics, queuing strategies, and queue buffer sizes.

* Power Consumption and Power Source:
  The number of battery- and mains-powered nodes and their positions in the topology created by them in a LoWPAN affect routing protocols in their selection of paths that optimize network lifetime.

* Transmission Range:
  This parameter affects routing. For example, a high transmission range may cause a dense network, which in turn results in more direct neighbors of a node, higher connectivity, and a larger routing state.

* Traffic Pattern:
  This parameter affects routing, since highly loaded nodes (either because they are the source of packets to be transmitted or due to forwarding) may contribute to higher delivery delays and may consume more energy than lightly loaded nodes. This applies to both data packets and routing control messages.

c. Link Parameters:
   This section discusses link parameters that apply to IEEE 802.15.4 legacy mode (i.e., not making use of improved modulation schemes).

   * Throughput:
     The maximum user data throughput of a bulk data transmission between a single sender and a single receiver through an unslotted IEEE 802.15.4 2.4 GHz channel in ideal conditions is as follows [Latre]:

     + 16-bit MAC addresses, unreliable mode: 151.6 kbit/s

     + 16-bit MAC addresses, reliable mode: 139.0 kbit/s

     + 64-bit MAC addresses, unreliable mode: 135.6 kbit/s

     + 64-bit MAC addresses, reliable mode: 124.4 kbit/s

     Throughput for the 915 MHz band is as follows:

     + 16-bit MAC addresses, unreliable mode: 31.1 kbit/s

     + 16-bit MAC addresses, reliable mode: 28.6 kbit/s

     + 64-bit MAC addresses, unreliable mode: 27.8 kbit/s

     + 64-bit MAC addresses, reliable mode: 25.6 kbit/s

     Throughput for the 868 MHz band is as follows:

     + 16-bit MAC addresses, unreliable mode: 15.5 kbit/s

     + 16-bit MAC addresses, reliable mode: 14.3 kbit/s

     + 64-bit MAC addresses, unreliable mode: 13.9 kbit/s

     + 64-bit MAC addresses, reliable mode: 12.8 kbit/s

* Latency:
  Latency ranges -- depending on payload size -- of a frame transmission between a single sender and a single receiver through an unslotted IEEE 802.15.4 2.4 GHz channel in ideal conditions are as shown below [Latre]. For unreliable mode, the actual latency is provided. For reliable mode, the round-trip time, including transmission of a Layer-2 acknowledgment, is provided:

  + 16-bit MAC addresses, unreliable mode: [1.92 ms, 6.02 ms]

  + 16-bit MAC addresses, reliable mode: [2.46 ms, 6.56 ms]

  + 64-bit MAC addresses, unreliable mode: [2.75 ms, 6.02 ms]

  + 64-bit MAC addresses, reliable mode: [3.30 ms, 6.56 ms]

  Latency ranges for the 915 MHz band are as follows:

  + 16-bit MAC addresses, unreliable mode: [5.85 ms, 29.35 ms]

  + 16-bit MAC addresses, reliable mode: [8.35 ms, 31.85 ms]

  + 64-bit MAC addresses, unreliable mode: [8.95 ms, 29.35 ms]

  + 64-bit MAC addresses, reliable mode: [11.45 ms, 31.82 ms]

  Latency ranges for the 868 MHz band are as follows:

  + 16-bit MAC addresses, unreliable mode: [11.7 ms, 58.7 ms]

  + 16-bit MAC addresses, reliable mode: [16.7 ms, 63.7 ms]

  + 64-bit MAC addresses, unreliable mode: [17.9 ms, 58.7 ms]

  + 64-bit MAC addresses, reliable mode: [22.9 ms, 63.7 ms]

Note that some of the parameters presented in this section may be used as link or node evaluation metrics. However, multi-criteria routing may be too expensive for 6LoWPAN nodes. Rather, various single-criteria metrics are available and can be selected to suit the environment or application.

5. 6LoWPAN Routing Requirements

This section defines a list of requirements for 6LoWPAN routing. An important design property specific to low-power networks is that LoWPANs have to support multiple device types and roles, such as

- o host nodes drawing their power from primary batteries or using energy harvesting (sometimes called "power-constrained nodes")
- o mains-powered host nodes (an example of what we call "power-affluent nodes")
- o power-affluent (but not necessarily mains-powered) high-performance gateway(s)
- o nodes with various functionality (data aggregators, relays, local manager/coordinators, etc.)

Due to these different device types and roles, LoWPANs need to consider the following two primary attributes:

- o Power conservation: some devices are mains-powered, but many are battery-operated and need to last several months to a few years with a single AA battery. Many devices are mains-powered most of the time but still need to function on batteries for possibly extended periods (e.g., on a construction site before building power is switched on for the first time).
- o Low performance: tiny devices, small memory sizes, low-performance processors, low bandwidth, high loss rates, etc.

These fundamental attributes of LoWPANs affect the design of routing solutions. Whether existing routing specifications are simplified and modified, or new solutions are introduced in order to fit the low-power requirements of LoWPANs, they need to meet the requirements described below.

5.1. Support of 6LoWPAN Device Properties

The general objectives listed in this section should be met by 6LoWPAN routing protocols. The importance of each requirement is dependent on what node type the protocol is running on and what the role of the node is. The following requirements consider the presence of battery-powered nodes in LoWPANs.

[R01] 6LoWPAN routing protocols SHOULD allow implementation with small code size and require low routing state to fit the typical 6LoWPAN node capacity. Generally speaking, the code size is bounded by available flash memory size, and the routing table is bounded by RAM size, possibly limiting it to less than 32 entries.

The RAM size of LoWPAN nodes often ranges between 4 KB and 10 KB (2 KB minimum), and program flash memory normally consists of 48 KB to 128 KB. (For example, in the current market, MICAz has 128 KB program flash, 4 KB EEPROM, and 512 KB external flash ROM; TIP700CM has 48 KB program flash, 10 KB RAM, and 1 MB external flash ROM.)

Due to these hardware restrictions, code SHOULD fit within a small memory size -- no more than 48 KB to 128 KB of flash memory, including at least a few tens of KB of application code size. (As a general observation, a routing protocol of low complexity may help achieve the goal of reducing power consumption, improves robustness, requires lower routing state, is easier to analyze, and may be less prone to security attacks.)

In addition, operation with limited amounts of routing state (such as routing tables and neighbor lists) SHOULD be maintained, since some typical memory sizes preclude storing state of a large number of nodes. For instance, industrial monitoring applications may need to support a maximum of 20 hops [RFC5673]. Small networks can be designed to support a smaller number of hops. While the need for this is highly dependent on the network architecture, there should be at least one mode of operation that can function with 32 forwarding entries or less.

[R02] 6LoWPAN routing protocols SHOULD cause minimal power consumption by efficiently using control packets (e.g., minimizing expensive IP multicast, which causes link broadcast to the entire LoWPAN) and by efficiently routing data packets.

One way of optimizing battery lifetime is by achieving a minimal control message overhead. Compared to such functions as computational operations or taking sensor samples, radio communication is by far the dominant factor of power consumption [Doherty]. Power consumption of transmission and/or reception depends linearly on the length of data units and on the frequency of transmission and reception of the data units [Shih].

The energy consumption of two example radio frequency (RF) controllers for low-power nodes is shown in [Hill]. The TR1000 radio consumes 21 mW when transmitting at 0.75 mW, and 15 mW during reception (with a receiver sensitivity of -85 dBm). The

CC1000 consumes 31.6 mW when transmitting at 0.75 mW, and 20 mW during reception (with a receiver sensitivity of -105 dBm). Power endurance under the concept of an idealized power source is explained in [Hill]. Based on the energy of an idealized AA battery, the CC1000 can transmit for approximately 4 days straight or receive for 9 consecutive days. Note that availability for reception consumes power as well.

As multicast may cause flooding in the LoWPAN, a 6LoWPAN routing protocol SHOULD minimize the control cost by multicasting routing packets.

Control cost of routing protocols in low-power and lossy networks is discussed in more detail in [ROLL-PROTOCOLS].

5.2. Support of 6LoWPAN Link Properties

6LoWPAN links have the characteristics of low data rate and possibly high loss rates. The routing requirements described in this section are derived from the link properties.

[R03] 6LoWPAN routing protocol control messages SHOULD NOT exceed a single IEEE 802.15.4 frame size, in order to avoid packet fragmentation and the overhead for reassembly.

In order to save energy, routing overhead should be minimized to prevent fragmentation of frames. Therefore, 6LoWPAN routing should not cause packets to exceed the IEEE 802.15.4 frame size. This reduces the energy required for transmission, avoids unnecessary waste of bandwidth, and prevents the need for packet reassembly. The [IEEE802.15.4] standard specifies an MTU of 127 bytes, yielding about 80 octets of actual MAC payload with security enabled, some of which is taken for the (typically compressed) IP header [RFC6282]. Avoiding fragmentation at the adaptation layer may imply the use of semantic fragmentation and/or algorithms that can work on small increments of routing information.

[R04] The design of routing protocols for LoWPANs must consider the fact that packets are to be delivered with sufficient probability according to application requirements.

Requirements for a successful end-to-end packet delivery ratio (where delivery may be bounded within certain latency levels) vary, depending on the application. In industrial applications, some non-critical monitoring applications may tolerate a successful delivery ratio of less than 90% with hours of latency;

in some other cases, a delivery ratio of 99.9% is required [RFC5673]. In building automation applications, application-layer errors must be below 0.01% [RFC5867].

Successful end-to-end delivery of packets in an IEEE 802.15.4 mesh depends on the quality of the path selected by the routing protocol and on the ability of the routing protocol to cope with short-term and long-term quality variation. The metric of the routing protocol strongly influences performance of the routing protocol in terms of delivery ratio.

The quality of a given path depends on the individual qualities of the links (including the devices) that compose that path. IEEE 802.15.4 settings affect the quality perceived at upper layers. In particular, in IEEE 802.15.4 reliable mode, if an acknowledgment frame is not received after a given period, the originator retries frame transmission up to a maximum number of times. If an acknowledgment frame is still not received by the sender after performing the maximum number of transmission attempts, the MAC layer assumes that the transmission has failed and notifies the next higher layer of the failure. Note that excessive retransmissions may be detrimental; see RFC 3819 [RFC3819].

[R05] The design of routing protocols for LoWPANs must consider the latency requirements of applications and IEEE 802.15.4 link latency characteristics.

Latency requirements may differ -- e.g., from a few hundred milliseconds to minutes -- depending on the type of application. Real-time building automation applications usually need response times below 500 ms between egress and ingress, while forced-entry security alerts must be routed to one or more fixed or mobile user devices within 5 seconds [RFC5867]. Non-critical closed-loop applications for industrial automation have latency requirements that can be as low as 100 ms, but many control loops are tolerant of latencies above 1 s [RFC5673]. In contrast, urban monitoring applications allow latencies smaller than the typical intervals used for reporting sensed information -- for instance, on the order of seconds to minutes [RFC5548].

The range of latencies of a frame transmission between a single sender and a single receiver through an ideal unslotted IEEE 802.15.4 2.4 GHz channel is between 2.46 ms and 6.02 ms with 64-bit MAC addresses in unreliable mode, and between 2.20 ms and 6.56 ms with 64-bit MAC addresses in reliable mode. The range of latencies of the 868 MHz band is from 11.7 ms to 63.7 ms, depending on the address type and mode used (reliable or unreliable). Note that the latencies may be larger than that, depending on channel load, the MAC-layer settings, and the choice of reliable or unreliable mode. Note that MAC approaches other than legacy 802.15.4 may be used (e.g., TDMA). Duty cycling may further affect latency (see [R08]). Depending on the routing path chosen and the network diameter, multiple hops may contribute to the end-to-end latency that an application may experience.

Note that a tradeoff exists between [R05] and [R04].

[R06] 6LoWPAN routing protocols SHOULD be robust to dynamic loss caused by link failure or device unavailability either in the short term (approx. 30 ms) -- due to Received Signal Strength Indication (RSSI) variation, interference variation, noise, and asynchrony -- or in the long term, due to a depleted power source, hardware breakdown, operating system misbehavior, etc.

An important trait of 6LoWPAN devices is their unreliability, which can be due to limited system capabilities and possibly being closely coupled to the physical world with all its unpredictable variations. In harsh environments, LoWPANs easily suffer from link failure. Collisions or link failures easily increase send and receive queues and can lead to queue overflow and packet losses.

For home applications, where users expect feedback after carrying out certain actions (such as handling a remote control while moving around), routing protocols must converge within 2 seconds if the destination node of the packet has moved and must converge within 0.5 seconds if only the sender has moved [RFC5826]. The tolerance of the recovery time can vary, depending on the application; however, the routing protocol must provide the detection of short-term unavailability and long-term disappearance. The routing protocol has to exploit network resources (e.g., path redundancy) to offer good network behavior despite node failure.

Different routing protocols may exhibit different scaling characteristics with respect to the recovery/convergence time and the computational resources to achieve recovery after a convergence; see also [R01] and [R10].

[R07] 6LoWPAN routing protocols SHOULD be designed to correctly operate in the presence of link asymmetry.

Link asymmetry occurs when the probability of successful transmission between two nodes is significantly higher in one direction than in the other. This phenomenon has been reported in a large number of experimental studies, and it is expected that 6LoWPANs will exhibit link asymmetry.

5.3. Support of 6LoWPAN Characteristics

6LoWPANs can be deployed in different sizes and topologies, adhere to various models of mobility, be exposed to various levels of interference, etc. In any case, LoWPANs must maintain low energy consumption. The requirements described in this subsection are derived from the network attributes of 6LoWPANs.

[R08] The design of 6LoWPAN routing protocols SHOULD take into account that some nodes may be unresponsive during certain time intervals, due to periodic hibernation.

Many nodes in LoWPAN environments might periodically hibernate (i.e., disable their transceiver activity) in order to save energy. Therefore, routing protocols must ensure robust packet delivery despite nodes frequently shutting off their radio transmission interface. Feedback from the lower IEEE 802.15.4 layer may be considered to enhance the power awareness of 6LoWPAN routing protocols.

CC1000-based nodes must operate at a duty cycle of approximately 2% to survive for one year from an idealized AA battery power source [Hill]. For home automation purposes, it is suggested that the devices have to maximize the sleep phase with a duty cycle lower than 1% [RFC5826], while in building automation applications, batteries must be operational for at least 5 years when the sensing devices are transmitting data (e.g., 64 bytes) once per minute [RFC5867].

Depending on the application in use, packet rates may range from one per second to one per day, or beyond. Routing protocols may take advantage of knowledge about the packet transmission rate and utilize this information in calculating routing paths. In many IEEE 802.15.4 deployments, and in other wireless low-power technologies, forwarders are mains-powered devices (and hence do not need to sleep). However, it cannot be assumed that all forwarders are mains-powered. A routing protocol that addresses this case SHOULD provide a mode in which power consumption is a metric. In addition, using nodes in power-saving modes for forwarding may increase delay and reduce the probability of packet delivery, which in this case also should be available as an input into the path computation.

[R09] The metric used by 6LoWPAN routing protocols SHOULD provide some flexibility with respect to the inputs provided by the lower layers and other measures to optimize path selection, considering energy balance and link qualities.

In homes, buildings, or infrastructure, some nodes will be installed with mains power. Such power-installed nodes MUST be considered as relay points for a prominent role in packet delivery. 6LoWPAN routing protocols MUST know the power constraints of the nodes.

Simple hop-count-only mechanisms may be inefficient in 6LoWPANs. There is a Link Quality Indication (LQI) and/or RSSI from IEEE 802.15.4 that may be taken into account for better metrics. The metric to be used (and its goal) may depend on applications and requirements.

The numbers in Figure 4 represent the Link Delivery Ratio (LDR) of each pair of nodes. There are studies that show a piecewise linear dependence between the LQI and the LDR [Chen].

```
           0.6
        A-------C
         \     /
     0.9 \   / 0.9
           \ /
            B
```

Figure 4: An Example Network

In this simple example, there are two options in routing from node A to node C, with the following features:

A. Path AC:

- (1/0.6) = 1.67 avg. transmissions needed for each packet (confirmed link-layer delivery with retransmissions and negligible ACK loss have been assumed)

- one-hop path

+ good energy consumption and end-to-end latency of data packets, poor delivery ratio (0.6)

+ poor probability of route reconfigurations

B. Path ABC:

+ (1/0.9)+(1/0.9) = 2.22 avg. transmissions needed for each packet (under the same assumptions as above)

+ two-hop path

+ poor energy consumption and end-to-end latency of data packets, good delivery ratio (0.81)

If energy consumption of the network must be minimized, path AC is the best (this path would be chosen based on a hop-count metric). However, if the delivery ratio in that case is not sufficient, the best path is ABC (it would be chosen by an LQI-based metric). Combinations of both metrics can be used.

The metric also affects the probability of route reconfiguration. Route reconfiguration, which may be triggered by packet losses, may require transmission of routing protocol messages. It is possible to use a metric aimed at selecting the path with a low route reconfiguration rate by using the LQI as an input to the metric. Such a path has good properties, including stability and low control message overhead.

Note that a tradeoff exists between [R09] and [R01].

[R10] 6LoWPAN routing protocols SHOULD be designed to achieve both scalability -- from a few nodes to maybe millions of nodes -- and minimal use of system resources.

A LoWPAN may consist of just a couple of nodes (for instance, in a body-area network), but may also contain much higher numbers of devices (e.g., monitoring of a city infrastructure or a highway). For home automation applications, it is envisioned that the routing protocol must support 250 devices in the network [RFC5826], while routing protocols for metropolitan-scale sensor networks must be capable of clustering a large number of sensing nodes into regions containing on the order of 10^2 to 10^4 sensing nodes each [RFC5548]. It is therefore necessary that routing mechanisms are designed to be scalable for operation in networks of various sizes. However, due to a lack of memory size and computational power, 6LoWPAN routing might limit forwarding entries to a small number, such as a maximum of 32 routing table entries. Particularly in large networks, the routing mechanism MUST be designed in such a way that the number of routers is smaller than the number of hosts.

[R11] The procedure of route repair and related control messages SHOULD NOT harm overall energy consumption from the routing protocols.

Local repair improves throughput and end-to-end latency, especially in large networks. Since routes are repaired quickly, fewer data packets are dropped, and a smaller number of routing protocol packet transmissions are needed, since routes can be repaired without source-initiated route discovery [Lee]. One important consideration here may be to avoid premature energy depletion, even if that impairs other requirements.

[R12] 6LoWPAN routing protocols SHOULD allow for dynamically adaptive topologies and mobile nodes. When supporting dynamic topologies and mobile nodes, route maintenance should keep in mind the goal of a minimal routing state and routing protocol message overhead.

Topological node mobility may be the result of physical movement and/or a changing radio environment, making it very likely that mobility needs to be handled even in a network with physically static nodes. 6LoWPANs do not make use of a separate protocol to maintain connectivity to moving nodes but expects the routing protocol to handle it.

In addition, some nodes may move from one 6LoWPAN to another and are expected to become functional members of the latter 6LoWPAN in a limited amount of time.

Building monitoring applications, for instance, have a number of requirements with respect to recovery and settling time for mobility that range between 5 and 20 seconds (Section 5.3.1 of [RFC5867]). For more interactive applications such as those used in home automation systems, where users provide input and expect instant feedback, mobility requirements are also stricter and, for moves within a network, a convergence time below 0.5 seconds is commonly required (Section 3.2 of [RFC5826]). In industrial environments, where mobile equipment (e.g., cranes) moves around, the routing protocol needs to support vehicular speeds of up to 35 km/h [RFC5673]. Currently, 6LoWPANs are not normally being used for such fast mobility, but dynamic association and disassociation MUST be supported in 6LoWPANs.

There are several challenges that should be addressed by a 6LoWPAN routing protocol in order to create robust routing in dynamic environments:

* Mobile Nodes Changing Their Location inside a LoWPAN:
  If the nodes' movement pattern is unknown, mobility cannot easily be detected or distinguished by the routing protocols. Mobile nodes can be treated as nodes that disappear and reappear in another place. The tracking of movement patterns increases complexity and can be avoided by handling moving nodes using reactive route updates.

* Movement of a LoWPAN with Respect to Other (Inter)Connected LoWPANs:
  Within each stub network, (one or more) relatively powerful gateway nodes (6LBRs) need to be configured to handle moving LoWPANs.

* Nodes Permanently Joining or Leaving the LoWPAN:
  In order to ease routing table updates, reduce the size of these updates, and minimize error control messages, nodes leaving the network may announce their disassociation to the closest edge router or to a specific node (if any) that takes charge of local association and disassociation.

[R13] A 6LoWPAN routing protocol SHOULD support various traffic patterns -- point-to-point, point-to-multipoint, and multipoint-to-point -- while avoiding excessive multicast traffic in a LoWPAN.

6LoWPANs often have point-to-multipoint or multipoint-to-point traffic patterns. Many emerging applications include point-to-point communication as well. 6LoWPAN routing protocols should be designed with the consideration of forwarding packets from/to multiple sources/destinations. Current documents of the ROLL WG explain that the workload or traffic pattern of use cases for LoWPANs tends to be highly structured, unlike the any-to-any data transfers that dominate typical client and server workloads. In many cases, exploiting such structure may simplify difficult problems arising from resource constraints or variation in connectivity.

5.4. Support of Security

The routing requirement described in this subsection allows secure transmission of routing messages. As in traditional networks, routing mechanisms in 6LoWPANs present another window from which an attacker might disrupt and significantly degrade the overall performance of the 6LoWPAN. Attacks against non-secure routing aim mainly to contaminate WPANs with false routing information, resulting in routing inconsistencies. A malicious node can also snoop packets and then launch replay attacks on the 6LoWPAN nodes. These attacks can cause harm, especially when the attacker is a high-power device, such as a laptop. It can also easily drain the batteries of 6LoWPAN devices by sending broadcast messages, redirecting routes, etc.

[R14] 6LoWPAN routing protocols MUST support confidentiality, authentication, and integrity services as required for secure delivery of control messages.

A general set of requirements that may apply to these services can be found in [KARP-THREATS].

Security is very important for designing robust routing protocols, but it should not cause significant transmission overhead. The security aspect, however, seems to be a bit of a tradeoff in a 6LoWPAN, since security is always a costly function. A 6LoWPAN poses unique challenges to which traditional security techniques cannot be applied directly. For example, public key cryptography primitives are typically avoided (as being too expensive), as are relatively heavyweight conventional encryption methods.

Consequently, it becomes questionable whether the 6LoWPAN devices can support IPsec as it is. While [RFC6434] makes support of the IPsec architecture a SHOULD for all IPv6 nodes, considering the power constraints and limited processing capabilities of IEEE 802.15.4-capable devices, IPsec is computationally expensive. Internet Key Exchange (IKEv2) messaging as described in RFC 5996 [RFC5996] will not work well in 6LoWPANs, as we want to minimize the amount of signaling in these networks. IPsec supports the Authentication Header (AH) for authenticating the IP header and the Encapsulating Security Payload (ESP) for authenticating and encrypting the payload. The main issues of using IPsec are two-fold: (1) processing power and (2) key management. Since these tiny 6LoWPAN devices do not process huge amounts of data or communicate with many different nodes, whether complete implementation of a Security Association Database (SAD), policy database, and dynamic key-management protocol are appropriate for these small battery-powered devices or not is not well understood.

Bandwidth is a very scarce resource in 6LoWPAN environments. The fact that IPsec additionally requires another header (AH or ESP) in every packet makes its use problematic in 6LoWPAN environments. IPsec requires two communicating peers to share a secret key that is typically established dynamically with IKEv2. Thus, it has an additional packet overhead incurred by the exchange of IKEv2 packets.

Given existing constraints in 6LoWPAN environments, IPsec may not be suitable for use in such environments, especially since a 6LoWPAN node may not be capable of operating all IPsec algorithms on its own. Thus, a 6LoWPAN may need to define its own keying management method(s) that require minimum overhead in packet size and in the number of signaling messages that are exchanged. IPsec will provide 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 most cases, the security may be requested at the application layer as needed, while other messages can flow in the network without security overhead.

Security threats within LoWPANs may be different from existing threat models in ad hoc network environments. If IEEE 802.15.4 security is not used, Neighbor Discovery (ND) in IEEE 802.15.4 links is susceptible to threats. These include Neighbor Solicitation/Neighbor Advertisement (NS/NA) spoofing, a malicious router, a default router that is "killed", a good router that goes bad, a spoofed redirect, replay attacks, and remote ND DoS [RFC3756]. However, if IEEE 802.15.4 security is used, no other protection is needed for ND, as long as none of the nodes become compromised, because the Corporate Intranet Model of RFC 3756 can be assumed [6LoWPAN-ND].

Bootstrapping may also impose additional threats. For example, a malicious node can obtain initial configuration information in order to appear as a legitimate node and then carry out various types of attacks. Such a node can also keep legitimate nodes busy by broadcasting authentication/join requests. One option for mitigating such threats is the use of mutual authentication schemes based on the use of pre-shared keys [Ikram].

The IEEE 802.15.4 MAC provides an AES-based security mechanism. Routing protocols may define how this mechanism (in conjunction with IPsec whenever available) can be used to obtain the intended security, either for the routing protocol alone or in conjunction with the security used for the data. Byte overhead of the mechanism, which depends on the security services selected, must be considered. In the worst case in terms of overhead, the mechanism consumes 21 bytes of MAC payload.

The IEEE 802.15.4 MAC security is typically supported by crypto hardware, even in very simple chips that will be used in a 6LoWPAN. Even if the IEEE 802.15.4 MAC security mechanisms are not used, this crypto hardware is usually available for use by application code running on these chips. A security protocol outside IEEE 802.15.4 MAC security SHOULD therefore provide a mode of operation that is covered by this crypto hardware.

IEEE 802.15.4 does not specify protection for acknowledgment frames. Since the sequence numbers of data frames are sent in the clear, an adversary can forge an acknowledgment for each data frame. Exploitation of this weakness can be combined with targeted jamming to prevent delivery of selected packets. Consequently, IEEE 802.15.4 acknowledgments cannot be relied upon. In applications that require high security, the routing protocol must not exploit feedback from acknowledgments (e.g., to keep track of neighbor connectivity, see [R16]).

5.5. Support of Mesh-Under Forwarding

One LoWPAN may be built as one IPv6 link. In this case, mesh-under forwarding mechanisms must be supported. While this document provides general, layer-agnostic guidelines about the design of 6LoWPAN routing, the requirements in this section are specifically related to Layer 2. These requirements are directed to bodies that might consider working on mesh-under routing, such as the IEEE. The requirements described in this subsection allow optimization and correct operation of routing solutions, taking into account the specific features of the mesh-under configuration.

[R15] Mesh-under requires the development of a routing protocol operating below IP. This protocol MUST support 16-bit short and 64-bit extended MAC addresses.

[R16] In order to perform discovery and maintenance of neighbors (i.e., neighborhood discovery as opposed to ND-style neighbor discovery), LoWPAN nodes SHOULD avoid sending separate "Hello" messages. Instead, link-layer mechanisms (such as acknowledgments) MAY be utilized to keep track of active neighbors.

Reception of an acknowledgment after a frame transmission may render unnecessary the transmission of explicit Hello messages, for example. In a more general view, any frame received by a node may be used as an input to evaluate the connectivity between the sender and receiver of that frame.

[R17] If the routing protocol functionality includes enabling IP multicast, then it MAY employ structure in the network for efficient distribution in order to minimize link-layer broadcast.

5.6. Support of Management

When a new protocol is designed, the operational environment and manageability of the protocol should be considered from the start [RFC5706]. This subsection provides a requirement for the manageability of 6LoWPAN routing protocols.

[R18] A 6LoWPAN routing protocol SHOULD be designed according to the guidelines for operations and management stated in [RFC5706].

The management operations that a 6LoWPAN routing protocol implementation can support depend on the memory and processing capabilities of the 6LoWPAN devices used, which are typically constrained. However, 6LoWPANs may benefit significantly from supporting such 6LoWPAN routing protocol management operations as configuration and performance monitoring.

The design of 6LoWPAN routing protocols should take into account that, according to "Architectural Principles of the Internet" [RFC1958], "options and parameters should be configured or negotiated dynamically rather than manually". This is especially important for 6LoWPANs, which can be composed of a large number of devices (and, in addition, these devices may not have an appropriate user interface). Therefore, parameter autoconfiguration is a desirable property for a 6LoWPAN routing protocol, although some subset of routing protocol parameters may allow other forms of configuration as well.

In order to verify the correct operation of the 6LoWPAN routing protocol and the network itself, a 6LoWPAN routing protocol should allow monitoring of the status and/or value of 6LoWPAN routing protocol parameters and data structures such as routing table entries. In order to enable fault management, further monitoring of the 6LoWPAN routing protocol operation is needed. For this, faults can be reported via error log messages. These messages may contain information such as the number of times a packet could not be sent to a valid next hop, the duration of each period without connectivity, memory overflow and its causes, etc.

[RFC5706] -- in particular its Section 3 -- provides a comprehensive guide to properly designing the management solution for a 6LoWPAN routing protocol.

6. Security Considerations

Security issues are described in Section 5.4. The security considerations in RFC 4919 [RFC4919], RFC 4944 [RFC4944], and RFC 4593 [RFC4593] apply as well.

The use of wireless links renders a 6LoWPAN susceptible to attacks like any other wireless network. In outdoor 6LoWPANs, the physical exposure of the nodes allows an adversary to capture, clone, or tamper with these devices. In ad hoc 6LoWPANs that are dynamic in both their topology and node memberships, a static security configuration does not suffice. Spoofed, altered, or replayed routing information might occur, while multihopping could delay the detection and treatment of attacks.

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 routing protocol packets. Time synchronization, self-organization, and secure localization for multi-hop routing are also critical to support.

For secure routing protocol operation, it may be necessary to consider authenticated broadcast (and multicast) and bidirectional link verification. On the other hand, secure end-to-end data delivery can be assisted by the routing protocol. For example, multi-path routing could be considered for increasing security to prevent selective forwarding. However, the challenge is that 6LoWPANs already have high resource constraints, so that 6LBR and LoWPAN nodes may require different security solutions.

7. Acknowledgments

The authors of this document highly appreciate the authors of "IPv6 over Low Power WPAN Security Analysis" [6LoWPAN-SEC]. Although their security analysis work is not ongoing at the time of this writing, the valuable information and text in that document are used in Section 5.4 of this document, per advice received during IESG review procedures. Thanks to their work, Section 5.4 is much improved. The authors also thank S. Chakrabarti, who gave valuable comments regarding mesh-under requirements, and A. Petrescu for significant review.

Carles Gomez has been supported in part by FEDER and by the Spanish Government through projects TIC2006-04504 and TEC2009-11453.

8. References

8.1. Normative References

[IEEE802.15.4] 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.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC3819] Karn, P., Ed., Bormann, C., Fairhurst, G., Grossman, D., Ludwig, R., Mahdavi, J., Montenegro, G., Touch, J., and L. Wood, "Advice for Internet Subnetwork Designers", BCP 89, RFC 3819, July 2004.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC4919] 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.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC5548] Dohler, M., Ed., Watteyne, T., Ed., Winter, T., Ed., and D. Barthel, Ed., "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, May 2009.

[RFC5673] Pister, K., Ed., Thubert, P., Ed., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 2009.

8.2. Informative References

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

[6LoWPAN-SEC]
Park, S., Kim, K., Haddad, W., Ed., Chakrabarti, S., and J. Laganier, "IPv6 over Low Power WPAN Security Analysis", Work in Progress, March 2011.

[Bulusu] Bulusu, N., Ed., and S. Jha, Ed., "Wireless Sensor Networks: A Systems Perspective", Artech House, ISBN 9781580538671, July 2005.

[Chen] Chen, B., Muniswamy-Reddy, K., and M. Welsh, "Ad-Hoc Multicast Routing on Resource-Limited Sensor Nodes", Proc. 2nd International Workshop on Multi-hop Ad Hoc Networks, May 2006.

[Doherty] Doherty, L., Warneke, B., Boser, B., and K. Pister, "Energy and Performance Considerations for Smart Dust", International Journal of Parallel and Distributed Systems and Networks, Vol. 4, No. 3, 2001.

[Hill] Hill, J., "System Architecture for Wireless Sensor Networks", Ph.D. Thesis, UC Berkeley, 2003.

[Ikram] Ikram, M., Chowdhury, A., Zafar, B., Cha, H., Kim, K., Yoo, S., and D. Kim, "A Simple Lightweight Authentic Bootstrapping Protocol for IPv6-based Low Rate Wireless Personal Area Networks (6LoWPANs)", Proc. International Conference on Wireless Communications and Mobile Computing, June 2009.

[KARP-THREATS]
Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", Work in Progress, May 2012.

[Kuhn] Kuhn, F., Wattenhofer, R., and A. Zollinger, "Worst-Case Optimal and Average-Case Efficient Ad-Hoc Geometric Routing", MobiHoc ’03: Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 2003.

[Latre] Latre, B., De Mil, P., Moerman, I., Dhoedt, B., and P. Demeester, "Throughput and Delay Analysis of Unslotted IEEE 802.15.4", Journal of Networks, Vol. 1, No. 1, May 2006.

[Lee] Lee, S., Belding-Royer, E., and C. Perkins, "Scalability Study of the Ad Hoc On-Demand Distance-Vector Routing Protocol", International Journal of Network Management, Vol. 13, pp. 97-114, March 2003.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, June 1996.

[RFC5556] Touch, J. and R. Perlman, "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement", RFC 5556, May 2009.

[RFC5706] Harrington, D., "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions", RFC 5706, November 2009.

[RFC5826] Brandt, A., Buron, J., and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5826, April 2010.

[RFC5867] Martocci, J., Ed., De Mil, P., Riou, N., and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5867, June 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6282] Hui, J., Ed., and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.

[ROLL-PROTOCOLS] Levis, P., Tavakoli, A., and S. Dawson-Haggerty, "Overview of Existing Routing Protocols for Low Power and Lossy Networks", Work in Progress, April 2009.

[Shih] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A., and A. Chandrakasan, "Physical Layer Driven Protocols and Algorithm Design for Energy-Efficient Wireless Sensor Networks", MobiCom ’01: Proceedings of the 7th ACM Annual International Conference on Mobile Computing and Networking, July 2001.

[Watteyne] Watteyne, T., Molinaro, A., Richichi, M., and M. Dohler, "From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols", IEEE Communications Surveys and Tutorials, Vol. 13, Issue 4, pp. 688-707, 2011, <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5581105>.

Authors' Addresses

Eunsook Eunah 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
Fornebu 1364
Norway

Phone: +47-6782-8223
EMail: dokaspar.ietf@gmail.com

Carles Gomez
Universitat Politecnica de Catalunya/Fundacio i2CAT
Escola d'Enginyeria de Telecomunicacio i Aeroespacial
de Castelldefels
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Phone: +34-93-413-7206
EMail: carlesgo@entel.upc.edu

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63921
EMail: cabo@tzi.org