

Networking Working Group  
Internet Draft  
Intended status: Informational  
Expires: March 2010

A. Brandt  
Zensys, Inc.  
G. Porcu  
Telecom Italia  
September 16, 2009

**Home Automation Routing Requirements in Low Power and Lossy  
Networks  
draft-ietf-roll-home-routing-reqs-08**

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 16, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>).

Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Brandt

Expires March 16, 2010

[Page 1]

## Abstract

This document presents home control and automation application specific requirements for Routing Over Low power and Lossy networks (ROLL). In the near future many homes will contain high numbers of wireless devices for a wide set of purposes. Examples include actuators (relay, light dimmer, heating valve), sensors (wall switch, water leak, blood pressure) and advanced controllers (RF-based AV remote control, Central server for light and heat control). Because such devices only cover a limited radio range, routing is often required. The aim of this document is to specify the routing requirements for networks comprising such constrained devices in a home control and automation environment.

## Requirements Language

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 [RFC-2119](#) [RFC2119].

Brandt

Expires March 16, 2010

[Page 2]

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction.....</a>	<a href="#">4</a>
<a href="#">1.1.</a>	<a href="#">Terminology.....</a>	<a href="#">5</a>
<a href="#">2.</a>	<a href="#">Home Automation Applications.....</a>	<a href="#">6</a>
<a href="#">2.1.</a>	<a href="#">Lighting Application In Action.....</a>	<a href="#">6</a>
<a href="#">2.2.</a>	<a href="#">Energy Conservation and Optimizing Energy Consumption....</a>	<a href="#">7</a>
<a href="#">2.3.</a>	<a href="#">Moving a Remote Control Around.....</a>	<a href="#">7</a>
<a href="#">2.4.</a>	<a href="#">Adding A New Module To The System.....</a>	<a href="#">8</a>
<a href="#">2.5.</a>	<a href="#">Controlling Battery Operated Window Shades.....</a>	<a href="#">8</a>
<a href="#">2.6.</a>	<a href="#">Remote Video Surveillance.....</a>	<a href="#">8</a>
<a href="#">2.7.</a>	<a href="#">Healthcare.....</a>	<a href="#">8</a>
<a href="#">2.7.1.</a>	<a href="#">At-home Health Reporting.....</a>	<a href="#">9</a>
<a href="#">2.7.2.</a>	<a href="#">At-home Health Monitoring.....</a>	<a href="#">10</a>
<a href="#">2.8.</a>	<a href="#">Alarm Systems.....</a>	<a href="#">10</a>
<a href="#">3.</a>	<a href="#">Unique Routing Requirements of Home Automation Applications..</a>	<a href="#">11</a>
<a href="#">3.1.</a>	<a href="#">Constraint-based Routing.....</a>	<a href="#">11</a>
<a href="#">3.2.</a>	<a href="#">Support of Mobility.....</a>	<a href="#">12</a>
<a href="#">3.3.</a>	<a href="#">Sleeping Nodes.....</a>	<a href="#">13</a>
<a href="#">3.4.</a>	<a href="#">Healthcare Routing.....</a>	<a href="#">13</a>
<a href="#">3.5.</a>	<a href="#">Scalability.....</a>	<a href="#">13</a>
<a href="#">3.6.</a>	<a href="#">Convergence Time.....</a>	<a href="#">14</a>
<a href="#">3.7.</a>	<a href="#">Manageability.....</a>	<a href="#">14</a>
<a href="#">3.8.</a>	<a href="#">Stability.....</a>	<a href="#">14</a>
<a href="#">4.</a>	<a href="#">Traffic Pattern.....</a>	<a href="#">14</a>
<a href="#">5.</a>	<a href="#">Security Considerations.....</a>	<a href="#">15</a>
<a href="#">6.</a>	<a href="#">IANA Considerations.....</a>	<a href="#">17</a>
<a href="#">7.</a>	<a href="#">Acknowledgments.....</a>	<a href="#">17</a>
<a href="#">8.</a>	<a href="#">Disclaimer for pre-RFC5378 work.....</a>	<a href="#">17</a>
<a href="#">9.</a>	<a href="#">References.....</a>	<a href="#">17</a>
<a href="#">9.1.</a>	<a href="#">Normative References.....</a>	<a href="#">17</a>
<a href="#">9.2.</a>	<a href="#">Informative References.....</a>	<a href="#">18</a>

Brandt

Expires March 16, 2010

[Page 3]

## **1. Introduction**

This document presents home control and automation application specific requirements for Routing Over Low power and Lossy networks (ROLL). In the near future many homes will contain high numbers of wireless devices for a wide set of purposes. Examples include actuators (relay, light dimmer, heating valve), sensors (wall switch, water leak, blood pressure) and advanced controllers. Basic home control modules such as wall switches and plug-in modules may be turned into an advanced home automation solution via the use of an IP-enabled application responding to events generated by wall switches, motion sensors, light sensors, rain sensors, and so on.

Network nodes may be sensors and actuators at the same time. An example is a wall switch for replacement in existing homes. The push buttons may generate events for a controller node or for activating other actuator nodes. At the same time, a built-in relay may act as actuator for a controller or other remote sensors.

Because ROLL nodes only cover a limited radio range, routing is often required. These devices are usually highly constrained in term of resources such as battery and memory and operate in unstable environments. Persons moving around in a house, opening or closing a door or starting a microwave oven affect the reception of weak radio signals. Reflection and absorption may cause a reliable radio link to turn unreliable for a period of time and then being reusable again, thus the term "lossy". All traffic in a ROLL network is carried as IPv6 packets.

Unlike other categories of Personal Area Networks (PANs), the connected home area is very much consumer-oriented. The implication on network nodes is that devices are very cost sensitive, which leads to resource-constrained environments having slow CPUs and small memory footprints. At the same time, nodes have to be physically small which puts a limit to the physical size of the battery; and thus, the battery capacity. As a result, it is common for low-power sensor-style nodes to shut down radio and CPU resources for most of the time. The radio tends to use the same power for listening as for transmitting

[Section 2](#) describes a few typical use cases for home automation applications. [Section 3](#) discusses the routing requirements for networks comprising such constrained devices in a home network environment. These requirements may be overlapping requirements derived from other application-specific routing requirements presented in [[I-D.Martocci-Building-reqs](#)], [[I-D.Pister-Industrial-](#)

reqs] and [[RFC5548](#)].

A full list of requirements documents may be found in [section 9](#).



### **1.1. Terminology**

ROLL:	Routing Over Low-power and Lossy networks A ROLL node may be classified as sensor, actuator or controller.
Actuator:	Network node which performs some physical action. Dimmers and relays are examples of actuators. If sufficiently powered, actuator nodes may participate in routing network messages.
Border router:	Infrastructure device that connects a ROLL network to the Internet or some backbone network.
Channel:	Radio frequency band used to carry network packets.
Controller:	Network node that controls actuators. Control decisions may be based on sensor readings, sensor events, scheduled actions or incoming commands from the Internet or other backbone networks. If sufficiently powered, controller nodes may participate in routing network messages.
Downstream:	Data direction traveling from a Local Area Network (LAN) to a Personal Area Network (PAN) device.
DR:	Demand-Response The mechanism of users adjusting their power consumption in response to actual pricing of power.
DSM:	Demand Side Management Process allowing power utilities to enable and disable loads in consumer premises. Where DR relies on voluntary action from users, DSM may be based on enrollment in a formal program.
HC-LLN:	Home Control in Low-Power and Lossy Networks
LAN:	Local Area Network.
PAN:	Personal Area Network. A geographically limited wireless network based on e.g. 802.15.4 or Z-Wave radio.
PDA	Personal Digital Assistant. A small, handheld computer.
PLC	Power Line Communication

RAM

Random Access Memory

Brandt

Expires March 16, 2010

[Page 5]

**Sensor:** Network node that measures some physical parameter and/or detects an event.  
The sensor may generate a trap message to notify a controller or directly activate an actuator.  
If sufficiently powered, sensor nodes may participate in routing network messages.

**Upstream:** Data direction traveling from a PAN to a LAN device.

Refer to the roll-terminology reference document [I-D.Vasseur-Terminology] for a full list of terms used in the IETF ROLL WG.

## **2. Home Automation Applications**

Home automation applications represent a special segment of networked devices with its unique set of requirements. Historically, such applications used wired networks or power line communication (PLC), but wireless solutions have emerged; allowing existing homes to be upgraded more easily.

To facilitate the requirements discussion in [Section 3](#), this section lists a few typical use cases of home automation applications. New applications are being developed at a high pace and this section does not mean to be exhaustive. Most home automation applications tend to be running some kind of command/response protocol. The command may come from several places.

### **2.1. Lighting Application In Action**

A lamp may be turned on, not only by a wall switch but also by a movement sensor. The wall switch module may itself be a push-button sensor and an actuator at the same time. This will often be the case when upgrading existing homes as existing wiring is not prepared for automation.

One event may cause many actuators to be activated at the same time.

Using the direct analogy to an electronic car key, a house owner may activate the "leaving home" function from an electronic house key, mobile phone, etc. For the sake of visual impression, all lights should turn off at the same time. At least, it should appear to happen at the same time. A well-known problem in wireless home automation is the "popcorn effect": Lamps are turned on one at a time, at a rate so slow that it is clearly visible.

Some existing home automation solutions address this by sending an

Brandt

Expires March 16, 2010

[Page 6]

unacknowledged multicast message in direct range before sending acknowledged singlecast messages to each device.

## **2.2. Energy Conservation and Optimizing Energy Consumption**

In order to save energy, air conditioning, central heating, window shades etc. may be controlled by timers, motion sensors or remotely via internet or cell. Central heating may also be set to a reduced temperature during night time.

The power grid may experience periods where more wind-generated power is produced than is needed. Typically this may happen during night hours.

In periods where electricity demands exceed available supply, appliances such as air conditioning, climate control systems, washing machines etc. can be turned off to avoid overloading the power grid.

This is known as Demand-Side Management (DSM).

Remote control of household appliances is well-suited for this application.

The start/stop decision for the appliances can also be regulated by dynamic power pricing information obtained from the electricity utility companies. This method called Demand-Response (DR) works by motivation of users via pricing, bonus points, etc. For example, the washing machine and dish washer may just as well work while power is cheap. The electric car should also charge its batteries on cheap power.

In order to achieve effective electricity savings, the energy monitoring application must guarantee that the power consumption of the ROLL devices is much lower than that of the appliance itself.

Most of these appliances are mains powered and are thus ideal for providing reliable, always-on routing resources. Battery-powered nodes, by comparison, are constrained routing resources and may only provide reliable routing under some circumstances.

## **2.3. Moving a Remote Control Around**

A remote control is a typical example of a mobile device in a home automation network. An advanced remote control may be used for dimming the light in the dining room while eating and later on, turning up the music while doing the dishes in the kitchen. Reaction must appear to be instant (within a few hundred

milliseconds) even when the remote control has moved to a new location. The remote control may be communicating to either a

Brandt

Expires March 16, 2010

[Page 7]

central home automation controller or directly to the lamps and the media center.

#### **2.4. Adding A New Module To The System**

Small-size, low-cost modules may have no user interface except for a single button. Thus, an automated inclusion process is needed for controllers to find new modules. Inclusion covers the detection of neighbors and assignment of a unique node ID. Inclusion should be completed within a few seconds.

If assignment of unique addresses is performed by a central controller, it must be possible to route the inclusion request from the joining node to the central controller before the joining node has been included in the network.

#### **2.5. Controlling Battery Operated Window Shades**

In consumer premises, window shades are often battery-powered as there is no access to mains power over the windows. For battery conservation purposes, such an actuator node is sleeping most of the time. A controller sending commands to a sleeping actuator node via ROLL devices will have no problems delivering the packet to the nearest powered router, but that router may experience a delay until the next wake-up time before the command can be delivered.

#### **2.6. Remote Video Surveillance**

Remote video surveillance is a fairly classic application for Home networking providing the ability for the end user to get a video stream from a Web Cam reached via the Internet. The video stream may be triggered by the end-user after receiving an alarm from a sensor (movement or smoke detector) or the user simply wants to check the home status via video.

Note that in the former case, more than likely, there will be a form of inter-device communication: Upon detecting some movement in the home, the movement sensor may send a request to the light controller to turn on the lights, to the Web Cam to start a video stream that would then be directed to the end user's cell phone or Personal Digital Assistant (PDA) via the Internet.

In contrast to other applications, e.g. industrial sensors, where data would mainly be originated by a sensor to a sink and vice versa, this scenario implicates a direct inter-device communication between ROLL devices.

#### **2.7. Healthcare**

By adding communication capability to devices, patients and

elderly citizens may be able to do simple measurements at home.  
Thanks to online devices, a doctor can keep an eye on the



patient's health and receive warnings if a new trend is discovered by automated filters.

Fine-grained daily measurements presented in proper ways may allow the doctor to establish a more precise diagnosis.

Such applications may be realized as wearable products which frequently do a measurement and automatically deliver the result to a data sink locally or over the Internet.

Applications falling in this category are referred to as at-home health reporting. Whether measurements are done in a fixed interval or if they are manually activated, they leave all processing to the receiving data sink.

A more active category of applications may send an alarm if some alarm condition is triggered. This category of applications is referred to as at-home health monitoring. Measurements are interpreted in the device and may cause reporting of an event if an alarm is triggered.

Many implementations may overlap both categories.

Since wireless and battery operated systems may never reach 100% guaranteed operational time, healthcare and security systems will need a management layer implementing alarm mechanisms for low battery, report activity, etc.

For instance if a blood pressure sensor did not report a new measurement, say 5 minutes after the scheduled time, some responsible person must be notified.

The structure and performance of such a management layer is outside the scope of the routing requirements listed in this document.

#### **2.7.1. At-home Health Reporting**

Applications might include:

- o Temperature
- o Weight
- o Blood pressure
- o Insulin level

Measurements may be stored for long term statistics. At the same time, a critically high blood pressure may cause the generation of an alarm report. Refer to 2.7.2.

To avoid a high number of request messages, nodes may be configured to autonomously do a measurement and send a report in

intervals.

Brandt

Expires March 16, 2010

[Page 9]

### **2.7.2. At-home Health Monitoring**

An alarm event may become active e.g. if the measured blood pressure exceeds a threshold or if a person falls to the ground. Alarm conditions must be reported with the highest priority and timeliness.

Applications might include:

- o Temperature
- o Weight
- o Blood pressure
- o Insulin level
- o Electrocardiogram (ECG)
- o Position tracker

### **2.8. Alarm Systems**

A home security alarm system is comprised of various sensors (vibration, fire or carbon monoxide, door/window, glass-break, presence, panic button, etc.).

Some smoke alarms are battery powered and at the same time mounted in a high place. Battery-powered safety devices should only be used for routing if no other alternatives exist to avoid draining the battery. A smoke alarm with a drained battery does not provide a lot of safety. Also, it may be inconvenient to exchange battery in a smoke alarm.

Alarm system applications may have both a synchronous and an asynchronous behavior; i.e. they may be periodically queried by a central control application (e.g. for a periodical refreshment of the network state), or send a message to the control application on their own initiative.

When a node (or a group of nodes) identifies a risk situation (e.g. intrusion, smoke, fire), it sends an alarm message to a central controller that could autonomously forward it via Internet or interact with other network nodes (e.g. try to obtain more detailed information or ask other nodes close to the alarm event).

Finally, routing via battery-powered nodes may be very slow if the nodes are sleeping most of the time (they could appear unresponsive to the alarm detection). To ensure fast message delivery and avoid battery drain, routing should be avoided via sleeping devices.

Brandt

Expires March 16, 2010

[Page 10]

### 3. Unique Routing Requirements of Home Automation Applications

Home automation applications have a number of specific routing requirements related to the set of home networking applications and the perceived operation of the system.

The relations of use cases to requirements are outlined in the table below:

+-----+   Use case +-----+	+-----+   Requirement +-----+
2.1. Lighting Application In   Action 	3.2. Support of Mobility   3.5. Scalability 
+-----+	+-----+
2.2. Energy Conservation and   Optimizing Energy Consumption	3.1. Constraint-based Routing 
+-----+	+-----+
2.3. Moving a Remote Control   Around	3.2. Support of Mobility   3.6. Convergence Time 
+-----+	+-----+
2.4. Adding A New Module To The   System	3.6. Convergence Time   3.7. Manageability 
+-----+	+-----+
2.5. Controlling Battery   Operated Window Shades	3.3. Sleeping Nodes 
+-----+	+-----+
2.6. Remote Video Surveillance 	3.3. Sleeping Nodes   3.6. Convergence Time 
+-----+	+-----+
2.7. Healthcare     	3.1. Constraint-based Routing   3.2. Support of Mobility   3.4. Healthcare Routing   3.6. Convergence Time 
+-----+	+-----+
2.8. Alarm Systems 	3.5. Scalability   3.6. Convergence Time 
+-----+	+-----+

#### 3.1. Constraint-based Routing

For convenience and low operational costs, power consumption of consumer products must be kept at a very low level to achieve a long battery lifetime. One implication of this fact is that Random Access Memory (RAM) is limited and it may even be powered down; leaving only a few 100 bytes of RAM alive during the sleep phase.

Brandt

Expires March 16, 2010

[Page 11]

The use of battery powered devices reduces installation costs and does enable installation of devices even where main power lines are not available. On the other hand, in order to be cost effective and efficient, the devices have to maximize the sleep phase with a duty cycle lower than 1%.

Some devices only wake up in response to an event, e.g. a push button.

Simple battery-powered nodes such as movement sensors on garage doors and rain sensors may not be able to assist in routing. Depending on the node type, the node never listens at all, listens rarely or makes contact on demand to a pre-configured target node. Attempting to communicate to such nodes may at best require long time before getting a response.

Other battery-powered nodes may have the capability to participate in routing. The routing protocol **SHOULD** route via mains-powered nodes if possible.

The routing protocol **MUST** support constraint-based routing taking into account node properties (CPU, memory, level of energy, sleep intervals, safety/convenience of changing battery).

### **3.2. Support of Mobility**

In a home environment, although the majority of devices are fixed devices, there is still a variety of mobile devices: for example a multi-purpose remote control is likely to move. Another example of mobile devices is wearable healthcare devices.

While healthcare devices delivering measurement results can tolerate route discovery times measured in seconds, a remote control appears unresponsive if using more than 0.5 seconds to e.g. pause the music.

While, in theory, all battery-powered devices and mains-powered plug-in modules may be moved, the predominant case is that the sending node has moved while the rest of the network has not changed.

The routing protocol **MUST** provide mobility with convergence time below 0.5 second if only the sender has moved.

In more rare occasions, receiving nodes may also have moved. Examples include safety-off switch in a clothes iron or the wireless chime of doorbell set.

The routing protocol **MUST** provide mobility with convergence time

below 4 seconds if the receiver has moved.

Brandt

Expires March 16, 2010

[Page 12]



A non-responsive node can either be caused by 1) a failure in the node, 2) a failed link on the path to the node or 3) a moved node. In the first two cases, the node can be expected to reappear at roughly the same location in the network, whereas it can return anywhere in the network in the latter case.

### **3.3. Sleeping Nodes**

Sleeping nodes may appear to be non-responsive. The routing protocol MUST take into account the delivery time to a sleeping target node.

### **3.4. Healthcare Routing**

Because most health care applications may run on battery, this leads to specific requirements for the routing protocol. Most health care applications may also be portable and therefore need to locate a new neighbor router on a frequent basis.

Not being powered most of the time, the nodes should not be used as routing nodes. However, battery-powered nodes may be involved in routing. Examples include cases where a person falls during a power blackout. In that case it may be that no mains-powered routers are available for forwarding the alarm message to a (battery-backed) internet gateway located out of direct range.

Delivery of measurement data has a more relaxed requirement for route discovery time compared to a remote control. On the other hand, it is critical that a "person fell" alarm is actually delivered.

If possible at all, the routing protocol MUST deliver a health-care related message. It is NOT a requirement that such message is delivered in less than a second.

The routing protocol SHOULD support acknowledged transmission. If the routing protocol does not support acknowledged transmission, some higher-layer transport protocol or application MUST ensure delivery of such messages.

### **3.5. Scalability**

Looking at the number of wall switches, power outlets, sensors of various nature, video equipment and so on in a modern house, it seems quite realistic that hundreds of low power devices may form a home automation network in a fully populated "smart" home. Moving towards professional building automation, the number of such devices may be in the order of several thousands.

The routing protocol MUST support 250 devices in the network.

Brandt

Expires March 16, 2010

[Page 13]

### **3.6. Convergence Time**

A wireless home automation network is subject to various instabilities due to signal strength variation, moving persons and the like. Furthermore, as the number of devices increases, the probability of a node failure also increases.

Measured from the transmission of a packet, the following convergence time requirements apply.

The routing protocol MUST converge within 0.5 second if no nodes have moved.

The routing protocol MUST converge within 2 seconds if the destination node of the packet has moved.

In both cases, "converge" means "the originator node has received a response from the destination node".

### **3.7. Manageability**

The ability of the home network to support auto-configuration is of the utmost importance. Indeed, most end users will not have the expertise and the skills to perform advanced configuration and troubleshooting. Thus the routing protocol designed for home automation networks MUST provide a set of features including zero-configuration of the routing protocol for a new node to be added to the network. From a routing perspective, zero-configuration means that a node can obtain an address and join the network on its own, without human intervention.

### **3.8. Stability**

The routing protocol MUST support the ability to isolate a misbehaving node thus preserving the correct operation of the overall network.

In other words, if a node is found to fail often compared to the rest of the network, this node should not be the first choice for routing of traffic.

## **4. Traffic Pattern**

Depending on the design philosophy of the home network, wall switches may be configured to directly control individual lamps or alternatively, all wall switches send control commands to a central lighting control computer which again sends out control commands to relevant devices.

Brandt

Expires March 16, 2010

[Page 14]

In a distributed system, the traffic tends to be multipoint-to-multipoint. In a centralized system, it is a mix of multipoint-to-point and point-to-multipoint.

Wall switches only generate traffic when activated, which typically happens from a one to tens of times per hour.

Remote controls have a similar transmit pattern to wall switches, but are activated more frequently.

Temperature/air pressure/rain sensors send frames when queried by the user or can be preconfigured to send measurements at fixed intervals (typically minutes). Motion sensors typically send a frame when motion is first detected and another frame when an idle period with no movement has elapsed. The highest transmission frequency depends on the idle period used in the sensor. Sometimes, a timer will trigger a frame transmission when an extended period without status change has elapsed.

All frames sent in the above examples are quite short, typically less than 5 bytes of payload. Lost frames and interference from other transmitters may lead to retransmissions. In all cases, acknowledgment frames with a size of a few bytes are used.

As mentioned in the introduction, all messages are carried in IPv6 packets; typically as UDP but ICMP echo and other types may also appear.

In order to save bandwidth, the transport layer will typically be using header compression [[I-D.Hui-HeaderCompression](#)].

## 5. Security Considerations

As every network, HC-LLNs are exposed to routing security threats that need to be addressed. The wireless and distributed nature of these networks increases the spectrum of potential routing security threats. This is further amplified by the resource constraints of the nodes, thereby preventing resource-intensive routing security approaches from being deployed. A viable routing security approach SHOULD be sufficiently lightweight that it may be implemented across all nodes in a HC-LLN. These issues require special attention during the design process, so as to facilitate a commercially attractive deployment.

The HC-LLN MUST deny any node that has not been authenticated to the HC-LLN and authorized to participate to the routing decision process.

An attacker SHOULD be prevented from manipulating or disabling the routing function, for example, by compromising routing control

Brandt

Expires March 16, 2010

[Page 15]

messages. To this end, the routing protocol(s) MUST support message integrity.

Further examples of routing security issues that may arise are the abnormal behavior of nodes that exhibit an egoistic conduct, such as not obeying network rules or forwarding no or false packets. Other important issues may arise in the context of denial-of-service (DoS) attacks, malicious address space allocations, advertisement of variable addresses, a wrong neighborhood, etc. The routing protocol(s) SHOULD support defense against DoS attacks and other attempts to maliciously or inadvertently cause the mechanisms of the routing protocol(s) to over-consume the limited resources of LLN nodes, e.g., by constructing forwarding loops or causing excessive routing protocol overhead traffic, etc.

The properties of self-configuration and self-organization that are desirable in a HC-LLN introduce additional routing security considerations. Mechanisms MUST be in place to deny any node that attempts to take malicious advantage of self-configuration and self-organization procedures. Such attacks may attempt, for example, to cause DoS, drain the energy of power-constrained devices, or to hijack the routing mechanism. A node MUST authenticate itself to a trusted node that is already associated with the HC-LLN before the former can take part in self-configuration or self-organization. A node that has already authenticated and associated with the HC-LLN MUST deny, to the maximum extent possible, the allocation of resources to any unauthenticated peer. The routing protocol(s) MUST deny service to any node that has not clearly established trust with the HC-LLN.

If connected to a backbone network, the HC-LLN SHOULD be capable of limiting the resources utilized by nodes in said backbone network so as not to be vulnerable to DoS. This should typically be handled by border routers providing access from a backbone network to resources in the HC-LLN.

With low computation power and scarce energy resources, HC-LLNs' nodes may not be able to resist any attack from high-power malicious nodes (e.g., laptops and strong radios). However, the amount of damage generated to the whole network SHOULD be commensurate with the number of nodes physically compromised. For example, an intruder taking control over a single node SHOULD NOT be able to completely deny service to the whole network.

In general, the routing protocol(s) SHOULD support the implementation of routing security best practices across the HC-LLN. Such an implementation ought to include defense against, for

example, eavesdropping, replay, message insertion, modification, and man-in-the-middle attacks.



The choice of the routing security solutions will have an impact on the routing protocol(s). To this end, routing protocol(s) proposed in the context of HC-LLNs MUST support authentication and integrity measures and SHOULD support confidentiality (routing security) measures.

## **6. IANA Considerations**

This document includes no request to IANA.

## **7. Acknowledgments**

J. P. Vasseur, Jonathan Hui, Eunsook "Eunah" Kim, Mischa Dohler and Massimo Maggiorotti are gratefully acknowledged for their contributions to this document.

This document was prepared using 2-Word-v2.0.template.dot.

## **8. Disclaimer for pre-RFC5378 work**

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

## **9. References**

### **9.1. Normative References**

- [I-D.Vasseur-Terminology] Vasseur, JP. "Terminology in Low power And Lossy Networks", [draft-vasseur-roll-terminology-02](#) (work in progress), October 2008.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [I-D.Hui-HeaderCompression] Hui, J., "Compression Format for IPv6 Datagrams in 6LoWPAN Networks ", [draft-ietf-6lowpan-hc](#) (work in progress), December 2008.

Brandt

Expires March 16, 2010

[Page 17]

## **9.2. Informative References**

- [RFC5548] Dohler, M., "Routing Requirements for Urban Low-Power and Lossy Networks", [BCP 14](#), [RFC 5548](#), May 2009.
- [I-D.Pister-Industrial-reqs] Pister, K., "Industrial Routing Requirements in Low Power and Lossy Networks ", [draft-ietf-roll-indus-routing-reqs](#) (work in progress)
- [I-D.Martocci-Building-reqs] Martocci, J., "Building Automation Routing Requirements in Low Power and Lossy Networks ", [draft-ietf-roll-building-routing-reqs](#) (work in progress)
- [I-D.Lewis-Protocols-survey] Lewis, P. "Overview of Existing Routing Protocols for Low Power and Lossy Networks", [draft-ietf-roll-protocols-survey](#) (work in progress)

### Author's Addresses

Anders Brandt

Sigma Designs, Inc.  
Emdrupvej 26  
Copenhagen, DK-2100  
Denmark

Email: [abr@zen-sys.com](mailto:abr@zen-sys.com)

Jakob Buron  
Sigma Designs, Inc.  
Emdrupvej 26  
Copenhagen, DK-2100  
Denmark

Email: [jbu@zen-sys.com](mailto:jbu@zen-sys.com)

Giorgio Porcu  
Telecom Italia  
Piazza degli Affari, 2  
20123 Milan  
Italy

Email: [giorgio.porcu@guest.telecomitalia.it](mailto:giorgio.porcu@guest.telecomitalia.it)

Brandt

Expires March 16, 2010

[Page 18]

Internet-Draft [draft-ietf-roll-home-routing-regs](#) September 16, 2009

#### Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

