Networking Working Group
Internet Draft
Intended status: Informational
Expires: January 2009

A. Brandt
Zensys, Inc.
G. Porcu
Telecom Italia

July 14, 2008

Home Automation Routing Requirement in Low Power and Lossy Networks
draft-ietf-roll-home-routing-reqs-02

Status of this Memo

Copyright Notice

Abstract

This document presents home control and automation application specific requirements for ROuting in Low power and Lossy networks (ROLL). In a modern home, a high number of wireless devices are used for a wide set of purposes. Examples include lighting control, heating control, sensors, leak detectors, healthcare systems and advanced remote controls. Because such devices only cover a limited

radio range, multi-hop routing is often required. The aim of this document is to specify the routing requirements for networks comprising such constrained devices in a home network 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].

Table of Contents

1. Terminology

ROLL: ROuting in Low-power and Lossy networks

ROLL device: A ROLL network node with constrained CPU and memory resources; potentially constrained power resources.

Access Point: The access point is an infrastructure device that connects the low power and lossy network system to the Internet, possibly via a customer premises local area network (LAN).

LAN: Local Area Network.

PAN: Personal Area Network.
A geographically limited wireless network based on e.g. 802.15.4 or Z-Wave radio.

Channel: Radio frequency band used to transmit a modulated signal carrying packets.

Downstream: Data direction traveling from a Local Area Network (LAN) to a Personal Area Network (PAN) device.

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

Sensor: A PAN device that measures data and/or detects an event.

2. Introduction

This document presents the home control and automation application specific requirements for Routing in Low power and Lossy Networks (ROLL). In a modern home, a high number of wireless devices are used for a wide set of purposes. Examples include lighting control modules, heating control panels, light sensors, temperature sensors, gas/water leak detectors, motion detectors, video surveillance, healthcare systems and advanced remote controls. 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.

Because such devices only cover a limited radio range, multi-hop 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".

Unlike other categories of PANs, the connected home area is very much consumer-oriented. The implications on network nodes in this aspect, 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. Often, the radio uses the same power for listening as for transmitting.

Section 3 describes a few typical use cases for home automation applications. Section 4 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 requirements.

3. Home automation applications

Home automation applications represent a special segment of networked wireless devices with its unique set of requirements. To facilitate the requirements discussion in Section 4, 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. For instance a lamp may be turned on, not only be a wall switch but also from a movement sensor.

3.1. Turning off the house when leaving

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 use a clever mix of a "subnet groupcast"

message with no acknowledgement and no forwarding before sending acknowledged singlecast messages to each lighting device.

The controller forms the groups and decides which nodes should receive "turn-off" or "turn-on" requests.

3.2. Energy conservation and optimizing energy consumption

Parts of the world using air conditioning may let shades go down and turn off the AC device when leaving home. Air conditioning may start by timer or via motion sensor when the owner returns home. The owner may even activate the air conditioning via cell phone before getting home.

Geographical areas using central heating may turn off heating when not at home and use 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. 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 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. Wireless remote control of the household appliances is well-suited for this application. The start/stop decision for the appliances can be regulated by dynamic power pricing information obtained from the electricity utility companies. Moreover, in order to achieve effective electricity savings, the energy monitoring application running on the Wireless Sensor Network (WSN) must guarantee that the power consumption of the ROLL devices is much lower than that of the appliance itself.

Most of these applications 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.

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

3.4. Adding a new lamp 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.

Distribution of unique addresses is usually performed by a central controller. In this case, it must be possible to route the inclusion request from the joining node to the central controller even before the joining node is assigned a unique address.

3.5. 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, the receiver is sleeping most of the time. A home automation controller sending commands to window shades via ROLL devices will have no problems delivering the packet to the router, but the router may have to wait for some time before the command can be delivered to the window shades if the receiver is sleeping; e.g. up to 250ms.

3.6. 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, which can be triggered by the end-user that has received an alarm from a movement sensor 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: indeed, 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 (cell phone, PDA) via the Internet.
By contrast with other applications, e.g. industrial sensors where data would mainly be originated by sensor to a sink and vice versa, this scenario implicates a direct inter-device communication between ROLL devices.

3.7. 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.

3.7.1. At-home health reporting

Applications might include:

- Temperature
- Weight
- Blood pressure
- 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 3.7.2.

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

3.7.2. 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.

Applications might include:

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

3.7.3. Healthcare routing considerations

From a ROLL perspective, all the above-mentioned applications may run on battery. They 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, sleeping, 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 in the end.

3.8. Alarm systems

A home security alarm system is comprised of various devices like vibration detectors, fire or carbon monoxide detection system, door or window contacts, glass-break detector, presence sensor, panic button, home security key.

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 basing upon the status of the environment they monitor.

When a node (or a group of nodes) identifies a risk situation (e.g. intrusion, smoke, fire), it sends an alarm message to the control centre that could autonomously forward it via Internet or interact with the WSN (e.g. trying to obtain more detailed information or asking to other nodes close to the alarm event). Alarm messages have, obviously, strict low-latency requirements.

Finally, routing via battery-powered nodes may be very slowly reacting 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 this category of devices.

3.9. Battery-powered devices

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 RAM memory is limited and it may even be powered down; leaving only a few 100 bytes of RAM alive during the sleep phase.

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 10%.

4. Unique requirements of home automation applications

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

4.1. Support of groupcast

Groupcast, in the context of home automation, is defined as the ability to simultaneously transmit a message to a group of recipients

without prior interaction with the group members (i.e. group setup). A use-case for groupcast is given in Section 3.1.

Broadcast and groupcast in home automation MAY be used to deliver the illusion that all recipients respond simultaneously. Distant recipients out of direct range may not react to the (unacknowledged) groupcast. Acknowledged unicast delivery MUST be used subsequently.

The support of unicast, groupcast and broadcast also has an implication on the addressing scheme and are outside the scope of this document that focuses on the routing requirements aspects.

It MUST be to possible to address a group of receivers known by the sender even if the receivers do not know that they have been grouped by the sender.

4.2. Constraint-based Routing

Simple battery-powered nodes such as movement sensors on garage doors and rain meters 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 require long time before getting a response.

Other battery-powered nodes may have the capability to participate in routing. The routing protocol should either share the load between nodes to preserve battery or only route via mains-powered nodes if possible. The most reliable routing resource may be a battery-backed, mains-powered smoke alarm.

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).

4.3. 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.

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. The search strategy in the routing protocol will behave differently depending on this expectation. The routing protocol SHOULD make use of the fact that if not being able to deliver a packet, it is most likely that the sending node moved; rather than a failure occurred in that node or in a link on the path towards it.

4.4. Support of Periodical Scanning

The routing protocol MUST support the recognition of neighbors and periodical scanning. This process SHOULD preserve energy capacity as much as possible.

(Derived from use case 3.8. Alarm Systems)

4.5. 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.

Thus, the routing protocol MUST support 250 devices in a subnet.
The routing protocol SHOULD support 2500 devices in a subnet.

4.6. Convergence Time

A home automation Personal Area Network (PAN) is subject to various instability 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.

4.7. 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 PAN MUST provide a set of features including zero-configuration of the routing protocol for a new node to be added to the network. From ROLL perspective, zero-configuration means that a node can obtain an address and join the network on its own, without human intervention.

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

5. Traffic Pattern

Depending on the 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.

In a distributed system, the traffic tends to be any-to-many. In a centralized system, it is a mix of any-to-one and one-to-many.

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.

6. Open issues

Other items to be addressed in further revisions of this document include:

- Load Balancing (Symmetrical and Asymmetrical)
- Security

7. Security Considerations

Encryption can be employed to provide confidentiality, integrity and authentication of the messages carried on the wireless links. Adding these capabilities to the ROLL devices will degrade energy efficiency and increase cost, so a trade-off must be made for each specific application.

Door locks, alarm sensors and medication dosage equipment are examples where strong encryption and authentication are needed. The command to unlock a door must be authenticated, as must the communication between an alarm sensor and the central alarm controller. Furthermore, traffic analysis of the alarm system communication must not reveal if the alarm is activated.

Light dimmers, window shades, motion sensors, weight sensors etc. may not need encryption.

Protection against unintentional inclusion in neighboring networks must be provided. Providing confidentiality, integrity and authentication against malicious opponents is optional.

8. IANA Considerations

This document includes no request to IANA.

9. 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.

10. References

10.1. Normative References

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

10.2. Informative References

Author's Addresses

Anders Brandt
Zensys, Inc.
Emdrupvej 26
Copenhagen, DK-2100
Denmark

Email: abr@zen-sys.com

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

Email: giorgio.porcu@guest.telecomitalia.it

Intellectual Property Statement

made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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