Roll
Internet-Draft
Intended status: Informational
Expires: August 17, 2014

A. Brandt
Sigma Designs
E. Baccelli
INRIA
R. Cragie
Gridmerge
P. van der Stok
Consultant

February 13, 2014

Applicability Statement: The use of the RPL protocol set in Home Automation and Building Control
draft-ietf-roll-applicability-home-building-02

Abstract

The purpose of this document is to provide guidance in the selection and use of RPL protocols to implement the features required for control in building and home environments.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on August 17, 2014.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Terminology 3
1.2. Required Reading 4
1.3. Out of scope requirements 4
2. Deployment Scenario 4
2.1. Network Topologies 5
2.2. Traffic Characteristics 6
2.2.1. General 7
2.2.2. Source-sink (SS) communication paradigm 7
2.2.3. Publish-subscribe (PS, or pub/sub)) communication paradigm 7
2.2.4. Peer-to-peer (P2P) communication paradigm 8
2.2.5. Peer-to-multipeer (P2MP) communication paradigm . . . 8
2.2.6. N-cast communication paradigm 8
2.2.7. RPL applicability per communication paradigm 8
2.3. Layer-2 applicability 10
3. Using RPL to meet Functional Requirements 10
4. RPL Profile 11
4.1. RPL Features 11
4.1.1. RPL Instances 11
4.1.2. Storing vs. Non-Storing Mode 12
4.1.3. DAO Policy 12
4.1.4. Path Metrics 12
4.1.5. Objective Function 12
4.1.6. DODAG Repair 12
4.1.7. Multicast 12
4.1.8. Security 13
4.1.9. P2P communications 13
4.1.10. IPv6 adddress configuration 13
4.2. Layer 2 features 14
4.3. Recommended Configuration Defaults and Ranges 14
4.3.1. RPL-P2P parameters 14
4.3.2. Trickle parameters 14
4.3.3. MPL parameters 14
5. Manageability Considerations 15
6. Security Considerations 15
6.1. Security context considerations 15
6.2. MPL routing 16
6.3. Security Considerations for distribution of credentials required for RPL 16
6.4. Security Considerations for P2P uses 16

7. Other related protocols 17
8. IANA Considerations 17
9. Acknowledgements 17
10. Changelog 17
11. References 18
11.1. Normative References 18
11.2. Informative References 20
Appendix A. RPL shortcomings in home and building deployments . 21
A.1. Risk of undesired long P2P routes 21
A.1.1. Traffic concentration at the root 21
A.1.2. Excessive battery consumption in source nodes 22
A.2. Risk of delayed route repair 22
A.2.1. Broken service 22
Appendix B. Communication failures 22
Authors' Addresses 24

1. Introduction

Home automation and building control application spaces share a substantial number of properties.

- Both (home and building) can be disconnected from the ISP and they will (must) continue to provide control to the occupants of the home c.q. building. This has an impact on routing because most control communication does (must) not pass via the border routers.

- Both are confronted with unreliable links and want instant very reliable reactions. This has impact on routing because of timeliness and multipath routing.

- The difference between the two mostly appears in the commissioning, maintenance and user interface which does not affect the routing.

So the focus of this applicability document is control in buildings and home, involving: reliability, timeliness, and local routing.

The purpose of this document is to give guidance in the use of the RPL protocol suite to provide the features required by the requirements documents "Home Automation Routing Requirements in Low-Power and Lossy Networks" [RFC5826] and "Building Automation Routing Requirements in Low-Power and Lossy Networks" [RFC5867].

1.1. 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].

Additionally, this document uses terminology from [RFC6997], [I-D.ietf-roll-trickle-mcast], and [RFC6550].

1.2. Required Reading

Applicable requirements are described in [RFC5826] and [RFC5867].

1.3. Out of scope requirements

The considered network diameter is limited to a max diameter of 10 hops and a typical diameter of 5 hops, which captures the most common cases in home automation and building control networks.

This document does not consider the applicability of RPL-related specifications for urban and industrial applications [RFC5548], [RFC5673], which may exhibit significantly larger network diameters.

2. Deployment Scenario

The use of communications networks in buildings is essential to satisfy the energy saving regulations. Environmental conditions of buildings can be adapted to suit the comfort of the individuals present. Consequently when no one is present, energy consumption can be reduced. Cost is the main driving factor behind utilizing wireless networking in buildings. Especially for retrofit, wireless connectivity saves cabling costs.

A typical home automation network is comprised of less than 100 nodes. Large building deployments may span 10,000 nodes but to ensure uninterrupted service of light and air conditioning systems in individual zones of the building, nodes are typically organized in sub-networks. Each sub-network in a building automation deployment typically contains tens to hundreds of nodes.

The main purpose of the home or building automation network is to provide control over light and heating/cooling resources. User intervention may be enabled via wall controllers combined with movement, light and temperature sensors to enable automatic adjustment of window blinds, reduction of room temperature, etc. In general, the sensors and actuators in a home or building typically have fixed physical locations and will remain in the same home- or building automation network.

People expect an immediate and reliable response to their presence or actions. A light not switching on after entry into a room may lead to confusion and a profound dissatisfaction with the lighting product.

Monitoring of functional correctness is at least as important. Devices typically communicate their status regularly and send alarm messages notifying a malfunction of equipment or network.

In building control, the infrastructure of the building management network can be shared with the security/access, the IP telephony, and the fire/alarm networks. This approach has a positive impact on the operation and cost of the network.

In homes the network for audio/video streaming and gaming has different requirements, where the most important one is the high need in bandwith for entertainment not needed for control. It is expected that the entertainment network in the home will mostly be separate from the control network.

2.1. Network Topologies

In general, The home automation network or building control network consists of wired and wireless sub-networks. In large buildings especially, the wireless sub-networks can be connected to an IP backbone network where all infrastructure services are located, such as DNS, automation servers, etc.

The wireless sub-network can be configured according to any of the following topologies:

- A stand-alone network of 10-100 nodes without border router. This typically occurs in the home with a stand-alone control network, in low cost buildings, and during installation of high end control systems in buildings.

- A connected network with one border router. This configuration will happen in homes where home appliances are controlled from outside the home or via the telephone, and in many building control scenarios.

- A connected network with multiple border routers. This will typically happen in installations of large buildings.

Many of the nodes are batery-powered and may be sleeping nodes which wake-up according to clock signals or external events.

In a building control network, for large installation with multiple border routers, sub-networks often overlap geographically and from a wireless coverage perspective. Due to two purposes of the network, (i) direct control and (ii) monitoring, there may exist two types of routing topologies in a given sub-network: (i) a tree-shaped collection of routes spanning from a central building controller via

the border router, on to destination nodes in the sub-network; and/or (ii) a flat, un-directed collection of intra-network routes between functionally related nodes in the sub-network.

The majority of nodes in home and building automation networks are typically devices with very low memory capacity, such as individual wall switches. Only a few nodes (such as multi-purpose remote controls) are more expensive devices, which can afford more memory capacity.

2.2. Traffic Characteristics

Traffic may enter the network originating from a central controller or it may originate from an intra-network node. The majority of traffic is light-weight point-to-point control style; e.g. Put-Ack or Get-Response. There are however exceptions. Bulk data transfer is used for firmware update and logging, where firmware updates enter the network and logs leave the network. Group communication is used for service discovery or to control groups of nodes, such as light fixtures.

Often, there is a direct physical relation between a controlling sensor and the controlled equipment. For example the temperature sensor and thermostat are located in the same room sharing the same climate conditions. Consequently, the bulk of senders and receivers are separated by a distance that allows one-hop direct path communication. A graph of the communication will show several fully connected subsets of nodes. However, due to interference, multipath fading, reflection and other transmission mechanisms, the one-hop direct path may be temporally disconnected. For reliability purposes, it is therefore essential that alternative n-hop communication routes exist for quick error recovery. (See Appendix B for motivation.)

Looking over time periods of a day, the networks are very lightly loaded. However, bursts of traffic can be generated by pushing permanently the button of a remote control, the occurrence of a defect, and other unforeseen events. Under those conditions, the timeliness must nevertheless be maintained. Therefore, measures are necessary to remove any unnecessary traffic. Short routes are preferred. Long multi-hop routes via the border router, should be avoided whenever possible.

Group communication is essential for lighting control. For example, once the presence of a person is detected in a given room, lighting control applies to that room only and no other lights should be dimmed, or switched on/off. In many cases, this means that a multicast message with a 1-hop and 2-hop radius would suffice to

control the required lights. The same argument holds for HVAC and other climate control devices. To reduce network load, it is advisable that messages to the lights in a room are not distributed any further in the mesh than necessary based on intended receivers.

2.2.1. General

Whilst air conditioning and other environmental-control applications may accept response delays of tens of seconds or longer, alarm and light control applications may be regarded as soft real-time systems. A slight delay is acceptable, but the perceived quality of service degrades significantly if response times exceed 250 msec. If the light does not turn on at short notice, a user may activate the controls again, thus causing a sequence of commands such as Light{on,off,on,off,..} or Volume{up,up,up,up,up,...}. In addition the repetitive sending of commands creates an unnecessary loading of the network, which in turn increases the bad responsiveness of the network.

2.2.2. Source-sink (SS) communication paradigm

This paradigm translates to many sources sending messages to the same sink, sometimes reachable via the border router. As such, source-sink (SS) traffic can be present in home and building networks. The traffic is generated by environmental sensors (often present in a wireless sub-network) which push periodic readings to a central server. The readings may be used for pure logging, or more often, processed to adjust light, heating and ventilation. Alarm sensors also generate SS style traffic. The central server in a home automation network will be connected mostly to a wired sub-network, although it is suspected that cloud services will become available. The central server in a building automation network may be connected to a backbone or be placed outside the building.

With regards to message latency, most SS transmissions can tolerate worst-case delays measured in tens of seconds. Alarm sensors, however, represent an exception. Special provisions with respect to the location of the Alarm server(s) need to be put in place to respect the specified delays.

2.2.3. Publish-subscribe (PS, or pub/sub)) communication paradigm

This paradigm translates to a number of devices expressing their interest for a service provided by a server device. For example, a server device can be a sensor delivering temperature readings on the basis of delivery criteria, like changes in acquisition value or age of the latest acquisition. In building automation networks, this paradigm may be closely related to the SS paradigm given that

servers, which are connected to the backbone or outside the building, can subscribe to data collectors that are present at strategic places in the building automation network. The use of PS will probably differ significantly from installation to installation.

2.2.4. Peer-to-peer (P2P) communication paradigm

This paradigm translates to a device transferring data to another device often connected to the same sub-network. Peer-to-peer (P2P) traffic is a common traffic type in home automation networks. Some building automation networks also rely on P2P traffic while others send all control traffic to a local controller box for advanced scene and group control. The latter controller boxes can be connected to service control boxes thus generating more SS or PS traffic.

P2P traffic is typically generated by remote controls and wall controllers which push control messages directly to light or heat sources. P2P traffic has a strong requirement for low latency since P2P traffic often carries application messages that are invoked by humans. As mentioned in Section 2.2.1 application messages should be delivered within a few hundred milliseconds - even when connections fail momentarily.

2.2.5. Peer-to-multipeer (P2MP) communication paradigm

This paradigm translates to a device sending a message as many times as there are destination devices. Peer-to-multipeer (P2MP) traffic is common in home and building automation networks. Often, a thermostat in a living room responds to temperature changes by sending temperature acquisitions to several fans and valves consecutively.

2.2.6. N-cast communication paradigm

This paradigm translates to a device sending a message to many destinations in one network transfer invocation. Multicast is well suited for lighting where a presence sensor sends a presence message to a set of lighting devices. Multicast increases the probability that the message is delivered within the strict time constraints. The chosen multicast algorithm (e.g. [I-D.ietf-roll-trickle-mcast]) assures that messages are delivered to ALL destinations.

2.2.7. RPL applicability per communication paradigm

In the case of SS over a wireless sub-network to a server reachable via a border router, the use of RPL [RFC6550] is recommended. Given the low resources of the devices, source routing will be used for messages from outside the wireless sub-network to the destination in

the wireless sub-network. No specific timing constraints are associated with the SS type messages so network repair does not violate the operational constraints. When no SS traffic takes place, it is recommended to load only RPL-P2P code into the network stack to satisfy memory requirements by reducing code.

All P2P and P2MP traffic, taking place within a wireless sub-network, requires P2P-RPL [RFC6997] to assure responsiveness. Source and destination are typically close together to satisfy the living conditions of one room. Consequently, most P2P and P2MP traffic is 1-hop or 2-hop traffic. Appendix A explains why RPL-P2P is preferable to RPL for this type of communication. Appendix B explains why reliability measures such as multi-path routing are necessary even when 1-hop communication dominates.

Additional advantages of RPL-P2P for home and building automation networks are, for example:

- Individual wall switches are typically inexpensive devices with extremely low memory capacities. Multi-purpose remote controls for use in a home environment typically have more memory but such devices are asleep when there is no user activity. RPL-P2P reactive discovery allows a node to wake up and find new routes within a few seconds while memory constrained nodes only have to keep routes to relevant targets.

- The reactive discovery features of RPL-P2P ensure that commands are normally delivered within the 250 msec time window and when connectivity needs to be restored, it is typically completed within seconds. In most cases an alternative (earlier discovered) route will work. Thus, route rediscovery is not even necessary.

- Broadcast storms as happening during road discovery for AODV is less disruptive for P2P-RPL. P2P-RPL has a "STOP" bit which is set by the target of a route discovery to notify all other nodes that no more DIOs should be forwarded for this temporary DAG. Something looking like a broadcast storm may happen when no target is responding. And in this case, the Trickle suppression mechanism kicks in; limiting the number of DIO forwards in dense networks.

Due to the limited memory of the majority of devices, RPL-P2P MUST be used with source routing in non-storing mode as explained in Section 4.1.2.

N-cast over the wireless network will be done using multicast with MPL [I-D.ietf-roll-trickle-mcast]. Configuration constraints that

are necessary to meet reliability and timeliness with MPL are discussed in Section 4.1.7.

2.3. Layer-2 applicability

This document applies to [IEEE802.15.4] and [G.9959] which are adapted to IPv6 by the adaption layers [RFC4944] and [I-D.ietf-6lo-lowpanz].

The above mentioned adaptation layers leverage on the compression capabilities of [RFC6554] and [RFC6282]. Header compression allows small IP packets to fit into a single layer 2 frame even when source routing is used. A network diameter limited to 5 hops helps to achieve this.

Dropped packets are often experienced in the targeted environments. ICMP, UDP and even TCP flows may benefit from link layer unicast acknowledgments and retransmissions. Link layer unicast acknowledgments MUST be enabled when [IEEE802.15.4] or [G.9959] is used with RPL and RPL-P2P.

3. Using RPL to meet Functional Requirements

RPL-P2P MUST be present in home automation and building control networks, as point-to-point style traffic is substantial and route repair needs to be completed within seconds. RPL-P2P provides a reactive mechanism for quick, efficient and root-independent route discovery/repair. The use of RPL-P2P furthermore allows data traffic to avoid having to go through a central region around the root of the tree, and drastically reduces path length [SOFT11] [INTEROP12]. These characteristics are desirable in home and building automation networks because they substantially decrease unnecessary network congestion around the root of the tree.

When reliability is required, multiple independent paths are used with RPL-P2P. For 1-hop destinations this means that one 1-hop communication and a second 2-hop communication take place via a neigboring node. The same reliability can be achieved by using MPL where the seed is a repeater and a second repeater is 1 hop removed from the seed and the destination node.

RPL-P2P is recommended to keep two independent paths per destination in the source. When one path is temporarily impossible, as described in Appendix B, the alternative can be used without throwing away the temporarily failing path. The blocked path can be safely thrown away after 15 minutes. A new route discovery is done when the number of paths is exhausted, or when a path needs to abandoned because it fails over a too long period.

4. RPL Profile

RPL-P2P MUST be used in home automation and building control networks. Non-storing mode allows for constrained memory in repeaters when source routing is used. Reactive discovery allows for low application response times even when on-the-fly route repair is needed.

4.1. RPL Features

An important constraint on the application of RPL is the presence of sleeping nodes.

For example in the stand-alone network, the link layer node (master node, or coordinator)handing out the logical network identifier and unique node identifiers may be a remote control which returns to sleep once new nodes have been added. Due to the absence of the border router there may be no global routable prefixes at all. Likewise, there may be no authoritative always-on root node since there is no border router to host this function.

In a network with a border router and many sleeping nodes, there may be battery powered sensors and wall controllers configured to contact other nodes in response to events and then return to sleep. Such nodes may never detect the announcement of new prefixes via multicast.

In each of the above mentioned constrained deployments, a link layer node (e.g. coordinator or master) SHOULD assume the role as authoritative root node, transmitting singlecast RAs with a ULA prefix information option to nodes during the inclusion process to prepare the nodes for a later operational phase, where a border router is added.

A border router SHOULD be designed to be aware of sleeping nodes in order to support the distribution of updated global prefixes to such sleeping nodes.

One COULD implement gateway-centric tree-based routing and global prefix distribution as defined by [RFC6550]. This would however only work for always-on nodes.

4.1.1. RPL Instances

When operating P2P-RPL on a stand-alone basis, there is no authoritative root node maintaining a permanent RPL DODAG. A node MUST be able to join one RPL instance as an instance is created

during each P2P-RPL route discovery operation. A node MAY be designed to join multiple RPL instances.

4.1.2. Storing vs. Non-Storing Mode

Non-storing mode MUST be used to cope with the extremely constrained memory of a majority of nodes in the network (such as individual light switches).

4.1.3. DAO Policy

A node MAY be designed to join multiple RPL instances; in that case DAO policies may be needed.

DAO policy is out of scope for this applicability statement.

4.1.4. Path Metrics

OF0 is RECOMMENDED. [RFC6551] provides other options. Using other objective functions than OF0 may affect inter-operability.

4.1.5. Objective Function

OF0 MUST be supported and is the RECOMMENDED Objective Function to use. Other Objective Functions MAY be used as well.

4.1.6. DODAG Repair

Since RPL-P2P only creates DODAGs on a temporary basis during route repair, there is no need to repair DODAGs.

TODO: there is a DODAG needed for SS communication.

4.1.7. Multicast

Commercial light deployments may have a need for multicast to distribute commands to a group of lights in a timely fashion. Several mechanisms exist for achieving such functionality; [I-D.ietf-roll-trickle-mcast] is RECOMMENDED for home and building deployments. This section relies heavily on the conclusions of [RT-MPL].

Guaranteeing timeliness is intimately related to the density of the MPL routers. In ideal circumstances the message is propagated as a single wave through the network, such that the maximum delay is related to the number of hops times the smallest repetition interval of MPL. Each forwarder that receives the message, passes the message on to the next hop by repeating the message. When several copies of

a message reach the forwarder, it is specified that the copy need not be repeated. Repetition of the message can be inhibited by a small value of k. To assure timeliness, the value of k should be chosen high enough to make sure that messages are repeated at the first arrival of the message in the forwarder. However, a network that is too dense leads to a saturation of the medium that can only be prevented by selecting a low value of k. Consequently, timeliness is assured by choosing a relatively high value of k but assuring at the same time a low enough density of forwarders to reduce the risk of medium saturation. Depending on the reliability of the network channels, it is advisable to choose the network such that at least 2 forwarders (one forwarder located on the seed) can repeat messages to the same set of destinations.

There are no rules about selecting forwarders for MPL. In buildings with central managment tools, the forwarders can be selected, but in the home is not possible to automatically configure the forwarder topology at this moment.

4.1.8. Security

In order to support low-cost devices and devices running on battery, RPL MAY use either unsecured messages or secured messages. If RPL is used with unsecured messages, link layer security SHOULD be used. If RPL is used with secured messages, the following RPL security parameter values SHOULD be used:

- T = ’0’: Do not use timestamp in the Counter Field.
- Algorithm = ’0’: Use CCM with AES-128
- KIM = ’10’: Use group key, Key Source present, Key Index present
- LVL = 0: Use MAC-32

4.1.9. P2P communications

[RFC6997] MUST be used to accommodate P2P traffic, which is typically substantial in home and building automation networks.

4.1.10. IPv6 adddress configuration

Assigned IP addresses MUST be routable and unique within the routing domain.

4.2. Layer 2 features

No particular requirements exist for layer 2 but for the ones cited in the IP over Foo RFCs.

4.3. Recommended Configuration Defaults and Ranges

The following sections describe the recommended parameter values for RPL-P2P, Trickle, and MPL.

4.3.1. RPL-P2P parameters

RPL-P2P [RFC6997] provides the features requested by [RFC5826] and [RFC5867]. RPL-P2P uses a subset of the frame formats and features defined for RPL [RFC6550] but may be combined with RPL frame flows in advanced deployments.

Parameter values for RPL-P2P are:

- MinHopRankIncrease 1
- MaxRankIncrease 0
- MaxRank 6
- Objective function: OF0

4.3.2. Trickle parameters

Trickle is used to distribute network parameter values to all nodes without stringent time restrictions. Trickle parameter values are:

- DIOIntervalMin 4 = 16 ms
- DIOIntervalDoublings 14
- DIORedundancyConstant 1

4.3.3. MPL parameters

MPL is used to distribute values to groups of devices. In MPL, based on Trickle algorithm, also timeliness should be guaranteed. Under the condition that the density of MPL repeaters can be limited, it is possible to choose low MPL repeat intervals (Imin) connected to k values such that k>2. The minimum value of k is related to:

- Value of Imin. The length of Imin determines the number of packets that can be received within the listening period of Imin.

- Number of repeaters repeating the same 1-hop broadcast message. These repeaters repeat within the same Imin interval, thus increasing the c counter.

Assuming that at most q message copies can reach a given forwarder within the first repeat interval of length Imin, the following MPL parameter values are suggested:

- I_min = 10 - 50.
- I_max = 200 - 400.
- k > q (see condition above).
- max_expiration = 2 - 4.

5. Manageability Considerations

Manageability is out of scope for home network scenarios. In building automation scenarios, central control should be applied based on MIBs.

6. Security Considerations

Refer to the security considerations of [RFC6997], [RFC6550], [I-D.ietf-roll-trickle-mcast].

6.1. Security context considerations

Wireless networks are typically secured at the link-layer to prevent unauthorized parties to access the information exchanged over the links. In mesh networks, it is good practice to create a network of nodes which share the same keys for link layer encryptions and exclude nodes sending non encrypted messages. The consequence is that unauthorized nodes cannot join the mesh. This is ensured with the Protocol for carrying Authentication for Network Access (PANA) Relay Element [RFC6345] with the use of PANA [RFC5191] for network access. A new DTLS based protocol is proposed in [I-D.kumar-dice-dtls-relay].

Unauthorized nodes can access the nodes of the mesh via a router. End-to-end security between applications is recommended by using DTLS [RFC6347] or TLS [RFC5246].

A thorough analysis of security threats and proposed countermeasures relevant to RPL is done in [I-D.ietf-roll-security-threats].

6.2. MPL routing

The routing of MPL is determined by the enabling of the interfaces for specified Multicast addresses. The specification of these addresses can be done via a CoAP application as specified in [I-D.ietf-core-groupcomm]. An alternative is the creation of a MPL MIB and use of SNMPv3 [RFC3411] or CoMI [I-D.vanderstok-core-comi] to specify the Multicast addresses in the MIB. The application of security measures for the specification of the multicast addresses assures that the routing of MPL packets is secured.

6.3. Security Considerations for distribution of credentials required for RPL

Communications network security is based on providing integrity protection and encryption to messages. This can be applied at various layers in the network protocol stack based on using various credentials and a network identity.

The credentials which are relevant in the case of RPL are: (i) the credential used at the link layer in the case where link layer security is applied or (ii) the credential used for securing RPL messages. In both cases, the assumption is that the credential is a shared key. Therefore, there MUST be a mechanism in place which allows secure distribution of a shared key and configuration of network identity. Both MAY be done using (i) pre-installation using an out-of-band method, (ii) delivered securely when a device is introduced into the network or (iii) delivered securely by a trusted neighboring device. The shared key MUST be stored in a secure fashion which makes it difficult to be read by an unauthorized party.

Securely delivering a key means that the delivery mechanism MUST have data origin authentication, confidentiality and integrity protection. Securely storing a key means that the storage mechanism MUST have confidentiality and integrity protection and MUST only be accessible by an authorized party.

6.4. Security Considerations for P2P uses

Refer to the security considerations of [RFC6997]. Many initiatives are under way to provide light weight security such as: [I-D.keoh-dice-dtls-profile-iot] and [I-D.keoh-dice-multicast-security].

7. Other related protocols

Application transport protocols may be CoAP over UDP or equivalents. Typically, UDP is used for IP transport to keep down the application response time and bandwidth overhead.

Several features required by [RFC5826], [RFC5867] challenge the P2P paths provided by RPL. Appendix A reviews these challenges. In some cases, a node may need to spontaneously initiate the discovery of a path towards a desired destination that is neither the root of a DAG, nor a destination originating DAO signaling. Furthermore, P2P paths provided by RPL are not satisfactory in all cases because they involve too many intermediate nodes before reaching the destination.

8. IANA Considerations

No considerations for IANA pertain to this document.

9. Acknowledgements

This document reflects discussions and remarks from several individuals including (in alphabetical order): Mukul Goyal, Jerry Martocci, Charles Perkins, Michael Richardson, and Zach Shelby

10. Changelog

Changes from version 0 to version 1.

- Adapted section structure to template.
- Standardized the reference syntax.
- Section 2.2, moved everything concerning algorithms to section 2.2.7, and adpted text in 2.2.1-2.2.6.
- Added MPL parameter text to section 4.1.7 and section 4.3.1.
- Replaced all TODO sections with text.
- Consistent use of border router, mintoring, home- and building network.
- Reformulated security aspects with references to other publications.
- MPL and RPL parameter values introduced.

Changes form version 1 to version 2.

- Clarified common characteristics of control in home and building.
- Clarified failure behavior of point to point communication in appendix.
- Changed examples, more hvac and less lighting.
- Clarified network topologies.
- replaced reference to smart_object paper by reference to I-D.roll-security-threats
- Added a concise definition of secure delivery and secure storage
- text about securing network with PANA

11. References

11.1. Normative References

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

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

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

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

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

[RFC5673] Pister, K., Thubert, P., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 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., De Mil, P., Riou, N., and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5867, June 2010.

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

[RFC6345] Duffy, P., Chakrabarti, S., Cragie, R., Ohba, Y., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Relay Element", RFC 6345, August 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC6551] Vasseur, JP., Kim, M., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, March 2012.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, March 2012.

[RFC6997] Goyal, M., Baccelli, E., Philipp, M., Brandt, A., and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks", RFC 6997, August 2013.

[I-D.ietf-6lo-lowpanz] Brandt, A. and J. Buron, "Transmission of IPv6 packets over ITU-T G.9959 Networks", draft-ietf-6lo-lowpanz-02 (work in progress), February 2014.

[I-D.ietf-roll-trickle-mcast] Hui, J. and R. Kelsey, "Multicast Protocol for Low power and Lossy Networks (MPL)", draft-ietf-roll-trickle-mcast-06 (work in progress), January 2014.

[I-D.ietf-roll-security-threats]
Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)", draft-ietf-roll-security-threats-06 (work in progress), December 2013.

[I-D.keoh-dice-dtls-profile-iot]
Keoh, S., Kumar, S., and Z. Shelby, "Profiling of DTLS for CoAP-based IoT Applications", draft-keoh-dice-dtls-profile-iot-00 (work in progress), November 2013.

[I-D.keoh-dice-multicast-security]
Keoh, S., Kumar, S., Garcia-Morchon, O., Dijk, E., and A. Rahman, "DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs)", draft-keoh-dice-multicast-security-04 (work in progress), February 2014.

[I-D.kumar-dice-dtls-relay]
Kumar, S., Keoh, S., and O. Garcia-Morchon, "DTLS Relay for Constrained Environments", draft-kumar-dice-dtls-relay-00 (work in progress), October 2013.

[I-D.ietf-core-groupcomm]
Rahman, A. and E. Dijk, "Group Communication for CoAP", draft-ietf-core-groupcomm-18 (work in progress), December 2013.

[I-D.vanderstok-core-comi]
Stok, P. and B. Greevenbosch, "CoAp Management Interfaces", draft-vanderstok-core-comi-02 (work in progress), January 2014.

[IEEE802.15.4]
"IEEE 802.15.4 - Standard for Local and metropolitan area networks -- Part 15.4: Low-Rate Wireless Personal Area Networks", <IEEE Standard 802.15.4>.

[G.9959] "ITU-T G.9959 Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", <ITU-T G.9959>.

11.2. Informative References

[SOFT11] Baccelli, E., Phillip, M., and M. Goyal, "The P2P-RPL Routing Protocol for IPv6 Sensor Networks: Testbed Experiments", Proceedings of the Conference on Software Telecommunications and Computer Networks, Split, Croatia,, September 2011.

[INTEROP12] Baccelli, E., Phillip, M., Brandt, A., Valev , H., and J. Buron , "Report on P2P-RPL Interoperability Testing", RR-7864 INRIA Research Report RR-7864, January 2012.

[RT-MPL] van der Stok, P., "Real-Time IP-based multicast for low-resource wireless network", To be published,, April 2014.

[RTN2011] Holtman, K. and P. van der Stok, "Real-time routing for low-latency 802.15.4 control networks", International Workshop on Real-Time Networks; Euromicro Conference on Real-Time Systems, July 2011.

[MEAS] Holtman, K., "Connectivity loss in large scale IEEE 802.15.4 network", Private Communication, November 2013.

Appendix A. RPL shortcomings in home and building deployments

A.1. Risk of undesired long P2P routes

The DAG, being a tree structure is formed from a root. If nodes residing in different branches have a need for communicating internally, DAG mechanisms provided in RPL [RFC6550] will propagate traffic towards the root, potentially all the way to the root, and down along another branch. In a typical example two nodes could reach each other via just two router nodes but in unfortunate cases, RPL may send traffic three hops up and three hops down again. This leads to several undesired phenomena described in the following sections

A.1.1. Traffic concentration at the root

If many P2P data flows have to move up towards the root to get down again in another branch there is an increased risk of congestion the nearer to the root of the DAG the data flows. Due to the broadcast nature of RF systems any child node of the root is not just directing RF power downwards its sub-tree but just as much upwards towards the root; potentially jamming other MP2P traffic leaving the tree or preventing the root of the DAG from sending P2MP traffic into the DAG because the listen-before-talk link-layer protection kicks in.

A.1.2. Excessive battery consumption in source nodes

Battery-powered nodes originating P2P traffic depend on the route length. Long routes cause source nodes to stay awake for longer periods before returning to sleep. Thus, a longer route translates proportionally (more or less) into higher battery consumption.

A.2. Risk of delayed route repair

The RPL DAG mechanism uses DIO and DAO messages to monitor the health of the DAG. In rare occasions, changed radio conditions may render routes unusable just after a destination node has returned a DAO indicating that the destination is reachable. Given enough time, the next Trickle timer-controlled DIO/DAO update will eventually repair the broken routes, however this may not occur in a timely manner appropriate to the application. In an apparently stable DAG, Trickle-timer dynamics may reduce the update rate to a few times every hour. If a user issues an actuator command, e.g. light on in the time interval between the last DAO message was issued the destination module and the time one of the parents sends the next DIO, the destination cannot be reached. There is no mechanism in RPL to initiate restoration of connectivity in a reactive fashion. The consequence is a broken service in home and building applications.

A.2.1. Broken service

Experience from the telecom industry shows that if the voice delay exceeds 250ms, users start getting confused, frustrated and/or annoyed. In the same way, if the light does not turn on within the same period of time, a home control user will activate the controls again, causing a sequence of commands such as Light{on,off,off,on,off,..} or Volume{up,up,up,up,up,...}. Whether the outcome is nothing or some unintended response this is unacceptable. A controlling system must be able to restore connectivity to recover from the error situation. Waiting for an unknown period of time is not an option. While this issue was identified during the P2P analysis, it applies just as well to application scenarios where an IP application outside the LLN controls actuators, lights, etc.

Appendix B. Communication failures

Measurements on the connectivity between neigbouring nodes are discussed in [RTN2011] and [MEAS].

The work is motivated by the measurements in literature which affirm that the range of an antenna is not circle symmetric but that the signal strength of a given level follows an intricate pattern around

the antenna, and there may be holes within the area delineated by an iso-strength line. It is reported that communication is not symmetric: reception of messages from node A by node B does not imply reception of messages from node B by node A. The quality of the signal fluctuates over time, and also the the height of the antenna within a room can have consequences for the range. As function of the distance from the source, three regions are generally recognized: (1) a clear region with excellent signal quality, (2) a region with fluctuating signal quality, (3) a region without reception. In the text below it is shown that installation of meshes with neigbours in the clear region is not sufficient.

[RTN2011] extends existing work by:

- Observations over periods of at least a week,
- Testing links that are in the clear region,
- Observation in an office building during working hours,
- Concentrating on one-hop and two-hop routes.

Eight nodes were distributed over a surface of 30m2. All nodes are at one hop distance from each other and are situated in the clear region of each other. Each node sends messages to each of its neigbours, and repeats the message until it arrives. The latency of the message was measured over periods of at least a week. It is noticed that latencies longer than a second ocurred without apparent reasons, but only during working days and never in the weekends. Bad periods could last for minutes. By sending messages via two paths: (1) one hop path directly, and (2) two hop path via random neigbour, the probability of delays larger than 100 ms decreased significantly.

The conclusion is that even for 1-hop communication between not too distant "Line of Sight" nodes, there are periods of low reception in which communication deadlines of 200 ms are exceeded. It pays to send a second message over a 2-hop path to increase the reliability of timely message transfer.

[MEAS] confirms that temporary bad reception by close neigbours can occur within other types of areas. Nodes were installed on the ceiling in a grid with a distance of 30-50 cm between nodes. 200 nodes were distributed over an area of 10m x 5m. It clearly transpired that with increasing distance the probability of reception decreases. At the same time a few nodes furthest away from the sender had a high probability of message reception, while some close neigbours of the sender did not receive messages. The patterns of clear reception nodes evolved over time.

The conclusion is that even for direct neighbours reception can temporarily be bad during periods of several minutes. For a reliable and timely communication it is imperative to have at least two communication paths available (e.g. two hop paths next to the 1-hop path for direct neigbours).

Authors' Addresses

Anders Brandt
Sigma Designs

Email: abr@sdesigns.dk

Emmanuel Baccelli
INRIA

Email: Emmanuel.Baccelli@inria.fr

Robert Cragie
Gridmerge

Email: robert.cragie@gridmerge.com

Peter van der Stok
Consultant

Email: consultancy@vanderstok.org