Networking Working Group   M. Dohler
Internet-Draft   G. Madhusudan
Intended status: Informational   G. Chegaray
Expires: June 4, 2008   T. Watteyne
                                                     C. Jacquenet
                                                France Telecom R&D

                                                  December 5, 2007

Urban WSNs Routing Requirements in Low Power and Lossy Networks
draft-dohler-rl2n-urban-routing-reqs-00

Status of this Memo

Copyright Notice

Abstract

   The application specific routing requirements for Urban Low Power and
   Lossy Networks (U-L2Ns) are presented in this document. In the near
   future, sensing and actuating nodes will be placed outdoors in urban
   environments so as to improve the citizens' living conditions as well

as to monitor compliance with increasingly strict environmental laws.
These field nodes are expected to measure and report a wide gamut of
data, such as required in smart metering, waste disposal,
meteorological, pollution and allergy reporting applications. The
majority of these nodes is expected to communicate wirelessly which
- given the limited radio range - requires the use of suitable
multi-hop routing protocols. The design of such protocols will be
mainly impacted by the limited resources of the nodes (memory,
processing power, battery, etc) and the particularities of the
outdoors urban application scenario. As such, for a wireless RL2N
solution to be competitive with other incumbent and emerging
solutions, the protocol ought to be energy-efficient, scalable and
autonomous. This documents aims to specify a set of requirements
reflecting these and further U-L2Ns tailored characteristics.

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

Access Point: The access point is an infrastructure device that connects the low power and lossy network system to a backbone network.

Actuator: a field device that moves or controls equipment.

Field Device: physical device placed in the urban operating environment. Field devices include sensors, actuators and repeaters.

L2N: Low Power and Lossy Network

Schedule: An agreed execution, wake-up, transmission, reception, etc, time-table between two or more field devices.

Timeslot: A fixed time interval that may be used for the transmission or reception of a packet between two field devices. A timeslot used for communications is associated with a slotted-link.

RL2N: Routing in Low power and Lossy Networks

2. Introduction

We detail here some application specific routing requirements for Urban Low Power and Lossy Networks (U-L2Ns). A U-L2N is understood to be a network composed of four key elements, i.e.
 1) sensors,
 2) actuators,
 3) repeaters, and
 4) access points,
which communicate wirelessly.

The access point can be used as:
 1) gateway to a wider infrastructure (e.g. Internet),
 2) data sink (e.g. data collection & processing from sensors), and
 3) data source (e.g. instructions towards actuators).
There can be several access points connected to the same U-L2N; however, the number of access points is well below the amount of sensing nodes. The access points are mainly static, i.e. fixed to a random or pre-planned location, but can be nomadic, i.e. in form of a walking supervisor. Access points may but generally do not suffer from any form of (long-term) resource constraint, except that they need to be small and sufficiently cheap.

Repeaters generally act as relays with the aim to close coverage and
routing gaps; examples of their use are:
    1) prolong the U-L2N's lifetime,
    2) balance nodes' energy depletion,
    3) build advanced sensing infrastructures.
There can be several repeaters supporting the same U-L2N; however, the
number of repeaters is well below the amount of sensing nodes. The
repeaters are mainly static, i.e. fixed to a random or pre-planned
location. Repeaters may but generally do not suffer from any form of
(long-term) resource constraint, except that they need to be small and
sufficiently cheap.

Actuator nodes control urban devices upon being instructed by signaling
arriving from access point(s); examples are street or traffic lights.
The amount of actuator points is well below the number of sensing nodes.
Actuators are capable to relay, i.e. route data. Actuators may generally
be mobile but are likely to be static in the majority of near-future
roll-outs. Similar to the access points, actuator nodes do not suffer
from any long-term resource constraints.

Sensing nodes measure a wide gamut of physical data, including but not
limited to:
    1) municipal consumption data, such as the smart-metering of gas,
       water, electricity, waste, etc;
    2) meteorological data, such as temperature, pressure, humidity, sun
       index, strength and direction of wind, etc;
    3) pollution data, such as polluting gases (SO2, NOx, CO, Ozone),
       heavy metals (e.g. Mercury), pH, radioactivity, etc;
    4) ambient data, such as allergic elements (pollen, dust), EM
pollution, noise levels, etc.
Whilst million of sensing nodes may very well be deployed in an urban
area, they are likely to be associated to more than one network where
these networks may or may not communicate between each other. The number
of sensing nodes connected to a single network is expected to be in the
order of 10^2-10^4; this is still very large and unprecedented in
current roll-outs. Deployment of nodes is likely to happen in batches,
i.e. a box of hundreds of nodes arrives and is deployed. The location of
the nodes is random within given topological constraints, e.g. placement
along a road or river. The nodes are highly resource constraint, i.e.
cheap hardware, low memory and no infinite energy source. Different node
powering mechanisms are available, such as:
    1) non-rechargeable battery;
    2) rechargeable battery with regular recharging (e.g. sunlight);
    3) rechargeable battery with irregular recharging (e.g. opportunistic
energy scavenging);

        4) capacitive/inductive energy provision (e.g. active RFID).
The battery life-time is usually in the order of 10-15 years, rendering
network lifetime maximization with battery-powered nodes beyond this
lifespan useless.

The physical and electromagnetic distances between the four keyelements,
i.e. sensors, actuators, repeaters and access points, can generally be
very large, i.e. from several hundreds of meters to one kilometer. Not
every field node is likely to reach the access point in a single hop,
thereby requiring suitable multi-hop routing protocols which manage the
information flow in an energy-efficient manner. Sensor nodes are capable
to relay, i.e. route data.

Unlike traditional ad hoc networks, the information flow in U-L2Ns is
highly directed. There are three main flows to be distinguished:
        1) sensed information from the sensing nodes towards the access
           point(s);
        2) query requests from the access point(s) to the sensing nodes;
           and
        3) control information from the access point(s) to the actuators.
Some of the flows may need the reverse route for delivering
acknowledgements.

Sensed data is likely to be highly correlated in space, time and
observed events; an example of the latter is when temperature and
humidity increase as the day commences. Data may be sensed and delivered
at different rates with both rates being typically fairly low, i.e. in
the range of hours, days, etc. Data may be delivered regularly according
to a schedule or a regular query; it may also be delivered irregularly
after an externally triggered query; it may also be triggered after a
sudden network-internal event or alert. The network hence needs to be
able to adjust to the varying activity duty cycles, as well as to period
and aperiodic traffic. Also, sensed data ought to be secured and
locatable.

Finally, the outdoors deployment of U-L2Ns has also implications for the
interference temperature and hence link reliability and range if ISM
bands are to be used. For instance, if the 2.4GHz ISM band is used to
facilitate communication between U-L2N nodes, then heavily loaded WLAN
hot-spots become a detrimental performance factor jeopardizing the
reliability of the U-L2N.

Section 3 describes a few typical use cases for the urban L2N
applications. Section 4 discusses the routing requirements for networks
comprising such constrained devices in a U-L2N environment. These

requirements may be overlapping requirements derived from other
application-specific requirements documents or as listed in [I-D.culler-
rl2n-routing-reqs].

3. Urban L2N application scenarios

Urban applications represent a special segment of L2Ns with its unique
set of requirements. To facilitate the requirements discussion in
Section 4, this section lists a few typical but not exhaustive
deployment problems and usage cases of U-L2N.

3.1. Deployment of nodes

Contrary to other L2N applications, deployment of nodes is likely to
happen in batches out of a box. Typically, hundreds of nodes are being
shipped by the manufacturer with pre-programmed functionalities which
are then rolled-out by a service provider or subcontracted entities.
Prior or after roll-out, the network needs to be ramped-up. This
initialization phase may include, among others, allocation of addresses,
(hierarchical) roles in the network, synchronization, determination of
schedules, etc.

If initialization is performed prior to roll-out, all nodes are likely
to be in each others 1-hop radio neighborhood. Pre-programmed MAC and
routing protocols may hence fail to function properly, thereby wasting a
large amount of energy. Whilst the major burden will be on resolving MAC
conflicts, any proposed U-L2N routing protocol needs to cater for such a
case.

If initialization is performed after roll-out, nodes will have a finite
set of one-hop neighbors, likely of low cardinality. Any proposed L2N
routing protocol ought to support the autonomous organization and
configuration of the network at lowest possible energy cost [Lu2007].
The result of such organization ought to be that each node or sets of
nodes are uniquely addressable so as to facilitate the set up of
schedules, etc. The L2N protocol hence ought to support unicast and
multicast transmission schemes, among others. Solutions should refrain
from broadcasting.

3.2. Association and disassociation/disappearance of nodes

After the initialization phase and possibly some operational time, new
nodes may be injected into the network as well as existing nodes removed
from the network. The former may be because a removed node is replaced,
denser readings/actuations are needed or the protocol reports

connectivity problems. The latter might be because a node's battery is depleted, the node is removed for maintenance, the node is stolen or accidentally destroyed, etc. Differentiation should be made between node disassociation, where the node has enough time to inform the network about its removal, and disappearance, where the node simply disappears without prior notification.

The protocol hence ought to support the pinpointing of problematic routing areas as well as an organization of the network which facilitates reconfiguration in the case of association and disassociation/disappearance of nodes at lowest possible energy and delay. The latter may include the change of hierarchies, routing paths, schedules, etc. Furthermore, to inform the access point(s) of the node's arrival and association with the network, unicast and multicast should be supported. To inform freshly associated nodes about schedules, roles, etc, unicast ought to be supported.

3.3. Regular measurement reporting

The majority of sensing nodes will be configured to report their readings on a regular basis. The frequency of data sensing and reporting may be different but is generally expected to be fairly low, i.e. in the range of once per hour, per day, etc. The ratio between data sensing and reporting frequencies will determine the memory and data aggregation capabilities of the nodes. Latency of an end-to-end delivery and acknowledgements of a successful data delivery are not vital as sensing outages can be observed at the access point(s) - when, for instance, there is no reading arriving from a given sensor or cluster of sensors within a day. In this case, a query can be launched to check upon the state and availability of a sensing node or sensing cluster.

The protocol hence ought to support a large number of highly directed unicast flows from the sensing nodes or sensing clusters towards the access point or highly directed multicast or anycast flows from the nodes towards multiple access points. Routing paths may depend on the transmitted information, the frequency of reporting, the amount of energy remaining in the routing nodes, the recharging pattern of energy-scavenged nodes, etc. For instance, temperature readings are reported every hour via one set of routing paths, whereas air quality indicators are reported every quarter of an hour via different paths. Or, certain routing areas are avoided at night but heavily used during the day when nodes are scavenging from sunlight.

3.4. Queried measurement reporting

Occasionally, network external data queries can be launched by one or
several access points. For instance, it is desirable to know the level
of pollution at a specific point or along a given road in the urban
environment. The queries' rates of occurrence are not regular but rather
random, where heavy-tail distributions seem appropriate to model their
behavior. Queries do not necessarily need to be reported back to the
same access point from where the query was launched. Round-trip times,
i.e. from the launch of a query from an access point towards the
delivery of the measured data to an access point, are of importance.
However, they are not very stringent where latencies should simply be
sufficiently smaller than typical reporting intervals; for instance, in
the order of seconds or minute. To facilitate the query process, U-L2N
network devices should support unicast and multicast routing
capabilities.

The same approach is also applicable for schedule update, provisioning
of patches and upgrades, etc. In this case, however, the provision of
acknowledgements and the support of broadcast (in addition to unicast
and multicast) are of importance.

3.5. Alert reporting

Rarely, the sensing nodes will measure an event which classifies as
alarm where such a classification is typically done locally within each
node by means of a pre-programmed or prior diffused threshold. Note that
on approaching the alert threshold level, nodes may wish to change their
sensing and reporting cycles. An alarm is likely being registered by a
plurality of sensing nodes where the delivery of a single alert message
with its location of origin suffices in most cases. One example of alert
reporting is if the level of toxic gases rises above a threshold,
thereupon the sensing nodes in the vicinity of this event report the
danger. Another example of alert reporting is when a glass container -
equipped with a sensor measuring its level of occupancy - reports that
the container is full and hence needs to be emptied.

Routes clearly need to be unicast (towards one access point) or
multicast (towards multiple access points). Delays and latencies are
important; however, again, deliveries within seconds should suffice in
most of the cases.

4. Unique requirements of urban L2N applications

Urban low power and lossy network applications have a number of specific requirements related to the set of operating conditions, as exemplified in the previous section.

4.1. Scalability

The large and diverse measurement space of U-L2N nodes - coupled with the typically large urban areas - will yield extremely large network sizes. Current urban roll-outs are composed of sometimes more than hundred nodes; future roll-outs, however, may easily reach numbers in the tenth of thousands. One of the utmost important L2N routing protocol design criteria is hence scalability.

The routing protocol MUST be scalable to be able to accommodate a very large and increasing number of nodes without deteriorating to-be-specified performance parameters below to-be-specified thresholds.

4.2. Parameter constrained routing

Batteries in some nodes may deplete quicker than in others; the existence of one node for the maintenance of a routing path may not be as important as of another node; the battery scavenging methods may recharge the battery at regular or irregular intervals; some nodes may have a larger memory and are hence be able to store more neighborhood information; some nodes may have a stronger CPU and are hence able to perform more sophisticated data aggregation methods; etc.

To this end, the routing protocol MUST support parameter constrained routing, where examples of such parameters have been given in the previous paragraph.

4.3. Support of autonomous and alien configuration

With the large number of nodes, manually configuring and troubleshooting each node is not possible. The network is expected to self-organize and self-configure according to some prior defined rules and protocols, as well as to support externally triggered configurations (for instance through a commissioning tool which may facilitate the organization of the network at a minimum energy cost).

To this end, the routing protocol MUST provide a set of features including 0-configuration at network ramp-up, (network-internal) self-organization and configuration due to topological changes, ability to

support (network-external) patches and configuration updates. For the
latter, the protocol SHOULD support multicast and broadcast addressing.
The protocol SHOULD also support the formation and identification of
groups of field devices in the network.

4.4. Support of highly directed information flows

The reporting of the data readings by a large amount of spatially
dispersed nodes towards a few access points will lead to highly directed
information flows.

To this end, the routing protocol SHOULD support and utilize this fact
to facilitate scalability and parameter constrained routing.

4.5. Support of heterogeneous field devices

The sheer amount of different field devices will unlikely be provided by
a single manufacturer. A heterogeneous roll-out with nodes using
different physical and medium access control layers is hence likely.

To this end, the routing protocols proposed in U-L2N SHOULD support a
variety of different devices without compromising the operability and
energy efficiency of the network.

4.6. Support of multi and groupcast

Some urban sensing systems require low-level addressing of a group of
nodes in the same subnet without any prior creation of multicast groups,
simply carrying a list of recipients in the subnet [draft-brandt-rl2n-
home-routing-reqs-01].

To this end, the routing protocol MUST support multicast, where the
routing protocol MUST provide the ability to route a packet towards a
single field device (unicast) or a set of devices, which explicitly
(multicast) or implicitly (groupcast) belong to the same group/cast.
Note that if groups correspond to a geographical area, groupcast is
synonymous to geocast.

The support of unicast, groupcast and multicast also has an implication
on the addressing scheme but is beyond the scope of this document that
focuses on the routing requirements aspects.

Note: with IP multicast, signaling mechanisms are used by a receiver to
join a group and the sender does not necessarily know the receivers of
the group. What is required is the ability to address a group of

receivers known by the sender even if the receivers do not need to know that they have been grouped by the sender (since requesting each individual node to join a multicast group would be very energy-consuming).

4.7. Network dynamicity

Although mobility is assumed to be low in urban L2Ns, network dynamicity due to node association, disassociation and disappearance is not negligible. This in turn impacts re-organization and re-configuration convergence as well as route establishment times.

To this end, local network dynamics SHOULD NOT impact the entire network to be re-organized or re-reconfigured; however, the network SHOULD be locally optimized to cater for the encountered changes. Convergence and route establishment times SHOULD be significantly lower than the inverse of the smallest reporting cycle.

4.8. Latency

With the exception of alert reporting solutions and to a certain extent queried reporting, U-L2N are delay tolerant as long as the information arrives within a fraction of the inverse of the respective reporting cycle.

To this end, the routing protocol is RECOMMENDED to support minimum latency for alert reporting and time-critical data queries. For regular data reporting, it SHOULD support latencies not exceeding a fraction of the inverse of the respective reporting cycle.

5. Traffic Pattern

tbd

6. Security Considerations

As every network, also U-L2Ns are exposed to security threats which, if not properly addressed, exclude them to be deployed in the envisaged scenarios. The wireless and distributed nature of these networks drastically increases the spectrum of potential security threats; this is further amplified by the serious constraints in node battery power, thereby preventing previously known security approaches to be deployed. Above mentioned issues require special attention during the design process, so as to facilitate a commercially attractive deployment.

A secure communication in a wireless network encompasses three main
elements, i.e. confidentiality (encryption of data), integrity
(correctness of data), and authentication (legitimacy of data). Since
the majority of measured date in U-L2Ns is publicly available, the main
emphasis is on integrity and authenticity of data reportings.
Authentication can e.g. be violated if external sources insert incorrect
data packets; integrity can e.g. be violated if nodes start to break
down and hence commence measuring and relaying data incorrectly.
Nonetheless, some sensor readings as well as the actuator control
signals need to be confidential.

Further example security issues which may arise are the abnormal
behavior of nodes which 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, external attacks aimed at injecting dummy traffic to drain
the network power, etc.

The choice of the security solutions will have an impact onto routing
protocols. To this end, routing protocols proposed in the context of U-
L2Ns MUST support integrity measures and SHOULD support confidentiality
(security) measures.

7. Open Issues

Other items to be addressed in further revisions of this document
include:
    * node mobility; and
    * traffic patterns.

8. IANA Considerations

This document includes no request to IANA.

9. Acknowledgements

10. References

10.1   Normative References

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

10.2   Informative References

[I-D.culler-rl2n-routing-reqs]
J.P. Vasseur and D. Culler, "Routing Requirements for Low-Power Wireless Networks", draft-culler-rl2n-routing-reqs-00 (work in progress), July 2007.

[Lu2007]
J.L. Lu, F. Valois, D. Barthel, M. Dohler, "FISCO: A Fully Integrated Scheme of Self-Configuration and Self-Organization for WSN," IEEE WCNC 2007, Hong Kong, China, 11-15 March 2007, pp. 3370-3375.

[draft-brandt-rl2n-home-routing-reqs-01]
A. Brand and J.P. Vasseur, "Home Automation Routing Requirement in Low Power and Lossy Networks," draft-brandt-rl2n-home-routing-reqs-01 (work in progress), July 2007.

Authors' Addresses

Mischa Dohler
France Telecom R&D
28 Chemin du Vieux Chene
38243 Meylan Cedex
France
Email: mischa.dohler@orange-ftgroup.com

Giyyarpuram Madhusudan
France Telecom R&D
28 Chemin du Vieux Chene
38243 Meylan Cedex
France
Email: giyyarpuram.madhusudan@orange-ftgroup.com

Gabriel Chegaray
France Telecom R&D
28 Chemin du Vieux Chene
38243 Meylan Cedex
France
Email: gabriel.chegaray@orange-ftgroup.com

Thomas Watteyne
France Telecom R&D
28 Chemin du Vieux Chene
38243 Meylan Cedex
France
Email: thomas.watteyne@orange-ftgroup.com

Christian Jacquenet
France Telecom R&D
4 rue du Clos Courtel BP 91226
35512 Cesson Sevigne
France
Email: christian.jacquenet@orange-ftgroup.com

Acknowledgment