Networking Working Group
Internet-Draft
Intended status: Informational
Expires: December 3, 2008

M. Dohler, Ed.
CTTC
T. Watteyne, Ed.
France Telecom R&D
T. Winter, Ed.
Eka Systems

June 30, 2008

Urban WSNs Routing Requirements in Low Power and Lossy Networks
draft-ietf-roll-urban-routing-reqs-01

Status of this Memo

Abstract

The application-specific routing requirements for Urban Low Power and Lossy Networks (U-LLNs) 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 people's 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 and the large number of nodes - requires the use of suitable 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 scenarios. As such, for a wireless ROLL solution to be useful, the protocol(s) ought to be energy-efficient, scalable, and autonomous. This documents aims to specify a set of requirements reflecting these and further U-LLNs 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. Introduction

This document details application-specific routing requirements for Urban Low Power and Lossy Networks (U-LLNs). U-LLN use cases and associated routing protocol requirements will be described.

Section 2 defines terminology useful in describing U-LLNs.

Section 3 provides an overview of U-LLN applications.

Section 4 describes a few typical use cases for U-LLN applications exemplifying deployment problems and related routing issues.

Section 5 describes traffic flows that will be typical for U-LLN applications.

Section 6 discusses the routing requirements for networks comprising such constrained devices in a U-LLN environment. These requirements may be overlapping requirements derived from other application-specific requirements documents or as listed in [I-D.culler-rl2n-routing-reqs].

Section 7 provides an overview of security considerations of U-LLN implementations.

2. 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

AMI: Advanced Metering Infrastructure, part of Smart Grid. Encompasses smart-metering applications.

DA: Distribution Automation, part of Smart Grid. Encompasses technologies for maintenance and management of electrical distribution systems.

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

LLN: Low power and Lossy Network

ROLL: Routing over Low power and Lossy networks

Smart Grid: a broad class of applications to network and automate utility infrastructure.

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

U-LLN: Urban LLN

3. Overview of Urban Low Power Lossy Networks

3.1. Canonical Network Elements

A U-LLN is understood to be a network composed of four key elements, i.e.

1. access points,

2. repeaters,

3. actuators, and

4. sensors

which communicate wirelessly.

3.1.1. Access Points

The access point can be used as:

1. router 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-LLN; 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.

3.1.2. Repeaters

Repeaters generally act as relays with the aim to close coverage and routing gaps; examples of their use are:

1. prolong the U-LLN's lifetime,

2. balance nodes' energy depletion,

3. build advanced sensing infrastructures.

There can be several repeaters supporting the same U-LLN; 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. Repeaters differ from access points in that they do not act as a data sink/source. They differ from actuator and sensing nodes in that they neither control nor sense.

3.1.3. Actuators

Actuator nodes control urban devices upon being instructed by signaling arriving from or being forwarded by the access point(s); examples are street or traffic lights. The amount of actuator points is well below the number of sensing nodes. Some sensing nodes may include an actuator component, e.g. an electric meter node with integrated support for remote service disconnect. Actuators are capable to forward 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.

3.1.4. Sensors

Sensing nodes measure a wide gamut of physical data, including but not limited to:

1. municipal consumption data, such as 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 (SO_2, NO_x, CO, Ozone), heavy metals (e.g. Mercury), pH, radioactivity, etc;

4. ambient data, such as allergic elements (pollen, dust), electromagnetic pollution, noise levels, etc.

A prominent example is a Smart Grid application which consists of a city-wide network of smart meters and distribution monitoring sensors. Smart meters in an urban Smart Grid application will include electric, gas, and/or water meters typically administered by one or multiple utility companies. These meters will be capable of advanced sensing functionalities such as measuring quality of service, providing granular interval data, or automating the detection of alarm conditions. In addition they may be capable of advanced interactive functionalities such as remote service disconnect or remote demand reset. More advanced scenarios include demand response systems for managing peak load, and distribution automation systems to monitor the infrastructure which delivers energy throughout the urban environment. Sensor nodes capable of providing this type of functionality may sometimes be referred to as Advanced Metering Infrastructure (AMI).

3.2. Topology

Whilst millions 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 one other. The number of sensing nodes deployed in the urban environment in support of some applications is expected to be in the order of 10^2-10^7; this is still very large and unprecedented in current roll-outs. The network MUST be capable of supporting the organization of a large number of sensing nodes into regions containing on the order of 10^2 to 10^4 sensing nodes each.

Deployment of nodes is likely to happen in batches, e.g. boxes of hundreds to thousands of nodes arrive and are deployed. The location of the nodes is random within given topological constraints, e.g. placement along a road, river, or at individual residences.

3.3. Resource Constraints

The nodes are highly resource constrained, 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);

5. always on (e.g. powered electricity meter).

In the case of a battery powered sensing node, 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 key elements, 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 routing protocols which manage the information flow in an energy-efficient manner. Sensor nodes are capable of forwarding data.

3.4. Link Reliability

The links between the network elements are volatile due to the following set of non-exclusive effects:

1. packet errors due to wireless channel effects;

2. packet errors due to medium access control;

3. packet errors due to interference from other systems;

4. link unavailability due to network dynamicity; etc.

The wireless channel causes the received power to drop below a given threshold in a random fashion, thereby causing detection errors in the receiving node. The underlying effects are path loss, shadowing and fading.

Since the wireless medium is broadcast in nature, nodes in their communication radios require suitable medium access control protocols which are capable of resolving any arising contention. Some available protocols may cause packets of neighbouring nodes to collide and hence cause a link outage.

Furthermore, the outdoors deployment of U-LLNs also has 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-LLN nodes, then heavily loaded WLAN hot-spots become a detrimental performance factor jeopardizing the functioning of the U-LLN.

Finally, nodes appearing and disappearing causes dynamics in the network which can yield link outages and changes of topologies.

4. Urban LLN Application Scenarios

Urban applications represent a special segment of LLNs 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-LLN.

4.1. Deployment of Nodes

Contrary to other LLN applications, deployment of nodes is likely to happen in batches out of a box. Typically, hundreds to thousands 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, (possibly 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 one another's 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-LLN routing protocol needs to cater for such a case. For instance, 0-configuration and network address allocation needs to be properly supported, etc.

After roll-out, nodes will have a finite set of one-hop neighbors, likely of low cardinality (in the order of 5- 10). However, some nodes may be deployed in areas where there are hundreds of neighboring devices. In the resulting topology there may be regions where many (redundant) paths are possible through the network. Other regions may be dependant on critical links to achieve connectivity with the rest of the network. Any proposed LLN routing protocol ought to support the autonomous organization and configuration of the network at lowest possible energy cost [Lu2007], where autonomy is understood to be the ability of the network to operate without external influence. For example, nodes in urban sensor nodes SHOULD be able to:

- o Dynamically adapt to ever-changing conditions of communication (possible degradation of QoS, variable nature of the traffic (real time vs. non real time, sensed data vs. alerts, node mobility, a combination thereof, etc.),

- o Dynamically provision the service-specific (if not traffic-specific) resources that will comply with the QoS and security requirements of the service,

- o Dynamically compute, select and possibly optimize the (multiple) path(s) that will be used by the participating devices to forward the traffic towards the actuators and/or the access point according to the service-specific and traffic-specific QoS, traffic engineering and security policies that will have to be enforced at the scale of a routing domain (that is, a set of networking devices administered by a globally unique entity), or a region of such domain (e.g. a metropolitan area composed of clusters of sensors).

The result of such organization SHOULD be that each node or set of nodes is uniquely addressable so as to facilitate the set up of schedules, etc.

The U-LLN routing protocol(s) MUST accommodate both unicast and multicast forwarding schemes. The U-LLN routing protocol(s) SHOULD support anycast forwarding schemes. Unless exceptionally needed, broadcast forwarding schemes are not advised in urban sensor networking environments.

4.2. 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 might be because a removed node is replaced or denser readings/actuations are needed or routing protocols report 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 disappearance, where the node disappears without prior notification, and user or node-initiated disassociation ("phased-out"), where the node has enough time to inform the network about its removal.

The protocol(s) hence SHOULD 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, packet forwarding schedules, etc. Furthermore, to inform the access point(s) of the node's arrival and association with the network as well as freshly associated nodes about packet forwarding schedules, roles, etc, appropriate (link state) updating mechanisms SHOULD be supported.

4.3. 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 may not be 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(s) hence MUST support a large number of highly directional 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.

Route computation and selection may depend on the transmitted information, the frequency of reporting, the amount of energy remaining in the nodes, the recharging pattern of energy-scavenged nodes, etc. For instance, temperature readings could be reported every hour via one set of battery-powered nodes, whereas air quality indicators are reported only during daytime via nodes powered by solar energy. More generally, entire routing areas may be avoided at e.g. night but heavily used during the day when nodes are scavenging from sunlight.

4.4. 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-LLN 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 unicast, multicast, and anycast are of importance.

4.5. 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 recycling glass container - equipped with a sensor measuring its level of occupancy - reports that the container is full and hence needs to be emptied.

Routing within urban sensor networks SHOULD require the U-LLN nodes to dynamically compute, select and install different paths towards a same destination, depending on the nature of the traffic. From this perspective, such nodes SHOULD inspect the contents of traffic payload for making routing and forwarding decisions: for example, the analysis of the traffic payload SHOULD be derived into aggregation capabilities for the sake of forwarding efficiency.

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.

5. Traffic Pattern

Unlike traditional ad hoc networks, the information flow in U-LLNs is highly directional. There are three main flows to be distinguished:

1. sensed information from the sensing nodes towards one or a subset of the access point(s);

2. query requests from the access point(s) towards the sensing nodes;

3. control information from the access point(s) towards the actuators.

Some of the flows may need the reverse route for delivering acknowledgements. Finally, in the future, some direct information flows between field devices without access points may also occur.

Sensed data is likely to be highly correlated in space, time and observed events; an example of the latter is when temperature increase and humidity decrease 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 minutes, 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. Data delivery may trigger acknowledgements or maintenance traffic in the reverse direction. The network hence needs to be able to adjust to the varying activity duty cycles, as well as to periodic and sporadic traffic. Also, sensed data ought to be secured and locatable.

Some data delivery may have tight latency requirements, for example in a case such as a live meter reading for customer service in a smart-metering application, or in a case where a sensor reading response must arrive within a certain time in order to be useful. The network SHOULD take into consideration that different application traffic may require different priorities when traversing the network, and that some traffic may be more sensitive to latency.

An U-LLN SHOULD support occasional large scale traffic flows from sensing nodes to access points, such as system-wide alerts. In the example of an AMI U-LLN this could be in response to events such as a city wide power outage. In this scenario all powered devices in a large segment of the network may have lost power and are running off of a temporary `last gasp' source such as a capacitor or small battery. A node MUST be able to send its own alerts toward an access point while continuing to forward traffic on behalf of other devices who are also experiencing an alert condition. The network MUST be able to manage this sudden large traffic flow. It may be useful for the routing layer to collaborate with the application layer to perform data aggregation, in order to reduce the total volume of a large traffic flow, and make more efficient use of the limited energy available.

An U-LLN may also need to support efficient large scale messaging to groups of actuators. For example, an AMI U-LLN supporting a city-wide demand response system will need to efficiently broadcast demand response control information to a large subset of actuators in the system.

Some scenarios will require internetworking between the U-LLN and

another network, such as a home network. For example, an AMI application that implements a demand-response system may need to forward traffic from a utility, across the U-LLN, into a home automation network. A typical use case would be to inform a customer of incentives to reduce demand during peaks, or to automatically adjust the thermostat of customers who have enrolled in such a demand management program. Subsequent traffic may be triggered to flow back through the U-LLN to the utility. The network SHOULD support internetworking, while giving attention to security implications of interfacing, for example, a home network with a utility U-LLN.

6. Requirements of Urban LLN 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.

6.1. Scalability

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

The routing protocol(s) MUST be scalable so as to accommodate a very large and increasing number of nodes without deteriorating to-be-specified performance parameters below to-be-specified thresholds. The routing protocols(s) SHOULD support the organization of a large number of nodes into regions of to-be-specified size.

6.2. 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 constant power source; 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(s) MUST support parameter constrained routing, where examples of such parameters (CPU, memory size, battery level, etc.) have been given in the previous paragraph.

6.3. Support of Autonomous and Alien Configuration

With the large number of nodes, manually configuring and troubleshooting each node is not efficient. The scale and the large number of possible topologies that may be encountered in the U-LLN encourages the development of automated management capabilities that may (partly) rely upon self-organizing techniques. 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(s) 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(s) MUST support multi- and any-cast addressing. The protocol(s) SHOULD also support the formation and identification of groups of field devices in the network.

6.4. 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. For instance, a suitable addressing scheme can be devised which facilitates the data flow. Also, as one gets closer to the access point, the traffic concentration increases which may lead to high load imbalances in node usage.

To this end, the routing protocol(s) SHOULD support and utilize the fact of highly directed traffic flow to facilitate scalability and parameter constrained routing.

6.5. 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 mandate fully interoperable implementations, the routing protocol(s) proposed in U-LLN MUST support different devices and underlying technologies without compromising the operability and energy efficiency of the network.

6.6. Support of Multicast, Anycast, and Implementation of Groupcast

Some urban sensing systems require low-level addressing of a group of nodes in the same subnet, or for a node representative of a group of nodes, without any prior creation of multicast groups, simply carrying a list of recipients in the subnet [I-D.brandt-roll-home-routing-reqs].

Routing protocols activated in urban sensor networks MUST support unicast (traffic is sent to a single field device), multicast (traffic is sent to a set of devices that are subscribed to the same multicast group), and anycast (where multiple field devices are configured to accept traffic sent on a single IP anycast address) transmission schemes [RFC4291] [RFC1546]. Routing protocols activated in urban sensor networks SHOULD accommodate "groupcast" forwarding schemes, where traffic is sent to a set of devices that implicitly belong to the same group/cast.

The support of unicast, groupcast, multicast, and anycast 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 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).

6.7. Network Dynamicity

Although mobility is assumed to be low in urban LLNs, network dynamicity due to node association, disassociation and disappearance, as well as long-term link perturbations is not negligible. This in turn impacts re-organization and re-configuration convergence as well as routing protocol convergence.

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 smallest reporting interval.

6.8. Latency

With the exception of alert reporting solutions and to a certain extent queried reporting, U-LLN are delay tolerant as long as the

information arrives within a fraction of the smallest reporting interval, e.g. a few seconds if reporting is done every 4 hours.

To this end, the routing protocol(s) SHOULD 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 smallest reporting interval. Due to the different latency requirements, the routing protocol(s) SHOULD support the ability of dealing with different latency requirements. The routing protocol(s) SHOULD also support the ability to route according to different metrics (one of which could e.g. be latency).

7. Security Considerations

As every network, U-LLNs are exposed to security threats that MUST be addressed. The wireless and distributed nature of these networks increases the spectrum of potential security threats. This is further amplified by the resource constraints of the nodes, thereby preventing resource intensive security approaches from being deployed. A viable security approach SHOULD be sufficiently lightweight that it may be implemented across all nodes in a U-LLN. These 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).

U-LLN networks SHOULD support mechanisms to preserve the confidentiality of the traffic that they forward. The U-LLN network SHOULD NOT prevent an application from employing additional confidentiality mechanisms.

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.

The U-LLN network MUST deny all routing services to any node who has not been authenticated to the U-LLN and authorized for the use of routing services.

The U-LLN MUST be protected against attempts to inject false or modified packets. For example, an attacker SHOULD be prevented from manipulating or disabling the routing function by compromising routing update messages. Moreover, it SHOULD NOT be possible to

coerce the network into routing packets which have been modified in transit. To this end the routing protocol(s) MUST support message integrity.

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

Consideration SHOULD be given to cases where the U-LLN may interface with other networks such as a home network. The U-LLN SHOULD NOT interface with any external network which has not established trust. The U-LLN SHOULD be capable of limiting the resources granted in support of an external network so as not to be vulnerable to denial of service.

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

In general, the routing protocol(s) SHOULD support the implementation of security best practices across the U-LLN. Such an implementation ought to include defense against, for example, eavesdropping, replay, message insertion, modification, and man-in-the-middle attacks.

The choice of the security solutions will have an impact onto routing

protocol(s). To this end, routing protocol(s) proposed in the context of U-LLNs MUST support integrity measures and SHOULD support confidentiality (security) measures.

8. Open Issues

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

- o node mobility

9. IANA Considerations

This document makes no request of IANA.

10. Acknowledgements

The in-depth feedback of JP Vasseur, Cisco, and Jonathan Hui, Arch Rock, is greatly appreciated.

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.

11.2. Informative References

[I-D.brandt-roll-home-routing-reqs] Brandt, A., "Home Automation Routing Requirement in Low Power and Lossy Networks", draft-brandt-roll-home-routing-reqs-01 (work in progress), May 2008.

[I-D.culler-rl2n-routing-reqs] Vasseur, J. and D. Cullerot, "Routing Requirements for Low Power And Lossy Networks", draft-culler-rl2n-routing-reqs-01 (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.

[RFC1546] Partridge, C., Mendez, T., and W. Milliken, "Host Anycasting Service", RFC 1546, November 1993.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

Authors' Addresses

Mischa Dohler (editor)
CTTC
Parc Mediterrani de la Tecnologia, Av. Canal Olimpic S/N
08860 Castelldefels, Barcelona
Spain

Email: mischa.dohler@cttc.es

Thomas Watteyne (editor)

France Telecom R&D
28 Chemin du Vieux Chene
38243 Meylan Cedex
France

Email: thomas.watteyne@orange-ftgroup.com

Tim Winter (editor)
Eka Systems
20201 Century Blvd. Suite 250
Germantown, MD 20874
USA

Email: tim.winter@ekasystems.com

Christian Jacquenet
France Telecom R&D
4 rue du Clos Courtel BP 91226
35512 Cesson Sevigne
France

Email: christian.jacquenet@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

Dominique Barthel
France Telecom R&D
28 Chemin du Vieux Chene
38243 Meylan Cedex
France

Email: Dominique.Barthel@orange-ftgroup.com

Full Copyright Statement

Intellectual Property