A Survey on Routing Requirements of IPv6 based Low Power and Lossy Network Applications

Sneha K
Associate Professor/ Dept of CSE
BNM Institute of Technology
Bangalore, India
Sneha.k30@gmail.com

Dr. B.G.Prasad
Professor& Head / Dept of CSE
BNM Institute of Technology
Bangalore, India
drbgprasad@gmail.com

Abstract— Class of networks made up of many embedded devices in which links between nodes are unstable and also have limited power, memory and processing resources are called as Low Power and Lossy Networks (LLNs).Routing over LLNs is one of the greatest challenges of current technology.IPv6 has become the standard for LLNs. Protocol like RPL has specifically been designed for IPv6 based LLNs. In this paper we present a survey on routing requirements of IPv6 based Low Power and Lossy Network applications such as Urban routing, Home automation routing, Building automation routing and Industrial routing.

Index Terms—LLNs, RPL, IPv6, Routing Requirements.

1 INTRODUCTION

Low Power Network devices play an important role of our everyday infrastructure. With low-power networked devices such as sensors and actuators, it is important that the networking community gets involved in developing and evaluating network mechanisms for these devices.

LLNs operate with a hard and very small bound on state. They support point-to-point, multipoint-to-point and point-to-multipoint traffic flows. LLNs' link bandwidth is usually in the range of a few dozens of Kbits/s and may greatly vary over time with down-periods that could last dozens of seconds or minutes. Also, the nodes are highly constrained in terms of resources with few Kbytes of RAM, a 8 to 32 bit micro-controller and could be battery operated where energy may dictate the lifetime of the network [1].

Given that the LLN's characteristics are quite unique, the IETF ROLL (Routing over Low Power and Lossy Networks) Working Group concluded that none of the existing routing protocols (RIP, ISIS, OSPF etc.) would meet the LLN's routing requirements. This conclusion led to the design of a new IPv6 routing protocol called RPL (Routing protocol for Low Power and Lossy Networks).Wireless link qualities can vary significantly over time, requiring protocols to make agile decisions yet minimize topology change energy costs. Routing over such Low power and Lossy Networks introduces requirements that the routing protocol has to address [2].
The introduction of IPv6 in LLNs opens the way for large numbers of smart objects to communicate, not only between each other, but also potentially with every other IP device over the Internet. This interconnection of all daily-life objects is leading the way towards an Internet of things [3]. Communicating natively with IPv6, nodes can communicate end-to-end with each other and any arbitrary IP device over the wide-area at the network layer [4]. Low Power networked devices such as sensors can sense, measure and gather information from the environment and based on some local decision process, they can transmit the sensed data to user. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment [5] .Battery is the main power source in a sensor node. Depending on the application and the type of sensors used ,actuators may be incorporated in the sensor[6].
The goal of this paper is to study the routing requirements of various applications of LLNs and get an insight on it. The remainder of the paper is organized as follows: Section II presents application areas of LLNs, Section III presents the routing requirements of LLN applications. Section IV presents the relation of usecases of various LLN applications to the routing requirements.

2 APPLICATIONS OF LLN

There is wide scope of application areas for LLNs including industrial monitoring, building automation, urban sensor networks, home automation, healthcare, environmental monitoring, asset tracking [7].In this paper we have specified the routing requirements for four different application areas as shown in the below fig 1.

.

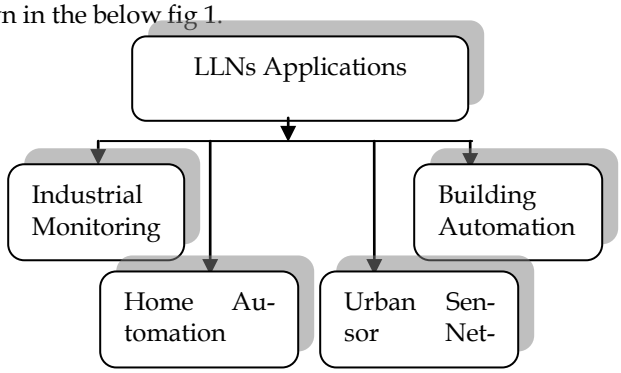


Fig. 1, Application areas of LLN

3 ROUTING REQUIREMENTS OF LLN APPLICATIONS

3.1 INDUSTRIAL –LLN ROUTING REQUIREMENTS [8]

The wireless, low power field devices facilitate a significant increase in the amount of information which industrial users can collect and the number of control points that can be remotely managed. The requirements from the industrial environment for a routing protocol in IPv6 based LLN is as shown in the below fig 2.

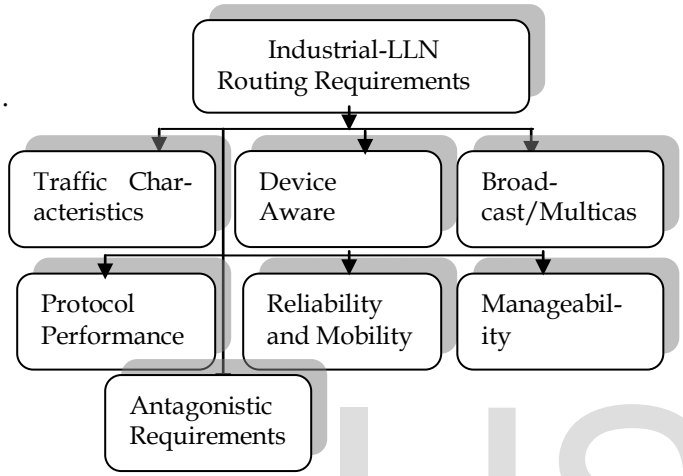


Fig 2, Industrial Routing Requirements in LLN

3.1.1 Requirements related to Traffic characteristics

a) Service Requirements

The service parameters that can affect routing decisions in a resource-constrained network are as follows

Data Bandwidth- the bandwidth might be allocated permanently or for a period of time to a specific flow that usually exhibits well defined properties of burstiness and throughput.

Latency - the time taken for the data to transit the network from the source to the destination.

Transmission phase - process applications can be synchronized to wall clock time and require coordinated transmissions. A common coordination frequency is 4 Hz (250 ms).

Service contract type - revocation priority. LLNs have limited network resources that can vary with time. This means the system can become fully subscribed or even over subscribed.

Transmission priority-the means by which limited resources within field devices are allocated across multiple services. Packet priority is used as one criterion for selecting the next packet .Packet priority is used to select which packets are stored or discarded.

b) Configurable application Requirement

The routing protocol must support the ability to recompute paths based on Network layer abstractions of the link attributes or metrics that may change dynamically.

c) Different routes for different flows

It is often desirable to have different routes for different data flows between the same two endpoints because different services categories have different service requirements.

3.1.2 Device –Aware Routing Requirements

Wireless LLN nodes in industrial environments are powered by a variety of sources. Battery operated devices with lifetime requirements of at least five years are the most common. Energy scavenging devices are more complex. These systems contain both a power scavenging device (such as solar, vibration, or temperature difference) and an energy storage device, such as a rechargeable battery or a capacitor. The routing algorithm must support node-constrained routing (e.g. taking into account the existing energy state as a node constraint).Node constraints include power and memory, as well as constraints placed on the device by the user, such as battery life.

3.1.3 Broadcast/Multicast Requirements

The industrial process automation environments use broadcast or multicast addressing to communicate to field devices. Multicast over IP is used to deliver to multiple nodes that may be functionally similar or not. Example usages are:

- Delivery of alerts to multiple similar servers in an automation control room.
- Delivery of common packets to multiple routers over a backbone, where the packets results in each receiving router initiating multicast (sometimes as a full broadcast) within the LLN.
- Publication of measurement data to more than one subscriber. This feature is useful in some peer to peer control applications.For example, level position may be useful to a controller that operates the flow valve and also to the overfill alarm indicator. Both controller and alarm indicator would receive the same publication sent as a multicast by the level gauge.

3.1.4 Protocol Performance Requirements

The routing protocol must converge after the addition of new devices within several minutes and should converge within tens of seconds.The routing algorithm must be capable of routing packets to and from a newly added device within the several minutes of its addition, and should be able to perform this function within tens of seconds.The routing protocol must distribute sufficient information about link failures to enable traffic to be routed such that all service requirements (especially latency) continue to be met.

3.1.5 Reliability and Mobility Requirements

a) LLN reliability constitutes several unrelated aspects such as

- Availability of source to destination connectivity when the application needs it, expressed in number of succeses / number of attempts.
- Availability of source to destination connectivity when the application might need it, expressed in number of potential failures / available bandwidth.
- Ability, expressed in number of successes divided by number of attempts to get data delivered from source to destination within a capped time.

- How well a network (serving many applications) achieves end-to-end delivery of packets within a bounded latency.
- Trustworthiness of data that is delivered to the sinks.

b) Various economic factors have contributed to a reduction of trained workers in the plant. The industry as a whole appears to be trying to solve this problem with what is called the "wireless worker". The worker will be wirelessly connected to the plant IT system to download documentation, instructions, etc. Some field devices will be mobile. These devices may be located on moving parts such as rotating components or they may be located on vehicles such as cranes or fork lifts. The routing protocol should support vehicular speeds of up to 35 kmph. The routing protocol should support the wireless worker with fast network connection times of a few of seconds, and low command and response latencies to the plant behind the LLN access points, to applications, and to field devices. The routing protocol should also support the bandwidth allocation for bulk transfers between the field device and the handheld device of the wireless worker. The routing protocol should support walking speeds for maintaining network connectivity as the handheld device changes position in the wireless network.

3.1.6 Manageability Routing Requirements

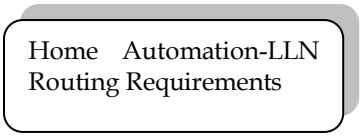
The routing protocol for LLNs is expected to be easy to deploy and manage. Because the number of field devices in a network is large, provisioning the devices manually may not make sense. The proper operation of the routing protocol require that the node be commissioned with information about itself, like identity, security tokens, radio standards and frequencies, etc...The routing protocol should not require to preprovision information about the environment where the node will be deployed. The routing protocol must enable the full discovery and setup of the environment (available links, selected peers, reachable network). The protocol must enable the distribution of its own configuration to be performed by some external mechanism from a centralized management controller.

3.1.7 Antagonistic Routing Requirements

Convergence time and network size are antagonistic.It is acceptable to grow reasonably the convergence time with the network size.

3.2 Home Automation-LLN Routing Requirements [9]

In the near future many homes will contain high numbers of wireless devices for a wide set of purposes. Examples include actuators (relay, light dimmer, heating valve), sensors (wall switch, water leak, blood pressure) and advanced controllers (RF-based AV remote control, Central server for light and heat control). Because such devices only cover a limited radio range, routing is often required. Routing requirements for networks comprising such constrained devices in a home control and automation environment are as shown in the below Fig 3.



.

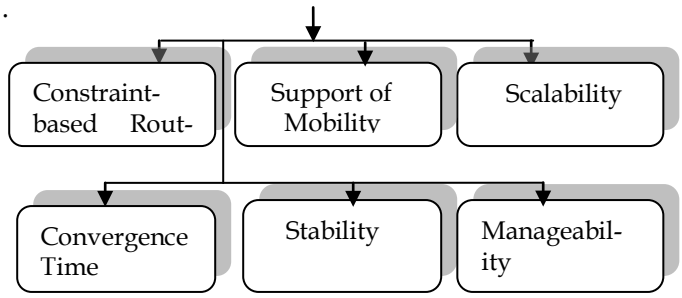


Fig 3, Home Automation Routing Requirements in LLN

3.2.1 Constraint-based Routing

For convenience and low operational costs, power consumption of consumer products must be kept at a very low level to achieve a long battery lifetime.The use of battery powered devices reduces installation costs and does enable installation of devices even where main power lines are not available.
The routing protocol should route via mains-powered nodes if possible. The routing protocol must support constraint-based routing taking into account node properties (CPU, memory, level of energy, sleep intervals, sleep intervals safety/convenience of changing battery).

3.2.2 Support of mobility

In a home environment, although the majority of devices are fixed devices, there is still a variety of mobile devices, for example a remote control is likely to move. Another example of mobile devices is wearable healthcare devices. While healthcare devices delivering measurement results can tolerate route discovery times measured in seconds, a remote control appears unresponsive if using more than 0.5 seconds. Non-responsive node can either be caused by a failure in the node, a failed link on the path to the node or a moved node. In the first two cases, the node can be expected to reappear at roughly the same location in the network, whereas it can return anywhere in the network in the latter case.

3.2.3 Scalability

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

3.2.4 Convergence Time

A wireless home automation network is subject to various instabilities due to signal strength variation, moving persons and the like. Measured from the transmission of a packet, the following convergence time requirements apply. First the routing protocol must converge within 0.5 second if no nodes have moved. Second the routing protocol must converge within 4 seconds if nodes have moved.In both cases, "converge" means "the originator node has received a response from the destination node". The above-mentioned convergence time requirements apply to a home control network environment of

up to 250 nodes with up to 4 repeating nodes between source and destination.

3.2.5 Stability

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

3.2.6 Manageability

The ability of the home network to support auto-configuration is of the utmost importance. The routing protocol designed for home automation networks must provide a set of features including zero configuration of the routing protocol for a new node to be added to the network. From a routing perspective, zero-configuration means that a node can obtain an address and join the network on its own, almost without human intervention.

3.3. Urban-LLN Routing Requirements [10]

It is believed that in the near future inorder to improve the people's living condition and also to monitor compliance with increasingly strict environmental laws, sensing and actuating nodes will be placed outdoors. These nodes have the capability of measuring and reporting wide gamut of data. For these nodes to communicate it requires the suitable routing protocols because of its wireless nature. The design of such protocols will be impacted by the limited resources of the nodes such as memory, processing power, battery, etc.
The IPv6 routing requirements for urban-LLN are as shown in the below fig 4

.

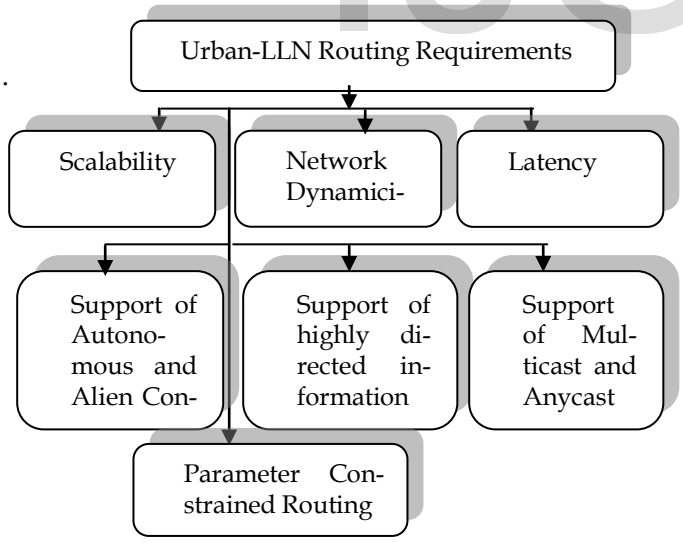


Fig 4, Urban-LLN Routing Requirements in LLN

3.3.1 Scalability

The large and diverse measurement space of Urban-LLN nodes coupled with the typically large urban areas will yield extremely large network sizes. The routing protocol 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. The routing protocol must be scalable so as to accommodate a very large and increasing number of nodes without deteriorating selected performance parameters below configurable thresholds. The routing protocol should support the organization of a large number of nodes into regions of configurable size.

3.3.2 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. The routing protocol should support appropriate mechanisms in order to be informed of the association, disassociation, and disappearance of nodes. The routing protocol should support appropriate updating mechanisms in order to be informed of changes in connectivity. The routing protocol should use this information to initiate protocol specific mechanisms for reorganization and reconfiguration as necessary to maintain overall routing efficiency. Convergence and route establishment times should be significantly lower than the smallest reporting interval.

3.3.3 Latency

Urban-LLNs 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. The routing protocol should support the ability to route according to different metrics (one of which could e.g. be latency).

3.3.4 Support of Autonomous and Alien Configuration

The scale and the large number of possible topologies that may be encountered in the Urban-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.
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, and the ability to support network-external) patches and configuration updates. For the latter, the protocol must support multi- and any-cast addressing. The protocol should also support the information and identification of groups of field devices in the network.
The routing protocol should be able to dynamically adapt, e.g. through the application of appropriate routing metrics, to everchanging 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.)The routing protocol should be able to 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 a LBR(Low Power and Lossy Network Border Router) according to the service-specific and traffic-specific QoS, traffic engineering and routing 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).

3.3.5 Support of highly directed information flow

The routing protocol should support and utilize the fact of a large number of highly directed traffic flows to facilitate scalability and parameter constrained routing. The routing protocol must be able to accommodate traffic bursts by dynamically computing and selecting multiple paths towards the same destination.

3.3.6 Support of Multicast and Anycast

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.

The network should support internetworking when identical protocols are used, while giving attention to routing security implications of interfacing, for example, a home network with a utility Urban-LLN. The network may support the ability to interact with another network using a different protocol, for example by supporting route redistribution.

3.3.7 Parameter Constrained Routing

The routing protocol must support parameter constrained routing such as CPU, memory size, battery level, etc. Routing protocol must be able to advertise node capabilities that will be exclusively used by the routing protocol engine for routing decision. Routing within urban sensor networks should require the Urban-LLN nodes to dynamically compute, select and install different paths towards a same destination, depending on the nature of the traffic.

3.4 Building Automation –LLN Routing Requirements [11]

Recent economic and technical advances in wireless communication allow facilities to increasingly utilize a wireless solution in lieu of a wired solution, thereby reducing installation costs while maintaining highly reliant communication.

Wireless solutions will be adapted from their existing wired counterparts in many of the building applications including, but not limited to Heating, Ventilation, and Air Conditioning (HVAC), Lighting, Physical Security, Fire, and Elevator/Lift systems. These devices will be developed to reduce installation costs, while increasing installation and retrofit flexibility, as well as increasing the sensing fidelity to improve efficiency and building service quality.

Facility Management Systems (FMS) are deployed in a large set of vertical markets including universities; hospitals; government facilities; Kindergarten through High School (K-12); pharmaceutical manufacturing facilities; and single-tenant or multi-tenant office buildings. These buildings range in size from 100K sqft structures (5story office buildings), to 1M sqft skyscrapers (100 story skyscrapers) to complex government facilities such as the Pentagon.Following are the building automation routing requirements for networks used to integrate building sensor, actuator and control products as shown in the below Fig 5

.

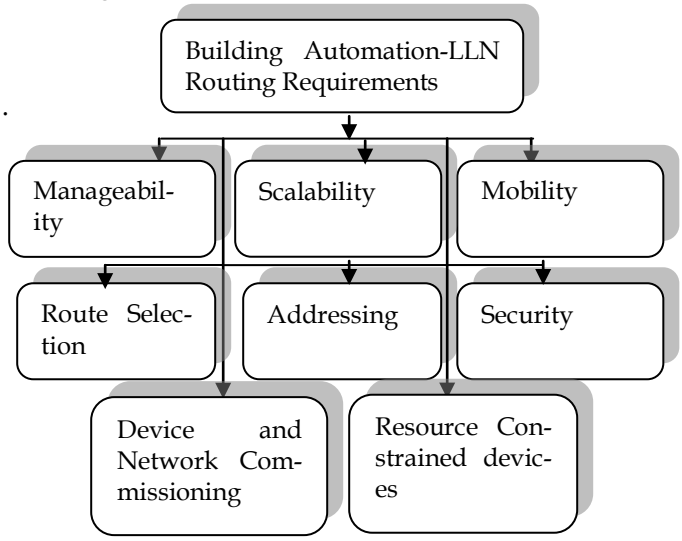


Fig 5, Building Automation Routing Requirements in LLN

3.4.1 Manageability

The need for diagnostics most often occurs during the installation and commissioning phase. Battery powered wireless devices typically will have a self diagnostic mode that can be initiated via a button press on the device. The device will display its link status and/or end-to-end connectivity when the button is depressed. Lines-powered devices will continuously display communication status via a bank of LEDs, possibly denoting signal strength and end-to-end application connectivity on operational networks, due to the mission critical nature of the application, the LLN devices will be temporally monitored by the higher layers to assure communication integrity is maintained.Failure to maintain this communication will result in an alarm being forwarded to the enterprise network from the monitoring node for analysis and remediation.

In addition to the initial installation and commissioning of the system, it is equally important for the ongoing maintenance of the system to be simple and inexpensive.

3.4.2 Scalability

The scalability requirements are as follows

a) Network Domain

The routing protocol must be able to support networks with at least 2000 nodes where 1000 nodes would act as routers and the other 1000 nodes would be hosts. Subnetworks (e.g., rooms, primary equipment) within the network must support upwards to 255 sensors and/or actuators.

b) Peer-to-Peer Communication

A network device must be able to communicate in an end-to-end manner with any other device on the network. Thus, the routing protocol must provide routes between arbitrary hosts within the appropriate administrative domain.

3.4.3 Mobility

Mobility can be implemented at various layers of the system,

and the specific requirements depend on the chosen layer. Mobile IP may be used or the set of routers in a building may give an impression of a building-wide network and allow devices to retain their addresses regardless of where they are,handling routing between the devices in the background.Mobility requirements in the routing layer for mobile devices are

a) Device Mobility within the LLN

An LLN typically spans a single floor in a commercial building. Mobile devices may move within this LLN. For example, a wheel chair may be moved from one room on the floor to another room on the same floor. A mobile LLN device that moves within the confines of the same LLN should reestablish end-to-end communication to a fixed device also in the LLN within 5 seconds after it ceases movement. The LLN network convergence time should be less than 10 seconds once the mobile device stops moving

b) Device Mobility across LLNs

A mobile device may move across LLNs, such as a wheel chair being moved to a different floor. A mobile device that moves outside its original LLN should reestablish end-to-end communication to a fixed device also in the new LLN within 10 seconds after the mobile device ceases movement. The network convergence time should be less than 20 seconds once the mobile device stops moving.

3.4.4 Route Selection

Route selection determines reliability and quality of the communication among the devices by optimizing routes over time and resolving any nuances developed at system startup when nodes are asynchronously adding themselves to the network.

a) Route Cost

The routing protocol must support a metric of route quality and optimize selection according to such metrics within constraints established for links along the routes. These metrics should reflect metrics such as signal strength, available bandwidth, hop count, energy availability and communication error rates.

b) Route Adaptation

Communication routes must be adaptive and converge toward optimality of the chosen metric (e.g., signal quality, hop count) in time Route Redundancy.The routing layer should be configurable to allow secondary and tertiary routes to be established and used upon failure of the primary route.

c) Route Discovery Time

Mission critical commercial applications (e.g., Fire, Security) require reliable communication and guaranteed end-to-end delivery of all messages in a timely fashion. Application layer time-outs must be selected judiciously to cover anomalous conditions such as lost packets and/or route discoveries; yet not be set too large to over damp the network response. If route discovery occurs during packet transmission time (proactive routing), it should not add more than 120ms of latency to the packet delivery time.

d) Route Preference

The routing protocol should allow for the support of manually configured static preferred routes.

e) Prioritized Routing

Network and application packet routing prioritization must be supported to assure that mission critical applications (e.g., Fire Detection) cannot be deferred while less critical applications access the network. The routing protocol must be able to provide routes with different characteristics, also referred to as "QoS" routing.

3.4.5 Addressing

Facility Management systems (FMS) require different communication schemes to solicit or post network information. Multicasts or anycasts need be used to resolve unresolved references within a device when the device first joins the network. Multicasts are typically used for network joins and application binding in embedded systems. Routing must support anycast, unicast, and multicast.

3.4.6 Device and Network Commissioning

The installation routing requirements are

a) Zero-Configuration Installation

It must be possible to fully commission network devices without requiring any additional commissioning device (e.g., laptop). From the ROLL perspective, zero-configuration means that a node can obtain an address and join the network on its own, without human intervention.

b) Local Testing

During installation, the room sensors, actuators and controllers should be able to route packets amongst themselves and to any other device within the LLN without requiring any additional routing infrastructure or routing configuration

c) Device Replacement

To eliminate the need to reconfigure the application upon replacing a failed device in the LLN; the replaced device must be able to advertise the old IP address of the failed device in addition to its new IP address. The routing protocols must support hosts and routers that advertise multiple IPv6 addresses.

3.4.7 Resource Constrained Devices

Sensing and actuator device processing power and memory may be 4 orders of magnitude less (i.e., 10,000x) than many more traditional client devices on an IP network. The routing mechanisms must therefore be tailored to fit these resource constrained devices.

a) Limited Memory Footprint on Host Devices

The software size requirement for non-routing devices (e.g., sleeping sensors and actuators) should be implementable in 8-bit devices with no more than 128KB of memory.

b) Limited Processing Power for Routers

The software size requirements for routing devices (e.g., room

controllers) should be implementable in 8-bit devices with no more than 256KB of flash memory

c) Sleeping Devices

Sleeping devices must be able to receive inbound data. Messages sent to battery powered nodes must be buffered and retried by the last hop router for a period of at least 20 seconds when the destination node is currently in its sleep cycle.

The routing protocol must take into account node properties such as 'Low-powered node' which produce efficient low latency routes that minimize radio 'on' time for these devices.

3.4.8 Security Requirements

Due to the variety of buildings and tenants, the FMS systems must be completely configurable on-site. Wireless encryption and device authentication security policies need to be considered in commercial buildings, while keeping in mind the impact on the limited processing capabilities and additional latency incurred on the sensors, actuators and controllers.FMS systems are typically highly configurable in the field and hence the security policy is most often dictated by the type of building to which the FMS is being installed. Single tenant owner occupied office buildings installing lighting or HVAC control are candidates for implementing a low level of security on the LLN.

4. RELATION OF USECASES TO REQUIREMENTS

4.1 Industrial –LLN Routing Requirements [8]:

Below table1 shows the relations of use cases to routing requirements of Industrial-LLN.

Use case	Requirements
Solar Panel	Device Aware Routing
Vibration scavenger	Device Aware Routing
Delivery of Alerts to multiple servers	Broadcast/Multicast
Delivery of Packets to multiple routers	Broadcast/Multicast
PDA's	Mobility
Route computation	Protocol Performance

Table 1

4.2 Home Automation-LLN Routing Requirements [9]:

The relations of use cases to requirements of Home Automation-LLN are outlined in the table 2 below:

Use case	Requirements
Lighting application in action	1.Support of Mobility 2. Scalability
Energy Conservation and Optimizing Energy Consumption	1.Constraint–based routing
Moving a remote control around	1.Support of Mobility 2.Convergence Time
Adding a new module to the system	1.Convergence Time
Healthcare	1.Constraint–based routing 2. Support of Mobility 3.Convergence Time
Alarm Systems	1.Scalability 2.Convergence Time

Table 2

4.3 Urban-LLN Routing Requirements [10]:

The relations of use cases to requirements of Urban-LLN are outlined in the table 3 below

Use case	Requirements
Regular measurement reporting	1.Support of Multicast 2.Latency
Queried measurement reporting	Support of Multicast or Anycast
Alert reporting	1.Support of Multicast 2.Latency
Configuration updates	Support of Autonomous and Alien Configuration
Route Redistribution	Support of Multicast or Anycast
Association and Disassociation or Disappearance of Nodes	Network Dynamicity

Table 3

4.4. Building Automation –LLN Routing Requirements[11]:

The relations of use cases to requirements of Building Automation-LLN are outlined in the table 4.

Use case	Requirements
Building Control Systems	Device and Network Commissioning
Primary Equipments, rooms	Scalability
Tracking capital equipment such as wheel chair's	Mobility
Room Controllers	Resource Constrianed Devices
Authentication, Encryption	Security
Diagnostics, Route tracking	Manageability

Table 4

V. CONCLUSION

Motivated by the need to support the upcoming Industrial routing, Home automation, Building automation, Urban routing applications, the IETF has started standardizing protocols

and underlie the emerging Internet of things. In this paper we have presented a survey on the routing requirements for the various LLN applications. The paper also highlighted the use-cases for four different LLN applications along with their corresponding routing requirements.

REFERENCES

[1] T. Winter and P. Thubert, "RPL: IPV6 Routing Protocol for Low Power and Lossy Networks", Internet-Draft, June 2010, pages 103, (draft-ietf-roll-rpl-09).

[2] P. Levis, A. Tavakoli, and S. Dawson-Haggerty, "Overview of Existing Routing Protocols for Low Power and Lossy Networks,"IETF ROLL, IETF draft, 14 February 2009, draft Ietf-roll-protocolssurvey-06 (work in progress).

[3] Interconnecting Smart Objects with IP The Next Internet by Jean-Philippe Vasseur and Adam Dunkels Published by Morgan Kaufmann, Copyright June 2010.

[4] J. Hui and D. Culler, IP is Dead, Long Live IP for Wireless Sensor Networks, in Proceedings of ACM SenSys, Raleigh, North Carolina, USA, November 2008

[5] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, vol. 11, no. 6, pp. 6–28, December 2004.

[6] Wireless sensor network survey ,Jennifer Yick ,Biswanath Mukherjee , Dipak Ghosal,Department of Computer Science, University of California, Davis, CA 95616, United States.

[7] J. Vasseur, "Terminology in Low power And Lossy Neworks", draft-ietf-roll-terminology-03(work in progress),March 2010

[8] K. Pister, P. Thubert, and S. Dwars, "Industrial Routing Requirements in Low-Power and Lossy Networks," RFC 5673, Oct. 2009.

[9] A. Brandt, J. Buron, and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks," RFC 5826, Apr. 2010.

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

[11] J. Martocci et al., "Building Automation Routing Requirements in Low-Power and Lossy Networks," RFC5867, June 2010