Internet Engineering Task Force (IETF)
Request for Comments: 7548
Category: Informational
ISSN: 2070-1721

M. Ersue, Ed.
Nokia Networks
D. Romascanu
Avaya
J. Schoenwaelder
A. Sehgal
Jacobs University Bremen

May 2015

Management of Networks with Constrained Devices: Use Cases

Abstract

This document discusses use cases concerning the management of networks in which constrained devices are involved. A problem statement, deployment options, and the requirements on the networks with constrained devices can be found in the companion document on "Management of Networks with Constrained Devices: Problem Statement and Requirements" (RFC 7547).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7548.

Table of Contents

1. Introduction 3
2. Access Technologies 4
   2.1. Constrained Access Technologies 4
   2.2. Cellular Access Technologies 5
3. Device Life Cycle 6
   3.1. Manufacturing and Initial Testing 6
   3.2. Installation and Configuration 6
   3.3. Operation and Maintenance 7
   3.4. Recommissioning and Decommissioning 7
4. Use Cases 8
   4.1. Environmental Monitoring 8
   4.2. Infrastructure Monitoring 9
   4.3. Industrial Applications 10
   4.4. Energy Management 12
   4.5. Medical Applications 14
   4.6. Building Automation 15
   4.7. Home Automation 17
   4.8. Transport Applications 18
   4.9. Community Network Applications 20
   4.10. Field Operations 22
5. Security Considerations 23
6. Informative References 24
Acknowledgments 25
Contributors 26
Authors' Addresses 26

1. Introduction

Constrained devices (also known as sensors, smart objects, or smart devices) with limited CPU, memory, and power resources can be connected to a network. Such a network of constrained devices itself may be constrained or challenged, e.g., with unreliable or lossy channels, wireless technologies with limited bandwidth and a dynamic topology, needing the service of a gateway or proxy to connect to the Internet. In other scenarios, the constrained devices can be connected to a unconstrained network using off-the-shelf protocol stacks. Constrained devices might be in charge of gathering information in diverse settings including natural ecosystems, buildings, and factories and sending the information to one or more server stations.

Network management is characterized by monitoring network status, detecting faults (and inferring their causes), setting network parameters, and carrying out actions to remove faults, maintain normal operation, and improve network efficiency and application performance. The traditional network management application periodically collects information from a set of managed network elements, it processes the collected data, and it presents the results to the network management users. Constrained devices, however, often have limited power, have low transmission range, and might be unreliable. Such unreliability might arise from device itself (e.g., battery exhausted) or from the channel being constrained (i.e., low-capacity and high-latency). They might also need to work in hostile environments with advanced security requirements or need to be used in harsh environments for a long time without supervision. Due to such constraints, the management of a network with constrained devices offers different types of challenges compared to the management of a traditional IP network.

This document aims to understand use cases for the management of a network in which constrained devices are involved. It lists and discusses diverse use cases for management from the network as well as from the application point of view. The list of discussed use cases is not an exhaustive one since other scenarios, currently unknown to the authors, are possible. The application scenarios discussed aim to show where networks of constrained devices are expected to be deployed. For each application scenario, we first briefly describe the characteristics followed by a discussion on how network management can be provided, who is likely going to be responsible for it, and on which time-scale management operations are likely to be carried out.

A problem statement, deployment and management topology options as well as the requirements on the networks with constrained devices can be found in the companion document [RFC7547].

This documents builds on the terminology defined in [RFC7228] and [RFC7547]. [RFC7228] is a base document for the terminology concerning constrained devices and constrained networks. Some use cases specific to IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) can be found in [RFC6568].

2. Access Technologies

Besides the management requirements imposed by the different use cases, the access technologies used by constrained devices can impose restrictions and requirements upon the Network Management System (NMS) and protocol of choice.

It is possible that some networks of constrained devices might utilize traditional unconstrained access technologies for network access, e.g., local area networks with plenty of capacity. In such scenarios, the constrainedness of the device presents special management restrictions and requirements rather than the access technology utilized.

However, in other situations, constrained or cellular access technologies might be used for network access, thereby causing management restrictions and requirements to arise as a result of the underlying access technologies.

A discussion regarding the impact of cellular and constrained access technologies is provided in this section since they impose some special requirements on the management of constrained networks. On the other hand, fixed-line networks (e.g., power-line communications) are not discussed here since tend to be quite static and do not typically impose any special requirements on the management of the network.

2.1. Constrained Access Technologies

Due to resource restrictions, embedded devices deployed as sensors and actuators in the various use cases utilize low-power, low-data-rate wireless access technologies such as [IEEE802.15.4], Digital Enhanced Cordless Telecommunication (DECT) Ultra Low Energy (ULE), or Bluetooth Low-Energy (BT-LE) for network connectivity.

In such scenarios, it is important for the NMS to be aware of the restrictions imposed by these access technologies to efficiently manage these constrained devices. Specifically, such low-power, low-

data-rate access technologies typically have small frame sizes. So it would be important for the NMS and management protocol of choice to craft packets in a way that avoids fragmentation and reassembly of packets since this can use valuable memory on constrained devices.

Devices using such access technologies might operate via a gateway that translates between these access technologies and more traditional Internet protocols. A hierarchical approach to device management in such a situation might be useful, wherein the gateway device is in-charge of devices connected to it, while the NMS conducts management operations only to the gateway.

2.2. Cellular Access Technologies

Machine-to-machine (M2M) services are increasingly provided by mobile service providers as numerous devices, home appliances, utility meters, cars, video surveillance cameras, and health monitors are connected with mobile broadband technologies. Different applications, e.g., in a home appliance or in-car network, use Bluetooth, Wi-Fi, or ZigBee locally and connect to a cellular module acting as a gateway between the constrained environment and the mobile cellular network.

Such a gateway might provide different options for the connectivity of mobile networks and constrained devices:

- a smartphone with 3G/4G and WLAN radio might use BT-LE to connect to the devices in a home area network,
- a femtocell might be combined with home gateway functionality acting as a low-power cellular base station connecting smart devices to the application server of a mobile service provider,
- an embedded cellular module with LTE radio connecting the devices in the car network with the server running the telematics service,
- an M2M gateway connected to the mobile operator network supporting diverse Internet of Things (IoT) connectivity technologies including ZigBee and Constrained Application Protocol (CoAP) over 6LoWPAN over IEEE 802.15.4.

Common to all scenarios above is that they are embedded in a service and connected to a network provided by a mobile service provider. Usually, there is a hierarchical deployment and management topology in place where different parts of the network are managed by different management entities and the count of devices to manage is high (e.g., many thousands). In general, the network is comprised of manifold types and sizes of devices matching to different device

classes. As such, the managing entity needs to be prepared to manage devices with diverse capabilities using different communication or management protocols. In the case in which the devices are directly connected to a gateway, they most likely are managed by a management entity integrated with the gateway, which itself is part of the NMS run by the mobile operator. Smartphones or embedded modules connected to a gateway might themselves be in charge of managing the devices on their level. The initial and subsequent configuration of such a device is mainly based on self-configuration and is triggered by the device itself.

The gateway might be in charge of filtering and aggregating the data received from the device as the information sent by the device might be mostly redundant.

3. Device Life Cycle

Since constrained devices deployed in a network might go through multiple phases in their lifetime, it is possible for different managers of networks and/or devices to exist during different parts of the device lifetimes. An in-depth discussion regarding the possible device life cycles can be found in [IOT-SEC].

3.1. Manufacturing and Initial Testing

Typically, the life cycle of a device begins at the manufacturing stage. During this phase, the manufacturer of the device is responsible for the management and configuration of the devices. It is also possible that a certain use case might utilize multiple types of constrained devices (e.g., temperature sensors, lighting controllers, etc.) and these could be manufactured by different entities. As such, during the manufacturing stage, different managers can exist for different devices. Similarly, during the initial testing phase, where device quality-assurance tasks might be performed, the manufacturer remains responsible for the management of devices and networks that might comprise them.

3.2. Installation and Configuration

The responsibility of managing the devices must be transferred to the installer during the installation phase. There must exist procedures for transferring management responsibility between the manufacturer and installer. The installer may be the customer or an intermediary contracted to set up the devices and their networks. It is important that the NMS that is utilized allows devices originating at different vendors to be managed, ensuring interoperability between them and the configuration of trust relationships between them as well.

It is possible that the installation and configuration responsibilities might lie with different entities. For example, the installer of a device might only be responsible for cabling a network, physically installing the devices, and ensuring initial network connectivity between them (e.g., configuring IP addresses). Following such an installation, the customer or a subcontractor might actually configure the operation of the device. As such, during installation and configuration multiple parties might be responsible for managing a device and appropriate methods must be available to ensure that this management responsibility is transferred suitably.

3.3. Operation and Maintenance

At the outset of the operation phase, the operational responsibility of a device and network should be passed on to the customer. It is possible that the customer, however, might contract the maintenance of the devices and network to a subcontractor. In this case, the NMS and management protocol should allow for configuring different levels of access to the devices. Since different maintenance vendors might be used for devices that perform different functions (e.g., HVAC, lighting, etc.), it should also be possible to restrict management access to devices based on the currently responsible manager.

3.4. Recommissioning and Decommissioning

The owner of a device might choose to replace, repurpose, or even decommission it. In each of these cases, either the customer or the contracted maintenance agency must ensure that appropriate steps are taken to meet the end goal.

In case the devices needs to be replaced, the manager of the network (customer or contractor responsible) must detach the device from the network, remove all appropriate configuration, and discard the device. A new device must then be configured to replace it. The NMS should allow for the transferring of the configuration and replacing an existing device. The management responsibility of the operation/maintenance manager would end once the device is removed from the network. During the installation of the new replacement device, the same responsibilities would apply as those during the Installation and Configuration phases.

The device being replaced may not have yet reached end-of-life, and as such, instead of being discarded, it may be installed in a new location. In this case, the management responsibilities are once again resting in the hands of the entities responsible for the Installation and Configuration phases at the new location.

If a device is repurposed, then it is possible that the management responsibility for this device changes as well. For example, a device might be moved from one building to another. In this case, the managers responsible for devices and networks in each building could be different. As such, the NMS must not only allow for changing configuration but also the transferring of management responsibilities.

In case a device is decommissioned, the management responsibility typically ends at that point.

4. Use Cases

4.1. Environmental Monitoring

Environmental monitoring applications are characterized by the deployment of a number of sensors to monitor emissions, water quality, or even the movements and habits of wildlife. Other applications in this category include earthquake or tsunami early-warning systems. The sensors often span a large geographic area; they can be mobile; and they are often difficult to replace. Furthermore, the sensors are usually not protected against tampering.

Management of environmental-monitoring applications is largely concerned with monitoring whether the system is still functional and the roll out of new constrained devices in case the system loses too much of its structure. The constrained devices themselves need to be able to establish connectivity (autoconfiguration), and they need to be able to deal with events such as losing neighbors or being moved to other locations.

Management responsibility typically rests with the organization running the environmental-monitoring application. Since these monitoring applications must be designed to tolerate a number of failures, the time scale for detecting and recording failures is, for some of these applications, likely measured in hours and repairs might easily take days. In fact, in some scenarios it might be more cost- and time-effective not to repair such devices at all. However, for certain environmental monitoring applications, much tighter time scales may exist and might be enforced by regulations (e.g., monitoring of nuclear radiation).

Since many applications of environmental-monitoring sensors are likely to be in areas that are important to safety (flood monitoring, nuclear radiation monitoring, etc.), it is important for management protocols and NMSs to ensure appropriate security protections. These protections include not only access control, integrity, and

availability of data, but also provide appropriate mechanisms that can deal with situations that might be categorized as emergencies or when tampering with sensors/data might be detected.

4.2. Infrastructure Monitoring

Infrastructure monitoring is concerned with the monitoring of infrastructures such as bridges, railway tracks, or (offshore) windmills. The primary goal is usually to detect any events or changes of the structural conditions that can impact the risk and safety of the infrastructure being monitored. Another secondary goal is to schedule repair and maintenance activities in a cost-effective manner.

The infrastructure to monitor might be in a factory or spread over a wider area (but difficult to access). As such, the network in use might be based on a combination of fixed and wireless technologies, which use robust networking equipment and support reliable communication via application-layer transactions. It is likely that constrained devices in such a network are mainly C2 devices [RFC7228] and have to be controlled centrally by an application running on a server. In case such a distributed network is widely spread, the wireless devices might use diverse long-distance wireless technologies such as Worldwide Interoperability for Microwave Access (WiMAX) or 3G/LTE. In cases, where an in-building network is involved, the network can be based on Ethernet or wireless technologies suitable for in-building use.

The management of infrastructure monitoring applications is primarily concerned with the monitoring of the functioning of the system. Infrastructure monitoring devices are typically rolled out and installed by dedicated experts, and updates are rare since the infrastructure itself does not change often. However, monitoring devices are often deployed in unsupervised environments; hence, special attention must be given to protecting the devices from being modified.

Management responsibility typically rests with the organization owning the infrastructure or responsible for its operation. The time scale for detecting and recording failures is likely measured in hours and repairs might easily take days. However, certain events (e.g., natural disasters) may require that status information be obtained much more quickly and that replacements of failed sensors can be rolled out quickly (or redundant sensors are activated quickly). In case the devices are difficult to access, a self-healing feature on the device might become necessary. Since infrastructure monitoring is closely related to ensuring safety,

management protocols and systems must provide appropriate security protections to ensure confidentiality, integrity, and availability of data.

4.3. Industrial Applications

Industrial Applications and smart manufacturing refer to tasks such as networked control and monitoring of manufacturing equipment, asset and situation management, or manufacturing process control. For the management of a factory, it is becoming essential to implement smart capabilities. From an engineering standpoint, industrial applications are intelligent systems enabling rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply-chain networks. Potential industrial applications (e.g., for smart factories and smart manufacturing) are:

- Digital control systems with embedded, automated process controls; operator tools; and service information systems optimizing plant operations and safety.
- Asset management using predictive maintenance tools, statistical evaluation, and measurements maximizing plant reliability.
- Smart sensors detecting anomalies to avoid abnormal or catastrophic events.
- Smart systems integrated within the industrial energy-management system and externally with the smart grid enabling real-time energy optimization.

Management of Industrial Applications and smart manufacturing may, in some situations, involve Building Automation tasks such as control of energy, HVAC, lighting, or access control. Interacting with management systems from other application areas might be important in some cases (e.g., environmental monitoring for electric energy production, energy management for dynamically scaling manufacturing, vehicular networks for mobile asset tracking). Management of constrained devices and networks may not only refer to the management of their network connectivity. Since the capabilities of constrained devices are limited, it is quite possible that a management system would even be required to configure, monitor, and operate the primary functions for which a constrained device is utilized, besides managing its network connectivity.

Sensor networks are an essential technology used for smart manufacturing. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a

large number of networked sectors. Data interoperability and seamless exchange of product, process, and project data are enabled through interoperable data systems used by collaborating divisions or business systems. Intelligent automation and learning systems are vital to smart manufacturing, but they must be effectively integrated with the decision environment. The NMS utilized must ensure timely delivery of sensor data to the control unit so it may take appropriate decisions. Similarly, the relaying of commands must also be monitored and managed to ensure optimal functioning. Wireless sensor networks (WSNs) have been developed for machinery Condition-based Maintenance (CBM) as they offer significant cost savings and enable new functionalities. Inaccessible locations, rotating machinery, hazardous areas, and mobile assets can be reached with wireless sensors. Today, WSNs can provide wireless link reliability, real-time capabilities, and quality-of-service and they can enable industrial and related wireless sense and control applications.

Management of industrial and factory applications is largely focused on monitoring whether the system is still functional, real-time continuous performance monitoring, and optimization as necessary. The factory network might be part of a campus network or connected to the Internet. The constrained devices in such a network need to be able to establish configuration themselves (autoconfiguration) and might need to deal with error conditions as much as possible locally. Access control has to be provided with multi-level administrative access and security. Support and diagnostics can be provided through remote monitoring access centralized outside of the factory.

Factory-automation tasks require that continuous monitoring be used to optimize production. Groups of manufacturing and monitoring devices could be defined to establish relationships between them. To ensure timely optimization of processes, commands from the NMS must arrive at all destination within an appropriate duration. This duration could change based on the manufacturing task being performed. Installation and operation of factory networks have different requirements. During the installation phase, many networks, usually distributed along different parts of the factory/assembly line, coexist without a connection to a common backbone. A specialized installation tool is typically used to configure the functions of different types of devices, in different factory locations, in a secure manner. At the end of the installation phase, interoperability between these stand-alone networks and devices must be enabled. During the operation phase, these stand-alone networks are connected to a common backbone so that they may retrieve control information from and send commands to appropriate devices.

Management responsibility is typically owned by the organization running the industrial application. Since the monitoring applications must handle a potentially large number of failures, the time scale for detecting and recording failures is, for some of these applications, likely measured in minutes. However, for certain industrial applications, much tighter time scales may exist, e.g., in real-time, which might be enforced by the manufacturing process or the use of critical material. Management protocols and NMSs must ensure appropriate access control since different users of industrial control systems will have varying levels of permissions. For example, while supervisors might be allowed to change production parameters, they should not be allowed to modify the functional configuration of devices like a technician should. It is also important to ensure integrity and availability of data since malfunctions can potentially become safety issues. This also implies that management systems must be able to react to situations that may pose dangers to worker safety.

4.4. Energy Management

The EMAN working group developed an energy-management framework [RFC7326] for devices and device components within or connected to communication networks. This document observes that one of the challenges of energy management is that a power distribution network is responsible for the supply of energy to various devices and components, while a separate communication network is typically used to monitor and control the power distribution network. Devices in the context of energy management can be monitored for parameters like power, energy, demand and power quality. If a device contains batteries, they can be also monitored and managed.

Energy devices differ in complexity and may include basic sensors or switches, specialized electrical meters, or power distribution units (PDU), and subsystems inside the network devices (routers, network switches) or home or industrial appliances. The operators of an energy-management system are either the utility providers or customers that aim to control and reduce the energy consumption and the associated costs. The topology in use differs and the deployment can cover areas from small surfaces (individual homes) to large geographical areas. The EMAN requirements document [RFC6988] discusses the requirements for energy management concerning monitoring and control functions.

It is assumed that energy management will apply to a large range of devices of all classes and networks topologies. Specific resource monitoring, like battery utilization and availability, may be specific to devices with lower physical resources (device classes C0 or C1 [RFC7228]).

Energy management is especially relevant to the Smart Grid. A Smart Grid is an electrical grid that uses data networks to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.

Smart Metering is a good example of an energy-management application based on Smart Grid. Different types of possibly wireless small meters all together produce a large amount of data, which is collected by a central entity and processed by an application server, which may be located within the customer's residence or off site in a data center. The communication infrastructure can be provided by a mobile network operator as the meters in urban areas will most likely have a cellular or WiMAX radio. In case the application server is located within the residence, such meters are more likely to use Wi-Fi protocols to interconnect with an existing network.

An Advanced Metering Infrastructure (AMI) network is another example of the Smart Grid that enables an electric utility to retrieve frequent electric usage data from each electric meter installed at a customer's home or business. Unlike Smart Metering, in which case the customer or their agents install appliance-level meters, an AMI is typically managed by the utility providers and could also include other distribution automation devices like transformers and reclosers. Meters in AMI networks typically contain constrained devices that connect to mesh networks with a low-bandwidth radio. Usage data and outage notifications can be sent by these meters to the utility's headend systems, via aggregation points of higher-end router devices that bridge the constrained network to a less constrained network via cellular, WiMAX, or Ethernet. Unlike meters, these higher-end devices might be installed on utility poles owned and operated by a separate entity.

It thereby becomes important for a management application not only to be able to work with diverse types of devices, but also to work over multiple links that might be operated and managed by separate entities, each having divergent policies for their own devices and network segments. During management operations, like firmware updates, it is important that the management systems perform robustly in order to avoid accidental outages of critical power systems that could be part of AMI networks. In fact, since AMI networks must also report on outages, the management system might have to manage the energy properties of battery-operated AMI devices themselves as well.

A management system for home-based Smart Metering solutions is likely to have devices laid out in a simple topology. However, AMI network installations could have thousands of nodes per router, i.e., higher-end device, which organize themselves in an ad hoc manner. As such,

a management system for AMI networks will need to discover and operate over complex topologies as well. In some situations, it is possible that the management system might also have to set up and manage the topology of nodes, especially critical routers. Encryption-key management and sharing in both types of networks are also likely to be important for providing confidentiality for all data traffic. In AMI networks, the key may be obtained by a meter only after an end-to-end authentication process based on certificates. The Smart Metering solution could adopt a similar approach or the security may be implied due to the encrypted Wi-Fi networks they become part of.

The management of such a network requires end-to-end management of and information exchange through different types of networks. However, as of today, there is no integrated energy-management approach and no common information model available. Specific energy-management applications or network islands use their own management mechanisms.

4.5. Medical Applications

Constrained devices can be seen as an enabling technology for advanced and possibly remote health-monitoring and emergency-notification systems, ranging from monitors for blood pressure and heart rate to advanced devices capable of monitoring implanted technologies, such as pacemakers or advanced hearing aids. Medical sensors may not only be attached to human bodies, they might also exist in the infrastructure used by humans such as bathrooms or kitchens. Medical applications will also be used to ensure treatments are being applied properly, and they might guide people losing orientation. Fitness and wellness applications, such as connected scales or wearable heart monitors, encourage consumers to exercise and empower self-monitoring of key fitness indicators. Different applications use Bluetooth, Wi-Fi, or ZigBee connections to access the patient's smartphone or home cellular connection to access the Internet.

Constrained devices that are part of medical applications are managed either by the users of those devices or by an organization providing medical (monitoring) services for physicians. In the first case, management must be automatic and/or easy to install and set up by laypeople. In the second case, it can be expected that devices will be controlled by specially trained people. In both cases, however, it is crucial to protect the safety and privacy of the people who use medical devices. Security precautions to protect access (authentication, encryption, integrity protections, etc.) to such devices may be critical to safeguarding the individual. The level of access granted to different users also may need to be regulated. For

example, an authorized surgeon or doctor must be allowed to configure all necessary options on the devices; however, a nurse or technician may only be allowed to retrieve data that can assist in diagnosis. Even though the data collected by a heart monitor might be protected, the pure fact that someone carries such a device may need protection. As such, certain medical appliances may not want to participate in discovery and self-configuration protocols in order to remain invisible.

Many medical devices are likely to be used (and relied upon) to provide data to physicians in critical situations in which the patient might not be able to report such data themselves. Timely delivery of data can be quite important in certain applications like patient-mobility monitoring in nursing homes. Data must reach the physician and/or emergency services within specified limits of time in order to be useful. As such, fault detection of the communication network or the constrained devices becomes a crucial function of the management system that must be carried out with high reliability and, depending on the medical appliance and its application, within seconds.

4.6. Building Automation

Building automation comprises the distributed systems designed and deployed to monitor and control the mechanical, electrical, and electronic systems inside buildings with various destinations (e.g., public and private, industrial, institutions, or residential). Advanced Building Automation Systems (BASs) may be deployed concentrating the various functions of safety, environmental control, occupancy, and security. Increasingly, the deployment of the various functional systems is connected to the same communication infrastructure (possibly IP-based), which may involve wired or wireless communication networks inside the building.

Building automation requires the deployment of a large number (10 to 100,000) of sensors that monitor the status of devices, parameters inside the building, and controllers with different specialized functionality for areas within the building or the totality of the building. Inter-node distances between neighboring nodes vary from 1 to 20 meters. The NMS must, as a result, be able to manage and monitor a large number of devices, which may be organized in multi-hop meshed networks. Distances between the nodes, and the use of constrained protocols, means that networks of nodes might be segmented. The management of such network segments and nodes in these segments should be possible. Contrary to home automation, in building management the devices are expected to be managed assets and known to a set of commissioning tools and a data storage, such that every connected device has a known origin. This requires the

management system to be able to discover devices on the network and ensure that the expected list of devices is currently matched. Management here includes verifying the presence of the expected devices and detecting the presence of unwanted devices.

Examples of functions performed by controllers in building automation are regulating the quality, humidity, and temperature of the air inside the building as well as regulating the lighting. Other systems may report the status of the machinery inside the building like elevators or inside the rooms like projectors in meeting rooms. Security cameras and sensors may be deployed and operated on separate dedicated infrastructures connected to the common backbone. The deployment area of a BAS is typically inside one building (or part of it) or several buildings geographically grouped in a campus. A building network can be composed of network segments, where a network segment covers a floor, an area on the floor, or a given functionality (e.g., security cameras). It is possible that the management tasks of different types of some devices might be separated from others (e.g, security cameras might operate and be managed via a network separate from that of the HVAC in a building).

Some of the sensors in BASs (for example, fire alarms or security systems) register, record, and transfer critical alarm information; therefore, they must be resilient to events like loss of power or security attacks. A management system must be able to deal with unintentional segmentation of networks due to power loss or channel unavailability. It must also be able to detect security events. Due to specific operating conditions required from certain devices, there might be a need to certify components and subsystems operating in such constrained conditions based on specific requirements. Also, in some environments, the malfunctioning of a control system (like temperature control) needs to be reported in the shortest possible time. Complex control systems can misbehave, and their critical status reporting and safety algorithms need to be basic and robust and perform even in critical conditions. Providing this monitoring, configuration and notification service is an important task of the management system used in building automation.

In some cases, building automation solutions are deployed in newly designed buildings; in other cases, it might be over existing infrastructures. In the first case, there is a broader range of possible solutions, which can be planned for the infrastructure of the building. In the second case, the solution needs to be deployed over an existing infrastructure taking into account factors like existing wiring, distance limitations, and the propagation of radio signals over walls and floors, thereby making deployment difficult. As a result, some of the existing WLAN solutions (e.g., [IEEE802.11] or [IEEE802.15]) may be deployed. In mission-critical or security-

sensitive environments and in cases where link failures happen often, topologies that allow for reconfiguration of the network and connection continuity may be required. Some of the sensors deployed in building automation may be very simple constrained devices for which C0 or C1 [RFC7228] may be assumed.

For lighting applications, groups of lights must be defined and managed. Commands to a group of light must arrive within 200 ms at all destinations. The installation and operation of a building network has different requirements. During the installation, many stand-alone networks of a few to 100 nodes coexist without a connection to the backbone. During this phase, the nodes are identified with a network identifier related to their physical location. Devices are accessed from an installation tool to connect them to the network in a secure fashion. During installation, the setting of parameters of common values to enable interoperability may be required. During operation, the networks are connected to the backbone while maintaining the network identifier to physical location relation. Network parameters like address and name are stored in the DNS. The names can assist in determining the physical location of the device.

It is also important for a building automation NMS to take safety and security into account. Ensuring privacy and confidentiality of data, such that unauthorized parties do not get access to it, is likely to be important since users' individual behaviors could be potentially understood via their settings. Appropriate security considerations for authorization and access control to the NMS is also important since different users are likely to have varied levels of operational permissions in the system. For example, while end users should be able to control lighting systems, HVAC systems, etc., only qualified technicians should be able to configure parameters that change the fundamental operation of a device. It is also important for devices and the NMS to be able to detect and report any tampering they might find, since these could lead to potential user safety concerns, e.g., if sensors controlling air quality are tampered with such that the levels of carbon monoxide become life threatening. This implies that an NMS should also be able to deal with and appropriately prioritize situations that might potentially lead to safety concerns.

4.7. Home Automation

Home automation includes the control of lighting, heating, ventilation, air conditioning, appliances, entertainment and home security devices to improve convenience, comfort, energy efficiency, and safety. It can be seen as a residential extension of building automation. However, unlike a BAS, the infrastructure in a home is operated in a considerably more ad hoc manner. While in some

installations it is likely that there is no centralized management system akin to a BAS available, in other situations outsourced and cloud-based systems responsible for managing devices in the home might be used.

Home-automation networks need a certain amount of configuration (associating switches or sensors to actuators) that is either provided by electricians deploying home-automation solutions, by third-party home-automation service providers (e.g., small specialized companies or home-automation device manufacturers) or by residents by using the application user interface provided by home-automation devices to configure (parts of) the home-automation solution. Similarly, failures may be reported via suitable interfaces to residents or they might be recorded and made available to services providers in charge of the maintenance of the home-automation infrastructure.

The management responsibility either lies with the residents or is outsourced to electricians and/or third parties providing management of home-automation solutions as a service. A varying combination of electricians, service providers, or the residents may be responsible for different aspects of managing the infrastructure. The time scale for failure detection and resolution is, in many cases, likely counted in hours to days.

4.8. Transport Applications

"Transport application" is a generic term for the integrated application of communications, control, and information processing in a transportation system. "Transport telematics" and "vehicle telematics" are both used as terms for the group of technologies that support transportation systems. Transport applications running on such a transportation system cover all modes of the transport and consider all elements of the transportation system, i.e. the vehicle, the infrastructure, and the driver or user, interacting together dynamically. Examples for transport applications are inter- and intra-vehicular communication, smart traffic control, smart parking, electronic toll-collection systems, logistic and fleet management, vehicle control, and safety and roadside assistance.

As a distributed system, transport applications require an end-to-end management of different types of networks. It is likely that constrained devices in a network (e.g., a moving in-car network) have to be controlled by an application running on an application server in the network of a service provider. Such a highly distributed network including cellular devices on vehicles is assumed to include a wireless access network using diverse long-distance wireless technologies such as WiMAX, 3G/LTE, or satellite communication, e.g.,

based on an embedded hardware module. As a result, the management of constrained devices in the transport system might be necessary to plan top-down and might need to use data models obliged from and defined on the application layer. The assumed device classes in use are mainly C2 [RFC7228] devices. In cases, where an in-vehicle network is involved, C1 devices [RFC7228] with limited capabilities and a short-distance constrained radio network, e.g., IEEE 802.15.4 might be used additionally.

All Transport Applications will require an IT infrastructure to run on top of, e.g., in public-transport scenarios like trains, buses, or metro networks infrastructure might be provided, maintained, and operated by third parties like mobile-network or satellite-network operators. However, the management responsibility of the transport application typically rests within the organization running the transport application (in the public-transport scenario, this would typically be the public-transport operator). Different aspects of the infrastructure might also be managed by different entities. For example, the in-car devices are likely to be installed and managed by the manufacturer, while the local government or transportation authority might be responsible for the on-road vehicular communication infrastructure used by these devices. The backend infrastructure is also likely to be maintained by third-party operators. As such, the NMS must be able to deal with different network segments (each being operated and controlled by separate entities) and enable appropriate access control and security.

Depending on the type of application domain (vehicular or stationary) and service being provided, it is important for the NMS to be able to function with different architectures, since different manufacturers might have their own proprietary systems relying on a specific management topology option, as described in [RFC7547]. Moreover, constituents of the network can either be private, belong to individuals or private companies, or be owned by public institutions leading to different legal and organization requirements. Across the entire infrastructure, a variety of constrained devices is likely to be used, and they must be individually managed. The NMS must be able to either work directly with different types of devices or have the ability to interoperate with multiple different systems.

The challenges in the management of vehicles in a mobile-transport application are manifold. The up-to-date position of each node in the network should be reported to the corresponding management entities, since the nodes could be moving within or roaming between different networks. Secondly, a variety of troubleshooting information, including sensitive location information, needs to be reported to the management system in order to provide accurate service to the customer. Management systems dealing with mobile

nodes could possibly exploit specific patterns in the mobility of the nodes. These patterns emerge due to repetitive vehicular usage in scenarios like people commuting to work and supply vehicles transporting shipments between warehouses, etc. The NMS must also be able to handle partitioned networks, which would arise due to the dynamic nature of traffic resulting in large inter-vehicle gaps in sparsely populated scenarios. Since mobile nodes might roam in remote networks, the NMS should be able to provide operating configuration updates regardless of node location.

The constrained devices in a moving transport network might be initially configured in a factory, and a reconfiguration might be needed only rarely. New devices might be integrated in an ad hoc manner based on self-management and self-configuration capabilities. Monitoring and data exchange might be necessary via a gateway entity connected to the backend transport infrastructure. The devices and entities in the transport infrastructure need to be monitored more frequently and may be able to communicate with a higher data rate. The connectivity of such entities does not necessarily need to be wireless. The time scale for detecting and recording failures in a moving transport network is likely measured in hours, and repairs might easily take days. It is likely that a self-healing feature would be used locally. On the other hand, failures in fixed transport-application infrastructure (e.g., traffic lights, digital-signage displays) are likely to be measured in minutes so as to avoid untoward traffic incidents. As such, the NMS must be able to deal with differing timeliness requirements based on the type of devices.

Since transport applications of the constrained devices and networks deal with automotive vehicles, malfunctions and misuse can potentially lead to safety concerns as well. As such, besides access control, privacy of user data, and timeliness, management systems should also be able to detect situations that are potentially hazardous to safety. Some of these situations could be automatically mitigated, e.g., traffic lights with incorrect timing, but others might require human intervention, e.g., failed traffic lights. The management system should take appropriate actions in these situations. Maintaining data confidentiality and integrity is also an important security aspect of a management system since tampering (or malfunction) can also lead to potentially dangerous situations.

4.9. Community Network Applications

Community networks are comprised of constrained routers in a multi-hop mesh topology, communicating over lossy, and often wireless, channels. While the routers are mostly non-mobile, the topology may be very dynamic because of fluctuations in link quality of the (wireless) channel caused by, e.g., obstacles, or other nearby radio

transmissions. Depending on the routers that are used in the community network, the resources of the routers (memory, CPU) may be more or less constrained -- available resources may range from only a few kilobytes of RAM to several megabytes or more, and CPUs may be small and embedded, or more powerful general-purpose processors. Examples of such community networks are the FunkFeuer network (Vienna, Austria), FreiFunk (Berlin, Germany), Seattle Wireless (Seattle, USA), and AWMN (Athens, Greece). These community networks are public and non-regulated, allowing their users to connect to each other and -- through an uplink to an ISP -- to the Internet. No fee, other than the initial purchase of a wireless router, is charged for these services. Applications of these community networks can be diverse, e.g., location-based services, free Internet access, file sharing between users, distributed chat services, social networking, video sharing, etc.

As an example of a community network, the FunkFeuer network comprises several hundred routers, many of which have several radio interfaces (with omnidirectional and some directed antennas). The routers of the network are small-sized wireless routers, such as the Linksys WRT54GL, available in 2011 for less than 50 euros. Each router, with 16 MB of RAM and 264 MHz of CPU power, is mounted on the rooftop of a user. When a new user wants to connect to the network, they acquire a wireless router, install the appropriate firmware and routing protocol, and mount the router on the rooftop. IP addresses for the router are assigned manually from a list of addresses (because of the lack of autoconfiguration standards for mesh networks in the IETF).

While the routers are non-mobile, fluctuations in link quality require an ad hoc routing protocol that allows for quick convergence to reflect the effective topology of the network (such as Neighborhood Discovery Protocol (NHDP) [RFC6130] and Optimized Link State Routing version 2 (OLSRv2) [RFC7181] developed in the MANET WG). Usually, no human interaction is required for these protocols, as all variable parameters required by the routing protocol are either negotiated in the control traffic exchange or are only of local importance to each router (i.e. do not influence interoperability). However, external management and monitoring of an ad hoc routing protocol may be desirable to optimize parameters of the routing protocol. Such an optimization may lead to a topology that is perceived to be more stable and to a lower control traffic overhead (and therefore to a higher delivery success ratio of data packets, a lower end-to-end delay, and less unnecessary bandwidth and energy use).

Different use cases for the management of community networks are possible:

- A single NMS, e.g., a border gateway providing connectivity to the Internet, requires managing or monitoring routers in the community network, in order to investigate problems (monitoring) or to improve performance by changing parameters (managing). As the topology of the network is dynamic, constant connectivity of each router towards the management station cannot be guaranteed. Current network management protocols, such as SNMP and Network Configuration Protocol (NETCONF), may be used (e.g., use of interfaces such as the NHDP-MIB [RFC6779]). However, when routers in the community network are constrained, existing protocols may require too many resources in terms of memory and CPU; and more importantly, the bandwidth requirements may exceed the available channel capacity in wireless mesh networks. Moreover, management and monitoring may be unfeasible if the connection between the NMS and the routers is frequently interrupted.

- Distributed network monitoring, in which more than one management station monitors or manages other routers. Because connectivity to a server cannot be guaranteed at all times, a distributed approach may provide a higher reliability, at the cost of increased complexity. Currently, no IETF standard exists for distributed monitoring and management.

- Monitoring and management of a whole network or a group of routers. Monitoring the performance of a community network may require more information than what can be acquired from a single router using a network management protocol. Statistics, such as topology changes over time, data throughput along certain routing paths, congestion, etc., are of interest for a group of routers (or the routing domain) as a whole. As of 2014, no IETF standard allows for monitoring or managing whole networks instead of single routers.

4.10. Field Operations

The challenges of configuring and monitoring networks operated in the field by rescue and security agencies can be different from the other use cases since the requirements and operating conditions of such networks are quite different.

With technology advancements, field networks operated nowadays are becoming large and can consist of a variety of different types of equipment that run different protocols and tools that obviously increase complexity of these mission-critical networks. In many scenarios, configurations are, most likely, manually performed.

Furthermore, some legacy and even modern devices do not even support IP networking. A majority of protocols and tools developed by vendors that are being used are proprietary, which makes integration more difficult.

The main reason for this disjoint operation scenario is that most equipment is developed with specific task requirements in mind, rather than interoperability of the varied equipment types. For example, the operating conditions experienced by high altitude security equipment is significantly different from that used in desert conditions. Similarly, equipment used in fire rescue has different requirements than flood-relief equipment. Furthermore, interoperation of equipment with telecommunication equipment was not an expected outcome or (in some scenarios) may not even be desirable.

Currently, field networks operate with a fixed Network Operations Center (NOC) that physically manages the configuration and evaluation of all field devices. Once configured, the devices might be deployed in fixed or mobile scenarios. Any configuration changes required would need to be appropriately encrypted and authenticated to prevent unauthorized access.

Hierarchical management of devices is a common requirement in such scenarios since local managers or operators may need to respond to changing conditions within their purview. The level of configuration management available at each hierarchy must also be closely governed.

Since many field operation devices are used in hostile environments, a high failure and disconnection rate should be tolerated by the NMS, which must also be able to deal with multiple gateways and disjoint management protocols.

Multi-national field operations involving search, rescue, and security are becoming increasingly common, requiring interoperation of a diverse set of equipment designed with different operating conditions in mind. Furthermore, different intra- and inter-governmental agencies are likely to have a different set of standards, best practices, rules and regulations, and implementation approaches that may contradict or conflict with each other. The NMS should be able to detect these and handle them in an acceptable manner, which may require human intervention.

5. Security Considerations

This document discusses use cases for management of networks with constrained devices. The security considerations described throughout the companion document [RFC7547] apply here as well.

6. Informative References

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <http://www.rfc-editor.org/info/rfc6130>.

[RFC6568] Kim, E., Kaspar, D., and JP. Vasseur, "Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6568, DOI 10.17487/RFC6568, April 2012, <http://www.rfc-editor.org/info/rfc6568>.

[RFC6779] Herberg, U., Cole, R., and I. Chakeres, "Definition of Managed Objects for the Neighborhood Discovery Protocol", RFC 6779, DOI 10.17487/RFC6779, October 2012, <http://www.rfc-editor.org/info/rfc6779>.

[RFC6988] Quittek, J., Ed., Chandramouli, M., Winter, R., Dietz, T., and B. Claise, "Requirements for Energy Management", RFC 6988, DOI 10.17487/RFC6988, September 2013, <http://www.rfc-editor.org/info/rfc6988>.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <http://www.rfc-editor.org/info/rfc7181>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <http://www.rfc-editor.org/info/rfc7228>.

[RFC7326] Parello, J., Claise, B., Schoening, B., and J. Quittek, "Energy Management Framework", RFC 7326, DOI 10.17487/RFC7326, September 2014, <http://www.rfc-editor.org/info/rfc7326>.

[RFC7547] Ersue, M., Ed., Romascanu, D., Schoenwaelder, J., and U. Herberg, "Management of Networks with Constrained Devices: Problem Statement and Requirements", RFC 7547, DOI 10.17487/RFC7547, May 2015, <http://www.rfc-editor.org/info/rfc7547>.

[IOT-SEC] Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., and R. Struik, "Security Considerations in the IP-based Internet of Things", Work in Progress, draft-garcia-core-security-06, September 2013.

[IEEE802.11]
IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11, March 2012, <http://standards.ieee.org/about/get/802/802.11.html>.

[IEEE802.15]
IEEE, "WIRELESS PERSONAL AREA NETWORKS (PANs)", IEEE Standard 802.15, 2003-2014, <https://standards.ieee.org/about/get/802/802.15.html>.

[IEEE802.15.4]
IEEE, "Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE Standard 802.15.4, September 2011, <https://standards.ieee.org/about/get/802/802.15.html>.

Acknowledgments

The following persons reviewed and provided valuable comments during the creation of this document:

Dominique Barthel, Carsten Bormann, Zhen Cao, Benoit Claise, Bert Greevenbosch, Ulrich Herberg, Ted Lemon, Kathleen Moriarty, James Nguyen, Zach Shelby, Peter van der Stok, and Martin Thomson.

The authors would like to thank the reviewers and the participants on the Coman mailing list for their valuable contributions and comments.

Juergen Schoenwaelder and Anuj Sehgal were partly funded by Flamingo, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

Contributors

The following persons made significant contributions to and reviewed this document:

- Ulrich Herberg contributed Section 4.9, "Community Network Applications".
- Peter van der Stok contributed to Section 4.6, "Building Automation".
- Zhen Cao contributed to Section 2.2, "Cellular Access Technologies".
- Gilman Tolle contributed Section 4.4 "Energy Management".
- James Nguyen and Ulrich Herberg contributed to Section 4.10 "Field Operations".

Authors' Addresses

Mehmet Ersue (editor)
Nokia Networks

EMail: mehmet.ersue@nokia.com

Dan Romascanu
Avaya

EMail: dromasca@avaya.com

Juergen Schoenwaelder
Jacobs University Bremen

EMail: j.schoenwaelder@jacobs-university.de

Anuj Sehgal
Jacobs University Bremen

EMail: s.anuj@jacobs-university.de