Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 28, 2014

M. Ersue, Ed.
Nokia Solutions and Networks
D. Romascanu
Avaya
J. Schoenwaelder
Jacobs University Bremen
October 25, 2013

# Management of Networks with Constrained Devices: Use Cases
draft-ersue-opsawg-coman-use-cases-00

## Abstract

This document discusses the use cases concerning the management of networks, where 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 [COM-REQ].

## Status of this Memo

## Copyright Notice

## Table of Contents

# 1. Introduction

## 1.1. Overview

Small devices with limited CPU, memory, and power resources, so called constrained devices (aka. sensor, smart object, or smart device) 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 non-constrained 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 send 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 elements that are needed to manage, processes the data, and presents them to the network management users. Constrained devices, however, often have limited power, low transmission range, and might be unreliable. 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 type of challenges compared to the management of a traditional IP network.

This document aims to understand the use cases for the management of a network, where constrained devices are involved. The document lists and discusses diverse use cases for the management from the network as well as from the application point of view. 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 [COM-REQ].

## 1.2. Terminology

This documents builds on the terminology defined in [I-D.ietf-lwig-terminology] and [COM-REQ]. [I-D.ietf-lwig-terminology] is a base document for the terminology concerning constrained devices and constrained networks.

## 2. Use Cases

### 2.1. 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 the monitoring whether the system is still functional and the roll-out of new constrained devices in case the system looses too much of its structure. The constrained devices themselves need to be able to establish connectivity (auto-configuration) and they need to be able to deal with events such as loosing 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. However, for certain environmental monitoring applications, much tighter time scales may exist and might be enforced by regulations (e.g., monitoring of nuclear radiation).

## 2.2. Medical Applications

Constrained devices can be seen as an enabling technology for advanced and possibly remote health monitoring and emergency notification systems, ranging from blood pressure and heart rate monitors to advanced devices capable to monitor 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 setup by average people. In the second case, it can be expected that devices be controlled by specially trained people. In both cases, however, it is crucial to protect the privacy of the people to which medical devices are attached. Even though the data collected by a heart beat 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 since the biggest market is likely elderly and handicapped people. As such, fault detection of the communication network or the constrained devices becomes a crucial function that must be carried out with high reliability and, depending on the medical appliance and its application, within seconds.

### 2.3. Industrial Applications

Industrial Applications and smart manufacturing refer not only to production equipment, but also to a factory that carries out centralized control of energy, HVAC (heating, ventilation, and air conditioning), lighting, access control, etc. via a network. 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 demand, 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, as well as 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.

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 must be effectively integrated with the decision environment. Wireless sensor networks (WSN) 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. WSNs can provide today wireless link reliability, real-time capabilities, and quality-of-service and enable industrial and related wireless sense and control applications.

Management of industrial and factory applications is largely focused on the 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 (auto-configuration) 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.

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.

## 2.4. Home Automation

Home automation includes the control of lighting, heating, ventilation, air conditioning, appliances, and entertainment devices to improve convenience, comfort, energy efficiency, and security. It can be seen as a residential extension of building automation.

Home automation networks need a certain amount of configuration (associating switches or sensors to actors) that is either provided by electricians deploying home automation solutions or done by residents by using the application user interface 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 electricians in charge of the maintenance of the home automation infrastructure.

The management responsibility lies either with the residents or it may be outsourced to electricians providing management of home automation solutions as a service. The time scale for failure detection and resolution is in many cases likely counted in hours to days.

## 2.5. 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 (BAS) may be deployed concentrating the various functions of safety, environmental control, occupancy, security. More and more the deployment of the various functional systems is connected to the same communication infrastructure (possibly Internet Protocol based), which may involve wired or wireless communications networks inside the building.

Building automation requires the deployment of a large number (10-100.000) of sensors that monitor the status of devices, and 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 between 1 to 20 meters. 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. The management includes verifying the presence of the expected devices and detecting the presence of unwanted devices.

Examples of functions performed by such controllers are regulating the quality, humidity, and temperature of the air inside the building and 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 subnets, where a subnet covers a floor, an area on the floor, or a given functionality (e.g. security cameras).

Some of the sensors in Building Automation Systems (for example fire alarms or security systems) register, record and transfer critical alarm information and therefore must be resilient to events like loss of power or security attacks. This leads to the need that some components and subsystems operate in constrained conditions and are separately certified. 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.

Building Automation solutions are deployed in some cases 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 structure taking into account factors like existing wiring, distance limitations, the propagation of radio signals over walls and floors. As a result, some of the existing WLAN solutions (e.g. IEEE 802.11 or IEEE 802.15) 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 class 0 or class 1 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 co-exist 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 to common values to enable interoperability may occur (e.g. Trickle parameter values). 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 DNS. The names can assist in determining the physical location of the device.

## 2.6. Energy Management

EMAN working group developed [I-D.ietf-eman-framework], which defines a framework for providing Energy Management for devices 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 that have energy management capability are defined as Energy Devices and identified components within a device (Energy Device Components) 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. An Energy Management System is a combination of hardware and software used to administer a network with the primary purpose being Energy Management. The operators of such a 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. 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).

Energy Management is especially relevant to 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. As such Smart Grid provides sustainable and reliable generation, transmission, distribution, storage and consumption of electrical energy based on advanced energy and ICT solutions and as such enables e.g. following specific application areas: Smart transmission systems, Demand Response/Load Management, Substation Automation, Advanced Distribution Management, Advanced Metering Infrastructure

(AMI), Smart Metering, Smart Home and Building Automation, E-mobility, etc.

Smart Metering is a good example of a M2M application and can be realized as one of the vertical applications in an M2M environment. Different types of possibly wireless small meters produce all together a huge amount of data, which is collected by a central entity and processed by an application server. The M2M infrastructure can be provided by a mobile network operator as the

meters in urban areas will have most likely a cellular or WiMAX radio.

Smart Grid is built on a distributed and heterogeneous network and can use a combination of diverse networking technologies, such as wireless Access Technologies (WiMAX, Cellular, etc.), wireline and Internet Technologies (e.g., IP/MPLS, Ethernet, SDH/PDH over Fiber optic, etc.) as well as low-power radio technologies enabling the networking of smart meters, home appliances, and constrained devices (e.g. BT-LE, ZigBee, Z-Wave, Wi-Fi, etc.). The operational effectiveness of the smart grid is highly dependent on a robust, two-way, secure, and reliable communications network with suitable availability.

The management of a distributed system like smart grid requires an end-to-end management of and information exchange through different type of networks. However, as of today there is no integrated smart grid management approach and no common smart grid information model available. Specific smart grid applications or network islands use their own management mechanisms. For example, the management of smart meters depends very much on the AMI environment they have been integrated to and the networking technologies they are using. In general, smart meters do only need seldom reconfiguration and they send a small amount of redundant data to a central entity. For a discussion on the management needs of an AMI network see Section 2.11. The management needs for Smart Home and Building Automation are discussed in Section 2.4 and Section 2.5.

## 2.7. Transport Applications

Transport Application is a generic term for the integrated application of communications, control, and information processing in a transportation system. Transport telematics or vehicle telematics are used as a term 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. The overall aim is to improve decision making, often in real time, by transport network controllers and other users, thereby improving the operation of the entire transport system. As such, transport applications can be seen as one of the important M2M service scenarios with the involvement of manifold small devices.

The definition encompasses a broad array of techniques and approaches that may be achieved through stand-alone technological applications or as enhancements to other transportation communication schemes. 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 road 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 mobile 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 devices. In cases, where an in-vehicle network is involved, C1 devices with limited capabilities and a short-distance constrained radio network, e.g. IEEE 802.15.4 might be used additionally.

Management responsibility typically rests within the organization running the transport application. 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 -configuration capabilities.  Monitoring and data exchange might be necessary to do via a gateway entity connected to the back-end transport infrastructure.  The devices and entities in the transport infrastructure need to be monitored more frequently and can 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.

## 2.8. 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.  It is likely that constrained devices in such a network are mainly C2 devices 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 WiMAX, or 3G/LTE, e.g. based on embedded hardware modules.  In cases, where an in-building network is involved, the network can be based on Ethernet or wireless technologies suitable for in-building usage.

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 changes are rare since the infrastructure itself changes rarely.  However, monitoring devices are often deployed in unsupervised environments and 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.

## 2.9. Community Network Applications

Community networks are comprised of constrained routers in a multi-hop mesh topology, communicating over a lossy, and often wireless channel. 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 etc, 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. These routers, with 16 MB of RAM and 264 MHz of CPU power, are mounted on the rooftops of the users. When new users want 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 NHDP [RFC6130] and OLSRv2 [I-D.ietf-manet-olsrv2] 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 more stable perceived topology 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 usage.

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

- One single Network Management Station (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 Netconf, may be used (e.g., using 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.

- A 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 2012, no IETF standard allows for monitoring or managing whole networks, instead of single routers.

## 2.10. Mobile Applications

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. This diverse range of machines brings new network and service requirements and challenges. Different applications e.g. in a home appliance or in-car network use Bluetooth, Wi-Fi or Zigbee 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, e.g.:

- a smart phone 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 IoT connectivity technologies including ZigBee and 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 by manifold type and size 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 case 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 Network Management System (NMS) run by the mobile operator. Smart phones or embedded modules connected to a gateway might be themselves in charge to manage 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 challenges in the management of devices in a mobile application are manifold. Firstly, the issues caused through the device mobility need to be taken into consideration. While the cellular devices are moving around or roaming between different regional networks, they should report their status to the corresponding management entities with regard to their proximity and management hierarchy. Secondly, a variety of device troubleshooting information needs to be reported to the management system in order to provide accurate service to the customer. Third but not least, the NMS and the used management protocol need to be tailored to keep the cellular devices lightweight and as energy efficient as possible.

The data models used in these scenario are mostly derived from the models of the operator NMS and might be used to monitor the status of the devices and to exchange the data sent by or read from the devices. 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.

## 2.11. Automated Metering Infrastructure (AMI)

An AMI network enables an electric utility to retrieve frequent electric usage data from each electric meter installed at a customer's home or business. With an AMI network, a utility can also receive immediate notification of power outages when they occur, directly from the electric meters that are experiencing those

outages. In addition, if the AMI network is designed to be open and extensible, it could serve as the backbone for communicating with other distribution automation devices besides meters, which could include transformers and reclosers.

In this use case, each meter in the AMI network contains a constrained device. These devices are typically C2 devices. Each meter connects to a constrained mesh network with a low-bandwidth radio. These radios can be 50, 150, or 200 kbps at raw link speed, but actual network throughput may be significantly lower due to forward error correction, multihop delays, MAC delays, lossy links, and protocol overhead.

The constrained devices are used to connect the metering logic with the network, so that usage data and outage notifications can be sent back to the utility's headend systems over the network. These headend systems are located in a data center managed by the utility, and may include meter data collection systems, meter data management systems, and outage management systems.

The meters are connected to a mesh network, and each meter can act as both a source of traffic and as a router for other meters' traffic. In a typical AMI application, smaller amounts of traffic (read requests, configuration) flow "downstream" from the headend to the mesh, and larger amounts of traffic flow "upstream" from the mesh to the headend. However, during a firmware update operation, larger amounts of traffic might flow downstream while smaller amounts flow upstream. Other applications that make use of the AMI network may have their own distinct traffic flows.

The mesh network is anchored by a collection of higher-end devices, which contain a mesh radio that connects to the constrained network as well as a backhaul link that connects to a less-constrained network. The backhaul link could be cellular, WiMAX, or Ethernet, depending on the backhaul networking technology that the utility has chosen. These higher-end devices (termed "routers" in this use case) are typically installed on utility poles throughout the service territory. Router devices are typically less constrained than meters, and often contain the full routing table for all the endpoints routing through them.

In this use case, the utility typically installs on the order of 1000 meters per router. The collection of meters comprised in a local network that are routing through a specific router is called in this use case a Local Meter Network (LMN). When powered on, each meter is designed to discover the nearby LMNs, select the optimal LMN to join, and select the optimal meters in that LMN to route through when sending data to the headend. After joining the LMN, the meter is

designed to continuously monitor and optimize its connection to the LMN, and it may change routes and LMNs as needed.

Each LMN may be configured e.g. to share an encryption key, providing confidentiality for all data traffic within the LMN. This key may be obtained by a meter only after an end-to-end authentication process based on certificates, ensuring that only authorized and authenticated meters are allowed to join the LMN, and by extension, the mesh network as a whole.

After joining the LMN, each endpoint obtains a routable and possibly private IPv6 address that enables end-to-end communication between the headend systems and each meter. In this use case, the meters are always-on. However, due to lossy links and network optimization, not every meter will be immediately accessible, though eventually every meter will be able to exchange data with the headend.

In a large AMI deployment, there may be 10 million meters supported by 10.000 routers, spread across a very large geographic area. Within a single LMN, the meters may range between 1 and approx. 20 hops from the router. During the deployment process, these meters are installed and turned on in large batches, and those meters must be authenticated, given addresses, and provisioned with any configuration information necessary for their operation. During deployment and after deployment is finished, the network must be monitored continuously and failures must be handled. Configuration parameters may need to be changed on large numbers of devices, but most of the devices will be running the same configuration. Moreover, eventually, the firmware in those meters will need to be upgraded, and this must also be done in large batches because most of the devices will be running the same firmware image.

Because there may be thousands of routers, this operational model (batch deployment, automatic provisioning, continuous monitoring, batch reconfiguration, batch firmware update) should also apply to the routers as well as the constrained devices. The scale is different (thousands instead of millions) but still large enough to make individual management impractical for routers as well.

### 2.12. MANET Concept of Operations (CONOPS) in Military

The use case on the Concept of Operations (CONOPS) focuses on the configuration and monitoring of networks that are currently being used in military and as such, it offers insights and challenges of network management that military agencies are facing.

As technology advances, military networks nowadays become large and consist of varieties of different types of equipments that run

different protocols and tools that obviously increase complexity of the tactical networks. Moreover, lacks of open common interfaces and Application Programming Interface (API) are often a challenge to network management. Configurations are, most likely, manually performed. Some devices do not support IP networks. Integration and evaluation process are no longer trivial for a large set of protocols and tools. In addition, majority of protocols and tools developed by vendors that are being used are proprietary which makes integration more difficult. The main reason that leads to this problem is that there is no clearly defined standard for the MANET Concept of Operations (CONOPS). In the following, a set of scenarios of network operations are described, which might lead to the development of network management protocols and a framework that can potentially be used in military networks.

Note: The term "node" is used at IETF for either a host or router. The term "unit" or "mobile unit" in military (e.g. Humvees, tanks) is a unit that contains multiple routers, hosts, and/or other non-IP-based communication devices.

Scenario: Parking Lot Staging Area:

The Parking Lot Staging Area is the most common network operation that is currently widely used in military prior to deployment. MANET routers, which can be identical such as the platoon leader's or rifleman's radio, are shipped to a remote location along with a Fixed

Network Operations Center (NOC), where they are all connected over traditional wired or wireless networks. The Fixed NOC then performs mass-configuration and evaluation of configuration processes. The same concept can be applied to mobile units. Once all units are successfully configured, they are ready to be deployed.

```
   +---------+             +----------+
   |  Fixed  |<---+------->| router_1 |
   |   NOC   |    |        +----------+
   +---------+    |
                  |        +----------+
                  +------->| router_2 |
                  |        +----------+
                  |            0
                  |            0
                  |            0
                  |        +----------+
                  +------->| router_N |
                           +----------+
```

Figure 1: Parking Lot Staging Area

Scenario: Monitoring with SatCom Reachback:

The Monitoring with SatCom Reachback, which is considered another possible common scenario to military's network operations, is similar to the Parking Lot Staging Area. Instead, the Fixed NOC and MANET routers are connected through a Satellite Communications (SatCom) network. The Monitoring with SatCom Reachback is a scenario where MANET routers are augmented with SatCom Reachback capabilities while On-The-Move (OTM). Vehicles carrying MANET routers support multiple types of wireless interfaces, including High Capacity Short Range Radio interfaces as well as Low Capacity OTM SatCom interfaces. The radio interfaces are the preferred interfaces for carrying data traffic due to their high capacity, but the range is limiting with respect to connectivity to a Fixed NOC. Hence, OTM SatCom interfaces offer a more persistent but lower capacity reachback capability. The existence of a SatCom persistent Reachback capability offers the NOC the ability to monitor and manage the MANET routers over the air.

Similarly to the Parking Lot Staging scenario, the same concept can be applied to mobile units.

```
                            ---   +--+    ---
                           /  /---|SC|---/  /
                           ---    +--+   ---
   +---------+                      |
   |  Fixed  |<---------------------+
   |   NOC   |       +--------------|
   +---------+       |              +-------------------+
                     |              |                   |
                 +----------+       |               +----------+
                 | router_1 |       +----------+    | router_N |
                 +----------+       |          |    +----------+
                     *              |          |      *   *
                     *        +----------+     |      *   *
                     *********| router_2 |*****|*******   *
                              +----------+     |          *
                                   *           |          *
                                   *       +----------+   *
                                   ********| router_3 |****
                                           +----------+

         ---  SatCom links
         ***  Radio links
```

Figure 2: Monitoring with one-hop SatCom Reachback network

Scenario: Hierarchical Management:

Another reasonable scenario common to military operations in a MANET environment is the Hierarchical Management scenario. Vehicles carry a rather complex set of networking devices, including routers running MANET control protocols. In this hierarchical architecture, the MANET mobile unit has a rather complex internal architecture where a local manager within the unit is responsible for local management. The local management includes management of the MANET router and control protocols, the firewall, servers, proxies, hosts and applications. In addition, a standard management interface is required in this architecture. Moreover, in addition to requiring standard management interfaces into the components comprising the MANET nodal architecture, the local manager is responsible for local monitoring and the generation of periodic reports back to the Fixed NOC.

```
                               Interface
                               |
                               V
   +---------+             +-------------------------+
   |  Fixed  |  Interface  | +---+     +---+         |
   |   NOC   |<---+------->| | R |--+--| F |         |
   +---------+    |        | +---+  |  +---+         |
                  |        |        |    |  +---+    |
                  |        | +---+  |    +--| P |    |
                  |        | | M |--+    |  +---+    |
                  |        | +---+       |           |
                  |        |             |  +---+    |
                  |        |             +--| D |    |
                  |        |             |  +---+    |
                  |        |             |           |
                  |        |             |  +---+    |
                  |        |             +--| H |    |
                  |        |             |  +---+    |
                  |        | unit_1                  |
                  |        +-------------------------+
                  |
                  |
                  |        +--------+
                  +------->| unit_2 |
                  |        +--------+
                  |            0
                  |            0
                  |            0
                  |        +--------+
                  +------->| unit_N |
                           +--------+

         Key: R-Router
              F-Firewall
              P-PEP (Performance Enhancing Proxy)
              D-Servers, e.g., DNS
              H-hosts
              M-Local Manager
```

Figure 3: Hierarchical Management

Scenario: Management over Lossy/Intermittent Links:

In the future of military operations, the standard management will be done over lossy and intermittent links and ideally the Fixed NOC will become mobile.  In this architecture, the nature and current quality of each link are distinct. However, there are a number of issues that would arise and need to be addressed:

1. Common and specific configurations are undefined:

    A. When mass-configuring devices, common set of configurations are undefined at this time.

    B. Similarly, when performing a specific device, set of specific configurations is unknown.

2. Once the total number of units becomes quite large, scalability would be an issue and need to be addressed.

3. The state of the devices are different and may be in various states of operations, e.g., ON/OFF, etc.

4. Pushing large data files over reliable transport, e.g., TCP, would be problematic. Would a new mechanism of transmitting large configurations over the air in low bandwidth be implemented? Which protocol would be used at transport layer?

5. How to validate network configuration (and local configuration) is complex, even when to cutover is an interesting question.

6. Security as a general issue needs to be addressed as it could be problematic in military operations.

```
+---------+             +----------+
|  Mobile |<----------->| router_1 |
|   NOC   |?--+         +----------+
+---------+    |
      ^        |        +----------+
      |        +------->| router_2 |
      |                 +----------+
      |                     0
      |                     0
      |                     0
      |                 +----------+
      +---------------->| router_N |
                        +----------+
```

Figure 4: Management over Lossy/intermittent Links

## 3. IANA Considerations

This document does not introduce any new code-points or namespaces for registration with IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

## 4. Security Considerations

This document discusses the use cases for a network of constrained devices and does not introduce any security issues by itself.

## 5. Contributors

Following persons made significant contributions to and reviewed this document:

- Ulrich Herberg (Fujitsu Laboratories of America) contributed the Section 2.9 on Community Network Applications.

- Peter van der Stok contributed to Section 2.5 on Building Automation.

- Zhen Cao contributed to Section 2.10 on Mobile Applications.

- Gilman Tolle contributed the Section 2.11 on Automated Metering Infrastructure.

- James Nguyen and Ulrich Herberg contributed the Section 2.12 on MANET Concept of Operations (CONOPS) in Military.

## 6. Acknowledgments

Following persons reviewed and provided valuable comments to different versions of this document:

Dominique Barthel, Carsten Bormann, Zhen Cao, Benoit Claise, Bert Greevenbosch, Ulrich Herberg, James Nguyen, Anuj Sehgal, Zach Shelby, and Peter van der Stok.

The editors would like to thank the reviewers and the participants on the Coman maillist for their valuable contributions and comments.

# 7. References

## 7.1. Normative References

## 7.2. Informative References

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC6779] Herberg, U., Cole, R., and I. Chakeres, "Definition of Managed Objects for the Neighborhood Discovery Protocol", RFC 6779, October 2012.

[RFC6988] Quittek, J., Chandramouli, M., Winter, R., Dietz, T., and B. Claise, "Requirements for Energy Management", RFC 6988, September 2013.

[I-D.ietf-lwig-terminology]
Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained Node Networks", draft-ietf-lwig-terminology-05 (work in progress), July 2013.

[I-D.ietf-eman-framework]
Parello, J., Claise, B., Schoening, B., and J. Quittek, "Energy Management Framework", draft-ietf-eman-framework-11 (work in progress), October 2013.

[I-D.ietf-manet-olsrv2]
Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol version 2", draft-ietf-manet-olsrv2-19 (work in progress), March 2013.

[COM-REQ] Ersue, M., "Constrained Management: Problem statement and Requirements", draft-ersue-coman-prostate-reqs (work in progress), October 2013.

## Appendix A. Open issues

- It has been noted that the use cases the Industrial Application, Home Automation and Building Automation have an intersect.

## Appendix B. Change Log

### B.1. draft-ersue-constrained-mgmt-03 - draft-ersue-opsawg-coman-use-cases-00

- Reduced the terminology section for terminology addressed in the LWIG and Coman Requirements drafts. Referenced the other drafts.

- Checked and aligned all terminology against the LWIG terminology draft.

- Spent some effort to resolve the intersection between the Industrial Application, Home Automation and Building Automation use cases.

- Moved section section 3. Use Cases from the companion document [COM-REQ] to this draft.

- Reformulation of some text parts for more clarity.

### B.2. draft-ersue-constrained-mgmt-02-03

- Extended the terminology section and removed some of the terminology addressed in the new LWIG terminology draft. Referenced the LWIG terminology draft.

- Moved Section 1.3. on Constrained Device Classes to the new LWIG terminology draft.

- Class of networks considering the different type of radio and communication technologies in use and dimensions extended.

- Extended the Problem Statement in Section 2. following the requirements listed in Section 4.

- Following requirements, which belong together and can be realized with similar or same kind of solutions, have been merged.

  * Distributed Management and Peer Configuration,

  * Device status monitoring and Neighbor-monitoring,

  * Passive Monitoring and Reactive Monitoring,

  * Event-driven self-management - Self-healing and Periodic self-management,

   - Authentication of management systems and Authentication of managed devices,

   - Access control on devices and Access control on management systems,

   - Management of Energy Resources and Data models for energy management,

   - Software distribution (group-based firmware update) and Group-based provisioning.

- Deleted the empty section on the gaps in network management standards, as it will be written in a separate draft.

- Added links to mentioned external pages.

- Added text on OMA M2M Device Classification in appendix.

## B.3. draft-ersue-constrained-mgmt-01-02

- Extended the terminology section.

- Added additional text for the use cases concerning deployment type, network topology in use, network size, network capabilities, radio technology, etc.

- Added examples for device classes in a use case.

- Added additional text provided by Cao Zhen (China Mobile) for Mobile Applications and by Peter van der Stok for Building Automation.

- Added the new use cases 'Advanced Metering Infrastructure' and 'MANET Concept of Operations in Military'.

- Added the section 'Managing the Constrainedness of a Device or Network' discussing the needs of very constrained devices.

- Added a note that the requirements in [COM-REQ] need to be seen as standalone requirements and the current document does not recommend any profile of requirements.

- Added a section in [COM-REQ] for the detailed requirements on constrained management matched to management tasks like fault, monitoring, configuration management, Security and Access Control, Energy Management, etc.

- Solved nits and added references.

- Added Appendix A on the related development in other bodies.

- Added Appendix B on the work in related research projects.

### B.4. draft-ersue-constrained-mgmt-00-01

- Splitted the section on 'Networks of Constrained Devices' into the sections 'Network Topology Options' and 'Management Topology Options'.

- Added the use case 'Community Network Applications' and 'Mobile Applications'.

- Provided a Contributors section.

- Extended the section on 'Medical Applications'.

- Solved nits and added references.

## Authors' Addresses

Mehmet Ersue (editor)
Nokia Solutions and Networks

Email: mehmet.ersue@nsn.com

Dan Romascanu
Avaya

Email: dromasca@avaya.com

Juergen Schoenwaelder
Jacobs University Bremen

Email: j.schoenwaelder@jacobs-university.de