ACCEPTED FROM OPEN CALL

# A NETWORK ARCHITECTURE SOLUTION FOR EFFICIENT IOT WSN BACKHAULING: CHALLENGES AND OPPORTUNITIES

ROMANO FANTACCI, TOMMASO PECORELLA, ROBERTO VITI, AND CAMILLO CARLINI

## ABSTRACT

At present, Sensor Networks and the emerging Internet of Things paradigm are playing a key role in the industry and in academic research. In this article we outline a common scenario, currently arising standards, and other emerging technologies having a direct impact on network architecture. In particular we introduce a novel network architecture based on an M2M Gateway and discuss it in relation to smart building applications. The proposed network architecture will improve services for users and will offer new opportunities for both service providers and network operators.

## INTRODUCTION

Sensor Networks, and in particular Wireless Sensor Networks (WSNs), are playing a key role in the industry and in academic research. The constant miniaturization of sensors and wireless technologies, along with the progressive improvement in battery efficiency, have made it possible to offer solutions for a wide range of applications.

Currently, smart sensors are primarily conceived to offer a service to single users (e.g. personal antitheft systems, home automation, etc.), or, at best, to buildings or campus-wide scenarios (e.g. remote managed temperature for energy savings). In the future, leveraging the Internet of Things (IoT) capabilities, sensors will be used to build large scale systems, where a service provider will be able to leverage gathered data.

In order to achieve this goal, it is mandatory to provide efficient network architectures and suitable telecommunication standards. WSNs usually adopt different communication and security protocols than "normal" Internet (e.g. CoRE instead of HTTP, OMA-DM Lightweight instead of OMA-DM, etc.) in order to be supported by the WSN limited hardware. In particular, suitable methodologies to perform a protocol translation and security enforcement must be implemented. In this scenario, the Network Operator (NO) role can become central in order to ensure the WSN provisioning and management, and to offer the WSN delivered services to other service providers (e.g. energy utilities, municipalities, etc.).

The outlined scenario radically differs from the current mobile or landline NO service model, where the user and related devices are basically connected through IPv4 NATs and the communication is almost always user-initiated. Moreover, there are several additional requirements. As an example, IP connections will have to be assigned on a semi-permanent basis, security will have to be enforced, and suitable techniques will be made available to handle traffic patterns largely dependent on devices and services.

All these elements are challenging for the NOs, due to the need for adaptations to existing network infrastructures and correctly planning new ones (e.g. 4G/5G networks).

With the aim of satisfying most of these requirements, we propose a network architecture that involves the Internet gateway, already available at the user site, to remotely manage the WSN and user's devices.

The aim of this article is to analyze and critically discuss the role of the proposed network architecture in service provisioning for IoT sensing devices. Potential breakthroughs and open challenges related to technologies and standards will also be investigated. Finally, a viable architectural view of the communication hub for WSN managed by the NO will be presented and discussed.

## NETWORK TECHNOLOGIES OVERVIEW

Protocols involving WSNs and its sensors are evolving from a nearly closed ecosystem (e.g. ZigBee Alliance) to open protocols. Nevertheless, as in most open-protocol systems, there is not a single protocol for each task. A competing set of standards are emerging, particularly at the transport and application levels. Standardization bodies are working to provide good alternatives to existing Home Automation systems (e.g. KNX), based on the IoT concepts. If successful, these efforts will enable better integration, more

*Romano Fantacci, Tommaso Pecorella, and Roberto Viti are with Università di Firenze.*

*Camillo Carlini is with Telecom Italia S.p.A.*


1536-1284/14/$25.00 © 2014 IEEE

Due to the Internet's pervasive presence, TCP/IP is often given as granted in smart ecosystems. Moreover, the forecasted number of new objects imposes the use of IPv6. IETF is working on Low Power and Lossy Networks (LLNs) in order to standardize some protocols specifically built for these devices.

compatibility and, certainly, open new markets. However, it will probably be a matter of economy and industrialization that determines which protocol(s) will gain a *de facto* standard status. In what follows, we provide a concise overview of some activities of standardization bodies concerning protocols and network architectures that have been recently developed.

## IEEE

IEEE is responsible for a number of protocols that are used worldwide. The 802.15.4 standard covers the PHY and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPANs). It is typically used by Wireless Sensors and Actuator Networks. A new standard (802.15.4e) is being developed to overcome current standard limitations, in particular concerning the guaranteed data rate needed by critical applications.

## IETF

Due to the Internet's pervasive presence, TCP/IP is often given as granted in smart ecosystems. Moreover, the forecasted number of new objects imposes the use of IPv6. IETF is working on Low Power and Lossy Networks (LLNs) in order to standardize some protocols specifically built for these devices. For our scenario, the following three IETF Working Groups are relevant.

**6lowpan WG —** This working group is standardizing protocols in order to adapt IPv6 to LLN. These standards act as middleware between IPv6 and MAC protocols (e.g. RFC 6282 covers IPv6 header compression and pocket fragmentation) or optimize IPv6 protocols for specific cases (e.g. RFC 6775 optimizes Neighbor Discovery, header compression, etc.).

**Roll WG —** The focus of this WG is on routing. The developed RFCs define a new routing protocol (IPv6 Routing Protocol for Low-Power and Lossy Networks, RPL) specifically designed for LLNs. The protocol is very interesting, and is supported by many WSN Operating Systems (e.g. Contiki, TinyOS, RiOT). In order to optimize the system, it is of paramount importance to study the protocol's behavior under different use-cases. At present, only a handful of simulators and emulators are available to study the protocols in great detail [1, 2].

**Core WG —** Core stands for Constrained RESTful Environments and, as the name suggests, this WG is working on the adaptation of the RESTful paradigm to the specific needs of constrained devices, such as Sensors and Actuators. Until now, no RFCs have been published. However, there are pre-release implementations of the protocols available in the most used WSN OSs. In particular, the Constrained Application Protocol (CoAP) is strongly influenced by HTTP. This enables the easy building of application-level gateways in order to translate HTTP to CoAP and vice-versa.

The CoRE/CoAP protocols are expected to have a high impact on traffic patterns from and to devices. Moreover, application protocols such as CoAP are foreseen to be used for both device management and data collection. Thus, the evaluation of their use and capabilities is of primary importance.

## WSN Operating Systems

The operating system of a sensor node is usually reduced to the bare minimum. The set of libraries used to build applications are often referred to as an "OS," even though they are very different from normal Operating Systems. There are three notable systems for WSN: Contiki,[1] TinyOS,[2] and RiOT.[3] Moreover, the ZigBee Alliance developed a set of specifications for IP-based ZigBee nodes.[4] All the above mentioned Operating Systems have been used extensively in academia. The specific market applicability of each one has to be evaluated according to the specific application.

## Open Mobile Alliance

The Open Mobile Alliance (OMA) has worked on Device Management (DM) standardization for the last decade, starting its focus with phones and moving to smartphones and non-human devices.

**OMA DM —** In April 2013 an ad-hoc OMA Incubator Group released a specification [3] providing a client profile for OMA DM Protocol v1.3. Such a profile is meant to be implemented on M2M devices, leveraging, at the same time, already deployed server-side assets. Moreover, M2M management is not limited to remote device management; it is also the basic building block to articulate and wrap the final service/business logics.

**OMA Lightweight —** The OMA Lightweight M2M (OMA LWM2M [4]) is a protocol suitable for resource-constrained devices, aimed at minimizing any overhead in device-server communication. The protocol is based on CoAP drafts and early implementations, attempting in this way to avoid any industry fragmentation and also to be familiar to the many developers already utilizing the RESTful paradigm. From the NO point of view, LWM2M is complementary to OMA DM.

**OMA M2M Gateway —** The rationale for the M2M Gateway [5], especially in its adaptation-mode variant, is the definition of a standard path to integrate non-OMA DM end devices into a fully OMA DM compliant architecture, making it possible to perform remote operations with virtually any M2M device, using the same OMA DM server entity.

## oneM2M

In July 2012 oneM2M was founded. It is a global organization whose main objective is driving the IoT industry toward a common Service Layer with standard protocols, APIs, and data structures (objects) for devices. Again, the most important goal is preventing industry fragmentation. For this reason, oneM2M has many other standards organizations as partners and is evaluating, harmonizing, and simplifying some existing key technical specifications (e.g. ETSI M2M Functional architecture [6] and, for remote management, the whole set of OMA DM specifications). Before the end of 2014, oneM2M Release 1 specifications (Requirements, Functional architecture, Protocols, Security) are expected to be published.

[1] http://www.contiki-os.org, BSD License

[2] http://www.tinyos.net, BSD License

[3] http://www.riot-os.org,GNU Lesser General Public License, version 2

[4] http://www.zigbee.org/Specifications/ZigBeeIP/Overview.aspx

## IPSO Alliance

The IPSO Alliance is not a standards development organization. Its aim is to promote a full IP-based approach in the construction of "Smart Objects" networks, stimulating the work of SDOs (e.g. IETF, OMA, etc.). Among IPSO Alliance initiatives, of particular interest is the effort to drive device vendors, and the IoT industry in general, toward a common representation of device capabilities and resources. This representation should be, in the IPSO approach, functional and technology-independent.

## IoT Managed Gateway: Concepts, Potential Breakthrough, and Challenges

Given an increasing demand for M2M services and a very good availability of commercial devices, the challenge is to identify a unified platform enabling the convergence of different end-to-end services. A key enabling element to achieve this goal is the M2M Gateway, able to abstract the diversity of end devices and integrate them into a standard architecture.

Network providers are able to remotely interoperate with M2M Gateways and offer managed services to end-users, both delivering the required business logic and, at the same time, ensuring total customer care, through remote configuration, fault, and performance management.

NOs able to build Gateway-centric infrastructures (sometimes called M2M capillary networks) may be able to play a key role in IoT value propositions, overcoming traditional communications commoditization and helping the industry in building crucial assets for IoT realization.

It must be emphasized that this approach goes beyond the old concept of services offered by the NO to its customers, due to the expansion of the horizon, to services offered also to second-level Service Providers, as outlined in Fig. 1. This is not to be confused with the classic case of telecommunication infrastructure shared by multiple NOs (unbundling). As a matter of fact, the new vision goes beyond the unbundling and the 'network as a tube' concepts. In the new model, the NO will be an active player in defining the service platform and, most importantly, in ensuring its provisioning, management, and operations.

The protocols needed to deploy WSN in the real world are certainly quite mature and there is enough space for a profitable scenario, even for a NO. Despite this, suitable network architectures and telecommunication standards are needed. The NO can actually play an important role in WSN provisioning, particularly in the areas of device life cycle management, service provisioning, and security enforcing. The NO can also build new services based on managed sensor networks. However, this could lead to potential lock-in effects and net-neutrality issues.

### Network Operator Challenges

**Traffic Patterns and QoS Management —** Telecommunication networks are usually built and operated according to pre-determined traffic patterns. Almost all standards consider traffic types that are not suitable to describe WSN traffic. The traffic pattern is still to be precisely characterized, and this could impact negatively the network. Moreover, WSN data will require QoS levels usually designed for industrial power plants. However, bandwidth requirements and traffic shape are the most critical part.

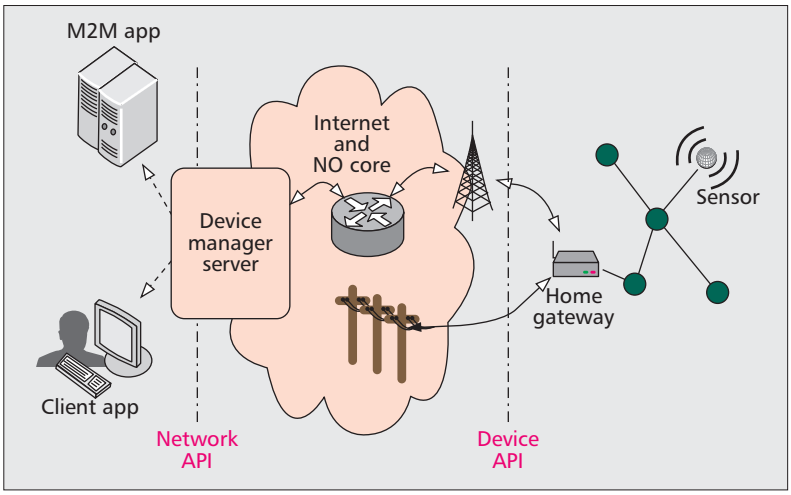


**Figure 1.** Role of the network operator.

**Security Enforcement —** In order to build a profitable ecosystem based on services provided through the NO, second level service providers will need to leverage trusted and seamless interfaces toward the WSN. Moreover, user privacy will have to be preserved. The NO will have to manage all security aspects, including the WSN and gateway security management.

**IP Address Provisioning —** The IoT paradigm is heavily based on IPv6. Moreover, Stateless Autoconfiguration assumes that WSN can use a /64 network. Even if this point could be mitigated by using ULA or Link-Local addresses, the NO will still need to assign fixed networks to users in order to manage devices. However, this approach raises some security concerns: an attacker could try to guess the Gateway address easily. IPv6 address management will be an important part, as it will require changes in the network element assigning addresses and, most probably, also in the Authorization, Authentication and Accounting (AAA) infrastructure.

**Device Supply Chain —** Devices can be installed either by a specialized technician or by the user. In the first case, the correct device provisioning and configuration is ensured. As for the second case, which is foreseen to become quite common, it raises some issues. In order to use the sensed data, the Service Operator should trust the device quality (e.g. its sensing precision, tolerance range, etc.). This goal can be met by a correct supply chain, where only devices sold by authorized dealers can be properly installed in the user's network (Fig. 2). The device configuration system will need to use standard device configuration protocols, which will be discussed in the following section.

It is worth pointing out that some devices may not need a rigid supply chain. In this case, the devices will not be trusted by the NO and the user will be able to use them only for private purposes.

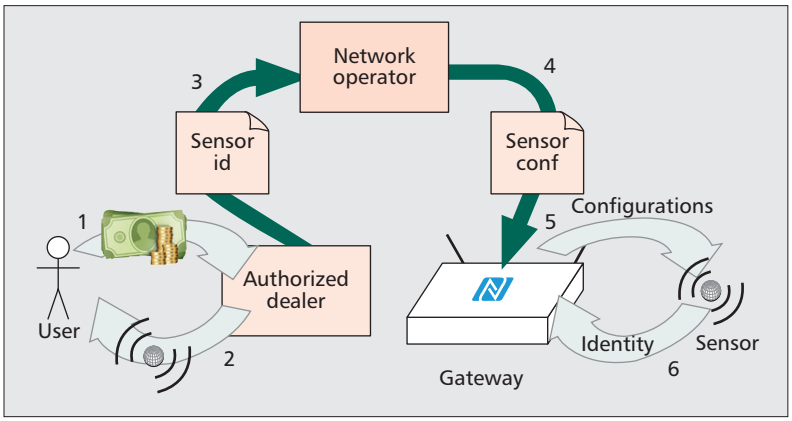


**Figure 2.** Supply chain for sensors.

## Standardization and Implementation Challenges

**Device Management Protocols —** As outlined previously, new IoT-based device management protocols are being standardized. Nevertheless, device management is not a new field, and several solutions are available (e.g. KNX, OpenWebNet, ZigBee, etc.). The challenge is to define open and flexible methods able to leverage existing systems. With this aim, OMA protocols seem to be promising.

**Security Interfaces and Protocols —** Security in WSN and IoT devices requires, so far, further research efforts. Many attacks are possible on 802.15.4 devices, and they can hinder both WSN operation and data reliability. Future smart environments cannot allow this. Although security elements exist in many protocols (e.g. 802.15.4, RPL, CoAP, etc.), a specific security analysis is still needed to assess the possible threats. Moreover, not every type of device will need the same protection level. In order to minimize the cryptography overhead and save precious resources, we think it is important to define security interfaces for different network segments (see also [7]). Borrowing the concepts of LTE security zones, a device functionality will be enabled only if it can comply with given security interfaces, basically consisting of a set of minimum secure protocols and certification levels.

**Device Life Cycle Management —** Device life cycle is only partially solved by remote management. Remote management can be used to read device data, control actuators, and even reprogram a device. However, device-first configuration can not leverage this system. Typically, WSN programming involves flashing in the device a firmware containing important information such as network security configurations, device ID, etc. Some protocols (e.g. 802.15.4, RPL, etc.) can be used to auto-configure devices. However, auto-configuration can raise further problems such as devices joining the wrong network in dense environments.

It is possible to ask users to perform a device activation though the Internet, basically flashing a custom firmware downloaded from the Internet (e.g. through a web-based NO device configuration service). However, in this case the device should be connected to a PC (e.g. via USB). This solution is error-prone and not ideal.

A simpler solution is to leverage low cost systems, such as NFC. By using NFC, the Communication Hub can install proper configurations in the device, leveraging the supply chain procedures as well. A device will be able to properly join a user's WSN only if a configuration element (bound to the particular device) has been installed in the Communication Hub by the NO.

Devices not requiring this procedure can acquire different configurations from the Hub. Users will be able to use them, but they will not be part of the NO managed system (and they will not harm it in case of faulty behavior).

## Lock-In and Net Neutrality

The lock-in effect and the net neutrality problem are closely related. The term *lock-in* defines the problem of a user being forced to keep the current NO or Service Provider due to the installed/used devices and services. Commercial entities are naturally willing to maintain the user fidelity. This can be done with "good" practices (e.g. the user's satisfaction) or by making it difficult (or even impossible) to change the NO/Service Provider without significative effort and financial loss.

WSNs are particularly critical for what concerns the lock-in effect. The WSN could be used only by the user, thus being completely transparent to the NO and Service Providers. The lock-in effect is possible whenever the WSN is managed or accessed by an external Service Provider. Moreover, if the NO is also a Service Provider, it could use traffic shaping and throttling systems to degrade third party Service Providers. The net-neutrality violations and the consequent lock-in effects must be monitored. Protective measures (e.g. regulations) are necessary in order to avoid service degradations.

# A Telecommunication Network Architecture Solution for IoT

Our scenario is a smart building with apartments equipped with various actuator/sensor devices able to communicate autonomously in order to accomplish tasks or to assist human needs. This scenario is outlined in Fig. 3.

In this apartment, Internet access is provided via a home router. The router connects to the ISP either through a mobile or a terrestrial network (i.e. 3G/4G, ADSL) and provides Ethernet and WiFi connections to the user devices. The key point is that, in addition to this standard configuration, the router is equipped with one or more IEEE 802.15.4 interfaces, becoming, in this way, an active element in the smart building environment. Being able to manage the WSN, it becomes a *Communication Hub* between smart devices, Service Operators, and users. It is worth noticing that the scenario is not limited to a smart building as the same technologies and concepts can be used for different environments, e.g. public areas.

The proposed network architecture features will include WSN support, OMA DM and AllJoyn [8] protocols, and a device activation

and configuration system, with the last one still in a design state. The global network architecture, shown in Fig. 4, is discussed in this section.

OMA DM [9, 10] is used by the NO to push configurations into the Gateway. These can either be "normal" configurations (e.g. DLS profiles, APN names, etc.), or belong to the WSN. In this case, the NO is able to manage and gather the WSN device sensed data. While *OMA DM Client* handles the connections, the data are saved in the *OMA DM Tree*. This tree-shaped dataset is constituted by smaller elements, the managed objects, representing a single device and carrying all the sensor-related information from configuration values (e.g. channel ID, network prefix) to actual sensed data.

Data are regularly updated through CoRE/CoAP by a sensor daemon (*SensorD*); this element generates CoAP messages to registered sensors to correctly refresh the information stored in the OMA DM Tree with new data, in order to simplify access to the service provider. These updates are also performed after specific requests coming from users or from other services (e.g. through AllJoyn). To achieve this behavior, while keeping the data updated, all the data requested from the user pass through the OMA DM Tree. All user requests (e.g. coming from AllJoyn) flag a desired managed object, representing the sensor, as "data requested." In this scenario, SensorD detects the flagged object and sends a request to the relative sensor to retrieve the new value.

In the proposed network architecture, the WSN facilities are provided by a Zolertia's Z1 mote connected via USB. This mote acts as a RPL border router, and CoAP messages are delivered in IPv6 datagram through a SLIP tunnel made over the USB connection.

## How Our Approach Helps Solve Open Issues

The proposed network architecture provides support to satisfy the following requirements:

***Traffic patterns and QoS Management —*** The M2M Gateway represents an important element for traffic engineering. It allows the Service Provider to access the sensor and actuator networks seamlessly. At the same time, it can isolate the Sensor Network from continuous network interactions possibly leading to battery discharge.

The QoS can be enforced by the M2M Gateway on the sensor network (e.g. by adapting the sensor data update rate to the current environment status) and on the operator's network (e.g. by prioritizing the data flows depending on their relevance and timeliness).

***Device Life Cycle Management —*** Device life cycle management is supported by standardized mechanisms, avoiding potential lock-in effects.

The M2M Gateway architecture enables the device secure configuration and its pairing with the user network (Fig. 2, phases 4–6). The OMA DM framework can easily be extended to include future device types, and allows a wide interoperability among gateways and devices provided by different vendors. The device identity can be defined according to the device type (e.g. a WSN node could have a Vendor/Product ID). The configuration of managed sensors is remotely deployed into the M2M gateway using OMA DM and is stored in the OMA DM tree. It includes the sensor capabilities, the network channel, and cryptographic keys (if needed), etc.

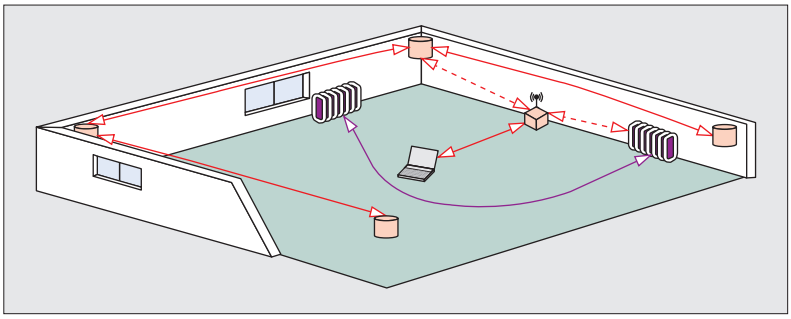

**Figure 3.** Heterogeneous sensors and actuators network in a smart building (e.g. an apartment) scenario.

The configuration procedure can use direct USB connections or Over The Air (OTA) programming/configuration systems. In both cases, the M2M Gateway must validate the device identity by comparing the unique device identity with its own device database. It must be pointed out that device activation must be supported by short-range communications only in order to avoid device identity spoofing. Sensors can also be added to the OMA DM tree autonomously by the M2M Gateway. In this case, the sensor will not be remotely managed. For a full discussion about managed and non-managed device differences, see [7].

***IPv6 Address Provisioning and Security —*** A device can obtain an IPv6 address in different ways. Moreover, users are expected to receive a /64 network from the NO, for the home devices address assignment. In the proposed architecture, the M2M Gateway is responsible for handling the sensor network IPv6 addresses, for example, by using 6LoWPAN-ND (RFC 6775). This can limit the number of /64 subnets assigned to the user.

The sensor network security is a very important element, and the M2M Gateway has a central role in the security enforcement architecture. It acts as a security enforcing point, dividing the various security zones and ensuring that in each zone the appropriate security techniques (protocols, cyphering, etc.) are used [7]. For this task, the M2M Gateway will have to be considered as a security enforcing point.

***Standardization/Lock-in —*** The proposed architecture is based on standard protocols, thus preventing (or at least minimizing) the lock-in effect. Moreover, IPv6 should ensure a global reachability of the WSN, which is not limited to the NO. As a consequence, a third-party Service Provider should be able to access the proposed architecture services. In case of NO switching, the user should be able to keep all the owned devices. The only potential problem is represent-

From the NO point of view, this new market will open extremely interesting business opportunities along with relevant challenges to comply with the QoS needed by the new traffic patterns and to provide support to the new type of devices. This will require non-trivial modifications to network elements and actual resource assignment policies.

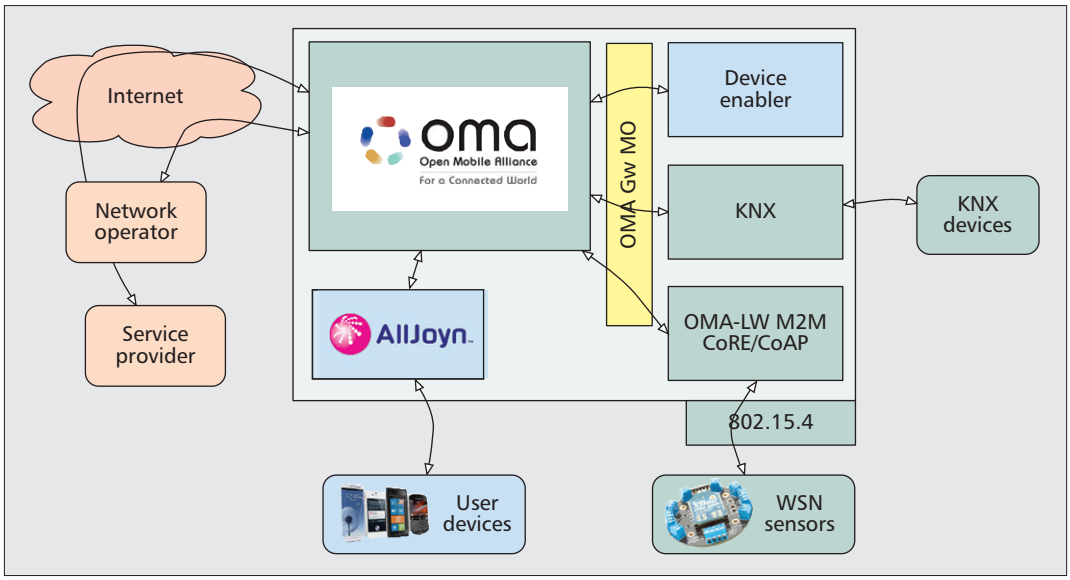


**Figure 4.** Architecture for the communication hub prototype.

ed by security associations between the gateway and the nodes. This point is mainly related to device management, and is left for further study.

Net neutrality violation may still affect the proposed architecture. However, data flows can not be totally blocked by a NO. In the worst case scenario, the NO could assign the best-effort class to the WSN data streams. Despite this, the expected WSN data rate is small compared to normal Internet connections. As a consequence, the lack of net neutrality is not considered as a real issue.

## Conclusions

The envisioned network architecture is currently deployed in *Telecom Italia Lab* offices in Roma in order to test how sensors deployed in a smart building (e.g. an apartment) can be remotely managed. A key point of this architecture is that, by turning the home gateway into a connection hub, all traffic directed to the WSN can be secured using standard Internet solutions (e.g. IPSec). In addition to this, it is important to stress that all the traffic directed to the WSN can leverage the network QoS mechanisms. As a result, sensors needing particular QoS guarantees (e.g. health monitoring devices) will have enhanced reliability, with benefits for M2M communications, and the consistent growth of IoT.

As outlined in the article, some relevant points will have to be addressed by standardization bodies, manufacturers, and network operators. From the NO point of view, this new market will open extremely interesting business opportunities along with relevant challenges to comply with the QoS needed by the new traffic patterns and to provide support to the new type of devices. This will require non-trivial modifications to network elements and actual resource assignment policies. We strongly believe that these modifications can be implemented and deployed, opening new possibilities for users, Network Operators, and other Service Providers.

## References


[1] L. Ben Saad, C. Chauvenet, and B. Tourancheau, "Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: Two Case Studies," *Proc. Int'l Conf. Sensor Technologies and Applications SENSORCOMM 2011*, Nice, France: IARIA, Aug. 2011; available at http://hal.inria.fr/hal-00647869.

[2] L. Bartolozzi, T. Pecorella, and R. Fantacci, "ns-3 RPL Module: IPv6 Routing Protocol for Low Power and Lossy Networks," *Proc. Workshop on ns-3*, ACM, 6 2012.

[3] Open Mobile Alliance, "Client Profile of OMA Device Management v1.3," Tech. Rep., 2013; available at http://technical.openmobilealliance.org/Technical/releaseprogram/docs/OIG/V10-20130430-C/OMA-PD-DMClient-Profile-V10-20130430-C.pdf

[4] Open Mobile Alliance, "Lightweight Machine to Machine Requirements," Tech. Rep., 2013; available: at http://technical.openmobilealliance.org/Technical/releaseprogram/docs/copyrightclick.aspx?pck=LightweightM2M&file=V10-20121127-C/OMA-RD-LightweightM2M-V10-20121002-C.pdf.

[5] Open Mobile Alliance, "GwMO Architecture," Tech. Rep., 2013; available at http://technical.openmobilealliance.org/Technical/releaseprogram/docs/CopyrightClick.aspx?pck=GwMO&file=V10-20130618-A/OMA-AD-GwMO-V10-20130618-A.pdf.

[6] European Telecommunications Standards Institute, "TS102690 — Machine-to-Machine Communications (M2M) Functional Architecture," Tech. Rep., 2013; available at http://www.etsi.org/deliver/etsits/102600102699/102690/01.01.0160/ts102690v010101p.pdf.

[7] R. Fantacci *et al.*, "Enabling Technologies for Smart Building, What's Missing?" *Proc. AEIT Annual Conference*, 2013, Oct. 2013, pp. 1–5.

[8] Alljoyn — Proximity Based Peer-to-Peer Technology; available at http://www.alljoyn.org.

[9] Open Mobile Alliance, "OMA Device Management Protocol, Version 1.3," Tech. Rep., 2013; available at http://technical.openmobilealliance.org/Technical/releaseprogram/docs/CopyrightClick.aspx?pck=DM&file=V13-20121213-C/OMA-TS-DMProtocol-V13-20121009-C.pdf.

[10] Open Mobile Alliance, "OMA Gateway Management Object (GwMO) Requirements," Tech. Rep., 2013; available at http://technical.openmobilealliance.org/Technical/releaseprogram/GwMOV11.aspx.


## Biographies

Romano Fantacci [M'84–SM'90–F'05] received his Ph.D. degree in telecommunications in 1987 from the University of Florence, where he has been a full professor since 1999. He has been involved in several European Space Agency (ESA) and European Union research projects, and is an author of more than 300 papers. He is president of the

Information Communication Technology Consortium (TiCOM) a joint venture between the University of Florence and Selex ES SpA, a Finmeccanica Company. He has guest edited special issues in IEEE journals, and was an Associate Editor for several journals and founding Area Editor for *IEEE Transactions on Wireless Communications*.

TOMMASO PECORELLA [S'90–M'00] received the Dr.Ing. degree in electronics engineering from the University of Firenze, Firenze, Italy, in 1996, and the Ph.D. degree in telecommunications engineering in 1999. In 2000 he joined CNIT: Italian University Consortium for Telecommunications as a scientific researcher. Since 2001 he has been an assistant professor at the University of Firenze. His research interests involve computer communications, mobile communication networks, QoS-enabled access schemes, satellite communication networks, queuing theory, Wireless Sensor Networks, ad-hoc routing, network simulations, network management, and security.

ROBERTO VITI [S'13] received the First Level degree in computer engineering at University of Firenze, Firenze, Italy, in 2011. In 2012 joined the CNIT: Italian University Consortium for Telecommunications as a contract researcher. His research interests involve computer communications, mobile communication networks, Wireless Sensor Networks, network simulations, network security, QoS-enabled flow control, Mobile IP, and traffic offloading.

CAMILLO CARLINI received his M.Sc. degree in electronics engineering from the University of Florence in 2004. After working in the semiconductor industry, in 2006 he joined TILab, the Innovation and Engineering Department of Telecom Italia (TI). Within TILab, he is now a wireless devices manager, responsible for different projects aimed at increasing mobile users' quality of experience and services sustainability. In the area of mobile devices (from physical to apps layer), wireless access innovation and IoT ecosystems, he is in charge of assessing the impact and potential integration with TI Wireless Network of new technology trends. He is a TI delegate in OMA, W3C, Small Cell Forum, and 3GPP RAN5. He has authored technical papers published in international journals and is a frequent speaker at wireless industry conferences worldwide.