February 11, 2011

Position Paper on "Interconnecting Smart Objects with the Internet"

Mehmet Ersue (mehmet.ersue@nsn.com)
Jouni Korhonen (jouni.korhonen@nsn.com)

Introduction

The terminology for "Internet of Things" (IoT) is still nascent, and depending on the network type or layer in focus diverse technologies and terms are in use. Where some of the research work has been focusing on the wireless network of sensors, other work has concentrated on Radio-frequency identification (RFID) interconnection. Some of the available work prefers to talk on 'Internet of Objects' where others introduce a 'Web of Things'.

Common to all these considerations is the 'Things' or 'Objects' are supposed to have physical or virtual identities using interfaces to communicate. In this context, we need to differentiate between the "physical Things, Constrained or Smart Devices" (referred to as 'SD') with possibly multi-homed network interfaces identified by IP addresses and "Smart or Connected Objects" (referred to as 'SO'), which can be identified as a resource or a virtual object by using a unique identifier. Furthermore, the SDs usually have a limited memory and CPU power and aim to be self-configuring and easy to deploy.

The technologies for the networking of SDs became Internet-like and essential for IETF standardization work at the latest with the use of IEEE 802.15.4, IPv6 and 6LoWPAN as the adaptation layer in between. Today IPv6 is the natural choice for interconnecting the vast amount of SDs among each other and to the rest of the Internet. However, the tininess of the network nodes requires a rethinking of the protocol characteristics concerning power consumption, performance, memory, and CPU usage. As such, there is a demand for protocol simplification, energy-efficient communication, less CPU usage and small memory footprint.

Technical Challenges for Interconnecting Smart Objects

On application layer IETF already started working on protocols like Constrained Application Protocol (CoAP) supporting constrained devices and networks e.g. for smart energy or Home Grid environment. The deployment of such an environment involves in fact many, in some cases up to million smart meters or small devices, which produce a huge amount of data. This data needs to be collected, filtered, and pre-processed for further use in diverse services.

Considering the high number of nodes to deploy, one has to think on manageability aspects of the Things and plan for easy deployment. As a consequence, seamless monitoring and self-configuration of such network nodes becomes imperative.

Furthermore, with the huge number of Smart Devices, the interoperability of communication interfaces and management mechanisms becomes vitally important. Without sufficient standardization of the involved protocols and management technologies, IoT cannot be deployed in a ubiquitous manner.

Following technologies are already essential for the development of IoT:

- Radio technologies such as IEEE 802.15.4 aiming a low power consumption,
- IPv6 as the protocol for the Internet layer supporting millions of SDs, which need to be identified and networked,

- Routing protocols like RPL supporting point-to-multipoint and multipoint-to-point traffic flows,
- Lightweight application protocol CoAP enabling easy interoperation and proxying with existing REST-based applications.

As discussed in various research documents following technologies or mechanisms might become additionally important and contribute to the development of IoT (examples):

- Energy efficient wireless technologies and communication mechanisms as well as SDs, which become active and consume power only when it is necessary,
- Enhancements to TCP to solve the congestion issues on lossy networks and provide better reliability on links with packet loss,
- Development of secure-enough and lightweight authentication interfaces, which enable the use of off-the-shelf protocols relying on e.g. secure transport of messages such as NETCONF [5],
- Efficient payload compression to reduce the communication cost,
- Simple but effective geolocation determination and the transport of geotagging information in a secure and private manner,
- XML-based data models supporting energy management and other applications for monitoring and controlling of sensors, meters and SDs as well as a lightweight protocol for the transport of model information,
- Protocols and mechanisms for collecting, filtering and processing the huge amount of data numerous SOs produce,
- Standardization of a globally unique namespace enabling ubiquitous services on top of SOs.

Architectural Challenges for the Networking of Smart Objects

There is an evident scalability issue with the IoT. Networking every SD with each other and exchanging application information between every SO might be an attractive vision, however in such an environment the IP traffic can increase significantly. Based on the limited memory, energy, and transmission range of the SDs, one can assume that not every SD or SO needs to communicate end-to-end with each other.

An essential paradigm in the research of wireless sensor networks is the loosely coupled and decentralized system of SOs. The SOs aim to act in an autonomous manner; individually as well as in a cluster, communicating with each other, but also exchanging information with servers or humans. An autonomous SO cluster can ease e.g. software distribution within a cluster. SOs can leverage their abilities if they begin cooperating by linking their capabilities ending up as a collective system of objects.

It is likely that clusters of SDs will be interconnected and will have an interface to the outside Internet on the cluster level. As a result, it is expected that clusters of SDs will be required to be self-sufficient and self-configuring. It appears to be beneficial if SD-clusters use middle-boxes at their external interfaces, comprising e.g. edge router and management server functionalities.

Compared to the improvement of networking capabilities of SDs the “Web of Things” proposes to integrate SDs into the Web in a way that the resources on SDs become available like any other Web resource or object. Using a REST-based architecture for the object-to-object communication enables compatibility with existing web servers and applications as well as the usability of existing application logic in the SO context. An interoperable architecture for the communication between SOs and web applications provides SOs a notion of their own identity in the Web making it possible to access their resources via the WWW.

A simple application layer protocol, such as CoAP, is essential to address the issue of efficient object-to-object communication and information exchange. Such an information exchange should be done based on a joint information model to enable the exchange and interpretation of policy information and application data.

With the increasing amount of data generated by SDs, the handling of data, i.e. collecting, filtering, pre-processing, analyzing, transforming, and event generation, will become resource consuming. Thus it would be favorable to introduce a processing layer between transport and application layers with the aim to pre-process and reduce the amount of sensor data and to simplify further usage in applications.

APIs separate the application logic from the mechanisms and technology used for communication. They provide application portability and access to common lower layer functionality. There is a need for appropriate APIs on different layers that can hide the knowledge on the functional logic but also the location of the functions. As a result, the architecture and the application logic become agnostic to the underlying functionality.

Manageability of Smart Objects and the IoT Infrastructure

In an ideal world, we would have only one network management protocol for monitoring, alarming, configuration, and exchanging policy information, independently of the type of network (e.g. Smart Grid, IoT, wireless access or core network). Furthermore, it would be ideal to have only one core information model as a basis, which could be used to derive different data models for protocols and network elements and to enable reuse of functionality. Using data models derived from the same base model with a compatible namespace would also enable an end-to-end information exchange.

Such an ideal management environment is indeed required by different industry sectors. For instance, the Smart Grid community is requesting one protocol for all management tasks to reduce the memory footprint, and the development and operational costs for smart meters. Moreover, the Smart Grid community would like to use their IEC/CIM-based information model [7] further, e.g. in the Home Grid, and for diverse small devices seamlessly by deriving from existing classes and functionality.

We believe NETCONF can be easily modified to become a generic management protocol supporting both, monitoring and configuration. NETCONF can be also implemented in a simplified manner for SDs by skipping functionality, which is not mandatory or would be overkill for small devices. Furthermore, the XML-based modeling language YANG [6] can easily facilitate the transformation and mapping between CIM-based information models and the data models developed at IETF. Extending YANG with language abstractions such as class inheritance would further simplify reuse of already existing functionality in industry information models and ease the mapping between the model worlds.

With the introduction of a lightweight NETCONF, also a lightweight secure transport becomes necessary. To be able to realize a secure transport layer we need an optimized implementation of SSH or TLS as well as a reliable transport with TCP.

Self-configuration and self-management is already a reality in the standards of some of the bodies such as 3GPP and BBF. To introduce self-configuration of smart devices successfully we need a device-initiated connection establishment. A self-configuration solution based on so called “call-home” has been discussed in length in ISMS WG and has been withdrawn because of security issues with SSH and asymmetric authentication.

Conclusion

Even with IoT the Internet will remain to be a “network of networks” connected to a “network of IoTs”. As with CoAP, lightweight Internet protocols will be made available, which are compatible with their predecessors using the same REST-based architecture. Another ongoing trend is that SDs get increasingly better CPUs and larger memories, thus SDs may over the time become able to use off-the-shelf Internet protocols.

However, for the time being, optimized implementations of Internet protocols are indispensable for the interconnection of SDs with the Internet.

As of today 6LoWPAN, RPL and CoAP are essential technologies for the communication of SDs and SOs. It would be valuable to provide a lightweight version of NETCONF for the configuration of SDs in a secure and reliable manner. Using a lightweight and interoperable version of NETCONF enables also the reuse of already developed basis of YANG data models. YANG enhanced with inheritance can furthermore support the utilization of YANG models in other SDOs but also ease reuse of existing functionality in industry information models.

IETF did not address yet the essential issue of self-configuration sufficiently and should restart this discussion. Self-configuration appears to be essential for the deployment of millions of smart devices in a plug&play manner enabling a large-scale IoT eco-system.

However, it is assumed that SD-to-SD communication will be mostly within a cluster of SDs. Considering the increasing CPU power and communication capabilities of SDs over the time, the IoT will most likely become increasingly Internet-like and will, to a large extend, meld with the Internet. Thus to enable such an evolvement, we believe the communication and security interfaces of SDs and SOs should be derived from and kept interoperable with the Internet and Web communication mechanisms of today.

References

[1] Lars Schor, et al., Towards a Zero-Configuration Wireless Sensor Network Architecture for Smart Buildings (BuildSys'09, November 3, 2009)

[2] Angelo P. Castellani, et al., Architecture and Protocols for the Internet of Things: A Case Study, 8th IEEE International Conference on Pervasive Computing and Communications Workshops, 2010

[3] Miao Wu, et al., Research on the architecture of Internet of things, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010

[4] Kortuem, G., et al., Smart objects as building blocks for the Internet of things, IEEE Internet Computing, Volume: 14 Issue:1, Jan.-Feb. 2010

[5] draft-ietf-netconf-4741bis-07, Network Configuration Protocol (NETCONF), http://tools.ietf.org/html/draft-ietf-netconf-4741bis-07

[6] RFC 6020, YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), http://tools.ietf.org/html/rfc6020

[7] IEC 61850-1, Communication networks and systems in substations - Part 1: Introduction and overview, http://webstore.iec.ch/preview/info_iec61850-1%7Bed1.0%7Den.pdf