IEEE COMMUNICATIONS SOCIETY

Ad Hoc and Sensor Networks Technical Committee (AHSN TC) Newsletter

CONTENTS

PREFACE

The IEEE ComSoc Ad Hoc and Sensor Networks Technical Committee (AHSN TC) aims at sponsoring scientific and technical activities facilitating the dissemination of knowledge in the areas of ad hoc, sensor and mesh networks. In an attempt to make all the TC members as well as the AHSN worldwide community aware of what is going on within our main areas of concerns, this newsletter had been set up*. The newsletter aims at inviting the authors of successful research projects and experts from all around the world with large vision about AHSN-related research activities to share their experience and knowledge by contributing a short news. So, the sixth issue of the AHSN TC Newsletter features one high quality news item gently provided by Dr. Michele Rossi (University of Padova and CFR), Dr. Alessandro Bassi (ABC Consulting), Dr. Francois Carrez (University of Surrey) and Dr. Michele Zorzi (University of Padova and CFR). We thank them as well as all the previous contributors for their effort to make this newsletter successful towards fulfilling its objectives.

Newsletter Co-editor

Yacine Ghamri-Doudane, University of La Rochelle, France (EiC)
Sidi-Mohammed Senouci, University of Burgundy, France (Co-EiC)
Mohamed Fathy Feteiha, Queen's University, Canada
Burak Kantarci, University of Ottawa, Canada
Damla Turgut, University of Central Florida, U.S.A.

**The AHSN TC Newsletter has been started in 2008, and then re-started in 2012 after 2 years of a stop due to the sad and tragic loss of our friend and colleague Professor Mieso Denko, from the University of Guelph (Canada), who was one of the initiator and an active leader of this Newsletter. In his memory the newsletter had been re-started in 2012 as a tribute to his life's work in research, education and services to the networking community as a whole.*

TC OFFICERS AND NEWSLETTER EDITORS

TC Officers

Names	Affiliation	E-mail
Nei Kato	Tohoku University, Japan	kato@it.ecei.tohoku.ac.jp
Jalel Ben Othman	University of Paris 13, France	jalel.ben-othman@univ-paris13.fr
Cheng Li	Memorial University of Newfoundland, Canada	licheng@mun.ca

Editor-in-Chief

Names	Affiliation	E-mail
Yacine Ghamri-Doudane	University of La Rochelle, France	yacine.ghamri@univ-lr.fr

Co-Editor-in-Chief

Names	Affiliation	E-mail
Sidi-Mohammed Senouci	University of Burgundy, France	sidimohammed.senouci@orange-ftgroup.com

Co-Editors

Names	Affiliation	E-mail
Mohamed Fathy Feteiha	Queen's University, Canada	feteiha@cs.queensu.ca
Burak Kantarci	University of Ottawa, Canada	kantarci@site.uottawa.ca
Damla Turgut	University of Central Florida, U.S.A.	turgut@eecs.ucf.edu

IEEE ComSoc AHSN TC Newsletter

The EU IoT-A Project – Toward a Common Language for the Internet of Things

Michele Rossi†, Alessandro Bassi‡, Francois Carrez⋆, Michele Zorzi†

Abstract

The Internet of Things (IoT) has been a lively research field for a few years, and is currently also becoming an interesting area for companies and investors. IoT is about devices and systems that in the near future will become more and more capable of communicating in a coordinated and automated fashion via the Internet. While an authoritative definition for IoT is still missing, in practice some IoT systems have been developed, including for example sensor networks and machine-to-machine communications (M2M), which are reaching a good level of maturity and are expected to bring about societal changes, enabling new interaction models among users, devices and services.

In the last few years, IoT has become a unifying term for any type of interconnected object. Initial advancements were especially led by visionary startups and SMEs. However, many of the solutions developed so far were designed with an ad hoc methodology. While this made it possible to quickly get the products to market, the developed solutions are often non-interoperable, non-scalable and non-expandable. The same holds true for larger industrial companies, that often develop highly dedicated solutions without taking any common framework into account.

The European IoT-A project, successfully concluded in November 2013, took care of these aspects, conceiving an architectural reference model for the Internet of Things and devising a methodology for the creation of IoT applications in a structured manner. In addition, networking aspects related to transport, security and M2M were investigated. In this brief article, we provide an outline of the major IoT-A achievements, and briefly discuss open challenges and next steps.

I. Introduction

The term Internet of Things (IoT) refers to identifiable physical objects with communication and (possibly) sensing and actuation capabilities. Wireless Sensor Networks (WSN) were the first type of network with these features, which were then extended to the IoT paradigm to emphasize the fact that, with recent technology advancements, *any* physical object could theoretically be equipped with the mentioned functionalities and connected to the Internet for data collection, analysis and, possibly, for being acted upon. IoT covers many (diverse) fields, from environmental monitoring, smart cities, logistics, tracking and tracing of goods, smart metering in micro-grids, social networks, etc., enabling new business opportunities.

One of the essential features of IoT objects is their *communication* capability, which has to be implemented in a *secure* and *automated* manner. Also, to fully reap the benefits that the IoT paradigm brings about, different systems should be *interoperable*, i.e., they should somehow speak the same language or, at least, proper conversion functionalities should exist within the network to translate among the different languages. The **IoT Architecture (IoT-A)** project stemmed from the observation that many IoT systems are developed in a rather independent and unstructured manner and that, as a

†University of Padova and Consorzio Ferrara Ricerche (CFR), Italy. ‡ABC Consulting, France. ⋆University of Surrey Email: {rossi,zorzi}@dei.unipd.it, alessandro@bassiconsulting.eu, f.carrez@surrey.ac.uk.

matter of fact, they neither speak the same language nor rely upon standardized structural concepts. All of this leads to a sort of **Intranet of Things**, where compatibility across systems is very limited [1].

To cope with this, in 2009 a group of researchers from nineteen industrial companies and research institutions joined forces to lay the foundation of the needed common architectural model, giving rise to the European IoT-A project [2]. One of the main results of this project is the **Architectural Reference Model (ARM)**, which can be defined as *an abstract framework comprising a minimal set of unifying concepts, axioms and relationships*. This framework has been derived taking the state of the art into account and, from the very beginning, with the help of initial end-users (the "IoT-A stakeholders group"). The end-users have provided requirements for the design of the ARM, according to their product-oriented everyday experience.

The ARM is briefly introduced in Section II of this letter along with a discussion of the benefits that this model brings about in the definition of practical IoT architectures. After this, in Section III we go through some networking paradigms, which include a short description of a networking architecture, transport and security aspects. We conclude with Section IV, were we briefly outline open issues and future technological steps.

II. The IoT Architectural Reference Model (ARM)

The main contribution of the ARM is the **IoT Reference Model (RM)**, which provides the common ground, the definitions and a common language on which IoT architectures can be built. The RM contains several sub-models, among which: 1) the **IoT Domain Model**, 2) the **IoT Information Model** and 3) the **IoT Functional Model**, which are briefly discussed in the following:

1) **IoT Domain Model:** defines the basic concepts belonging to the IoT, their attributes and relationships. For instance, we have the concept of *physical entity*, which corresponds to the smart object that we are going to monitor or to operate upon. We have the concept of *device*, which can be a **sensor** or **actuator**, or simply a **tag**. Tags are used to identify the physical entity they are attached to, whereas sensors provide a richer information about the state of the physical entity or of a measurable physical quantity in its surroundings. Actuators can modify the physical state of a physical entity. In addition to these definitions, we have the definition of key concepts such as *services*, *resources* (either on-device or network) and *user*. The latter is especially important as it includes human users as well as machines, that may interact in an automated fashion with IoT resources, devices and services (referred to as machine-to-machine communication, M2M). All of this has been defined and structured, identifying the relationships among the involved concepts and their role.
2) **IoT Information Model:** defines the structure of the information that is handled and processed in an IoT system. Its main elements are *virtual entities*, *service descriptors* and *associations*. Virtual entities model and specify the attributes of physical entities (such as the type of physical entity, its sensing and actuation capabilities, etc.), service descriptors specify the relevant aspects of a service, including its interfaces and its exposed resources. Finally, associations connect attributes of a virtual entity to the corresponding service descriptor. For instance, a certain temperature reading (attribute) can be read (service) through a "get" function (association rule).
3) **IoT Functional Model:** identifies groups of functionalities, classified into *functionality groups (FG)*. Key functionalities are *communication* and *security* (also discussed in the next section). The former sits on the IoT Communication Model, whereas the latter is based upon the IoT Trust, Security and Privacy model.

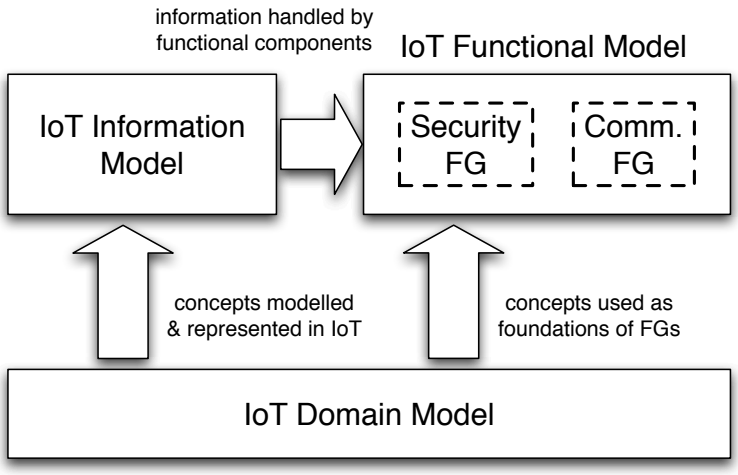

Fig. 1. Interaction of sub-models in the IoT Reference Model.

Interaction of the sub-models: the relations among the previous sub-models is shown in Fig. 1. There, arrows entering a block indicate that the concepts and models defined in the originating block are used as the basis for the current one. As shown in this figure, the IoT Domain Model (DM) serves as the basis for all other blocks in the IoT reference model. The idea is that the definitions and concepts therein are not expected to change over the next decade or longer. The concepts in the DM are then represented in the IoT Information Model (IM) through suitable information structures. Finally, the DM and the IM are used for the description of functionalities (in the figure we show the communication and the security FG).

Further, the IoT ARM is used to define the IoT-A reference architecture, from which practical architectures are finally derived. In general, the main benefits arising from the ARM are:

- **Generation of practical IoT architectures:** this is accomplished through a systematic approach that follows best practices and that can be, to a certain extent, automated. Also, the decisions made in the design follow a clear and well documented pattern. This entails a reduced risk regarding the effectiveness and correctness of the resulting product and, in turn, reduced R&D costs.
- **Improved performance assessment (***benchmarking***):** with the presented process any differences in the derived architectures can be attributed to specific sub-blocks, to the special features of the considered use case and to the design choices. Hence, using the IoT ARM a list of system function blocks, data models and the prediction of system complexity (for each sub-block) can be automatically obtained for the generated architecture. This will permit to pinpoint the performance of each functional group (and of each function therein) and to also weigh the complexity of the overall design, making it possible to check whether the architecture meets certain (user-defined) requirements.
- **Interoperability:** the proposed design process facilitates the identification of the design choices made for each architecture. This allows the quick identification of the points where architectures differ and, based on the supported communication and information models, the quick assessment of whether they are interoperable. In case they are not, the identified differences can be promptly used as guidelines toward the achievement of the desired interoperability.

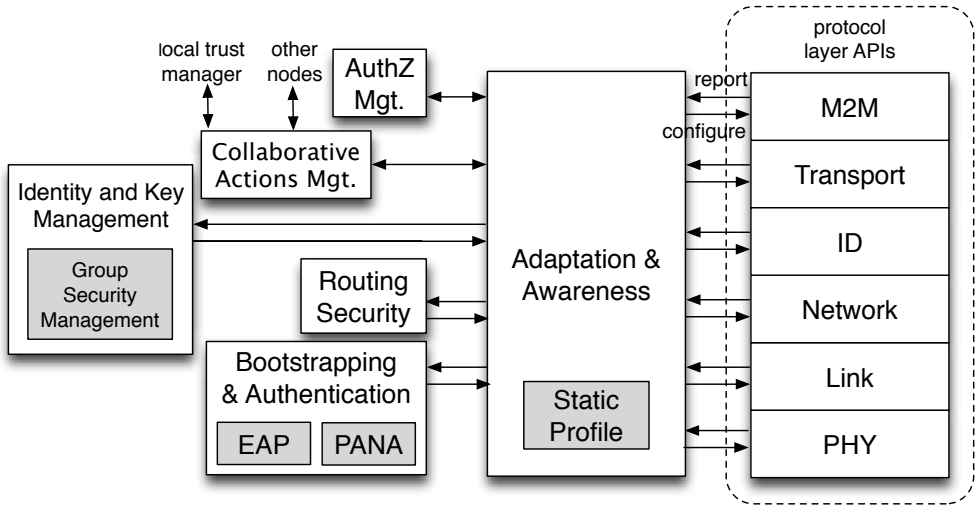

Fig. 2. IoT-A protocol architecture.

The ARM is described in details in the public IoT-A deliverable D1.5 [3], whereas the above concepts, along with detailed discussions about the usage models for the ARM and the generation of practical IoT architectures can be found in [4].

III. Networking Models for IoT

Besides the definition of the ARM, a great deal of work has been carried out in terms of protocol design. The final results are collected in the deliverables D3.5 [5] and D3.6 [6] and have also been disseminated at international conferences and through journal publications, e.g., see [7]–[11].

In Fig. 2 we show the IoT-A networking architecture [10]. In its right-hand side, we have the communication layers, which interact with the security functionalities that are shown in the left-hand side of the diagram.

The **Machine-to-Machine (M2M)** layer resides right below the application layer. It addresses the lack of interoperability of current M2M technology and enables communication among network elements either through the use of a common language or through language translation. In the IoT-A project, we have designed and implemented efficient solutions based on the **Constrained Application Protocol (CoAP)** as a replacement of HTTP and **Efficient XML Interchange (EXI)** as a compact descriptive language replacing XML, see [7], [9]. In addition to this, an M2M translation engine has been designed and implemented, see [5].

The **Transport (TRA)** layer provides end-to-end performance guarantees between communicating endpoints. Notably, the standard TCP protocol that is used at the transport layer to carry data over the Internet is not suitable for use within constrained network domains, as these are typically characterized by low bit rates, long delays and high error rates (especially when IoT objects communicate wirelessly). Additionally, the type of traffic patterns occurring over these networks substantially differ from those in the Internet, and TCP was not designed with these new patterns in mind. A possible solution that makes it possible to retain standard TCP over the Internet portion of the network, while optimizing the transport protocol utilized within the constrained network segment is *TCP split* (note that similar solutions have been successfully used in satellite networks). In [11] we propose and evaluate a number

of distributed techniques for the implementation of the transport layer within the constrained network segment.

For what concerns the remaining blocks, the **Identification (ID)** layer is an addition to standard Internet protocol stacks and allows the identification of devices within the IoT domain. Network, Link and Physical layers have standard meanings. The security blocks and their functions include **Bootstrapping and Authentication**, that controls the access of nodes to the network. The **Static Profile** represents the knowledge that an IoT endpoint has about its own resources and the security settings it intends to use or requires from the network. **Collaborative Actions Management** is invoked whenever an IoT node cannot fulfill a task by itself, for instance, when the task is computationally intensive. This functional block may interact with a trusted entity within the constrained network segment to learn about assisting peers. Collaborative security protocols were developed in, e.g., [8]. **Identity and Key Management** orchestrates the secure interaction between endpoints. It establishes node privacy by choosing a particular identity (or pseudonym) for use in the communication stack and provides secure communication. **Adaptation and Awareness** is responsible for dynamically configuring the protocol stack of the IoT node by gathering information about its status. **Group Security Management** is responsible for enforcing multicast security. **Routing Security** mitigates classical routing attacks, whereas **Authorization Management (AuthZ Mgt.)** manages inbound and outbound access to services, interacting with the existing authorization infrastructure to retrieve resource certificates, etc.

IV. Conclusions and Future Steps

In conclusion, the IoT-A project has provided a unified framework for the systematic definition of IoT architectures. Also, networking solutions have been designed and analyzed, especially regarding end-to-end unicast security and transport. Much has also been said about virtualization of services, ontologies for the structured representation of data and enabling communication technologies such as physical layer processing and routing. The IoT-A project ended in November 2013. Since then, the sustenance of the IoT ARM is taken care of by the WG2 “Architecture and Semantic Interoperability” of the IoT Forum (http://www.iot-forum.org/). Within this context, different IoT ARM “profiles,” e.g., focusing on Semantic Interoperability and Security, will be specified in greater detail. Further to this, the development of Open source profile-compliant components will be encouraged, and an eco-system of such off-the-shelf components maintained, so that newcomers in the IoT field (especially SME’s) can easily concoct their own IoT applications reusing such ARM compliant components.

Finally, we note that there are critical technical issues that still have to be addressed for a successful and secure development of the IoT. Next, we discuss some of them:

- **Traffic control:** the first that we mention here is *scalability*. While this concept has been widely discussed, it has been rarely tackled from a technical viewpoint. In the near future, the IoT is expected to generate data from billions of devices, which will all inject their traffic into the Internet. This means that dedicated solutions will be needed for Internet cloud services to harness this traffic upsurge. This has to be tackled through dedicated traffic engineering strategies.
- **Security:** while much has been said about unicast end-to-end security, very little is known about security when the communication occurs through multicast or broadcast IP channels. In addition, standard security mechanisms work well until the system is not breached but, once a malicious software gains access to the IoT system, nothing would be in place to stop it. This means that detection systems are especially important in the IoT domain. Compromised devices (or services) must be located and possibly isolated. Note that this also includes failures of IoT components.
- **IoT and 5G:** 5G cellular networks comprise IoT as part of their design. However, technological solutions are needed to properly interface base stations and (possibly) handheld terminals with

IoT devices, enabling their seamless integration into the cellular system.

- **Massive channel access:** in the not too distant future, we may assist to the advent of the "Internet of nano networks," featuring nanoscale communication and massive channel access. Special channel access and routing technologies would then be required to cope with the complexity arising from high densities of IoT devices.

REFERENCES

[1] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 44–51, 2010.

[2] "IoT-A Internet of Things – Architecture," Internet Site, 2013. [Online]. Available: http://www.iot-a.eu/

[3] "D1.5: Final architectural reference model for the IoT (v3.0)," IoT-A Public Deliverable, 2014. [Online]. Available: http://www.iot-a.eu/public/public-documents/d1.5/

[4] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner, *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*. Springer-Verlag, 2013, *Edited Book*.

[5] "D3.5: M2M API Definition," IoT-A Public Deliverable, 2013.

[6] "D3.6: IoT Protocol Suite definition," IoT-A Public Deliverable, 2013.

[7] A. P. Castellani, M. Gheda, N. Bui, M. Rossi, and M. Zorzi, "Web Services for the Internet of Things through CoAP and EXI," in *IEEE ICC Workshop on Embedding the Real World into the Future Internet (RWFI)*, Kyoto, Japan, Jun. 2011.

[8] Y. B. Saied, A. Olivereau, and D. Zeghlache, "Energy efficiency in M2M networks: A cooperative key establishment system," in *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Budapest, Hungary, Oct. 2011.

[9] A. P. Castellani, T. Fossati, and S. Loreto, "HTTP-CoAP cross protocol proxy: an implementation viewpoint," in *IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS)*, Las Vegas, NV, US, Oct. 2012.

[10] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, San Francisco, CA, US, Jun. 2012.

[11] A. P. Castellani, M. Rossi, and M. Zorzi, "Back Pressure Congestion Control for CoAP/6LoWPAN Networks," *Elsevier Ad Hoc Networks*, vol. 18, no. 1, pp. 71–84, 2013.