Realizing the Internet of Things using Information-Centric Networking

Nikos Fotiou and George C. Polyzos
Mobile Multimedia Laboratory, Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Patision 76, 104 34, Athens, Greece
Email:{fotiou, polyzos}@aueb.gr

***Abstract*—Nowadays, the Internet connects more objects than people. These devices generate vast amounts of information. Furthermore, identification technologies–such as Radio Frequency Identification (RFID)–enable the association of information with identifiable objects, not necessarily connected to the Internet. All this information is organized into vertical silos. These silos usually belong to different administrative domains and use their own specific communication protocols. In this paper, we present our vision for a global, all-encompassing Internet of Things (IoT) realized through an integrating architecture relying on information and its identifiers/names. We envision the IoT as the architecture that will interconnect all these silos and will make the information generated by or associated with objects globally accessible. Moreover, we argue that the Information-Centric Networking (ICN) paradigm is the ideal candidate architecture for the realization of that IoT vision. In line with this premise, we propose a research agenda for the realization of a full-fledged ICN-based IoT architecture.**

I. Introduction

In 2010 the number of devices connected to the Internet was 12.5 billion, whereas the world's population was 6.8 billion: this was the first time in history where the number of connected devices per person was more than 1 [1]. This explosion of the number of connected devices is mainly attributed to the growth of smart phones and tablet PCs. This ratio is expected to become even bigger, as new forms of smart devices (e.g., smart TVs, fridges, watches) become commodity. These devices are equipped with a variety of sensors and are able to generate information that can be used in many application scenarios. Nevertheless, the full potentials of this characteristic of smart devices have not yet been fully harvested: these devices are mainly used for Internet access and their sensor data is exploited only by specific applications. We argue that this happens due to the lack of *an architecture for efficient, seamless, and secure dissemination of information*. What is more, recent advances in identification technologies–such as Radio Frequency Identification (RFID)–enable the association of information with identifiable objects, not necessarily connected to the Internet. This information is restricted to certain application "silos", e.g., supply chains and stock management systems. We believe that, if we remove the barriers that these silos pose and release this information in a controlled and meaningful way in the Internet, a wide range of applications will arise. To our view, this is the purpose of the Internet of Thing (IoT): to facilitate the consumption of the information produced by/associated with "things", in the Internet scale. This view clearly differs from many approaches that treat IoT as another form of wireless sensor networks (WSN). Our vision of IoT is not limited to the (Internet) connection problem, instead it moves one step forwards and considers how "things" (connected or not) can be exploited in a meaningful way. The main pillar of our vision is information, therefore it comes as a natural choice to consider Information Centric Networking (ICN) as a paradigm for realizing this IoT vision.

IoT is considered as a scenario that can be used as a base for the evaluation of different ICN approaches [2]. Moreover, many research efforts have considered ICN as an IoT enabler. Rayes et al. [3] argue that ICN will be the most common deployment method for IoT and investigate key performance and security requirements. Francois et al. [4] adapt the CCN[1] ICN architecture for resource constrained devices. In particular they consider sensor networks and propose some optimizations for reducing traffic related to sensors data. Piro et al. [5] propose the usage of the CCN architecture for implementing services for Smart Cities by leveraging CCN to discover services, to initialize secure communications channels, and to invoke services. In [6] we propose an information lookup service for the IoT, inspired by the PURSUIT[2] ICN architecture. In this solution, information is organized in "scopes", with each scope representing an administrative domain.

In this paper, we propose a research agenda for implementing a full-fledged IoT architecture, based on ICN.

II. ICN for IoT: research challenges

ICN promises efficient information dissemination and access. By implementing all (inter)networking functions around information identifiers (rather than location identifiers), ICN is expected to facilitate information replication, multi-homing and caching, multicast delivery, mobility, and delay tolerant networking. Design choices for the following domains have to be made, in order to move from theory to a concrete IoT architecture.

[1] http://www.ccnx.org/
[2] http://www.fp7-pursuit.eu

QSHINE 2014, August 18-20, RHODES, Greece

DOI 10.4108/icst.qshine.2014.256425

A. Naming

Probably the most crucial design choice of an ICN architecture is that of naming. We believe that a name should be composed of three parts: a part associated with the owner/administrator/location of a thing, a part bound to the identity of a thing (e.g. to its RFID identity, QRcode, or barcode), and a part bound to some information associated with the thing (e.g., size, price, temperature). Names should provide the means for identification, content authentication and provenance verification: it should not be possible for a thing to pretend to be another thing, to produce fake information, as well as, to lie about the source of a piece of information. Names should be easily manageable and "revocable". The same information item may exist in multiple forms (e.g., an image may exist in different compression levels). Naming should assure that is possible to correlate the various forms of the same information item. A "name resolution" service should consider the mobility of things, their (dis)connectivity, as well as, name revocation.

B. Efficient and contextual information retrieval

An information-lookup service should allow for efficient information retrieval, based on the information name and/or information meta-data and/or user context. The design choices for this service should consider speed, scalability, and fault-tolerance. An API that hides the details of the underlay architecture, should enable automated information advertisement and lookup. The service should consider end-nodes capabilities and act accordingly. Things may implement their part of API or use proxies/gateways. In the latter case security issues should be considered.

C. Trust models

The design choices for trust should consider the limited–or even non existent–computational power of things. Moreover they should consider that things can be tampered and their software–if any–can not be easily updated. The traditional PKI model probably is not suitable and name-based solution should be considered. Trust should be transitive and should be possible for a thing to securely delegate functionalities to other things/proxies/gateways. Moreover, it should be possible to automatically generate globally acceptable trust primitives, without relying on 3^{rd} parties.

D. Privacy and access control

The information generated by/associated with things will be sensitive. Unauthorized access to this information–or even to its "meta-data"–may result in devastating results including revelation of corporate secrets, or violation of user privacy. ICN facilitates information replication. Although this constitutes to the availability of the architecture, it raises security concerns, since the (access) control over the distributed information may be lost. To this end, design choices for distributed access control and flexibly identity federations. should be considered. Moreover, context should be exploited for providing access control rules hints, as well as, during the enforcement of access control policies. As an example, it should be possible to define and enforce access control policies based on location data, time, weather conditions etc.

E. Information forwarding

Considering that things are expected to be mobile and not "always-connected", multiple design choices for information forwarding should be considered. An ICN-based IoT architecture should allow delay tolerant forwarding, persistent "subscriptions" (e.g., for events), as well as, ephemeral ones. It should be possible to engineer traffic, in order to make forwarding more efficient, to facilitate caching, or even to include "special" nodes in the path (e.g., nodes that will "morph" information).

III. Moving Forward

In recent years many ICN research efforts have emerged. All of them try to be as generic as possible and are mostly envisioned to replace current (inter)networking protocols, if not in reality, at least as the focus of the networking technology. We do not believe that the implementation of an ICN-based IoT architecture requires the replacement of the current Internet stack. In contrast, we advocate that such an architecture can be realized in an overlay manner, but also integrating application silos that continue avoiding IP internetworking. A deployment of an overlay architecture may not be optimal from a performance perspective, but still will give us the key universality and easy integration property and useful insights on the possibilities that ICN creates for the IoT. Moreover, by giving to the community a "playground" for experimentation, we anticipate the stimulation of many innovating applications that will trigger the real IoT launch.

Acknowledgment

This research has been co-financed by the European Union (European Social FundESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF)Research Funding Program: Aristeia II/I-CAN.

References

[1] E. Daves, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," April 2011, Cisco, white paper.

[2] K. Pentikousis et al., "Information-centric Networking: Baseline Scenarios," September 2014, IRTF draft. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-icnrg-scenarios/

[3] A. Rayes, M. Morrow, and D. Lake, "Internet of things implications on icn," in *Collaboration Technologies and Systems (CTS), 2012 International Conference on*, May 2012, pp. 27–33.

[4] J. François, T. Cholez, and T. Engel, "CCN Traffic Optimization for IoT," in *NoF 2013 : The 4th International Conference on Network of the Future*, IFIP/IEEE. IEEE, Oct 2013.

[5] G. Piro, I. Cianci, L. Grieco, G. Boggia, and P. Camarda, "Information centric services in smart cities," *Journal of Systems and Software*, vol. 88, no. 0, pp. 169 – 188, 2014.

[6] G. Marias, N. Fotiou, and G. Polyzos, "Efficient information lookup for the internet of things," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, June 2012, pp. 1–6.