Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 21 (2013) 442 – 448

Procedia Computer Science

International Workshop on Communications and Sensor Networks (ComSense-2013)

Smart, autonomous and reliable Internet of Things

Dimosthenis Kyriazis[a]*, Theodora Varvarigou[a]

[a]*National Technical University of Athens, Iroon Polytechniou 9, Zografou 15773, Athens, Greece*

Abstract

The dynamic rapidly changing and technology-rich digital environment enables the provision of added-value applications that exploit a multitude of devices contributing services and information. As the Internet of Things (IoT) techniques mature and become ubiquitous, emphasis is put upon approaches that allow things to become smarter, more reliable and more autonomous. In this paper we present challenges and enablers as technologies that will allow things to evolve and act in a more autonomous way, becoming more reliable and smarter. We describe decentralized management mechanisms targeting IoT-based systems in order to enable the exploitation of millions of devices, while we also present an architecture that allows things to learn based on others experiences. The proposed architectural approach also introduces situational knowledge acquisition and analysis techniques in order to make things aware of conditions and events affecting IoT-based systems behavior.

Keywords: Internet of Things; Autonomous Management; Social Networks; Privacy; Reliability

1. Introduction

Realizing the vision of sustainable IoT applications requires the enhancement of IoT technologies with new ways that will enable things and objects to become more reliable, more resilient, more autonomous and smarter. As highlighted in [1]: “Data is the raw material that is processed into information. Individual data by itself is not very useful, but volumes of it, which will come from the Internet of Things, can identify trends and patterns. This and other sources of information then come together to form knowledge. Wisdom is then born from knowledge plus experience.” The quotation is based on the fact that humans evolve because they communicate, creating knowledge out of data and wisdom based on experience. Applying this metaphor to the IoT domain means enhancing objects with technologies that would enable them to evolve based on the knowledge derived from the data streams and the experience of their

* Corresponding author. Tel.: +30-2107722546; fax: +30-2107722569.
E-mail address: dimos@mail.ntua.gr.

doi:10.1016/j.procs.2013.09.059

exploitation and of other objects exploitation by IoT applications. According to CISCO [2], during 2008, the number of things connected to the Internet exceeded the number of people on earth and by 2020 there will be 50 billion, shaping a rich digital environment. Sensors, intelligent fixed and mobile platforms (e.g. smartphones, tablets and home gateways), massive scale cloud infrastructures and other network-enabled devices will all need to cooperate and interact to create value across many sectors in smart cities. This digital environment creates a treasure trove of information, which is the key enabler for embedding wisdom into objects. The added value in a city context is that by making objects smarter cost savings and increased efficiencies will be created, thus allowing for long-term economic growth [3].

Furthermore, emphasis is currently put upon sustainable and green smart city applications [4]. While the technology already exists, the challenge is to put it all together into a unified, easily-managed environment [5]. Sustainability requires the management of millions of objects in an efficient way, optimizing energy and resource usage [6], while also considering that space is bound to get tight raising the need for new techniques that will coordinate and manage all available objects under different contexts, applications, environments, administrative domains and locations. Besides, making things more resilient and smarter in a smart city environment [7] implies services and ICT systems adaptability to IoT applications requests as well as to real-world events that need to be monitored and assessed since they may influence the lifecycle of these applications.

Things have identities, physical attributes and virtual personalities (as highlighted in the corresponding definition by ITU and IERC [4]) and according to a report by Economist [8], future smart cities will base IoT service provision on the digital reflection of things and citizens, which will bring much greater efficiency. Tussles of personal privacy [9] and freedom of expression [10] are expected to be a consequence. Even more, in spite of increased use of mobile devices for specific and well-defined uses, many remain skeptical about the broader deployment of Internet of Things [11], fearing Big Brother intrusion rather than seeing the opportunity of accessing and exploiting the content feeds in new and creative ways that benefit those same skeptical users. Consequently, developing sustainable IoT applications calls for mechanisms to ensure security and trust and preserve privacy [12]. Such approaches should address both the low levels of IoT environments (i.e. hardware-coded techniques) as well as the data management and application levels. Tamper-resistant smart devices, dynamic and evolutionary trust models, secure data stores, applications with build-in security and privacy are critical for sustainable IoT applications [13].

Based on the above, in this paper we present the challenges and enablers for enabling things and objects to become more reliable, more resilient, more autonomous and smarter as well as a conceptual architecture for realizing this vision.

2. Challenges and Enablers

2.1. Things semantics capturing their social behaviour

Networks of objects are formed to serve the needs of IoT applications. However, information about the things is currently limited to the assets (i.e. services and information) provided by these objects, the capabilities of the corresponding things, the environment characteristics under which they operate and the corresponding administrative information. For IoT applications, challenges are highlighted with respect to the formulation and development of the network of things, which should adapt based on different events. What is more, the lifecycle, access and QoS properties of the things should be dynamically updated based on their relationships and contributions within the network.

Based on the above and given that within IoT networks, objects follow the interaction and operation patterns of their contributors / owners, the structure of such dynamic communities and thus the things as actors have a specific social behavior that can be exploited. Capturing such information will allow things

to learn based on others experiences (further described in Section II.C) and managed in a more autonomous way. Thus, tools are needed to harvest and analyze data (such as raw data or logging information) in order to identify things' social-related information referring to interactions with other objects, administrative rules under which they operate, importance within a network of things, influence diffusion models that highlight the entities of high importance and triggering conditions. Furthermore, attributes may be overloaded depending on a wide set of domains: some are specific to the objects, others may be specific to the applications that use these objects, and yet others may be more general (e.g. pertain to the object's environment). Moreover, future IoT architectures should incorporate mechanisms to dynamically update structural and behavioral abstractions following the different lifecycles (bound by location or tailored to specific application offerings) of the things within a network.

2.2. Reliable objects on top of volatile things

The degree of unreliability and uncertainty introduced in IoT environments following the real-world dynamics, makes such environments dynamic, error prone and "unpredictable". Furthermore, the association of IoT resources and services is arbitrary resulting in unreliable and "un-trustable" offerings with questionable quality. Challenges refer to approaches for managing the uncertainty (e.g. disconnections, data quality variations, etc) introduced by such objects and enable the provision of Quality of Information (QoI) guarantees since such information is used to drive decisions regarding the management of the IoT infrastructure and the provision of services.

Enhancing the reliability of the devices and the data requires new strategies for managing the volatility and providing insight into reliability patterns and the potential future impact of them within IoT environments. Such strategies refer to methods for identifying reliability and reputation patterns for the things, the quality of information, the administrative domain under which they belong and operate, the conditions and contexts, and the sequence of events under which things are utilized. What is more, mechanisms are required that will enable the dynamic linkage between things and their attributes (e.g. administration domains, conditions, events, etc) and the impact such links will have on the reliability and use of data and information. Models and knowledge generation / derivation methods will allow for analyzing patterns of devices use and of information with respect to application demands, volatility levels (i.e. changing availability or engagement level of information sources) as well as infrastructure and service events and the way these events correlate with the corresponding reliability patterns.

2.3. Objects able to learn and adapt to different situations

Objects within an IoT environment experience various situations. Based on these, management techniques aim at coordinating things and networks of things in order to overcome limitations, deal with such unexpected conditions and optimize the operation and utilization of things. However, moving such management decisions to the things space, requires knowledge to be embedded to them, raising various challenges such as methods to access and exploit the information aggregated by other things and being available within a network, approaches for enabling objects to act based on self-learning techniques and mechanisms for the anticipation of IoT application requests to adapt offerings accordingly.

Taking into consideration that within and across networks of things, things share and exchange information and services, enabling objects to learn from the experience of others will allow for the exploitation of spatial-, societal-, application- and situational- knowledge. The latter will contribute to their situational awareness and thus to optimized data and service delivery as well as object management. The goal is to allow objects to have embedded intelligence for proactive reasoning and acting. To this direction, mechanisms are required to identify things with common characteristics in terms of the provided assets, their goals and interests (regarding assets offered to IoT applications), and have

experienced or are anticipated to experience similar situations. Furthermore, future IoT architectures should include frameworks that allow things to exchange experiences with respect to functional (e.g. performance, response time, availability, reliability, accuracy) and non-functional (e.g. trust, users experience, expectations, motivations) characteristics of the things, as well as mechanisms allowing for real-time adaptation by analyzing the snapshot of the network at any time and by detecting events and triggering actions with respect to the experiences of other things.

2.4. Privelets to preserve privacy

Privacy aspects are central in the IoT domain given that besides the sensitivity on the data, IoT applications may influence the physical environment through the deployed sensors and actuators. In this context, privacy becomes of major importance and mechanisms are required to preserve privacy and enable users and applications to deny exposure of their data.

We are introducing the concept of "Privelets" as a means to prevent information inference and preserve privacy. Privelets refer to the components of an application (as agents in contrast to the approach introduced in [14]) that can be executed in a trusted administrative domain – defined by a user / application, thus allowing processing and delivery of services to users without exposing their data to other infrastructures (i.e. moving the processing to the source of the data instead of moving the data). The latter allows for data owners to handle the private information they would like to expose but still exploit IoT application that would utilize data in a trusted environment (e.g. locally - "in house" - or in a trusted third party domain). Privelets as service components will be moved to the source of data eliminating the need to obtain the data from their owners, and thus enabling them to control the handling of private information by selecting which data can be sent and which should be retained and service components executed on them.

2.5. Autonomous management of the network of things

Things create dynamic networks that can have millions of nodes - often bounded by their location, and which operate under different administrative domains (with different rules). The latter highlights that centralized management of such networks is inefficient, highlighting the need for methods supporting the dynamic formation and re-formation of the networks of things and approaches for decentralized management.

By extending things semantics structures to capture social characteristics (often associated with the corresponding ones for their owners) decentralized management and coordination decisions can be provided based on service-, interaction-, location- and reputation-oriented principles. Coordination can be performed by identifying and monitoring critical elements, allowing management operations following the definition of the role and the participation scheme of the things based on a wide set of metrics (e.g. access properties per administrative and trust domain). What is more, IoT architectures should enable things to react in an autonomous and predictive way based on the information retrieved from other objects regarding their experiences under the same conditions, as well as enable the runtime adaptability of the network and of the things operation based on their state and their behavior as identified from the analysis of raw data regarding evolving relationships and events.

3. Conceptual Architecture

The goal of the proposed architecture is to enhance the sustainability of IoT applications by exploiting smart and reliable (networks of) things and by being able to utilize a big number of heterogeneous device platforms, utilization of which is either inefficient with current management approaches or unfeasible

since these platforms may be bounded by their location or the administrative rules under which they operate. Moreover, privacy issues are considered, while the architecture also enables for the provision of QoI guarantees through optimized management of the complete data and information lifecycle.

The proposed conceptual architecture (as depicted in the following figure) enables the development of an environment for IoT applications through cross-platform channels that incorporate technologies for Data, Information, Things and Decentralized Management.

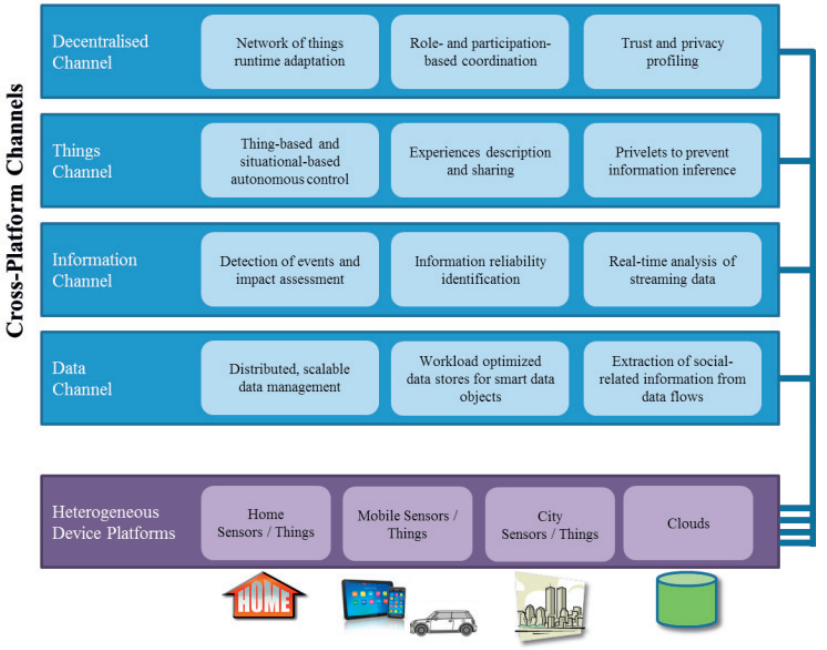

Fig. 1. Cross-platform channels

Things generate diverse data types of a huge amount which is often linked, aggregated and combined into new groupings or structures. The data channel includes technologies for storing data objects on workload optimized data stores, for enabling processing on networks of data objects and for distributed and scalable data management. One of the main elements of the data channel refers to the techniques for harvesting and analyzing data in order to identify relationships between different entities, detect events that (may) influence the behavior of both the things and the communities, generate influence diffusion models that highlight the entities of high importance within a collaborative environment, and analyze trends that (may) lead to a community formulation and contribution of assets. This social-related information will be captured to enriched metadata structures that complement and extend things semantics with the aforementioned information and which will be used both to allow things to evolve (thus becoming smarter and more reliable) and to manage the networks of things, as further discussed in sequel.

The information channel includes technologies for obtaining valuable knowledge from the data, either stored or at real-time through the analysis of streaming data. Identification of reliability and volatility patterns, evaluation of the information provided by the devices and mechanisms for overcoming the volatility of the information provision will enhance the QoI. Furthermore, events will be detected from the corresponding data flows and their impact will be assessed in order to deliver additional knowledge

both to the things and to the management mechanisms so as to perform the corresponding actions at runtime.

The things channel includes technologies for the description and sharing of experiences, which will allow things to learn based on their experiences and the experiences of others (with the same characteristics and operating under the same conditions) with respect to spatial-, societal-, application- and situational- related aspects. The things channel also includes privacy mechanisms as described above in order to enable the realization of the Privelets concept.

The decentralized channel refers to technologies that enable the efficient management and coordination of the big number of things. Overcoming the limitations for the management of the exponentially increasing number of things, calls for techniques that base management and coordination decisions on goal-, administration-, service-, interaction-, proximity-, location- and reputation-oriented principles. Given that rich metadata structures will capture the "social behavior" of things, this information will be utilized to perform decentralized management of networks of things. What is of major importance regarding the enhanced and autonomous "socially-enriched" management mechanisms is their ability to adapt to reality. Analyzing raw data will provide a snapshot of the network of things behavior and state at any time, triggering actions with respect to resources and data management.

4. Conclusions

Future IoT infrastructures will aim at supporting the on-going creation of IoT applications which will utilize data and services from many different (heterogeneous) device platforms, locations and environments. New decentralized management mechanisms are required to allow for efficient exploitation of the underlying devices overcoming the inefficiencies of centralized approaches when dealing with a huge number of devices. Runtime adaptation will allow for identification of events that impact the behavior and operation of the devices and the IoT applications, and for triggering decisions at runtime to ensure resilient IoT application provision. What is more, predictive reasoning of things contributing to ubiquitous IoT service offerings through experience sharing and exchange is required, providing the basis for proactive decisions or isolation of contexts and conditions that affect the IoT applications. Mechanisms will also be required to overcome the intrinsic information volatility in the IoT raising the reliability level of IoT applications, through tools to identify whether the provided data from the device are reliable and provided in the required time frame.

In this paper we have introduced challenges and enablers for smarter, more reliable and more autonomous IoT infrastructures along with a conceptual architecture encompassing various components as enabling technologies across four main pillars. The goal is to enable the provision of a scalable and privacy-aware IoT infrastructure that considers social relationships among objects, while being able to self-adapt itself according to environmental context changes in a decentralized and real-time way. Core to the architecture are the ability of things to learn and evolve by exploiting things social-behavior and use it as a basis to share and exchange experiences, as a means to make things smarter and more autonomous. The proposed enabling technologies allow new device platforms to be integrated at any time and become immediately available via the decentralized management mechanisms that base coordination decisions on the role and participation scheme of such devices in and across IoT networks. Furthermore we have introduced the concept of Privelets to support confidentiality and prevent personal information inference: components of IoT applications may be executed on the data instead of moving the data to the applications, allowing citizens and city authorities to keep "in house" their confidential data.

References

[1] D. Evans. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. CISCO white paper, 2011.

[2] CISCO. The Internet of Things, Infographic. Available online at http://blogs.cisco.com/news/the-internet-of-things-infographic, 2011.

[3] IBM. Cities Outlook 2012. Available online at http://www.ibm.com/cloud-computing/us/en, 2012.

[4] European Research Cluster on the Internet of Things – IERC. The Internet of Things 2012 - New Horizons. Cluster Book 2012, 2012.

[5] Orange Labs - France Telecom. Smart Cities: True icons of the 21st century. Available online at http://www.orange-business.com/microsite/solutions-operators/documentation/download/smart-cities/, 2011.

[6] Arup. The Smart Solutions for Cities. Arup UrbanLife, 2011.

[7] Gonzalez J, Rossi A. New Trends for Smart Cities. Available online at http://www.opencities.net/sites/opencities.net/files/content-files/repository/D2.2.21%20New%20trends%20for%20Smart%20Cities.pdf, 2011.

[8] Economist Report. It's a smart world. Available online at http://www.managementthinking.eiu.com/sites/default/files/downloads/Special%20report%20on%20smart%20systems.pdf, 2010.

[9] Boniface M, Pickering B. Legislative Tensions in Participation and Privacy. Available online at http://www.scribd.com/doc/55260687/Legislative-Tensions-In-Participation-And-Privacy, 2011.

[10] La Rue F, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council, 16, available online at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, 2011.

[11] Pickering B, Boniface M. Social Future Internet Activities. Available online at http://www.scribd.com/doc/68338983/D3-1-First-Report-on-Social-Future-Internet-Coordination-Activities, 2011 .

[12] Moss Kanter R, Litow S, Informed and interconnected: A manifesto for smarter cities, Harvard Business School General Management Unit Working Paper, 2009.

[13] Correia L, Wünstel K, Smart Cities Applications and Requirements, Net!Works European Technology Platform Expert Working Group White Paper, 2011.

[14] Xiao X, Wang G, Gehrke J. Differential Privacy via Wavelet Transforms. IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 8, pp. 1200-1214, August, 2011.