SIoT: Giving a Social Structure to the Internet of Things

Luigi Atzori, *Senior Member, IEEE,* Antonio Iera, *Senior Member, IEEE,* and Giacomo Morabito, *Member, IEEE*

***Abstract*—The actual development of the *Internet of Things* (IoT) needs major issues related to *things'* service discovery and composition to be addressed. This paper proposes a possible approach to solve such issues. We introduce a novel paradigm of "social network of intelligent objects", namely the *Social Internet of Things* (SIoT), based on the notion of *social relationships* among objects. Following the definition of a possible social structure among objects, a preliminary architecture for the implementation of SIoT is presented. Through the SIoT paradigm, the capability of humans and devices to discover, select, and use objects with their services in the IoT is augmented. Besides, a level of trustworthiness is enabled to steer the interaction among the billions of objects which will crowd the future IoT.**

***Index Terms*—Internet of things, social networks, ubiquitous computing.**

I. Introduction

THE realization of an effective and reliable IoT requires the definition of a complex architecture that takes into account the issues of sensing the real world, transmitting data, and managing the relevant services to build applications [1]. Recently, major architectural solutions have been proposed within ITU, EPCGlobal, the CASAGRAS initiative, and the uID research group [2]. The list is not exhaustive: the plethora of proposals from EC funded projects coordinated by the IERC cluster must be added [3]. From the analysis of these efforts, emerging priorities are: (i) enable full connectivity of things to the Internet by operating at sensing and network levels, (ii) provide middleware and application functionality and protocols to ease the exploitation of things-related services. Our contribution fits into the latter line of research, indeed we propose an innovative paradigm of interaction among objects.

Basic idea is the definition of a "social network of intelligent objects", named *Social Internet of Things* (SIoT). In analogy with Social Networks Services (SNS) for human beings, the novel paradigm introduces the concept of social relationships among objects. Advantages are the possibility to:

- Give the IoT a structure that can be shaped as required to guarantee network navigability, so as that object and service discovery is effectively performed and scalability is guaranteed like in human social networks (see [4], for example).
- Extend the use of models designed to study social networks to address IoT related issues (intrinsically related to extensive networks of interconnected objects).
- Create a level of trustworthiness to be used for leveraging the level of interaction among things that are "friends".

Ours is a distributed approach, which is expected to guarantee a higher scalability and a better reaction to frequent state changes characterizing objects involved in the IoT. As for the identification of a whole Architecture for SIoT, deriving it from "human" social network models is quite commonsense; although it is not exactly the same thing.

The exploitation of social networks in the context of the IoT has been investigated in [5]. In this paper, it was proposed to exploit (human) social network relationships to share the resources offered by a given smart thing (smart things enabled to support web services usable by friends of their owner). Also the research in [6] tries to lay the groundwork for the establishment of a so-called Ubiquitous IoT architecture inspired by social organizations of human beings. Authors of [7] investigate on the potential of combining social and technical networks and discuss about the implication of so-called "socio-technical networks" in the context of the IoT. The Pachube platform is close to the idea of a social network of objects, allowing developers to connect sensor data to the Web to build applications. What the platform does not allow is objects to form social groups autonomously, for the benefit of human beings but without their intervention. Actually, SIoT focuses on the latter aspect, in line with the notion of IoT devices with social connections introduced in [7].

A complementary perspective is considered in [8], where the focus is on solutions that enable smart wireless devices – mostly wireless sensors – to establish temporary *connections* and their owners to control such a process.

The approach we propose differs from the literature for three major reasons. *(i)* We are interested in establishing and then exploiting social relationships among things, not among their owners. The owner mediation can be foreseen but objects have to play the key role, as it happens in novel IoT-based applications. *(ii)* Through social relationships things can crawl the IoT and discover services and resources; this provides a distributed solution that is expected to be effective, efficient and, most important, relieves the humans from doing it. *(iii)* The envisioned IoT architecture is not a mere service platform centered on the concept of web of things, yet a real platform for SNSs with suitable components introduced to cope with the presence of objects instead of human beings.

II. The Social Structure

In this section, we analyze the types of social relationships in which things can be engaged. Like for human beings, first form of socialization among objects we foresee is a *parental object relationship*, defined among similar objects, built in the same period by the same manufacturer (the role of family is

Manuscript received June 23, 2011. The associate editor coordinating the review of this letter and approving it for publication was I.-R. Chen.

L. Atzori is with the University of Cagliari, Italy (e-mail: l.atzori@diee.unica.it).

A. Iera is with the University of Reggio Calabria, Italy (e-mail: antonio.iera@unirc.it).

G. Morabito is with the University of Catania, Italy (e-mail: giacomo.morabito@diit.unict.it).

Digital Object Identifier 10.1109/LCOMM.2011.090911.111340

played by the production batch). This relationship is easily implemented during the item production, it will not change over time and is only updated by events of disruption/obsolescence of a given device.

Moreover, objects can establish *co-location object relationship* and *co-work object relationship*, like humans do when they share personal (e.g., cohabitation) or public (e.g., work) experiences. These relations are determined whenever objects (e.g., sensors, actuators, RFID Tags, etc.) constantly reside in the same place (e.g., to offer home/industrial automation services) or periodically cooperate to provide a common IoT application, such as emergency response and telemedicine. These relationships are established as part of the initialization/implementation of either a "location-based application" profile or a "situation-based application" profile. Changes are frequent and usually based on time duration of co-location/co-working, frequency of the interaction, and reputation. These are the sort of relationships considered in [8].

A further type of relationship is defined for objects owned by the same user (mobile phones, game consoles, etc.). We name this *ownership object relationship*. Associating one another all devices of the same user is already a common procedure. A ownership object relationship is the logical generalization of this concept through a richer device profile.

The last relationship is established when objects come into contact, sporadically or continuously, for reasons purely related to relations among their owners (e.g., devices/sensors belonging to friends). We name this *social object relationship*. Similarly to people exchanging their contacts (phone numbers, e-mail addresses, etc.), the device, if properly authorized, autonomously exchanges its social profile. The driving idea is that devices with similar characteristics and profile can share best practice to solve problems already faced by "friends". Policies, exploiting ad-hoc metrics, measure the opportunity of maintaining a given relationship.

Accordingly, the relationships among objects in the SIoT evolve towards social structures that need to be studied to maximize the benefits of the SIoT in service discovery and exploitation. Sociology, Anthropology, or Cognition studies can provide useful hints in this direction. Alan Fiske "relational models" theory [9], furnishes four basic relational structures that can be applied to objects as well. In *Communal sharing* relationships, equivalence and collectivity membership emerge against any form of individual distinctiveness. These can be definitely associated with behaviors of objects that have collective relevance only. This is, for example, the case of "swarms" of objects for which is only important the service that the whole swarm can provide to users.

Equality matching, based on egalitarian relationships characterized by in-kind reciprocity and balanced exchange, may represent all forms of information exchange among objects that operate as equals during the IoT service provision while maintaining their individuality. In communal sharing relationship the service is associated to the whole group; in this second case each object has associated a service that it advertises.

Authority ranking relationships are asymmetrical, based on precedence, hierarchy, and status. These are established among objects of different complexity and hierarchical levels (RFID reader and tags, Bluetooth master and slaves, etc.) exchanging information asymmetrically. The service advertised is usually associated to the group or to the object of the highest rank.

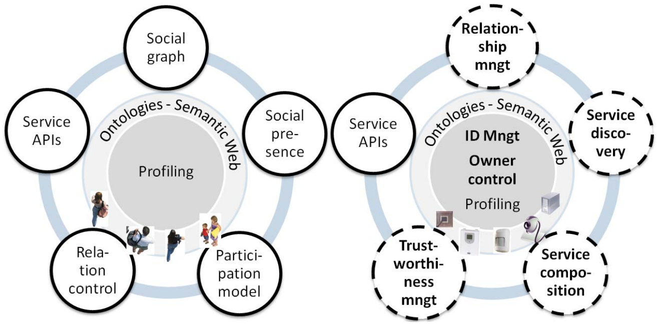

Fig. 1. Basic components of social network platforms for humans (on the left) and for objects (on the right).

Market pricing relationships are based on proportionality, with interactions organized by referring to a common scale of ratio values. They can be established among objects working together to achieve a mutual benefit. In many IoT applications, this implies that the participation in this relationship is considered only when it is worth the while to do so.

III. SIoT Architectural Model

In Fig. 1 (left side) we show a common architectural model of SNS for humans [10]. This is not applicable to the SIoT, but must be modified to take its specific features into account. In this context, criteria to consider are related to the main SIoT objectives, that is, object-related service discovery and composition as well as object trustworthiness management.

A. Components of SIoT

Accordingly, Fig. 1 compares the main components of a SNS and of SIoT. Differences in the novel architecture are shown with bold fonts and dashed contours. Three basic components can be envisioned:

ID management (ID): to assign an ID that universally identifies all object categories and to maintain existing object identification schemes, a simple XML-based protocol can be implemented, which allows to specify the ID mechanism adopted other than the ID itself. This system includes at least: IPv6 addresses, Universal Product Code (UPC), Electronic Product Code (EPC), Ubiquitous code (Ucode), OpenID, URI.

Object profiling (OP): it includes static and dynamic information about the object. Objects should be organized into classes on the basis of the main object features.

Owner control (OC): specific policies need to be defined by the owner to rule any possible operation the object performs (information to share, allowed relationships, etc.). To this aim, different security and access control policy definition languages already available can be used. Owner control includes the SNS functionality of the *Relation control* component.

We foresee the satellite components listed in the following[1].

Relationship management (RM): it introduces into the SIoT the "intelligence" that allows objects to start, update, and

[1] *Social graph* is a minor functionality of the SIoT. However, this tool may still be implemented to allow humans to visualize objects relationships.

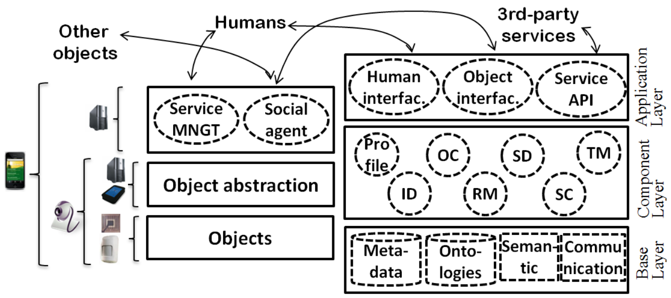

Fig. 2. Architecture for the SIoT: client side (left) and server side (right).

terminate relationships. The selection of which friendship to accept is based on human control settings. The rules described in Section II are implemented in this component.

Service discovery (SD): it replaces the *Social presence* and is finalized to find which objects can provide the required service in the same way humans seek for friendships and information in the SNSs. Indeed, to discover the service, the object queries its social relationship network.

Service composition (SC): it enables the interaction among objects and replaces the *Participation model*. The Service discovery exploits the object relationships to find the desired service, which is then activated by this component. Both a *reactive* or a *proactive* approach to service composition are envisaged. This component will also include the functionality of crowd information processing, to process the information obtained from different objects and obtain the most reliable answer to a query on the basis of different visions.

Trustworthiness management (TM): this is aimed at understanding how the information provided by other members has to be processed. Reliability is built on the basis of the behavior of the object and is strictly related to the RM module. Trustworthiness can be estimated by well-known SNS notions, such as *centrality* and *prestige*, and, again, built on the basis of the object social structure we propose.

Service APIs: this component is analogous to the one required in SNSs.

B. The SIoT architecture

We propose a system architecture made up of three main layers on the server side (Fig. 2). The *Base layer* encompasses: the database for storage and management of data with relevant descriptors, ontologies database, semantic engines, and communications. The *Component layer* hosts tools for basic and satellite component implementation. Interfaces to objects, humans, and third-party services are in the *Application layer*.

On the object side, the first architectural layer – named the *Object layer* – is where the physical objects are located and are reached through their specific communication interfaces. An *Object abstraction layer* is thus needed to harmonize the communication of the different devices through common languages and procedures. In the case of elementary objects, such as an RFID-tagged object, a gateway is required to implement this abstraction layer, while for more complex objects this layer can be implemented in the object itself.

In the third layer, the *Social agent* is devoted to the communication among objects and with SIoT servers to update profile and friendships and to discover/request services from the social network. Finally, the *Service management* is the interface of humans to control the object behavior in the SIoT.

IV. Conclusion

In this paper we introduced the novel concept of Social Internet of Things (SIoT), based on a sort of social relationship among objects, analogously to what happens for human beings. Currently, we are statistically analyzing the structure of the SIoT network through simulations that model the mobility of objects and their relationships. Preliminary results show that most of SIoT features are similar to those observed in social networks of humans. Based on the results of this analysis, we will investigate whether network navigability can be achieved in SIoT and we will identify techniques in the set up of social links that can improve navigability.

Possible application scenarios are those where objects share best practices. For instances, PCs in the same local area network can establish social relationships that can be used to find solutions to common setting problems, such as those related to the configuration of a tricky network printer or an AP. Similarly, cars of the same brand, model and year can provide information about possible solutions to frequent and common mechanical/electrical concerns. In other scenarios, devices that visit the same geographical area can establish friendships to exchange useful information on the physical world. This is the case of handsets that provide data on the radio coverage to new visitors so as improve their connectivity service (providing useful information to the user/owner).

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] L. Zheng *et al.*, "Technologies, applications, and governance in the Internet of things," *Internet of Things - Global Technological and Societal Trends*. River Publisher Ed., 2011.

[3] www.internet-of-things-research.eu, "European research cluster on iot."

[4] J. Kleinberg, "The small-world phenomenon: an algorithmic perspective," in *Proc. ACM Symposium on Theory and Computing*, 2000.

[5] D. Guinard, M. Fischer, and V. Trifa, "Sharing using social networks in a composable web of things," in *Proc. IEEE PERCOM*, 2010.

[6] H. Ning and Z. Wang;, "Future Internet of things architecture: like mankind neural system or social organization framework?" *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 461–463, 2011.

[7] M. Kranz, L. Roalter, and F. Michahelles, "Things that Twitter: social networks and the Internet of things," in *What can the Internet of Things do for the Citizen (CIoT) Workshop at Pervasive*, May 2010.

[8] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. Gellersen, "Smart-its friends: a technique for users to easily establish connections between smart artefacts," *ACM Ubicomp'01*.

[9] A. P. Fiske, "The four elementary forms of sociality: framework for a unified theory of social relations," *Psychological Review*, vol. 99, 1992.

[10] D. M. Boyd and N. B. Ellison, "Social network sites: definition, history, and scholarship," *J. Computer-Mediated Commun.*, vol. 1-13, 2007.