# On-site Service Discovery along User Roaming over Internet of Things

Soochang PARK, Dina HUSSEIN, and Noel CRESPI, *Member, IEEE*
Institut Mines-Telecom, Telecom SudParis, Evry, France
{ soochang.park, dina.hussein}@telecom-sudparis.eu and noel.crespi@mines-telecom.fr

***Abstract*--This paper presents service discovery architecture to find out available computing/intelligence resources on Internet of Things. Although mobile users roam around heterogeneous IoT fields, the architecture supports seamless service provision of ubiquitous resources from deployed smart devices' federations in different ownership, policy, communication technologies.**

## I. Introduction

Internet of Things (IoT) consists of billions of computing objects interconnected globally, such as sensors, RFID tags, and smart electronic/electromechanical devices surrounding us. The objects disappear and weave themselves into the fabric of our everyday life for supporting us in carrying out daily life activities, tasks, and rituals in an easy and natural way using information and intelligence, hidden in the network linking objects [1]. The ubiquitous nature of IoT-based intelligence is realized on a large-scale and complex networking architecture of such heterogeneous objects which take into account the issues of sensing/actuating the real world, transmitting data, and managing the relevant services to build applications [2].

For actual development of IoT, recently, there is a paradigm shifting from networks of smart objects to networks of social objects, denoted by *Social Internet of Things (SIoT)*, to solve objects' service discovery and composition issues [3], [4]. In order to guarantee effective object and service discovery and scalability like in human social networks, the SIoT paradigm adds a social structure to the IoT architecture. That is, since a social structure of objects narrows down the discovery range of objects and services due to social network properties (i.e., small world phenomenon and local clustering feature [3]), it could provide navigability to the large scale IoT architecture.

However, even though the previous studies have solved the scalability challenges driven by the large scale property of IoT, there are still the other hand issues regarding heterogeneity of the IoT nature. As mentioned above, IoT consists of various types, shapes, and formations of objects, but the studies have mainly taken into account standalone devices, which have high computing capability as well as sufficient energy and can act alone as a social object, to configure a social structure. In addition, to interoperate between heterogeneous objects, there is no consideration to solve the heterogeneous environment of communication protocols.

The objects that compose the IoT environment are typically resource-constrained devices, such as sensors, actuators, and RFID tags, despite their smart functionalities. So, efficiency of communication including energy, CPU and memory usage, and complexity of methodologies is traditionally one of the most important research issues. In other words, it should be relied on reasonable deployment of adequate communication protocols to establish the ubiquitous environment of IoT.

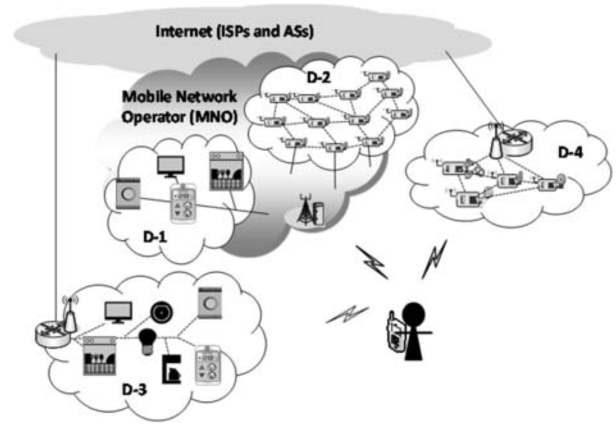


Fig. 1. Ubiquitous Computing Resource Deployments on IoT

Here, we move forward one step more by concerning highly heterogeneous environment of IoT from the current state of the novel SIoT paradigm evolution solved scalability issues. We first analyze two features of IoT's heterogeneity: 1) types and formations of objects with socialization issues and 2) communication protocols for interoperability. Then, to support seamless ubiquitous computing service provision, we present on-site service discovery architecture on the heterogeneous IoT environment, consisting of four main functional schemes: Discovery Region Determination, On-site Agent Selection, Location-based Query, and Roaming Management.

## II. Large Scale and Heterogeneity Of IoT

In this section, we explain heterogeneity of objects and their federations in IoT and of the evolutional nature, i.e., SIoT.

### A. Ownership and Federation Policy

Since an IoT-based service provider (e.g., Internet Service Providers (ISPs) and Mobile Network Operators (MNOs) is willing to get intelligent services and infrastructure based on autonomous operation, provider's IoT domain shares the same routing policies with not only static/dynamic topology but also routing technologies and RATs (radio access technologies) as shown in Fig. 1. It means that each IoT domain can belong to different service providers which follow the different service-level agreement (SLA) and security level. So, even if domains are deployed at the same place physically, they cannot allow inter-communication between them to support a user.

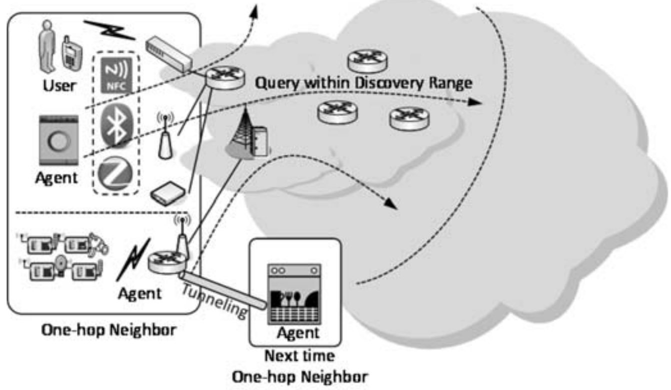


Fig. 2. On-site Service Discovery Architecture

### B. Technology and Formation Rule

As shown in Fig. 1, IoT domains are formed as four cases. First, each device adopts TCP/IP stack as well as application layer protocols over the stack. So, it can communicate with a user or the other devices directly as the standalone host in the Internet at domain 1 (D-1). Second, although each device has TCP/IP and application layer protocol stacks, it is only able to reach by the gateway as shown at D-3. It is because operators' policy regarding reachability and security. That is, if the IoT devices follow a SOAP-based control protocol, called DPWS (Devices Profile for Web Services), the operator may consider a transaction gateway (HTTP: RESTful approach/DPWS) for reducing communication cost [5]. In addition, the IoT devices containing compressing-based protocols like 6lowpan, CoAP, etc. could organize an ad-hoc network without base stations as D-2. In D-4, IoT devices which communicate without TCP/IP stack in non-IP manners as a typical wireless sensor network, so users can reach by the base station having TCP/IP stack.

Based on these deployment scenarios, the socialization agent to support the evolution toward SIoT could be embedded into some of IoT devices by the policy and capacity of themselves. That is, in D-1, all devices contain the agent; the devices in D-3 act as social objects with control by the gateway; and the devices forming D-2 and D-4 are considered logically as one social object with the difference that in D-2 all devices can be access nodes but in D-2 the base station is only access point.

## III. On-site Service Discovery Architecture

In this section, we explain our proposal, denoted by on-site service discovery architecture. The need of this architecture is come from provisioning available services on intelligence or information to a user when he/she roams around over the ubiquitous nature of IoT. However, each IoT domain takes the different position as mentioned above, so that he/she does not only connect IoT devices directly, but also know how to reach them by which way. Thus, here we exploit the socialization agent that can support devices' social networking via social relationships and trustworthiness between them. This service discovery architecture shown in Fig. 2 relies on four steps.

*Discovery Region Determination*: in this procedure, we can fit the range and scope of service discovery. In other words, it supports arranging discovery according to service providers, discovery goals or targets, physical or logical places, etc. It is used to create the *Hello message* for initial searches as well as all query messages to get service information.

*On-site Agent Selection*: for sending query messages and receiving response messages, we need to choose the agent in each IoT domain along its features and properties regarding formation and federation. Through the Hello message to one-hop neighbors, a user figures out the features and properties of every IoT domain surrounding him/her, and he/she selects an agent per each domain. Namely, it is linking points between all social devices targeted and the user to receive response messages when he/she roams around after querying.

*Location-based Query*: based on the location of a user, the query messages are transmitted in broadcasting within the pre-determined range of discovery. Social devices would establish dynamic (temporal) social relationships and create trust levels; they carry out data gathering on behalf of the user according to the queries; and, eventually, they response results to the user. Thanks to the dynamic social relationship, social objects can communicate each other in the relationship even though they are deployed from different IoT service providers with different operating policy including communication protocols and radio access technologies as well as domain configuration.

*Roaming Management*: via the agents, this architecture can support user roaming to provide seamless service delivery. For this, it relies on tunneling between agents. That is, continuous maintaining of the dynamic social relationship at the current location is provided by previous social objects.

## IV. Conclusion

In this paper, we bring the heterogeneity issue of the IoT nature that still causes many challenges for networking as well as smart service provisioning. Then, as a possible solution, we propose the on-site available service discovery architecture taking into consideration practical IoT domains' formations and federations, based on the novel paradigm by evolving from smart devices to social devices.

## References

[1] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in: Co-operation with the Working Group RFID of the ETP EPOSS, "Internet of things in 2020, roadmap for the future," Version 1.1, 27 May 2008.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, *et al.*, "Internet of things strategic research roadmap,"

[3] L. Atzori, A. Iera, and G. Morabito, "From "smart objects" to "social objects": The next evolutionary step of the internet of things," *IEEE Communications Magazine*, Vol. 52, No. 1, pp. 97–105, Jan. 2014.

[4] A.M. Ortiz *et al.*, "The Cluster between Internet of Things and Social Networks: Review and Research Challenges," *IEEE Internet of Things Journal*, Vol.1, No.3, pp.206-215, Jun. 2014.

[5] S. Han, S. Park, G. M. Lee, and N. Crespi, "Extending the Device Profile for Web Services (DPWS) standard using a REST Proxy," *IEEE Internet Computing*, vol. 99, no. PrePrints, p. 1, 2014.