A Study on Trustworthy Cyber-Physical ID/Location Mapping on IoT and NFV

Hyeontaek Oh[1], Sanghong Ahn[1], Jinhong Yang[2] and Jun Kyun Choi[1]

[1]*School of Electrical Engineering, KAIST, Republic of Korea*
[2]*Information and Communications Department, Korea Advanced Institute of Science and Technology, 291, Daehak-ro, Yuseong-gu, Daejeon 34141*
E-Mail: {hyeontaek; ancom21c; sunupnet}@kaist.ac.kr; jkchoi@ee.kaist.ac.kr

Received 20 January 2016; Accepted 1 March 2016;
Published 15 March 2016

Abstract

Information and Communication Technology (ICT) based industries, which are growing with advance of ICT technologies, are operated under trustworthiness of its ICT infrastructure. The identity trust targets the whole entities within the Internet of Things (IoT) and Network Functions Virtualization (NFV) environment that can be the creator, broker, modifier, and the end user of the data. Considering the dramatic growth of IoT service industry, its scalability, robustness, and efficient management are worth to be studied. Originally, conventional IDs for cyberspace are designed to consider having a relationship with physical address information. However, because of the wide-expansion of cyberspace, they are now very loosely-coupled. In this paper, the necessity of trustworthy cyber-physical mapping and its architecture would be discussed. The usage and demand of Cyber-Physical ID/Location mapping (CPID) will be discussed based on two use cases of real service environment. Furthermore, the requirements of CPID are introduced. A new CPID is needed to ensure trust location and trust identification, which includes location information explicitly for public goods in IoT and NFV environment, to make it easy to be recognized and used. Currently, related issues are under discussion in various standard organizations. To develop standards for trusted ICT infrastructure, it is needed to develop global CPID system by discussing ID/Location issues in global cyber identification or geolocation standardization groups.

Journal of Software Networking, 1–18.
doi: 10.13052/jsn2445-9739.20161.001

Keywords: trustworthy, cyber-physical, identity, locator.

1 Introduction

Industries on e-commerce, social services and the Internet of Things (IoT) are dramatically increasing, security and trust issues of cyberspace get emerged in multiple perspectives. Information and Communication Technology (ICT) based industries, which are growing with advance of ICT technologies, are operated under trustworthiness of its ICT infrastructure. In Seoul Conference on Cyberspace [1], they emphasize the importance of creating trustworthy cyberspace environment. Also, in World Summit on the Information Society forum 2015 [2], one of the important issues is "Building trust in cyberspace." Moreover, ITU-T Study Group 13 has been launched "Correspondence Group on Trust" for discussing trust provisioning for ICT environment [3].

The Internet of Things (IoTs) aims to provide whole-connected services based on ICT technology. Therefore, it is not only important to ensure security among IoT entities but also overall trust of data-driven services. It has led many researches related with Trust IoT environment to be done. The major issues of IoT Trust can be categorized into data perception trust, data fusion and mining trust, data transmission and communication trust, and identity trust [4]. The data perception trust and the data fusion and mining trust are related to the interpretation and use of data. The data transmission and communication trust is about delivery and distribution. The identity trust targets the whole entities within the IoT environment that can be the creator, broker, modifier, and the end user of the data. Considering the dramatic growth of IoT service industry, its scalability, robustness, and efficient management are worth to be studied.

Current forms of IDs in IoT services are designed for a device level, or oriented from a certain service to provide methods of object classification and recognition. For example, the identifier of EPCglobal standards adopted long hash code based combination, which is not suitable for human [5]. Especially, when IoT devices are widely deployed for public civil service (e.g. smart city, smart transportation, or disaster relief systems); if IoT devices and services utilize hash based identifiers, the users feel difficulties to recognize available services. It means that users, who unfamiliar with related services, are hard to intuitively identify the information from devices and services; and they are not able to recognize services and applications in cyberspace using physical addresses, which are one of the most popular identification mechanisms for human. In addition, even the virtualized network resources (e.g., routing, firewalling, load balancing, WAN optimization, etc.) need trusted ID system so that can be provided and utilized on the NFV environment. To build trusted connectivity between physical resources and virtualized ones, well designed cyber-physical ID structure is required.

Originally, conventional IDs for cyberspace are designed to consider having a relationship with physical address information. However, because of the wide-expansion of cyberspace, they are now very loosely-coupled [6]. As the number of networked devices and sensors is dramatically increased, and designed mapping between cyber ID and location is not working anymore.

Current loosely-coupled ID systems for cyberspace are not suitable for "cyber to physical" and "physical to cyber" based entity discovery and interoperating approaches which are required in cyber physical system (CPS) services [7]. These kinds of ID systems are not intuitive for users to identify a service that is related to devices/things in specific location, also it is hard to determine that resource of cyberspace affects actual location of physical area. Since everything has a location, therefore location information needs to be carefully described. In case of disaster or usage of public civil service, the infrastructure needs to provide methods that users could recognize and use resources, services and devices in the physical service area. For this purpose, a trustworthy cyber-physical identification and recognition system is required.

In this paper, the necessity of trustworthy cyber-physical mapping and its architecture would be discussed. To discuss these issues, current works for cyber-physical recognition and interoperation would be reviewed based on conventional cyber ID system. The necessity of cyber-physical mapping would be discussed with various scenarios in IoT and NFV environment. Also, current issues on cyber-physical ID/location mapping would be reviewed, which are discussed in ITU-T Trust Community Group. Based on them, the direction of studies and standardization for cyber-physical ID/location mapping and governance would be suggested.

2 Related Work for Cyber-Physical Identity and Location Mapping

Early ICT infrastructure was designed for a relatively small network of computers, where mobility was rare and participating nodes relatively homogenous. As a consequence, an early design decision established cyber ID as both a means to identify the end-point of communication and to specify its location within the network. However, when a number of cyber ID were dramatically increased, which caused by widespread of Internet and other ICT infrastructures, the implicit specification of this dual role for cyber ID has unforeseen at the time consequences.

In this section, we review history of physical address system and cyber ID system and their relationship, and also we review current issues of IoT environment based on cyber-physical ID/Location mapping perspective.

2.1 Physical Location Addressing Structure

Physical address system is widely used in everywhere, and the format of physical address is different based on their region. Until the advent of modern postal systems, most houses and buildings had no specific address, however, it has been commonly used after postal systems are introduced. Regarding physical address, in 1974, first version of ISO 3166 standard was published by the International Organization for Standardization (ISO) that defines codes for the names of countries, dependent territories, special areas of geographical interest, and their principal subdivisions [8]. Also, ISO standardized the universal postal union letter post regulations for unifying format of physical address. However, some countries kept their old address layouts and a few years ago the entire harmonization work collapsed and the standard specifications were declared deprecated. A postal code also is widely used, but every countries use in different way (in number 3-digit to 10-digit, in alphanumeric 6-digit to 8-digit). Today, there is no global unified standard for physical address system, each countries use their own format.

Satellite system is now utilized to geography survey, therefore, global positioning system (GPS) based location-based services are widely used. To standardize geo-location information, ISO and open geospatial consortium (OGC) has been developed related standards about protocols and interfaces for utilizing geospatial information in cyberspace domain.

2.2 Cyberspace Identification Structure

2.2.1 Telephony

A numbering plan for worldwide public switched telephone network is defined in ITU-T E.164 standard [9]. Plan-conforming numbers are limited to a maximum of 15 digits. In telephone number plan, each countries has their own country calling code and geographic area codes which can briefly describe the location information. However, a number of non-geographic area codes are increasing because of development of mobile telephony and

Internet telephony. It makes weaker relationship between telephone number and location information.

2.2.2 Internet

IP addresses (IPv4 and IPv6) are widely used for indicating hosts in the Internet. Since a number of connected devices are small, the IP can have both a means to identify the end-point of communication and to specify its location within the Internet.

However, as a number of connected devices in the Internet has been increased, this relationship has been changed. For example, a certain area has multiple classful IP addresses, and the number of private network is increased by network address translation (NAT) technique. These kinds of changes make hard to represent both cyber ID and physical location for IP address. Moreover, DHCP (Dynamic Host Configuration Protocol) based IP allocation makes it hard because IP address of network host periodically changed.

IPv6, which is developed to overcome IPv4 address exhaustion, is defined in IETF RFC 2460 [10]. IPv6 (and 6LoWPAN) uses stateless address auto-configuration scheme (which is similar to DHCP in IPv4), so network prefix is not able to bind with location information [11]. Domain name system (DNS) translates domain names (mostly using URL format), which can be easily memorized by humans, to the numerical IP addresses vice versa. Domain name space is consists of a tree of domain names, and the tree sub-divides into zones which is beginning at the root zone. DNS can represent some geolocation information by using DNS zones (e.g. country domain zones line ".us", ".eu", etc.) and domain name. However, since a number of domain names with general DNS zones (like ".com", ".net") are dramatically increased, domain name becomes loosely-coupled with its geolocation information.

2.3 Identification Methods for IoT Environment

The IoT environments aim at providing new services by connecting and collaborating various physical things in cyberspace domain using ICT infrastructure. For this purpose, the methods for identifying and discovering existing services and devices are needed.

For identification systems, EPCglobal (Electronic Product Code global) standards provide EPC based ID, which is used in RFID (Radio Frequency Identification) environment. In the Web of Things (WoT) concept in World Wide Web Consortium (W3C), WoT concentrates on utilizing resources and information that are able to access via HTTP (HyperText Transfer Protocol) only [12]. To identify these Web resources, URI (Uniform Resource Identifier) is used [13]. In CPS area, cyber-physical ID/Locator mapping modeling research are proceeded for connecting and interacting between virtual resources in cyberspace and physical devices/processes [7].

Current cyberspace identifiers are not able to present any physical location information. Although physical resources and cyber resources should be tightly coupled for advancing IoT applications, there is no human-friendly cyber-physical identification system.

There are several ways about discovering and connecting devices such as UPnP (Universal Plug and Play) [14] or DLNA (Digital Living Network Alliance). However, conventional methods use broadcasting beacon messages using specific network protocols for discovering devices/services, so it is hard to use as location identifier because protocols depend on their own specifications. Thus, they provide application based approaches, which actual users are not able to easily recognize.

3 Use Case and Motivating for Cyber-Physical ID/Location Mapping

As mentioned before, there is no method to acquire the representative service or information of a certain location in the IoT environment because mapping between physical address and cyber ID has been decoupled.

In this section, the usage and demand of Cyber-Physical ID/Location mapping (CPID) will be discussed based on two use cases of real service environment. Furthermore, the requirements of CPID are introduced.

3.1 Use Cases

3.1.1 Disaster network

The number of natural disaster is increasing, and its damage gets bigger and bigger, so the needs for standard of disaster network are dramatically increased. As response, ITU-T established the needs and requirements of disaster network in activities on “Focus Group on Disaster Relief Systems, Network Resilience and Recovery” [15]. In ITU-T Disaster-Relief (DR) requirement, it is said that a use of a wide variety of terminals and communication channels is a novel kind of method to early-disaster alert in disaster relief system. In previous disaster network, old-fashioned communication methods are used, such as radio, TV broadcast and wired telephone. However, in future disaster network, various kinds of devices would serve the disaster relief service, as wireless communication and digital signage technologies get evolved. On the network side, utilizing the NFV scheme, detouring network configurations can be much easily constructed. Moreover, these kinds of devices would provide area-specific or user-specific information to the user in disaster network [16].

When a disaster occurs, a wireless communication network might be congested by multiple coincident calls. In spite of this network status, an early alert message should be delivered to the users in the disaster area as soon as possible. Moreover, digital signage devices in bus station, railway station and retail outlet should be able to show proper messages for its area [17]. To guarantee these services trustworthy, it is required to be a public and easy-to-process cyber-physical ID mapping. A disaster network scenario is composed of following process - in the scenario, a fire in a public park and its remedy will be treated.

1) Observing location

A user in a public park sees a fire and reports it to the public park center or near fire station. The fire point gets recognized as a form of CPID based on representative point in the user's terminal and gets reported to the public park center. With spatial information in the report, the public park center is able to identify the fire location and its related resources, and make a proper decision to deal the disaster.

2) Broadcast information

The public park center decided to broadcast the fire information to users in the public park. The information of fire point is delivered as a form of CPID, so that it could be shown in proper form in user's mobile terminal and digital signage. The user is able to recognize the fire point by noticing the point that is included in the CPID form. This information could be applied to calculate refuge path or notify a safety zone.

3) Network disaster recovery

If there are any partial damage happens on the physical network around the public park, then re-configuration or detouring path can be straightforwardly build using NFV. By moving existing virtual appliance from the ruined place to other safe data center, associated application workload can be efficiently processed with minimum damage.

3.1.2 Smart city

A smart city environment has many scenarios for interpreting physical location to logical representation in IoT environment. In smart city or urban computing environment, a logical classification on the place gets complicated. Moreover, numerous heterogeneous services can be used in a certain area. To solve these issues, ITU-T discussed standardization issues on "Focus Group on Smart Sustainable Cites" [18]. In documents of smart sustainable cities overview and its standardization roadmap, components of services and ICT infrastructure are argued. Especially, in urban planning, intelligent building system and building information modelling, management of physical place and location with cyber system is essential. For this purpose, they argued that combination and harmony of related technologies are important.

For example, the location information scenario is one of representative scenarios for smart city environment. In previous, a visitor uses a map application or web search engine to acquire information of visiting location, or he/she can visit a web homepage of visiting location if it is served. However, the information of map application is dependent on its vendor, and it is not so detail for multi-story building or inside of building. Querying to web search engine is inconvenient solution to the user. If the visiting place provides some access points to get information, it would be better for the visitor. Still, it is incomplete solution since the access methods are dependent on its service vendor. Moreover, they just provide an isolated connection between physical location and cyber service. It is insufficient to apply to other mash-up services. A visitor scenario is composed of following process - in the scenario, a user visits a museum and uses a curator service by service discovering.

1) Observing location

A user visits a museum and recognizes his/her location using own mobile terminal. The mobile terminal acquires the location information from sensors or QR-code. The museum's location information get acquired in a form of CPID.

2) Service discovery and selection

The user searches services that are related to the museum by recognized locator. The location information in form of CPID is used as a parameter for searching. As results of service discovery, the user can find three services: information service of museum building, curator service for current display and information service for exhibition schedule. The user selects the curator service for current display.

When the user tries to search services related to current location, a searching method should not be depend on a certain vendor. It means that CPID needs to be public and platform-independent.

3.2 Requirements

From the use cases defined in Section 3.1, a list of requirements for CPID system has been identified. The detail and fined work of this list would be subject to future study. The requirements could be classified as three categories; presentation, sensibility and operability. Presentation requirements describe functional requirements to read, write and process CPID by computer or human. Sensibility requirements describe functional requirements for CPID to be easily sensible or readable by computer or human. Finally, operability requirements describe requirements of operations that ensure trustworthy services. The list of requirements is followed:

1) Presentation

- CPID needs to have a hierarchical structure. It makes easy to logically understand for human and provides advantages on sorting, searching and filtering process for computer.
- CPID presentation structure needs to be scalable and flexible, since logical classification on place could be modified by temporal, cultural or national reasons.
- CPID needs to be human-readable and have a clear unit of presentation.

2) Sensibility

- CPID needs to provide a trustworthy method to recognize user's location to provide area-specific or user-specific service.
- CPID system needs to provide a trustworthy method to recognize location of real estates or fixed devices like digital signage.

3) Operability

- CPID needs to provide users to make a data request or receive data via CPID, which is based on current nation's physical address system.
- CPID system needs to be trustfully operated by multi-stakeholders. For this purpose, CPID system needs to be defined as global standards.
- CPID information needs to be independent from application services.

- If new devices are connected to the network and get new cyberspace addresses, then CPID system needs to provide a method to acquire CPID for those cyberspace addresses. Furthermore, CPID system needs to provide a method of new devices discovery.
- The physical address needs to be trustworthy, which is acquired from CPID system.

From the list of requirements for CPID-based ID/location resolution, trustworthiness comes to the fore of important service component for public services and an ICT infrastructure. For example, service structure like Google's Physical Web [19] could be dependent to its object ID resolver vendor, so that it could not guarantee a public trust. For an ICT infrastructure as public goods or social overhead capital or network resources, it needs to be managed by governments or public organizations. Moreover, it needs to establish a global standards to make a trustworthy system since the ICT infrastructure could be inter-operated with multiple countries.

3.3 Trustworthy Cyber-Physical ID/Location Mapping System

Currently, object-oriented ID systems and cyber-physical ID/location mappings vary on nations, vendors and service domains. This situation would make it difficult to use location information, and make its domain be localized. Moreover, it would cause an additional cost for cross-domain conversion and a confidence problem among stakeholders in B2C/B2B transaction.

As shown in Figure 1, to provide trustworthy applications, the location information from physical things network and identifier from cyber

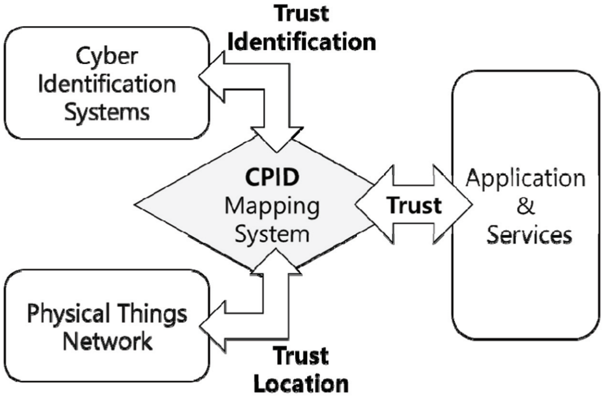

Figure 1 A concept of trustworthy cyber-physical ID/Location mapping system.

identification system should be trustworthy. A new cyber-physical ID/Location mapping system is needed to ensures trust location and trust identification, which includes location information explicitly for public goods in IoT environment, to make it easy to be recognized and used. Also, publicity and trustworthiness need to be ensured for this ID-based location mapping.

Structure that coupled with ID/location might have problems with massive routing or using in mobile environment [20]. However, a Cyber-Physical ID/Location (CPID) mapping system is needed for governance on public goods managed by location-based ID.

4 Standardization Activities and Trustworthy Cyber/Physical ID

In this section, we review current standardization activities about cyber ID and physical location.

4.1 Cyber Identification Standards

ITU-T Joint Coordination Activity for Identity Management (JCA-IdM) group has been established to standardize cyber identification system [21]. JCA-IdM also collaborates with various standardization groups such as ISO/IEC, ETSI, IETF, and so on.

The activities of JCA-IdM are based on ITU-T X.1252 document that provides a collection of terms and definitions used in identity management [22]. JCA-IdM has been discussed cyber identification systems, however, it is not considered that binding with location information or cyber-physical link.

The limitation of current cyber ID system is analyzed in ETSI GS INS 006 v.1.1.1 [23]. This document provides gap analysis for global discovery mechanism of identifier, provides and capabilities which is based on the assumption that the information required to provide a service is not available within a single service provider and must be dynamically discovered. Its main purpose is to investigate the current landscape on the IdM area and evaluate if there is a need for such a discovery mechanism, or whether this can be covered by existing solutions. In general, discovery of identity data across domains is realized with two different ways:

- Federated model: A service defined by a group of network entities which participate in a federation. Identity data are registered in the service and can be provided to all the participants of the group. The location of the discovery service and the protocol for exchanging messages is static and known to the participants of the group.

- User-centric model: By using an identifier of this format, a user directly points to a network point that holds identity information about itself. This location may hold information for only one profile of the user or for many profiles.

However, both approaches provide limited discovery of user's identity information. For the federated model, only the identity data, which exist within the federation of providers can be discovered. Information outside the federation cannot be discovered. For the user-centric model, the use of a specific predefined format instantly excludes the discovery of identity data from providers that are not familiar with it. Even though the adoption of a globally accepted identifier would solve major identity issues, which seems to be inapplicable.

4.2 Physical Location Standards

To utilize geo-location information in various area, it is needed that standards for aggregating, processing, and distributing geo-location data.

Open Geospatial Consortium (OGC) mainly develop and implement standards for geospatial content and services. OpenGSI Location Services (OpenLS) defines core services, their access and abstract data types which form together a framework for an open service platform, the so called GeoMobility server [24]. OpenLS provides four core services: Directory Service, Gateway Service, Geocoder Service, and Presentation Service. These services are based on GPS technology.

OGC has identified the need for standardized interfaces for sensors in the Web of Things (WoT). The Sensor Web interface for IoT SWG aims to develop such a standard based on existing WoT portals with consideration of the existing OGC Sensor Web Enablement (SWE) standards [25, 26]. The importance of location information and sensor observations to the IoT has been recognized.

OGC Sensor Web Enablement (SWE) has been established for building a unique and revolutionary framework of open standards for exploiting Web-connected sensors and sensor systems of all types: flood gauges, air pollution monitors, stress gauges on bridges, mobile heart monitors, Webcams, satellite-borne earth imaging devices and countless other sensors and sensor systems. SWE standards are the only ones that focus on the content of sensor information and on making the sensor observations useful to end user applications. SWE standards allow users to assessment the fitness for use of observations and to allow accurate processing on the sensed information to create derived information suitable to the user needs.

In much the same way that HTML and HTTP standards enabled the exchange of any type of information on the Web, the OGC SWE standards enable the discovery of sensors and corresponding observations, exchange, and processing of sensor observations, as well as the tasking of sensors and sensor systems.

Geographic information is gathered and used by OGC standards, however, geo-location information are not matched with cyber identifiers. Therefore, a new identification structure should be discussed for binding both cyber-physical ID/Location information.

5 Conclusion

As an age of the Internet of Things comes, cyberspace and physical world would be tightly and closely coupled. It makes that physical objects and locations are connected to cyberspace service, which usages are vary from a level of sensor network like smart home, smart factories to GPS-based navigation system, location-based services and disaster relief network using NFV. These kinds of connection start with mapping physical location and information to the cyberspace service.

However, trustworthiness on IoT and NFV services would be ensured when users or services could recognize and rely on services which are coupled with precise cyber-physical information. Therefore, new identification system is needed, which includes location information explicitly for public goods in IoT environment, to make it easy to be recognized and used. Also, publicity and trustworthiness need to be ensured for this ID-based location mapping.

Currently, related issues are under discussion in various standard organizations. To develop standards for trust ICT infrastructure, it is needed to develop global CPID system by discussing ID/Location issues in global cyber identification or geolocation standardization groups.

Acknowledgment

This work was supported by the ICT R&D program of MSIP/IITP. [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system].

References

[1] Global Conference on CyberSpace 2013. (2013). *Seoul Framework for and Commitment to Open and Secure Cyberspace*. Available at: http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf

[2] World Summit on the Information Society. (2015). *WSIS Forum 2015: Outcome Document*. Available at: http://www.itu.int/net4/wsis/forum/2015/Content/doc/outcomes/WSISForum2015_OutcomeDocument_ForumTrack.pdf

[3] ITU-T Study Group 13. (2015). *Trust Correspondence Group*. Available at: http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/correspondence.aspx

[4] Zheng Y., Zhangc, P., and Vasilakosd, A. V. (2014). A survey on trust management for internet of things. *J. Netw. Comput. Appl.* 42, 120–134.

[5] Roussos, G. (2008). *Networked RFID: Systems, Software and Services*. London: Springer SMB.

[6] Roussos, G., and Chartier, P. (2011). Scalable ID/Locator Resolution for the IoT," in *Proceedings of the 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*.

[7] Lee, E. A. (2010). "CPS Foundation," in *Proceedings of the 47th Design Automation Conference*, Anaheim, CA, 737–742.

[8] ISO. (1999). *Codes for the representation of names of countries and their subdivisions*, ISO 3166.

[9] ITU-T. (2010). *The International Public Telecommunication Numbering Plan*, ITU-T E.164.

[10] RFC. (1998). *Internet Protocl Version 6 (IPv6) Specification*, IETF RFC 2460.

[11] Hui, J., and Culler, D. (2009). "6LoWPAN: incorporating IEEE 802.15.4 into the IP architecture," *Internet Protocol for Smart Objects (IPSO) Alliance White paper*. Available at: http://www.ipso-alliance.org/wp-content/media/6lowpan.pdf

[12] Raggett, D. (2015). *An Introduction to Web of Things Framework*. Available at: http://www.w3.org/2015/04/w3c-wot-framework-munich-2015.pdf

[13] RFC. (2002). *Report from the Joint W3C/IETF URI Planning Interest Group: Uniform Resource Identifiers (URIs), URLs, and Uniform Resource Names (URNs): Clarifications and Recommendations*, IETF RFC 3305.

[14] ISO. (2011). *Information Technology - UPnP Device Architecture*, ISO/IEC 29341.

[15] ITU-T FG-DR&NRR. (2014). *ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery.* Available at: http://www.itu.int/en/ITU-T/focusgroups/drnrr/Pages/default.aspx

[16] ITU-T FG-DR&NRR. (2014). *Requirements for Disaster Reflief System.* Available at: http://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/fg-drnrr-tech-rep-2014-5-DR_requirement.pdf

[17] ITU-T FG-DR&NRR. (2014), *Promising Technologies and Use Cases - Part IV and V.* Available at: http://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/fg-drnrr-tech-rep-2014-2-2-Framework-usecase-part-4-5.pdf

[18] ITU-T FG-SCC. (2015). *ITU-T Focus Group on Smart Sustainable Cities.* Available at: http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx

[19] Google. (2015). *Google Physical Web.* Available at: https://google.github.io/physical-web/

[20] RFC. (2007). *Report from the IAB Workshop on Routing and Addressing,* IETF RFC 4984.

[21] ITU-T JCA-IdM. (2015). *ITU-T Joint Coordination Activity for Identity Management.* Available: http://www.itu.int/en/ITU-T/jca/idm/Pages/default.aspx

[22] ITU-T. (2010). *Baseline Identity Management Terms and Definitions*, ITU-T X.1252.

[23] GS INS. (2011). *Identity and Access Management for Networks and Services; Study to Identify the Need for a Global, Distributed Discovery Mechanism*, ETSI GS INS 006.

[24] OGC. (2008). *OpenGIS Location Service (OpenLS) Implementation Specification: Core Services*, OGC 07-074.

[25] OGC. (2011). *Sensor Web Enablement*. Available at: http://www.opengeospatial.org/domain/swe

[26] OGC. (2012). *SensorThings Standards Working Group.* Available at: http://www.opengeospatial.org/projects/groups/sweiotswg

Biographies

H. Oh received his B.S. and M.S. degree from Korea Advanced Institute of Science and Technology (KAIST) in 2012 and 2014, respectively. Currently, he is a Ph.D. student in KAIST. His current research interests include energy efficiency in heterogeneous access networks, Internet of things, Web of objects, and user interface/user experience on Web.

S. Ahn is a Ph.D candidate in electrical engineering (Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea). He received his Bachelor's degree in computer science from KAIST. He received his Master of engineering degree in electrical engineering from KAIST in 2010. His research interests include web engineering, insulated networking mobile cloud computing and services in the Internet of Things.

J. Yang (S'05) received M.S. in computer science from InJe University in 2005 and HERIT Inc. in 2008 and currently he is Ph.D. candidate student in Korea Advanced Institute of Science and Technology (KAIST). His main research interests include next generation network, multimedia streaming issues, and IoT.

J. K. Choi (M'88-SM'00) received the B.Sc. (Eng.) from Seoul National University in electronics engineering, Seoul, Korea in 1982, and M.Sc (Eng.) and Ph.D degree in 1985 and 1988, respectively, in electronics engineering from Korea Advanced Institute of Science and Technology (KAIST). From June 1986 until December 1997, he was with the Electronics and Telecommunication Research Institute (ETRI). In January 1998, he joined the Information and Communications University (ICU), Dae jeon, Korea as Professor. At year 2009, he moves to Korea Advanced Institute of Science and Technology (KAIST) as Professor. He is a Senior Member of IEEE, the executive member of The Institute of Electronics Engineers of Korea (IEEK), Editor Board of Member of Korea Information Processing Society (KIPS), Life member of Korea Institute of Communication Science (KICS).